Secureworks®

Taegis NGAV
Enterprise Administration Guide

v. 2024.2.0

Taegis NGAV Enterprise Administration Guide

Table of Content

Contents

Taegis NGAV Enterprise - Administration Guide

Thank you for using this product. It is the world's first cloud-based cognitive antivirus product that provides signature-free endpoint protection. This product provides real-time malware execution prevention.

About this Guide

This guide describes the Taegis NGAV Enterprise product, its installation, use and management.

Up and Running with Taegis NGAV

This section provides a rapid startup for *Taegis NGAV*.

Key Concepts

Before proceeding with this workflow, it is highly recommended that you become familiar with the following concepts:

- *User Roles*
- *Policy Settings*
- *Policy - Best Practices*
- *Device Group - Best Practices*
- Allow and Deny Lists
- *Two Factor Authentication*

The Up and Running Workflow

The rapid startup process flow includes the following:

1. Login
2. Add Additional Users
3. Security Policy Decisions
4. Device Group Decisions
5. Allow/Deny List Decisions
6. Deploy/Install Client
7. Customer Tasks in the Management Console

Up and Running

The following procedure is designed to get the product up and running in a short time, using preset defaults and provided templates. Perform the following steps:

1. **Login**: Log into the *Management Console* (use the emailed instruction

2. Select the **Administration** tab
3. **Add Additional Users** *(optional)*

   If you require additional users, perform the following:

   a) Navigate **Administration > Users**

   b) Click **Add User**

   c) Enter *user information*

   d) Set *User Role* (*administrator, manager, auditor*)

   Administrator –
   The *Administrator* role includes global permissions and complete access to product logs, tools and data. The Administrator has extensive modification powers.

   Manager –
   The *Manager* role includes permissions within any group they manage and partial access to product logs, tools, and data. The *Group Manager* has limited modification powers.

   Auditor –
   The *Auditor* role includes limited permissions and ability to modify.

   See *User Roles* for expanded information.

   e) Click **Submit**

   f) Navigate **Administration > Deployment**

   g) Send email (welcome) invitation that includes information on how to log in and download the client and associated files

4. **Security Policy -**
   Each device group (see below) must be assigned a security policy to be applied to the devices in that group. Preconfigured security policy templates are supplied.
   Either select a preconfigured policy template for use or create custom policies.

   Note: the policy associated with the default device group is the *Essential Protection Policy*. If you want to deploy the Essential Protection policy on all devices, no additional action is required in the *Security Policy* section. See *Device Group - Best Practices* for expanded information.

   If you want to customize or create a new security policy, perform the following:

   a) Click **Security Policies**

   b) Select a provided *Security Policy Template* and alter it to fit your needs or create a new policy

c) *(optional)* Create New policy

i. Click **Create New Security Policy**

ii. Enter the new *policy name*

iii. Click **Create** to launch the new policy page

iv. Edit and save the new policy to put it into effect

5. **Set Device Group(s)** -
Device groups are designed to be a collection of users or devices with similar *security needs* or *security policy*.

Groups can be created for various parameters, including:

- **Location**, for example the *New York Office*
- **Job Function**, for example *accounting*
- **Device Type**, for example MS Windows

See *Device Group - Best Practices* for expanded information.

Note that a default device group is provided for initial use. The policy associated with this group is called the *Essential Protection* policy.
If you want to create a new one, perform the following:

a) Navigate **Administration > Device Groups** to display the *Device Groups* pane

b) Click the **Create New Device Group** button to display the dialog.

c) Name the new *device group*

d) Define the device group (Use the drop-down menus):

- Select the device group *Type*
- Select the *Security Policy* to apply to this device group
- Click **Create** to save the information and exit the dialog

6. **Allow/Deny List Decisions** *(optional)* -
See Allow and Deny Lists for expanded information.

Define Global Allow/Deny Lists -

To define *Global Allow/Deny Lists*:

a) Navigate **Administration > Global Lists**

b) Edit the lists to add the names of files to allow or deny

c) Save the list(s)

7. **Deploy/Install Client** (local or push install)

a) Verify installation prerequisites, depending on your platform:
   - *Windows Client Requirements*
   - *Linux Client Requirements*

b) Consult the *welcome email* for console *URL* and *login* information

c) Access the management console to download the appropriate *installer* and associated files

d) Run the *installer* –

i. **Windows Client** –
   - See *Install Windows Client – Use Installation Packages*
   - See Install Windows Client – Use PowerShell Commands

***Note**:* A Reboot may be required if prerequisite software updates such as Visual C++ are performed as part of the installation process. See *Windows Client Requirements* for additional information.

ii. **Linux Client** –
   - *See Install Debian/Ubuntu Packages*
   - *See Install RHEL Packages*

e) Enter the *connection information* at the prompt

f) **Activate** to display the *client dashboard* (Windows only)

Customer Tasks in the Management Console

- **Verify** *device status* in the management console:
  a) Navigate: **Devices**
  b) Locate *device*
  c) View information, including *connection status* and *agent version*

- **View and manage** *Alerts/Threats* and *Quarantined Files* -
  - Alerts/Threats:
    See the *Navigating the Alerts Tab* and *Alerts* sections for expanded information.
  - Quarantined Files:
    See the *Quarantine Folder* and *Remediate Threat Actions* sections for expanded information.

- **Uninstall or Update** the Client, depending on platform:
  - **Windows Client** -
    See *Uninstall or Update Windows Client*

  - **Linux Client** -
    - Uninstall Linux Client -
      See *Uninstall/Remove Linux Client*

    - **Update Linux Client -**
      See *Update the Linux Client*

  - **Move Devices** to a new group
    i. Navigate: *Devices*
    ii. Locate the *device*
    iii. Click **Bulk Actions**
    iv. Select **Add to Group**
    v. Select the *group* to move the device into
    vi. Click **Confirm**

  - **Change Security Policy** assigned to a device
    Note: To change the policy applied to a device, there must be a *device group* with the policy *assigned*.
    - If *no group exists* –
      See Creating a New Device Group for instructions on how to create a device group

    - When the *group is created* –
      See Editing Devices for instructions on how to move devices to a new group

---

Introduction

This product is an intelligent cognitive protection solution. This product uses machine learning and natural language processing algorithms to analyze unknown files and identify malware and prevent its execution. It is available for Microsoft® Windows® and Linux clients.

Notes:

- This product does not support scanning external drives or monitoring network or cloud

repositories at this time
- This product focuses on activity, files and processes on the device or system

Taegis NGAV and Data Privacy

Taegis NGAV provides data privacy because, by default, it does not read or transfer specific file information. Because AI detection models are hosted on the client endpoint, it is not necessary to share file features. This product shares only device metadata and global caches with the cloud unless otherwise configured.

This product can optionally be configured to submit more information because it has the ability to upload files to the cloud.

By default, this product only sends *device and event (alert)* metadata to the cloud. This metadata information is used by the management console and stored on Google CloudSQL. Note that, if necessary, this product can establish Cloud SQL instances in any geographic local where Google has a data center.

Modules

This product consists of two essential modules:
- A web-based, OS-agnostic *Management Console* portal
- A *client (endpoint)* local application that communicates with the console. The currently supported operating system clients are for Microsoft Windows and a selection of Linux distributions.

Guide Content Areas

This guide contains the following topic areas:
- Quick Start Sections for:
  - **Management Console**
  - **Clients**
- **Management Console** - setup, configuration and tasks
- **Endpoint Client(s)** - installation, setup, and configuration
- **Malware Prevention Scenario Discussion** - discussion concerning malware, a demonstration, alert terms, definitions and logic
- **Reference** - topics include:
  - Hardware Requirements
  - Supported File Types
  - Best Practice Recommendations

- Definitions of User Roles
- Listing of Policy Settings
- Alert Actions Defined
- Windows Command Line Parameters

Management Console

The management console is a web-based, OS-agnostic interface that enables administrators to manage how endpoint client protection is configured.

The Taegis NGAV management console URL is https://ngav.taegis.secureworks.com/

The management console supports various tasks and procedures, including:

- Providing downloads for:
  - The dalicense license file for Information Technology **(IT)** deployments
  - The DAOTLICENSE license file for Industrial Operational Technology (**OT**) deployments
  - *Registration key* and *web server URL* information for IT deployments
  - This guide
- Creating, setting, and deploying policy and group definitions
- Managing users, including creating individual API keys
- Creating and maintaining curated allow and deny lists to customize application acceptance or rejection
- Viewing and sorting various statistics concerning threats, occurrences, and historical perspectives
- Defining, viewing, and exporting log files
- Viewing device Software Inventories for Windows-based machines

The dalicense File, Key and Web Server

The Management console *Downloads* page contains information specific to your IT client installation/re-installation:

- `dalicense` license file for IT deployments -
  This file contains the *registration key* and *Web Server* specification.
  Note: only 1 `dalicense` file can be on the disk for successful installation and registration. If more than one file exists, the installation will fail.
- *Registration key* -
  The registration key specific to your installation. Useful if manual client configuration is required.
- *Web Server URL*-
  The Web Server URL specific to your installation. Useful if manual client configuration is required.
- Redistributable package links -
  These are links to packages specific to particular Operating Systems and distributions.

DAOTLICENSE File, Key and Web Server

The Management console *Downloads* page contains information specific to your Industrial OT client installation/re-installation:

- DAOTLICENSE license file for OT client deployments.
  Note: The product *Registration Key* and *Server URL* for OT deployments are encrypted within the DAOTLICENSE license file.

Perform the following to access the various options for *Licenses*, *Web Service URLs*, and *redistributable packages*.

1. Log into the *Management Console*
2. Navigate to the *Deployment* page
3. Click the **Click to Select a Device Group** link to display known *Device Groups*
4. Click on a *device group name* to select it and display the *Downloads* page.

   This page includes various information including:

   - **Registration Key and Web Service URL information**.
     Click **Copy** to place information on clipboard.
     Note: The product *Registration Key* and *Server URL* for OT deployments are encrypted within the DAOTLICENSE license file.
   - **Methods to obtain the Installer**

     - Click **Protect this ... device** to download the appropriate installer to the device and copy the registration key
     - Click **Send email Invitations** to send email links to access the required installer and registration key. The email contains a **Download Now** link.

       The email link opens a window that displays the Registration Key and Web Service URL and automatically downloads the installer
     - Click **Copy download link** to display the link to the *Download Dashboard* and the option to share it via email

       Note: the download link has a default expiration set to 7 days
     - Click **Download a redistributable package** to display the list of available packages for download.

       These packages include Agent installers for Windows and various Linux distributions, and License files. Scroll to find your selection and click **Download** to access the *Downloads* page.

       Note: The `dalicense` file contains the *Client Installation key*. Click **Download a redistributable package** to download this file.

Management Console Quick Start

This quick start is for users familiar with the configuration of hosted and managed cloud

support solutions. If you require additional instructions or explanations, consult the more detailed instructions in Using the Management Portal section.

Taegis NGAV Console URL

The Taegis NGAV Management Console URL is https://ngav.taegis.secureworks.com/

Management Console Requirements

The management console does not require on-premise software because it is cloud-hosted. Endpoint clients require:

- Port 443 (HTTPS) - Open this port through the firewall to communicate with the *Cloud Management Console*, located at the URL: `https://ngav.taegis.secureworks.com/`

- `https://listener.logz.io:8071` - this URL must be accessible (not blocked by a firewall at the customer site)

The Management Console supports the following browsers and versions:

- Chrome 64+
- Microsoft Edge version 79 and later (Chromium-based)
- Firefox 52.6+

Quick Use of the Management Console

1. Log in to the *Management Portal* at https://ngav.taegis.secureworks.com/
   Use the provided *Username* and *Password*.
   Note: The console administrator login session has a default expiration if no activity is detected. The default setting is *1 hour 45 minutes*. A warning displays before the console automatically logs the administrator out.
2. Select the **Administration** tab.
3. Click **Security Policies**.
4. Select a provided Security Policy Template as the basis for a new policy or Click **Create New Security Policy** (upper right corner).
5. Enter the new *policy name*.
   Note: To clone an existing policy to the new name, select an existing policy from the *Clone Existing Policy* dropdown.
6. Click **Create** to launch the new policy page.
7. Edit and save the new policy to put it into effect.
8. Navigate **Administration > Device Groups** to display the *Device Groups* pane.
9. Click the **Create New Device Group** button in the upper right-hand corner to display the dialog.
10. Name the new group and use the drop-down menu to select which security policy will

apply to these systems.
Note: You can create multiple Device Groups for different security policies.

11. Click **Create** to save the information and close the dialog
12. Navigate **Administration > Global Lists** to display the *Global Lists* tab. This pane displays options to add specific executables to the Global Deny or Allow lists and specify files for a *Certificate Allow List*. You can add the hash of the specific executable if known or choose to include the certificate thumbprint generated for a file. Typically, these lists are used for business-specific software not previously referenced on the master database from the National Software Reference Library (NSRL).
13. After successfully configuring the console, proceed to download the endpoint client:
    a) Navigate to:
    ```
    Deployment -> Device Group ->
            Download a redistributable package -> Download
    ```
    b) Click the **Download** button to download the client installation file. This file is the installer for the individual Endpoints.

Management Console Setup Issues

If you encounter issues with the Management Console initial setup, read the Using the Management Portal section for a more in-depth description of setup options and product definitions. If issues persist, contact the support team.

Endpoint Clients

This product provides endpoint clients for Windows and Linux operating systems. The endpoint clients normally communicate with the management console, unless they are operating in the offline mode.

Client Quick Start

The following section provides quick start procedures for the Windows client. The Linux client does not have a quick start section. It is discussed in the main Linux Client section.

Verify General Client Requirements

Verify the following general requirements before beginning installation. Specific installation requirements for each operating system follow.

- Verify the downloaded installation package file is the latest and can be accessed.
- Ensure internet connectivity for the install system. This is necessary to download updates and register with the cloud service.
- *Administrative* rights are required to install this product. Regular, non-administrator users can use this product after it is successfully installed.

Client Firewall Settings

This product, by default, uses port 443 to communicate with the Management Console, located at the URL: `https://ngav.taegis.secureworks.com/`.

Notes:

- The `https://listener.logz.io:8071` URL must be accessible (not blocked) by the firewall at the customer site
- Taegis NGAV agent deployments are not supported in a network proxy environment
- Do not perform modifications of HTTPS traffic, such as TLS termination/inspection, because it will cause connectivity disruptions. Although these disruptions do not affect protection capabilities, server reporting and management will be affected.
- The `https://storage.googleapis.com/` URL must be accessible (not blocked) by the firewall at the customer site to update/download the client.

NGAV Incompatibilities Caution

NGAV is incompatible with the following 3rd party products and platforms**:**

- Cisco Meraki

Deployment with these incompatible products and/or platforms should be avoided.

Client Installation Notes

- It is possible to deploy the client with the `Display User Interface` option set to *Disabled* (without a GUI). See Deploy Client Without GUI for additional information**.**

- **Log files** - Client log files are maintained in the following locations:
  - **Windows:**

    `C:\ProgramData\SecureWorks\Taegis_NGAV\Taegis NGAV_smb_service.log`

    `C:\ProgramData\SecureWorks\Taegis_NGAV\Taegis NGAV_smb_gui.log`
  - **Linux**
    `/var/log/secureworks/secureworks/secureworks_linux_service.log`

Deploy Client without GUI

It is possible to deploy the client with the `Display User Interface` option set to *Disabled* (without a GUI). The parameter that controls this is the `NOGUI` specification. To deploy a client without the GUI, perform the following:

1. Configure the policy. Set the `Display User Interface` option to *disabled*

2. The `NOGUI` parameter must be set within the *dalicense* file, for example:
   `WebServiceURL Registeration_Key NOGUI=0`

   See Command Usage for additional information.

Windows Quick Installation

For Microsoft Windows users comfortable with installing and managing applications, use the following quick start. If additional assistance is required, follow the Windows Client Installation instructions.
Note: If this product is already installed, it prompts to uninstall before installing a new version.

Windows Client Requirements

The following sections describe the requirements for Windows clients.

Windows Software Requirements

The Windows Client has the following software requirements:

- Windows version(s) -

  Supported versions of Microsoft Windows include:

  - Windows 7 (SP1), 8.1, 10 (1809 and above), 11 (21H2 and above)
    Notes:
    - **Win 8.1** - USB protection is unavailable in Win 8.1
    - **Windows 7 SP1 32bit** - the following are required for successful installation:
      - Windows6.1-KB3063858-x86.msu
      - https://aka.ms/vs/16/release/vc_redist.x86.exe
      - Windows6.1-KB3020369-x86.msu
      - windows6.1-kb3125574-v4-x86_ba1ff5537312561795cc04db0b02fbb0a74b2cbd.msu
      - NDP472-KB4054530-x86-x64-AllOS-ENU.exe
  - Windows Server 2012 R2+, 2016, 2019, 2022
    Note: For Taegis NGAV on *Windows Server 2012 R2+* to function correctly, all Windows updates must be successfully installed.

  See the reference section *Windows Minimum Hardware Requirements* for additional information.

- Visual C++ -
  Visual C++ Redistributable 14.26 (or greater) is required, currently *14.26.28720*

  During installation, the installer checks for the appropriate version of *Visual C++ Redistributable*. The following two items are queried for verification:

  - **Registry Value** -

`HKLM\SOFTWARE\Microsoft\DevDiv\VC\Servicing\14.0\RuntimeMinimum\Version`

- **Version Number -**
  `vcruntime140.dll` (*System32* or *SysWoW64*)

  If a newer version than *14.26.28720* is installed either via the registry or the physical file on disk, the installer does not install the Visual C++ Redistributable.

  Installation Note: To prepare for deployment, the appropriate packages can be obtained from Microsoft and added to your SCM deployment. Visit the Microsoft latest supported Visual C++ downloads site to download the packages

- Windows must be updated with the latest important updates/fixes from Microsoft.
- Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 require the update corresponding to KB2919355 be installed.

Windows Hardware Requirements

This product hardware requirements match the minimum requirements to run the Windows version you are installing on. See the reference section *Windows Minimum Hardware Requirements* for additional information.

Windows Client Installation Options

There are two options to install Windows clients - via the executable download package or through the PowerShell command line.

Windows Installation Preparation

1. Verify Windows OS version. This product supports the following Windows versions:

   - Windows 7 (SP1), 8, 8.1, 10 (1809 and above), 11 (21H2 and above)
     Win 8.1 note: USB protection is unavailable in Win 8.1
   - Windows Server 2012 R2+, 2016, 2019, 2022
     Note: Taegis NGAV on *Windows Server 2012 R2+* requires all Windows updates to be downloaded and installed to function correctly.

2. Verify that Windows is completely updated. Windows update must run to completion.
   Notes:
   - Windows Update can require several runs to reach completion because it can discover new updates when previous ones are applied.
   - **Windows 7 SP1 32bit** - the following are required for successful installation:
     - Windows6.1-KB3063858-x86.msu
     - https://aka.ms/vs/16/release/vc_redist.x86.exe

- Windows6.1-KB3020369-x86.msu
- windows6.1-kb3125574-v4-x86_ba1ff5537312561795cc04db0b02fbb0a74b2cbd.msu
- NDP472-KB4054530-x86-x64-AllOS-ENU.exe

Download the Installation Package

To download the client application and registration key, use one of the following methods.

Download Using Invitation Email

1. Consult your *invitation email* for the download link
2. Open a browser
3. Copy the link in the email invitation into the browser to download the installation file. Save the file for later installation.
4. Copy and save the *Registration Key* and *Server URL*
   Note: The *Registration Key* and *Server URL* are required if the Taegis NGAV client is manually unregistered and needs to be re-registered.

Download from Deployments Page

1. Open a browser
2. Navigate to the *Management Console URL*
3. Click **Deployment** to display the *Downloads* pane
   Note: Select a *Device Group* to make options available (clickable).
4. Click **Download a redistributable package** to display the various packages
   Note: Windows installer files include both `.msi` files (for command line deployment) and `.exe` files (for manual deployment)
5. Click appropriate installer version to download the installer package
6. Save the *Registration Key* and *Server URL*
   Note: The *Registration Key* and *Server URL* are required if the Taegis NGAV client is manually unregistered and needs to be re-registered.

Install Windows Client - Use EXE Installation Package

1. **Begin Installation** - Run the downloaded `.exe` installation package.
   Note: For information about using the `.msi` deployment package, see the Install Windows Client - Use PowerShell Commandssection.
2. **Accept Agreement** - Navigate through the installation dialog wizard to read and accept the EULA and select configurations.
   Note: The final installation step launches this product and prompts for registration (first run only)..

3. Verify the installation location and select the *I have read and accept...* option.
4. Click **Install** to launch the installation process.
5. When this product successfully installs, a success dialog displays
6. click **Open Now** to complete the installation and display the *Client Activation* dialog
7. Enter the *Web Service URL* and *Registration Key* from your registration
   For additional information see the *dalicense File, Key and Web Server* section.
8. Click **Activate** to submit the information.
   When this product successfully registers, the *Client Dash Board* displays

Install Windows Client - Use PowerShell Commands

The Windows PowerShell command line enables manually installing the client. The client can be installed either interactively or non-interactively (without a GUI) using the *Windows Group Policy* tool (GPO), Microsoft *System Center Configuration Manager* (SCCM), and MSIEXEC (file to execute .msi installation files). The Microsoft Installer packages (.msi) can be customized with built-in parameters (shown below) or through parameters supplied from the command line. See Deploy Client without GUI for more information.
Note: Installation requires *administrative privileges*.

Windows Installation Parameters

Parameter	Value	Description
REGISTRATIONKEY	<Installation Token>	Auto input the Installation Token
WEBSERVICEURL	<Web Service URL>	Web Service URL
NOGUI (optional)	<0 or 1>	Enables installing the package without the Graphical User Interface **Notes**: • Policy settings must be configured to ensure successful operation without a user interface • Turn off *Display User Interface* from the policy settings • The `NOGUI` parameter ensures Taegis NGAV is installed with the *Graphical User Interface disabled*
/q (optional)	none	Enables installing the package in *quiet mode*; no user interaction requested/required

Example Command Line Installation

The following command line example shows how to run the Microsoft Windows Installer tool to install the Windows client. This example includes passing the REGISTRATIONKEY,

WEBSERVICEURL and installation parameters.

In the following example, *WEBSERVICEURL* is tst.us and the *REGISTRATIONKEY* is a1b2. Additionally, the command is issued as a single command without line breaks. The artificial line breaks shown below are to facilitate display.

Notes: Substitute your specific values in the command.
Commands that are displayed below as broken across multiple lines should be issued as a single command:

```
.\<version>_SecureWorks_EPP.msi WEBSERVICEURL=http:tst.us \
REGISTRATIONKEY=a1b2 NOGUI=0 /q
```

Note: This installation command requires *administrative privileges*

Perform the following steps to install the client.

1. Download an installation package to a local directory
2. Start Windows PowerShell
3. Change into the directory that contains the installation files
4. As a user with *administrator* authority, issue an installation command to install and configure the Windows client on a machine. In the following example, *WEBSERVICEURL* is `tst.us` and the *REGISTRATIONKEY* is `a1b2`.
   Note: Substitute your specific values in the command.

   ```
   .\<version>_SecureWorks_EPP.msi WEBSERVICEURL=http:tst.us \
   REGISTRATIONKEY=a1b2 NOGUI=0 /q
   ```

Note: This installation can be performed on remote machines by combining this command with an appropriate administration tool.

When this product successfully installs and registers with the cloud service, the target machine displays on the Management Console as a new device in the *Device* list.

Uninstalling or Updating the Windows Client

Uninstall the Windows Client

To manually uninstall the Windows client:

- **Open** Windows *Control Panel*
- **Select** the *Programs* option
- **Navigate** to *Program and Features*
- **Search** for *Taegis NGAV* within the list
- **Uninstall** the client
- **Notes:**

- If a password is set, it must be entered to proceed. All attempts, successful or not, are logged to the Administrative Console.
- Some files remain on the disk after uninstallation. These enable the client to recognize previous policy settings in the case of reinstallation.

Mass Uninstall the Windows Client using PowerShell

To manually mass uninstall the windows client, run the following commands using PowerShell:

```
$Taegis_NGAV = get-WMIObject -Classname Win32_Product | Where-Object Name -eq "Taegis NGAV";$Taegis_NGAV.Uninstall();
Remove-Item 'C:\ProgramData\SecureWorks\Taegis_NGAV' –Recurse
```

Update the Windows Client

This product normally updates automatically. Note that following an upgrade without a reboot, the service continues to protect the endpoint, although it might be necessary to manually open the GUI application to perform actions such as changing settings and viewing alert history.

Open or Start the Application

To open/start the GUI application, perform one of the following:

- Click the desktop shortcut
  OR
- Navigate **Start >** ,locate the product and click it
  OR
- Reboot
  Note: The GUI application starts automatically upon reboot

To manually update the Windows client:

- **Open** the *Taegis NGAV GUI*
- **Navigate** to the *Support* tab
- **Select *Update Now***
  Notes:
  - If *Update Now* cannot be selected, the client is up-to-date.
  - If a password is set, it must be entered to proceed. All attempts, successful or not, are logged to the Administrative Console.

Windows Client Setup Issues

If the client application does not successfully install, launch, or register, review the steps above and try again.

If issues persist, contact your support team. Be able to provide detailed step-by-step instructions to reproduce the issue, including error messages. Be able to provide the operating system version for the client installation.

Linux Quick Installation

Because the Linux client differs from the Windows client, a Quick Start is not appropriate. Linux client installation and use is discussed in the Linux Client section.

Notes:

- Enterprise Linux Client is currently supported on Linux Kernels up to 5.15, future releases will expand supported kernel versions.
- *Process Execution* is not supported on versions greater than 5.15.

Linux Directories Needed to be Whitelisted by Third-Party AV

- /usr/bin/secureworks/taegis-ngav
- /etc/secureworks/taegis-ngav
- /var/log/secureworks/taegis-ngav

Management Console Concepts

The following sections discuss concepts that are critical to understanding how the management console functions:

- Allow and Deny Lists
- Client Alert Settings

Allow and Deny Lists

Files or directories (folders) can be designated as *benign* (allow) or *malware* (deny) through *deny* or *allow* lists. These designations determine what action this product takes when encountering files or folders. If a file or folder is identified as malware, normal behavior is to block file execution and quarantine the file. If a folder or file is determined to be benign, they are not interfered with or changed (or moved) and normal file execution occurs. The lists can be applied through global policy to all clients. The lists are editable and can be searched or sorted using various criteria. Additionally, certificate thumbprints generated for each file can be used to allow files across devices. Certificates are added to the allow list using the *Take Action* workflow on the *Alerts Index & Details* Page.

See *Editing Security Policies* for more information about how add folders to the *Allow* list. See Adding a Certificate to a Global List| for additional information about adding a *certificate thumbprint* to the global list.

List scope can be defined and curated as specific file/folder names or expanded through the use of wildcards or regular expressions. Note that entries in allow and deny lists are case sensitive.

Administrators can change the designation of a file by moving it from one list to another. This means files are moved (toggled) between allow lists and deny lists. Note that if an item is moved from an allow list to a deny list, the status for that file displays a *Remediated* status.

Warning: Because it is possible to allow list directories/folders from the management console, **any** file located within an allow listed directory is considered benign (*allowed*) and will not trigger an alert or action. Use great care when using this option. See *False Positives* and *Editing Security Policies* for additional information.

Example Allow List

To create an allow list entry for all directories that start with the word work and include all permutations (for example *work1, works, working*):

1. Access the Management Console
2. Click **Administration** to display the administration tabs
3. Click **Security Policies**
4. Choose an existing policy template or create a new one
5. Click the **Security Policy** name to launch the *Security Policy Details* pane
6. Click the **Allow List Folder** tab
7. Click the **Edit** button to display the *Edit Device Policy* dialog box
8. Edit an existing folder name or click **+ Add New Folder** to add an additional specification.

   Folders can be specified as specific directory/folder names or expanded through the use of wildcards or regular expressions, for example:

   ```
   c:\work*
   ```

   Note: Folder or file path specifications are different between Windows and Linux:

   - Windows folder or file path specifications use the back-slash (\), for example:

     - `C:\Users\Pat\MySpecialFolder`
     - `C:\Users\Pat\TestFolder\*`

   - Linux folder or file path specifications use the forward-slash (/), for example:

     - `home/Pat/MySpecialFolder`

   - Folder allowlist support multi-wildcard entries, for example:

     - `C:\Users\*\Desktop\Login Attempt Test – Delete after\Release\Current\Files\BizCard\*\*.dll`

     - `home/*/Desktop/TestFolder/*/*.elf`

This means care must be taken to ensure the appropriate path type is specified to correctly identify a folder or file location.

9. Click **Save** to apply the changes and close the dialog box.

Allow Lists for Network Shares (Windows)

If *Scanning of Network Share Processes* is enabled for Windows, process execution on network shared drives can be blocked. Any application on the network is automatically blocked if this option is *enabled*.
NOTE: Scripts on the share are allowed.

In the event that a script must be added to the Allow list, it is supported through policy settings.

To allow a folder, perform the following, depending upon the folder location:

- **For folders on a host share**:
  - If there is a <host_name> and <share> folder with a file in the share folder, test_file.exe, for example and the file is accessed through the file system
  - The file is accessed through the path "DESKTOP-2URNV8S\Temp\test_file.exe" where **DESKTOP-2URNV8S** is the *host-name* and **Temp** is the *share*
  - To allow list that folder, add the DESKTOP-2URNV8S\Temp* to the allow list. This enables all applications within this share to run
- **For host share folders mounted locally**:
  - If the share drive is mounted as a drive on the local system, Z:\drive for example
  - Located within the mounted Z:\drive are directories and files. For example the Test_folder directory, with a file inside called test_file.exe
  - The test_file.exe is accessed through the path Z:\Test_Folder\test_file.exe
  - To allow list that file/folder, add the path Z:\Test_Folder* to the allow list. This enables all applications within this specific, locally mounted directory to run

Linux Directories Allowed by Default

This product allows the following Linux directories by default:

```
/bin
/boot
/dev
/etc
/root
/sbin
/usr/bin
/usr/lib
/usr/sbin
```

Quarantine Folder

Note: When a file is quarantined, it is moved from its launched location to the *quarantine folder*. The quarantine directory contains administrator-locked files. In the folder, the malware file is renamed and disabled so it cannot run.

The quarantine folder is located in the application installation folder, depending on the operating system:

- Windows (32-bit and 64-bit):
  `C:\ProgramData\SecureWorks\Taegis_NGAV\system\quarantine`
- Linux:
  `/usr/bin/secureworks/taegisngav/Quarantine`

Client Default Automatic Actions

The management console enables setting *default automatic actions* that specify how to alert and respond to alerts on client machines. The automatic settings can rely on curated *allow* and *deny* lists or databases to instruct action. Because management console settings override client settings, global automatic actions must be carefully considered. Available automatic client actions include the following:

- **Quarantine**
- **Alert**

Quarantine -

The *automatic quarantine* setting on the console overrides any setting on the client. This means that any files in the deny list are treated as malware and placed in quarantine. Any file found in the allow list is treated as non-malware and ignored. No automatic action occurs. If a file is considered malware, the following actions are applied:

1. File execution is stopped or blocked.
2. The file is moved to the quarantine directory.

Note: If a file cannot be quarantined for some reason, a pop-up window displays. Click **Ok** to close the pop-up.

3. An Alert pop-up screen message displays:

```
...File Detected
 detected the file ...
```

Alert -

The *automatic alert* setting on the console overrides any setting on the client. This means that any files on the deny list are treated as malware and placed in quarantine. Any file found in the allow list is treated as non-malware and ignored. No automatic action occurs. If a file is considered malware and not on the deny list, the following actions are applied:

1. File execution is **NOT** stopped, blocked, or paused.
2. An Alert pop-up screen message displays:

```
...File Detected
 detected the file …
```

Note: The pop-up alert window has no option buttons. It closes automatically after a short time

Software Inventory

A software inventory component for Windows based systems is included. This component currently provides listings of the software installed on protected Windows systems across the user base.

Periodically, the software automatically uploads the list to the server. This software list displays for each Windows device through the Management Console *Device Details* page, under the *Software Inventory* tab.
Note: The *Software Inventory* list includes all software that self-reported to Windows during installation. Self-reported software displays within the Windows *Add/Remove* dialog. Any software that does not self-report to Windows does not display in the Windows *Add/Remove* dialog and does not display in the inventory list for that device.

The *Software Inventory* component continues to evolve. The supported functionalities will grow to include additional organization wide reporting and analytics.

Software Inventory Information

The *Software Inventory* tab displays:

- The default display *Total* of known installed software
- A search field to locate software or vendors within the list
- A checkbox to display the status column that includes known *Uninstalled Software*

The Software Inventory component currently displays the following information for each piece of known software:

- **Status** -
  Select the *Show Uninstalled Software* checkbox on the page to display the *Status* column. Valid status options:
  - *Installed* -
    Default value - field is blank
    Software is currently installed on the system
  - *Uninstalled* -
    Previously installed software package removed by the user

- **Software Name** -
  Name of the software as reported by the manufacturer

- **Version** -
  Version of the installed software

- **Manufacturer** -
  Publisher of the installed software

- **Installation Location** -
  Installed software location on system hard drive

- **Installation Time** -
  Timestamp when software was installed

- **Installation Date** -
  Timestamp when software was installed

Note: The availability of this information for display depends on appropriate information reporting by the software manufacturer. If this information is missing, an empty data field displays.

Client Caching Types

There are two caches. One for admin protected folders called the ACL Cache that is in memory. And the other is stored in our model database. The later being based on a sha1. It will only get invalidated if new models come into play or someone overrides the value through the global lists. Both caches are used across RTFM and Process Execution.

Client Architecture Optimization

Client Architecture Optimization is a feature available for each supported client OS. The feature is controlled through the *Protection Settings* for each OS.

Clients are optimized by only loading Machine Learning models that are necessary for that OS. Limiting the number of loaded models results in less memory use.

Enabling Client Architecture Optimization loads only the following Machine Learning models, depending on the client OS:

- **Windows:**
  - LDOC
  - XDOC
  - .NET
  - PE
  - PowerShell
  - VBScript

- **Linux:**

- ELF
- ELF ARM
- LDOC
- XDOC

Using the Management Portal

The following sections describe the management console interface and explain the basic tasks available through the console.

Note: Refresh the browser window after performing actions to ensure a timely display. Failure to refresh can result in the perception that an action has not completed.

Logging into the Portal

1. Open the *Management Portal* login email.
2. Open a browser and navigate to the Taegis NGAV web URL https://ngav.taegis.secureworks.com/ to display the login screen
3. Consult your welcome email for the login credentials
4. Enter the login credentials to access the console.
   Note: The console administrator login session has a default expiration time limit. The default expiration time is 1 hr 45 minutes. If no activity is detected for that time span, a warning displays before the console automatically logs the administrator out.

   A successful login displays the dashboard.

   Note: The dashboard display is sensitive to browser window size/magnification. The dashboard display rearranges when the browser size or magnification drops below a certain value.

   Note: If you encounter issues logging in, contact your support team.

Dashboard

The initial and default dashboard consists of a main pane that displays various real-time information and a left pane that hosts tabs that provide additional actions or views. The information panel and filter block for the display also display.

Dashboard - Portal Left Pane

The left pane includes tabs for:

- **Dashboard** - return to this current, default view
- **Alerts** - display detailed threat information
- **Devices** - display detailed device information

- **Administration** - display essential administrative and policy functions
- **Deployment** - define new devices and access available client software installation files
- **Software Inventory** - display the software inventory information
- **Subscription** - display information about the license and number of devices in use
- **Current Logged in user** - provides logout from the console portal and ability to toggle two-factor authentication for the logged in user

Dashboard - Display Filters

The console Dashboard displays information in the right pane. This information can be filtered based on a *time range* or *device group(s)*, selectable through the drop-down display filters.

Click a filter chevron to display the display filter options. For example, click the left chevron (labeled *8 device groups selected* in this example) to display the available device groups.

Dashboard - Tabs

The console Dashboard displays information in the right pane, depending on which of the two tabs are selected:

- **Alerts** tab - this default, initial pane displays various summary information concerning alerts and threats across the monitored network
- **Devices** tab - Displays a summary of the number of devices, device groups, connection status, etc.
  Note: Do not confuse this display with the information displayed by the *Devices* tab located in the left pane.

Dashboard - Alerts Tab (Default, Right Pane)

The right pane of the *Dashboard* provides various information in real time. Included within the pane are the following:

- **Information Panel** that displays various information:
  - Tabs to select between **Alerts** and **Devices** display
  - (number of) *Licenses Used*
  - (total number of) *Alerts*
  - (total number of) *Threats*
  - *Add New Devices* button
- **Activity Timeline** - provides graphical information concerning activities by date and relative numbers of detected threats.
- **Alerts - Most Active Devices** - lists devices in descending order of the number of occurrences per device. Click a device to display additional information.
  Note: Alert timestamps will always be aligned to the timezone of the user logged in to the Management Console.See the section on Alert TimeStamps for additional information.

- **Alert Feed** - shows current device threats and their priority/severity
- **Alerts - Priority** - shows current numbers of alerts, categorized by *priority*
- **Threat Category -** Depending on the detected threats in your environment, this displays a list of all *unique threat categories* found
- **Threat File Type** - Depending on the detected threats found in your environment, this displays a list of all *unique file types* found

Dashboard - Devices Tab (Right Pane)

This tab displays a *dashboard view* of various summaries and includes the *High Risk Devices Feed* that provides a quick view of potentially endangered devices:

- *Agent Versions*
- *Device Risk*
- *Device Status*
- *Device by Platform*
- *High Risk Devices Feed*

Note: Do not confuse this display with the information displayed by the *Devices* tab located in the left pane.

Alerts Tab

The *Alerts* tab in the dashboard left-hand pane provides access to concise information about threats found on all connected systems. This product alerts when untrusted applications with a cognitive threat confidence above 50% attempt to run. These alerts display on both the client and the management console. Click this tab to display information in the right pane of the portal.

Note: Alert timestamps will always be aligned to the timezone of the user logged in to the Management Console. See the section on Alert TimeStamps for additional information.

The tab pane action bar includes drop-down selections to define which *device groups* display and *time range* display in the *Alerts* pane.

The *Alerts* pane includes the following information/actions:

- Licenses Used (total)
- Alerts (Total)
- Threats (Total)
- Add New Devices button
- Action Block with:
  - Search Field
  - Filter Settings (list filter)

- File Information Block (columns, ordered from left to right):
  - Alert Priority (L = Low, M = Medium, H = High)
  - Alert Type
  - Device Name|Group Name
  - Username
  - Date Created

Threat and Priority Levels

A threat level specifies a client reaction based on relative sensitivity to a threat detection. A priority level provides information concerning the relative importance concerning detected threats.

Threat Levels

- **Threat Level 1 -**
  Policy is set to *Cautious*
  The client alerts only on *Malicious* detections. A malicious detection is when the model is 100% confident a specific detection is malicious
- **Threat Level 2 -**
  Policy is set to *Moderate*
  The client alerts on *Malicious* and *Suspicious* detections
- **Threat Level 3 -**
  Policy is set to *Aggressive*
  The client alerts on *Malicious*, *Suspicious* and *Abnormal* detections

  NOTE: Although the confidence threshold levels change based on each update, the system always flags anything the model is 100% confident of being *Malicious* as well as any items included in the deny list. *Suspicious* and *Abnormal* detections are based on the model confidence on a particular threat.

  For additional information, see Editing Security Policies.

Priority Levels

Priority Levels are different from *Threat Levels*. Priority levels provide insights into the various detected threats. Detected threats are categorized as either *High Priority* or *Low Priority*.

- **High Priority -**
  a threat was detected but was not prevented (quarantined)
- **Low Priority -**
  a threat was mitigated successfully (quarantined)

Navigating the Alerts Tab

The *Alerts* tab displays system-wide alert information and enables various tasks:

- **Sort data display** -
  The data within the tab can be sorted by various criteria using the selectable filters. In some circumstances, click a *column name* to sort the threat list by the column topic.
- **Search** -
  The *Search* field enables searching various threat parameters, including, *name* (common and regular), *type*, and *HASH*.

  Enter the search term and click the magnifying glass to search.
- **Filter Settings** -
  Click the **Filter Settings** button to display the *Filter Settings* dialog

  Select search options using check boxes. Options include:
  - *Alert Priority*
  - *Alert Type*
  - *Threat Category*
  - *File Type*
  - *Threat Activity Type*
  - *OT/IT*
  - A *Clear Filters* button to reverse filter selection

Working with Alerts

Alerts display in the *Alerts* pane.

To select a particular alert for action:

1. Click the **Device Name** that contains the alert to display the *Alert Summary* dialog
2. Click the **Device Name | Group Name** to display the *Device Details* pane.

   See Device Details Pane for additional information.

To display additional information about a particular alert:

1. Choose an alert from the list
2. Click the **Alert** to display the *Alert Summary*
3. Click **View Alert Details** to display information about that particular threat

   The *Alert Details* include:
   - *File Name*
   - SHA1 value
   - *Threat File Type*
   - *Confidence Score*
   - *Device Name* (location)

- *Threat Activity Type (Detection Method)*
- *Alert Name & Type*
- *Status & Time stamp*
- *Alert Created*
- *Alert Latest Action*
- Sub Tabs- - various tabs will display depending on availability:
  - *Details* (default)
  - *Occurrences*
  - *Static File Analysis*
  - *Threat Identifiers*
  - *Mitre Attack Matrix*
  - *Process Tree*

  Note: All displayed dates originate from the client.

Notes on Alert Detail Timestamps

Two sets of timestamps display within the *Alert Details* pane:

- **File** timestamps:
  - *Created* (original) - the date the file was created
  - *File Modified* (current) - the most recent modification date

- **Alert** timestamps (Alert Details):
  - *Original Alert Timestamp* - date of *first* detection
  - *Current Alert Timestamp* - date of most recent alert
    See the section on Alert TimeStamps for additional information.

Remediate Threat Actions

This product includes the ability to perform *Remote Remediation* and *Restoration* of files on client machines. Administrators can initiate a remote action through the *Take Action* button.

Note: *Restore* and/or *Quarantine* actions are not available if the file is moved or deleted from the original path.

Click the *Take Action* button to display the options drop-down menu.

The available action choices are:

- *Remote Remediate* that enables various options depending on the target:
  - Device specific actions are quarantine of a malicious file or termination of a malicious process
  - Global action is to add the SHA1 identifier for the file or process to the global deny list so it is identified as malicious and apply the information to all occurrences.
    Action Failed Message
    Any downloaded threat that is moved to another location results in 2 occurrences of the threat. For example, moving the threat from the *Downloads* folder to the *Desktop*

folder. If the *Remote Remediate* action is applied to the threat, the process is successful for the *Desktop* location but a failure for the *Downloads* location. This is because the file was moved from the original location and the remediation action could not be completed. This generates an **Action Failed** message that can safely be ignored. The threat is successfully mitigated.

- *Remote Restore* enables the restoration of a file that was accidentally quarantined. The various options depend on the target for the action:
  - Device specific action is to restore the file. This means remove the file from quarantine and move it back to the original location.
  - Global Actions -
    Note: *Global Actions* are dynamic options that display according to the system status. Global actions include:
    - **Add SHA1 to Global Allow List** - adds the SHA1 identifier for the file or process to the global allow list so it is considered as benign and apply the information to all occurrences
    - **Add Certificate to Global Allow List** - adds the generated certificate thumbprint identifier for the file to the global allow list so it is considered benign.
      Note: The console does not validate whether the certificate is current or expired.
    - **Apply to All Occurrences** - applies the selected actions to all occurrences of the file or process.

    Action Failed Message
    Any threat that is moved to another location before it is accidentally quarantined and then restored can result in 2 occurrences of a file restoration. For example, moving a file from the *Downloads* folder to the *Desktop* folder and then (accidentally) quarantining the file. If the *Remote Restore* action is applied to the file, the process is successful for the *Desktop* location but a failure for the *Downloads* location. This is because the file was moved from the original location and the restoration action could not be completed. This generates an **Action Failed** message that can safely be ignored. Verify the file is correctly restored.
- *External Remediate* enables a threat to be marked as resolved by some action external to Taegis NGAV.

Alert Tab - Sub-tabs

Additional tabs display within the *Alert Details* pane. The default tab that displays is the *Details* tab, described above. Various tabs display depending on availability:

- **Occurrences -**
  Displays alert information together with devices affected by the particular threat alert.
- **Script Content -**
  This tab enables you to view detailed script information, including the body of the script for a particular threat.

Click **Script Content** to display the script content associated with the particular threat alert.

- **Static File Analysis -**
  Displays the file analysis for why the file was detected
- **Threat Identifiers -**
  Displays the identifiers used to classify the threat
- **Mitre Attack Matrix -**
  Displays the *Mitre Attack Matrix* information for this file
- **Process Tree -**
  Displays a graphical process tree for the file and its associated processes
- **Explainability** -
  This tab is populated only for Excel document detection and explains why the document was designated *malicious*

Devices Tab

Click the **Devices** tab (located in the left pane of the portal) to display the *Connected Devices* pane.

This pane provides a visual representation of all devices connected with the Management Console, with extensive information on each device.

Adjust the way the devices display - click the *Grid* or *List* icon to select between *List View* or *Grid View.*

The following information displays for each device:

- Platform icon, with indicator of protection:
  - Green check mark means *protected*
  - Red exclamation mark means *not protected*
  - Question mark (**?**) next to a device means protection information is *unknown*
- Device *IP address*
- Device name
- *Username* that created account
- Number of threats that require action
- Connection icons that indicate the connection status:
  - Connection icon that indicates the *connected* state
  - Un-plugged, disconnection icon that shows a *disconnection* state. With a disconnection, the display includes information about how long the device has been offline
- Trashcan - Hover over the device card to display the trashcan. Click the trashcan icon to

delete the device from the management console and remove settings saved to the device .
Note: This action does not remove the endpoint software from the client.

Device Status - Connection

The *Device Status* is a reflection of the connection between the management console and the device. The management console can be either a *cloud-based* or an *on-prem* management console.

The *Device Status* contains three connection categories: *Active, Inactive, Recycled*.

The categories are based on the time interval since the last successful device check-in to the management console. The default check-in frequency is normally every *10 minutes*.

Note: Restarting the TaegisNGAV service initiates an immediate check-in and restarts the check-in interval counter.

The device status is determined by the following rules:

- **Communicates Within 2 Hour Window** -
  A device is *Active* and *Connected* when it checks in within 2 hours
- **No Communication Within 2 Hour Window** -
  If a device fails to successfully check-in after *2 hours*, the device status changes to *Disconnected*, but still *Active*
- **No Communication 14 Days** -
  If the device fails to successfully check-in after *14 days*, the device status changes to *Disconnected* and *Inactive*
- **Successful Check IN** -
  When a device successfully checks back in, the device status changes to *Active*
- **No Communication 28 Days** -
  If the device fails to successfully check-in after *28 days*, the device status changes to *Recycled* and the device no longer counts against the number of device licenses

Connected Devices - General Actions

The following general actions are available:

- Search devices by *Device Name*
- Sort by *Device Groups*
- Sort by *Device Status* –
  Sort options include: *Active Devices*, *Inactive Devices, Recycled Devices*.
- Sort by *Device Risk* –
  Sort options include: *All*, *Low Risk Devices*, *Medium Risk Devices*, *High Risk Devices*
- Sort by *Device Platform* –
  Sort options, depending on devices, include:
  - *All*

- *Linux*
- *Windows*
- *Windows (OT)* (industrial)
- *Windows Isolated Device (OT)* (industrial, air-gapped)
- *Linux (OT)* (industrial)
- *Linux Isolated Device (OT)* (industrial, air-gapped)

- Sort by *Agent Version*

Connected Devices - Device Actions

Use the *Connected Devices* pane to perform actions on one or more devices. Designate devices for action using the device checkbox. Click the device or hover the mouse over the device to display the checkbox.

Available device actions include:

- **Add** the device(s) to a group
- **Recycle Devices**

Perform Actions on Devices

To perform actions on a device or devices:

1. Click **Devices** to display the *Connected Devices* pane
2. Click the **checkbox** for each device to select it for action
3. Click the **Bulk Actions** button (orange arrow, above) to display the action drop-down menu
4. Select the action to perform:
   - Select **Add to Group** to display the *Add Devices to Group* selection dialog
     i. Click the **chevron (>)** (orange arrow, above) to display the available groups
     ii. Select the group(s) for the device
     iii. Click **Confirm** to save the information and close the dialog.
   - Select **Recycle Devices** to recycle the devices from the Console association
   - Select **Export Device Reports** to display the *Export Device Reports* dialog:
     i. Use the check boxes to select what information to include in the report
     ii. Click **Export** to save the CSV formatted file, or **Cancel** to abandon the selections and close the dialog.
   - Select **Clear Selection** to uncheck (de-select) all selected devices and close the drop-down menu

Device Details Pane

To display additional device details:

From the console window, click the **Devices** tab to display the *Connected Devices* pane.

Select a device for more information. Click the **device name** or device icon to display additional details.

The *Device Details* screen displays.

The *Device Details* screen contains several sections, each with specific detail information:

Device Identification - The top section includes, from left to right:

- **Device Name**
- **AI Threat Protection (status)**
- **Device Risk Score** - this score indicates how well the device is protected. Higher scores are better, with a maximum of 100%. Lower scores indicate the device is vulnerable.
- **IP Address**
- **Operating System**
- **Last Device Sync**
- **First Device Sync**

Tabs - The middle section includes tabs to access sub-panes, from left to right:

- **Alerts** (default)
- **Agent Details**
- **Device Information**
- **USB Devices (Windows)**
- **Software Inventory (Windows)**
- **Activity Log**

Malware History - The bottom section includes the historical list of files identified as threats associated with this device. The information columns include, from left to right:

- **Alert Priority**
- **Alert Type**
- **Device Name | Group Name**
- **Username**
- **Date Created**

Devices - Take Action

The **Take Action** button enables selecting and applying various actions to device alerts.

1. Click an alert **filename** to display the *Alert Summary*
2. Click View Alert Details to display the *Alert Details* pane
3. Click **Take Action** to display the *Take Threat Action* dialog
4. Click the **chevron (>)** to display the drop-down list

   The drop-down options include:

   - **Remote Remediate** - provides both *Device Specific* and *Global* actions
   - **Remote Restore** - enables restoring the file to its original directory and adding its information the global allow list to mark it benign.
   - **External Remediation** - marks the file as already mediated through an external means.

Perform Actions

Chose the device alert actions:

- To perform *Remote Remediation* on the threat alert:
  1. Select the **Remote Remediate** option from the drop down to display the *Remote Remediate* dialog.
  2. Select the appropriate options
  3. Click **Submit** to apply the remediation and close the dialog.

- To perform *Remote Restoration* on the threat alert:
  1. Click **Remote Restore** to display the *Remote Restore* dialog.
  2. Select the appropriate options
  3. Click **Submit** to apply the remediation and close the dialog.

- To perform *External Remediation* (mark the file as handled external to Taegis NGAV):
  1. Click **External Remediate**.
  2. Click **Submit** to apply the remediation and close the dialog.

Device Details Sub Tabs

The Device Details pane includes tabs that display additional information:

- **Alerts** sub tab - the default Device Details display, described above
- **Agent Details** sub tab - The *Agent Details* sub tab displays two panes:
  - *Policy Settings* - shows the Security Policies of the Device Group the Client is registered with
  - *Device Security Profile* - shows the current settings on the Client. The Client sends the current settings to the Server to display on the Management Console.

    Note: Some information in this section is platform (operating system) specific.
- **Device Information** sub tab - The *Device Information* sub tab displays endpoint details.

NOTE: This feature is supported only with Windows Defender.

The Information that displays in the *Device Information* sub-tab includes:

- Host specific data such as *host name*, *platform*, and *user*
- Identification information such as *IP address*, *MAC address*, *group membership*, and *Active Directory* data
- Time stamp information

- **USB** sub tab - The *USB* sub tab displays USB related information, if any.
- **Software Inventory** sub tab - The *Software Inventory* sub tab displays a list of all software that self-reported to Windows during installation. See the Software Inventory section for additional information.
- **Activity Log** sub tab - The *Activity Log* sub tab displays logs with various activities relative to the endpoint.

Administration Tab

Click the **Administration** tab to expand it to show additional administration options, below:

- **Users**
- **Security Policies**
- **Global Lists**
- **Audit Logs**
- **Reporting**

User Management tab

Click the **Users** tab to display the *User Management* pane that includes information about users and an **Add User** button (red arrow, below) to launch a new user dialog. The *User Management* pane includes the column labels from left to right:

- **First Name**
- **Last Name**
- **Email**
- **Username**
- **Last Login** (date)
- **Joined** (date)

The *Users* pane enables various user management tasks, including:

- Viewing the list of users allowed to login to the Management Console. This list can be sorted and filtered based on the column headings.
- Creating new users
- Displaying and adjusting *User Details*. Click a **User row** to display the *User Details* pane.

  This pane enables:

  - Viewing and editing individual user information, including login history

- Viewing and editing *Managed Device Groups* associated with the user
- Managing passwords and permissions (*Administrator*, *Manager*, *Auditor*, *Report Viewer*).
  For additional information on permissions, see Management Console Roles.
- Creating or rescinding (invalidating) individual user API keys

Creating a New User

To create a new user that can access the Management Console:

1. Click the **Add User** button in the upper right-hand corner.

   The **New User** dialog displays.

2. Enter the user information:

   a. Enter the *First Name* and *Last Name*

   b. Provide an *Email Address*

   c. Assign a Role (*Auditor*, *Manager*, or *Administrator*)

   d. (optional) Toggle *Two-Factor Authentication*
   See Two-Factor Authentication for additional information.

   e. Click **Send Invitation** to save the information, send an email invitation to the new user with instructions about how to proceed, and close the dialog.
   Note: Click the **Cancel** button (or the **X** - top right corner of dialog) to close the dialog. Any entered information is lost.

Editing User Details

To edit an existing user:

1. Click **Users** in the left pane to display the *Users* pane
2. Locate the user
3. Click the user row to display the *User Details* pane
4. Choose the information to edit (from left to right):
   - User Information
   - Managed Device Groups
   - Generate or Invalidate (existing) API key
   - Copy (existing) API Key to Clipboard

Edit User Information

To edit user information:

1. Click **Edit** to display the *Edit User* dialog
2. Edit the information.

   Choices include changing the various fields, toggling two-factor authentication, reassigning a role, and deleting the user.
3. Click **Update** to save the changes and exit the dialog.

Change Account Owner

To change account owner:

1. Click **Edit** to display the *Edit User* dialog.
2. Enable the **Account owner** toggle.

   Note: Once the account owner role is set, it cannot be changed to any other role. The previous account owner should not be deleted either.
3. Click **Update** to save the changes and exit the dialog.

Assigning a Device Group Manager

It is possible to assign (specify) a user to be a *Group Manager* for a particular *Device Group*. To promote a user to a *Group Manager*, assign a group to that user. This action designates that particular user as the *Group Manager*. Be aware that if a *Device Group* is assigned to a user, that user not only becomes a *Group Manager* for that group but also receives the elevated permissions of a *Group Manager*. It is also possible to have multiple group managers for a particular device group.

Edit Managed Device Groups

To edit the managed device group information:

1. Click **Users** in the left pane to display the *Users* pane
2. Locate the user
3. Click the user row to display the *User Details* pane
4. Locate the *Managed Device Groups* section.
5. Click **Edit** to display the *Managed Device Groups* dialog
6. If a necessary, use the *search* field to find the appropriate device group name
7. Check (or uncheck) the box next to each *device group name* to assign to (or remove from) the user

8. Click **Save** to save the changes
9. Click **Close** to exit the dialog and apply the changes

Creating Individual API Keys

To create an API key for a user:

1. Log in to the console
2. Click the **Users** tab in left menu to display the *Users* list in the right-hand pane
3. Locate the appropriate *user*.
   Note: The *search* option enables sorting through large user lists.
4. Click the **User name** (row) to display the *User Details* pane.
5. Click the **Generate API key**

   The new key displays in the key field. The key can be copied or invalidated

Managing Security Policies

The *Security Policy* tab displays as part of the *Administration* group in the left pane.

This tab allows you to view, create, and manage Security Policies for the Management Console.

Click the tab to display the *Security Policies* pane on the right.

The *Security Policies* pane includes:

- Device Policy *Name*
- Number of Device Groups (included in policy)
- Last Modification Date
- The **Create New Security Policy** button

Creating New Security Policies

New security policies can be created to target various devices and/or groups. Descriptions of the various policy settings are described in the Policy Settings table.

This product provides default templates that can cloned and put directly into use or used as a starting point to create custom security policies.

To create a new policy:

1. Click the **Create New Security Policy** button (upper right-hand corner) to open the *Create Security Policy* dialog.
2. Enter a new *policy name*, with or without a description. Optionally select **Clone Existing Policy** to base the new policy on this *template*.
3. Click the **Create button** to display the new *Security Policy Details* pane.

4. Verify the correct *Device Policy* displays. Page through the settings and verify the settings are appropriate for your use:
   a. Click **Edit** to display the **+ Switch to Advanced View** option
   b. Click the **+ Switch to Advanced View** option to display the granular security options settings

   If you want to make changes, continue on to Editing Security Policies
   See Policy Settings for additional information.

Notes:

- To change the name, base template or delete this policy, click the top **Edit** button.
- To duplicate this policy, click the top **Duplicate** button.

Editing Security Policies

Policies can affect various device groups and devices. This product provides pre-configured default templates that can be cloned and put directly into use or used as starting points to create custom security policies. Additionally, currently defined security policies can be used as templates.

To view or edit security policy details:

1. Navigate **Administration > Security Policies**
2. Select a security policy to edit
3. Click the **Edit** button to display the basic edit dialog
4. Page through the Security Policy Details to determine what changes are required. The available tabs are:
   - *Detection and Protection Settings* - enables setting the relative intensity of protection reactions and sensitivity of detection.
     See SysLog Field & Event Descriptions for additional information about protection and detection settings.
   - *OS Protection Settings* - fine tunes how protection behaves including toggling various protections, including:
     - *Process Execution Monitoring*
     - *Scanning Network Share Processes* (Windows only)
   - Scanning Network Share Processes
     This Windows only capability provides process execution scanning on drives shared on the network. Any application on the network is automatically blocked if this option is enabled. Note that scripts on the share are allowed to run. Adding directories in the share to the Allow list is supported through policy. See Allow Lists for Network Shares (Windows) for additional information.

USB Device Notes:

- This tab includes the ability to toggle USB device control (protection) on/off.
- If USB Control is enabled, any USB Mass Storage device that does not have a serial number listed in the Global Lists > USB Allow List will be blocked.

- *Agent Settings* - sets agent options. See the Agent Settings section for additional information.
- *Folder Allow List* - enables expanding or rescinding folders or files in the Allow list. See Allow and Deny Lists for additional information.

5. To view the advanced, more granular *Detection and Protection Settings* options, click **+ Switch to Advanced View** to display the granular security options settings.
6. Click **Edit**
7. Make changes
8. Click **Save** to preserve the changes and exit the edit dialog.

Preserve Device Settings (Windows Only)

Preserve Device Settings is a Windows only feature that enables specifying which, if any device settings are maintained upon registration. Note that each device setting must be specifically selected for preservation.

To access the *Preserve Device Settings* options, from the Management console, navigate:

`Security Policies > Security Policy Details`

The settings that can be preserved include:

- *Personal Firewall*
- *User Access Control*
- *Trusted Application Verification*
- *Credential Guard*

Notes:

- When a new policy is created, the default settings for *Preservations* are set to **Off**
- For any setting with preservation disabled (turned off), the client falls back to the current Windows protection setting

Editing Devices

Device groups are collections of users or devices with similar security needs or security policies. Groups can be created for different user locations, associated working groups or device types.

The *Device Groups* tab displays as part of the *Administration* group in the left pane.

To edit an existing policy:

1. Click ***Administration > Device Groups*** to display the *Device Groups* pane on the right
2. Scroll through the list and select a *Device Group Name* to edit

   Note: The small padlock icon near the *Device Group Name* indicates whether the policy is **locked** or **unlocked**. If the policy is locked, the client cannot make changes to it and any changes to the policy are automatically pushed to the associated clients.

   Hover over any *Device Group Name* to display available options:

   - *View Devices* link
   - *Edit Device Group* button
   - *Copy* (registration key)
   - *Add New Devices to This Group* button
3. Click the *Edit Device Group* button to display the edit dialog
4. Enter the changes and click **Update** to save the changes and exit the dialog. Click **Delete this device group** to remove this group.
   Click **Cancel** to abandon changes and exit the dialog.
5. Click the padlock to change the state of the device group

Managing Device Groups

The *Device Groups* tab displays as part of the *Administration* group in the left pane.

Click the tab to display the *Device Groups* pane (right side). The *Device Groups* pane displays the existing device groups and a button to launch the *Create New device Group* dialog.

Each device group block displays information about that particular device group.

The information device group information includes, from left to right:

- *Device Group Name*
- *Padlock* icon to indicate locked/unlocked state
- Name of *Security Policy* in place and whether it is a template

  The following example shows 2 device groups and the different security policies implemented for each:
  - An Industrial client (**OT**) Security Policy implemented for the *Andrei's Windmill Farm* device group
  - An Endpoint Protection client IT Corporate (**IT**) Security Policy implemented for the *Customer Success Team* device group
- *Registration Key*
- (number of) *Devices* in the group

- Associated device types with a count of each type

Hover over the device name block to display the available actions.

Editing a Device Group

To edit an existing device group:

1. Navigate **Administration > Device Groups** to display the *Device Group* pane on the right.
   Note: Hover over a *Device group Name* to display available options, including the *Edit Device Group* button.
2. Select a device group *name*
3. Click the *Edit Device Group* button to launch the *Edit Device Group* dialog
4. Make the edits, as required:
   - Change the *device group name*
   - Select a different policy from the drop-down list to apply to the group.
5. Click the **Update** button to submit the changes or click **Close** to discard changes and exit the dialog.

Creating a New Device Group

To create a new device group:

1. Navigate **Administration > Device Groups** to display the *Device Group* pane on the right.
2. Click the **Create New Device Group** button in the upper right-hand corner of the page to open the *New Device Group* dialog:
3. Enter a *Device group Name* for the *New Device Group*.
4. Click the drop-down list to select a *Security Policy* to apply to this group.
5. Click the **Create** button to save the new policy and exit the dialog.
   Alternatively, click **Cancel** to abandon changes and exit without creating the group.

Global Lists (Allow and Deny)

The *Global Lists* tab displays as part of the *Administration* group in the left pane.

Navigate **Administration > Global Lists** to display the *Global Lists* pane.

The *Global Lists* pane enables creation and maintenance of *deny* and *allow* lists. The two lists contain known file names. Inclusion of a file within a list designates the file as benign or as malware. This product uses the lists to selectively and preemptively apply actions to files.

Administrators can change the designation of a file by moving it from one list to another. This means files are moved between allow lists and deny lists. Note that if an item is moved from an allow list to a deny list, the status for that file displays a *Remediated* status.

The list entries can be sorted by *Hash, user/data added, most common file name,* and *alert name/alert category*.

Note: It is possible to allow directories, just like allow listing files. See Editing Security Policies for additional information.
Warning: Because any file contained within an *allowed* directory is considered benign, great care and consideration must be used with this option.

Click the tab to display the *Global Lists* pane (right side).

The *Global Lists* pane contains:

- The **Add New Hash** button
- Tabs to select which file list to display: *File Deny List*, *File Allow List*, or *Certificate Allow*
- Filters:
  - Search field for *Search Global Lists...*
  - Alert Category type filter – examples include: *All*, *AI Detection*, *PUA*
- Filtered results, containing threat information columns, from left to right:
  - **SHA** (value)
  - **User/Date Added**
  - **Most Common File Name**
  - **Threat Name/ Alert Category**
  - **Type** - list type, *deny*, *allow*

Assigning a File to a Global List

To add a new file name entry to either an *Allow* or *Deny Global List*:

1. Click **Administration > Global Lists** to display the *Global Lists* pane
2. Click the appropriate tab for the type of list for the entry - *File Deny List* or *File Allow List*. The current list displays for that list type..
3. Depending on which list type displays:
   - Click the **Add New Hash to File Allow List** button to display the *Add New Hash* dialog
   - Click the **Add New Hash to File Deny List** button to display the *Add New Hash* dialog
4. Enter the identifying *SHA HASH* value or Click **Upload File**.
   Notes:
   - The HASH must be in *SHA-1* format. To discover this value, the HASH value

displays on the *Threats* page or it can be determined using a third-party HASH program.

- Wild cards and partial file names can be used to extend the coverage of allow listed files.

5. Click **Submit** to add the file, save and close the dialog or click **Cancel** to abandon the changes and exit the dialog.

Adding a Certificate to a Global List

Add a certificate to the Global List to *allow* or *block* a specific application or product:

1. Click **Administration > Global Lists > Certificate Allow List**
2. Click **Add** to display the Add Thumbprint dialog
3. Specify the *certificate information*:
   - **Display Name** – the name to appear in the *Certificate Allow List*
   - **Thumbprint** – Certificate Thumbprint string
     Note: Use a PowerShell command to retrieve an application certificate, for example:

     ```
     get-authenticodesignature "file_path_here" | select *
     ```

   - **Status** – Select *Allowed* or *Blocked*
   - **Notes** – **(**Optional) informational text
4. Click **Add** to add the certificate thumbprint and close the dialog or click **Cancel.** Cancel abandons the changes and exits the dialog.

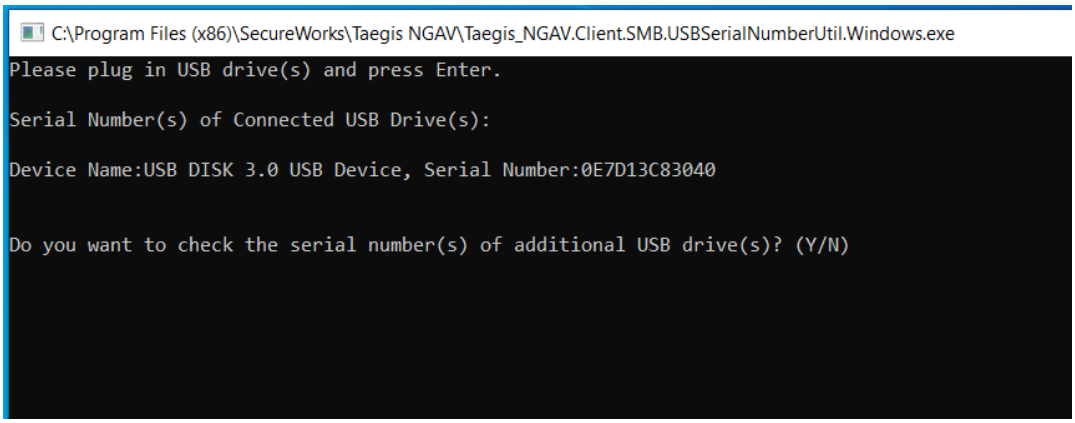
Adding a USB Device to a Global Allow List

To add a new USB Device to a *Global Allow List*:

1. Click **Administration > Global Lists** to display the *Global Lists* pane
2. Click the appropriate tab for the type of list for the entry - *USB Allow List*
3. Click the **Add USB to Allow List** button to display the *Add USB* dialog.
4. Specify the USB Device information or **Click Upload**:
   - **Name** – the name to appear in the *USB Allow List*
   - **Serial Number** – USB Serial Number string
5. Click **Submit** to add the USB to the List or click **Cancel** to abandon the changes and exit the dialog.

Notes:

- To discover *Serial Number*, locate the *Serial Number* on the *Threats* page or find the utility named **Taegis_NGAV.Client.SMB.USBSerialNumberUtil.Windows,** situated at **C:\Program Files (x86)\SecureWorks\Taegis NGAV**.



Industrial OT Certificate Files

Industrial OT includes the ability to upload a .csv certificate file containing multiple entries. Each entry in the file includes four fields:

- *Display Name* (the name to display on the console)
- *Thumbprint* (unique identification value)
- *Status* (allowed or blocked)
- *Notes* (optional text field for notes about the machine)

For example:

```
displayname,thumbprint,status,notes
name0,049334C225143F88FB46DE31FCF5501155EFCB22,allowed,notes0
name1,049334C225143F88FB46DE31FCF5501155EFCB23,allowed,notes1
name2,049334C225143F88FB46DE31FCF5501155EFCB24,blocked,
name3,049334C225143F88FB46DE31FCF5501155EFCB23,allow,notes1
```

Upload Industrial OT Certificate File

Perform the following to upload a certificate file to the console:

1. Navigate **Administration > Certificate Allow List**
2. Click **Add New File**
3. Click **Upload File**

4. Select the `.csv` file to upload
   When the .csv file is selected and parsed, the *Upload Certificate Preview* displays. This preview lists the certificates included within the file.
   The list can be expanded/contracted and filtered, as required.

   The preview provides details about which and how many of the certificates are ready to be added and how many are not ready (*not usable*).
   Note that the file cannot be imported if it contains files marked as *not usable*. Those entries must be corrected before the file can be imported.
   Notes:

   - Any certificate determined to be *not usable* is highlighted in the list, together with the reason it is considered not usable
   - If the file contains entries marked as duplicates, select **Replace Duplicated** to update those values

5. Click **Add** to complete the file importation and add the certificates, or **Cancel** to abandon the changes and close the preview.

Audit Logs Tab

The *Audit Logs* tab displays as part of the *Administration* group in the left pane.

Click **Administration > Audit Logs** to display the *Audit Logs* pane.

The Audit Logs section enables administrators to view/track changes made through the Management Console. The tracked changes include:

- login and logout events
- configuration changes such as creation, deletion, and update

Click the *Audit Logs* tab to display the *Audit Logs* pane (right side). The *Audit Logs* pane displays logging information of various kinds.

The pane includes:

- **Search** field
- Filter area, includes search filters, from left to right:
  - **Resource Type** (drop-down)
  - **Action** type (drop-down)
  - **Date/Time Range** (click launches calendar selector)
- Action buttons to **Expand All** and **Collapse All** log data
- Log entry information area that includes, columns from left to right:
  - **Summary** (of log)
  - **Username**

- **Timestamp** - relative time frame of activity
- **Resource Type** - *User* or *Device*
- **Action** - action types

- Colored Links that launch Device Detail windows

Reporting Tab

The *Reporting* tab displays as part of the *Administration* group in the left pane.

Click **Administration > Reporting** to display the *Reporting* pane.

The *Reporting Pane* enables creation of automated email reports for administrators with updated information about the current Enterprise system. The body of the report is auto-generated and cannot be customized. The information included within a report can include:

- Monthly, Weekly, Daily, or One-Time report time frames
- Specifics about:
  - Devices
  - Groups
  - Total risks
  - Connected status
- Threat activity charts

The *Reporting* pane displays various report items and includes two sub-tabs:

- **Reports** tab (default view) -

  The *Reporting* pane includes:

  - **Search Reports** field
  - **Type** - report filter (*All*, *Daily*, *Weekly*, *Monthly*, *One-time*)
  - **Status** - menu to select *Report Status*: *ALL*, *Enabled*, *Disabled*
  - **Add New Report** button - create a new automated report
  - Report List - columns include, from left to right:
    - *Report Name*
    - *Type*
    - *Recurrence* (period)
    - *Device Groups*
    - *Report Owner*

- **Syslog** tab -
  Displays the *Syslog pane* containing syslog information

  This pane includes *server information*, such as the IP address, port, and protocol as well as the message facility code, severity level, and type. Additionally, *syslog message configuration*, and three action buttons display:

- **Save Settings**
- **Test Syslog**
- **Delete Syslog**

For additional information about syslog message contents, see the SysLog Field & Event Descriptions section.

Creating a New Report

To create a new report:

1. From the *Reporting* pane, locate the **Add New Report** button
2. Choose a report type (*Scheduled Report* or *One-time Report*):
   - **Scheduled Report** -

     Click **Scheduled Report** to display the *New Scheduled Report* dialog.

     The dialog includes the **Add** button and the following:

     - **Report Name**
     - **Device Groups** - drop-down selection list
     - **Type** - report type (*Daily*, *Weekly*, *Monthly*)
     - **Report Recipients** - email address(es), Click (+) to add additional addresses to list
     - **Bypass Login** - this toggle includes a time-sensitive link in the email that bypasses login credentials to view the report(s)
   - **One-Time Report** -

     Click **One-Time Report** to display the *New One-Time Report* dialog.

     The dialog includes the **Run** button and the following:

     - **Report Name**
     - **Device Groups** - drop-down selection list
     - **Time Range** - specify time range. Click to use the calendar picker.
     - **Report Recipients** - email address(es). Click (+) to add additional addresses to list.
3. Select a device group from the drop-down list. Click the chevron to display the list
4. Click the **Run Report** button to create the automated report and exit the dialog

Deployment Tab

The *Deployment* tab is located below the *Administration* group in the left pane. This tab displays the *Deployment* pane containing the specific *Registration Key* and *Server URL*

specifications together with various download links. The links include:

- Installer downloads for the various operating systems and *Registration Keys*
- Send email invitations with instructions for added users
- Download a redistributable package

To view the specific *Registration Key*, *Server URL*, and available downloads:

1. Click the **Deployment** tab to display the *Deployment* pane on the right
   Note: Select a *Device Group* to make options available (clickable).
2. Click to *Select a Device Group* and use the drop-down to select an available device group. This enables the options links.
3. Click **Download a redistributable package** to display the various packages
4. Select the installer for the client platform
5. Click the **Download** button for the appropriate client platform
6. Save the file for later installation
7. For Linux, download the *License* file.
   Note: The License file enables automatic configuration and registration of the client. If this file is not used, the client must be manually configured and registered.
   See Linux Prerequisites for more information.

Two-Factor Authentication

This product supports two-factor (2-step) authentication to enhance secure login to the administrator console. Administrators can enable two-factor authentication for individual users.

This product uses the *Google Authenticator* application for mobile devices. The application supports both Apple iPhones and Android-based phones. Download the appropriate Google Authenticator application from the following links:

- Apple iPhones - Google App Store
- Android phones - Google Playstore

Enable Two-Factor Authentication

To enable two-factor authentication, perform the following:

1. Navigate to the *Console* web page
2. Navigate to **Administration > Users** to display the *User Management* tab
3. Select a *User*
4. Click the **Edit** button on the *User Details* pane to display the *Edit User* dialog
5. Slide the *Two-Factor Authentication* selector to the **On** position

6. Click **Update User** to save the changes and close the dialog

When two-factor authentication is enabled, the first time the enabled user attempts to access the Allow List, the user is presented with the initial screen that explains how to use the authentication.

For logins after the initial login, the login screen displays when the user attempts access.

Note: If two-factor authentication is canceled/removed for the user, the system reverts to a required password only access.

Reset Authentication Token

If it becomes necessary to reset the two-factor authentication token for a user:

1. Navigate to the *Console* web page
2. Navigate **Administration > Users** to display the *User Management* tab
3. Select the *User*
4. Click the **Edit** button on the *User Details* pane to display the *Edit User* dialog
5. Slide the *Two-Factor Authentication Disabled* toggle switch to **off**
6. Slide the *Two-Factor Authentication Disabled* toggle switch back to **on**

   Warning: The two-factor user token is *immediately* revoked when toggled between on and off. The token is destroyed and becomes non-retrievable.
7. Click **Update** to submit the change and close the dialog.
   When the user logs back in, they are prompted to create a new two-factor access token.

Endpoint Clients

This product provides endpoint clients for Windows and Linux operating systems. The endpoint clients normally communicate with the management console, unless they are operating in the offline mode. This product provides real-time malware prevention by intercepting malware before execution. This product performs a static analysis of the malware binary code, and extracts features. The extracted features securely and efficiently query the cloud service to perform malware prediction using patented cognitive algorithms.

Notes:

- A product registration key is required to authenticate with and query the cloud service.
- Enterprise Linux Client is currently supported on Linux Kernels up to 5.15, future releases will expand supported kernel versions.
- *Process Execution* is not supported on versions greater than 5.15.

This section explains how to download, install, and use the application to provide signature-

free malware prevention.

Download an Endpoint Client

To download the client application and registration key, perform the following:

1. Consult your invitation email for the download link
2. Open a supported web browser
3. Navigate to the email invitation supplied link. Click **Download Now** or copy the link into the browser.
4. Click **Deployment** to display the *Downloads* pane

   Note: Select a *Device Group* to make options available (clickable).
5. Click **Download a redistributable package** to display the various packages
6. Select the installer for the client platform.
7. Click the **Download** button for the appropriate client platform.
8. Save the file for later installation.
   Note: Windows client installers are available as both .EXE and .MSI versions.
9. Optionally, use the **Copy** button(s) to save the *Registration Key* or *Server URL* to the clipboard.
   Notes:
   - The *Registration Key* or *Server URL* are required if this product is manually un-registered and needs to be re-registered
   - This product uses a single registration key tied to the instance for all installers. This enables client deployment to images and devices without the requirement to enter individual keys.
   - The client installers and registration key for the clients are available from the downloads page listed in the welcome email.
   - The *Downloads* section includes the installer options for MS Windows and Linux. In the case of Windows, both EXE and MSI installers are available. For additional information about the differences between the two packages, see the installation note.

Verify General Requirements

Verify the following general requirements before beginning installation. Specific installation requirements for each operating system follow.

> **Note**: TaegisNGAV currently supports one license per device per user on persistent environments. This means environments with multiple concurrent users on a single device are not supported. Non persistent environments are also not supported.

- Verify the downloaded installation package file is the latest and it can be accessed.
- Ensure internet connectivity for the install system. This is necessary to download

updates and register with the cloud service.

- *Administrator* rights are required to install this product. When this product is successfully installed, regular, non-administrator users can use it.

Firewall Settings

Taegis NGAV, by default, uses port 443 to communicate with the Management Console. The default port number setting can be changed through the *Web Service URL* option available on both the client and the console settings pages.
Note: The following URL must be accessible (not blocked by a firewall at the customer site):
`https://listener.logz.io:8071`

Client Installation Notes

- It is possible to deploy the client without a GUI. See Silent Client Deployment for additional information.
- **Log files** - Client log files are maintained in the following locations:

  Windows 10:
  `C:\ProgramData\SecureWorks\Taegis_NGAV\Taegis NGAV_smb_service.log`

  `C:\ProgramData\SecureWorks\Taegis_NGAV\Taegis NGAV_smb_gui.log`

- **Linux**
  `/var/log/TaegisNGAV_linux_service.log`

Deploy Client without GUI

It is possible to deploy the client with the `Display User Interface` option set to *Disabled* (without a GUI). The parameter that controls this is the `NOGUI` specification. To deploy a client without the GUI, perform the following:

1. Configure the policy. Set the `Display User Interface` option to *disabled*
2. The `NOGUI` parameter must be set within the *dalicense* file, for example:

   ```
   WebServiceURL Registeration_Key NOGUI=0
   ```

   See Command Usage for additional information.

Windows Client

The following sections describe how to install and use the Windows client.

Windows Client Installation Options

There are two options to install Windows clients. You can either install via the executable download package or install using the PowerShell command line.

Windows Client Requirements

Supported versions of Microsoft Windows include:

- Windows 7 (SP1), 8, 8.1, 10 (1809 and above), Windows 11 (21H2 and above)
  Notes:
  - **Win 8.1** - USB protection is unavailable in Win 8.1
  - **Windows 7 SP1 32bit** - the following are required for successful installation:
    - Windows6.1-KB3063858-x86.msu
    - https://aka.ms/vs/16/release/vc_redist.x86.exe
    - Windows6.1-KB3020369-x86.msu
    - windows6.1-kb3125574-v4-x86_ba1ff5537312561795cc04db0b02fbb0a74b2cbd.msu
    - NDP472-KB4054530-x86-x64-AllOS-ENU.exe
- Windows Server 2012 R2+, 2016, 2019, 2022
  Note: Taegis NGAV on *Windows Server 2012 R2+* requires all Windows updates to be downloaded and installed to function correctly.

  Note: Other versions of Windows are not supported because:

  a) Version has not been tested with this product
  or
  b) Version no longer supported by Microsoft
  or
- This product requires all versions of Windows be updated (via Windows Update) with the latest important updates/fixes from Microsoft.
- Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 require the update corresponding to KB2919355 be installed **before** installing this product. If you have trouble installing KB2919355, run Windows Update to ensure additional update dependencies are met.
  Note: A Windows restart might be required, usually in the case of a driver upgrade. This product prompts for a restart if required.

Visual C++ Requirements

Visual C++ Redistributable 14.26 (or greater) is required, currently *14.26.28720*

During installation, the installer checks for the appropriate version of *Visual C++ Redistributable*. The following two items are queried for verification:

- **Registry Value** -
  `HKLM\SOFTWARE\Microsoft\DevDiv\VC\Servicing\14.0\RuntimeMinimum\Version`

- **Version Number** -

`vcruntime140.dll (System32 or SysWoW64)`

If a newer version than *14.26.28720* is installed either via the registry or the physical file on disk, the installer does not install the Visual C++ Redistributable.

Installation Note: To prepare for deployment, the appropriate packages can be obtained from Microsoft and added to your SCM deployment. Visit the Microsoft latest supported Visual C++ downloads site to download the packages.

Windows Client Hardware Requirements

The Enterprise product is designed to run with minimal hardware needs, because it has a very small footprint.

Officially, the supported minimum hardware requirements match the minimum requirements to run the Windows version you are installing on.

Windows Installer

1. Verify Windows OS version. Windows client requires one of the following Windows versions:
   - Windows 7 (SP1), 8, 8.1, 10 (1809 and above), 11 (21H2 and above)
   - Windows Server 2012 R2+, 2016, 2019, 2022
     Note: Taegis NGAV on *Windows Server 2012 R2+* requires all Windows updates to be downloaded and installed to function correctly.
2. Consult your invitation email for the download link
3. Open a browser
4. Navigate to the downloads page listed in the Secureworks welcome email
5. Click **Deployment** to display the *Downloads pane*
6. Select the installer for the client platform.
7. Click the **Download** button for the appropriate client platform.
8. Save the file for later installation.
   Note: Windows client installers are available as both .EXE and .MSI versions.
9. Optionally, use the **Copy** button(s) to save the *Registration Key* or *Server URL* to the clipboard.

   Notes:
   - The *Registration Key* or *Server URL* are required if this product is manually un-registered and needs to be re-registered.
   - This product uses a single registration key tied to the instance for all installers. This enables client deployment to images and devices without the requirement to enter individual keys.

- The client installers and registration key for the clients are available from the downloads page listed in the welcome email.
- The *Downloads* section includes the installer and Guide options for MS Windows. In the case of Windows, both EXE and MSI installers are available. For additional information about the differences between the two packages, see the installation note.

For additional information see the *dalicense File, Key and Web Server* section.

10. Optionally, use the **Copy** buttons to save the *Registration Key* and *Server URL*.
Note: The key is also required if this product is manually un-registered and must be manually re-registered.

Install Windows Client - Use Installation Package

To install the package:

1. Open the folder containing the application installer
2. **Begin Installation** - Run the downloaded installation package
3. **Accept Agreement** - Navigate through the installation dialog wizard to read and accept the EULA and select configurations.
Note: The final installation step launches the product and prompts for registration (first run only).
4. Verify the installation location and select the *I have read and accept...* option
5. Click **Install** to launch the installation process.

   The wizard scans the system for required software and verifies the system meets the minimum requirements. Missing required software, such as *Visual C++*, is automatically downloaded and installed.

   For each program that requires it:

   a. Agree to the terms.

   b. Click **Install** Successful installation displays a success message

   c. Click **Close** to exit the dialog and continue the installation
6. When the product successfully installs, a success dialog displays:
7. click **Open Now** to complete the installation and display the *Client Activation* dialog
8. Enter the *Web Service URL* and *Registration Key* from your registration
9. Click **Activate** to submit the information.
When this product successfully registers, the *Client Dash Board* displays.

Install Windows Client - Use PowerShell

1. Download an installation package to a local directory

2. Start Windows PowerShell
3. Change into the directory that contains the installation files
4. As a user with *administrator* authority, issue an installation command to install and configure the Windows client on a machine. In the following example, *WEBSERVICEURL* is `tst.us` and the *REGISTRATIONKEY* is `a1b2`.
   Note: substitute your specific values in the command.

```
.\<version>_SecureWorks_EPP.msi WEBSERVICEURL=http:tst.us REGISTRATIONKEY=a1b2
```

Note: This installation can be performed on remote machines by combining this command with an appropriate administration tool.

For additional information about using Powershell commands with installation, see the Install Windows Client - Use PowerShell Commands

When this product successfully installs and registers with the cloud service, the target machine displays as a new device in the *Device* list.

Uninstall or Update Windows Client

Uninstall the Windows Client

To manually uninstall the Windows client:

1. **Open** Windows *Control Panel*
2. **Select** the *Programs* option
3. **Navigate** to *Program and Features*
4. **Search** for *Taegis NGAV* within the list
5. **Uninstall** the client

   Notes:

   - If a password is set, it must be entered to proceed. All attempts, successful or not, are logged to the Administrative Console.
   - Some files remain on the disk after uninstallation. These enable the client to recognize previous policy settings in the case of reinstallation.

Update the Windows Client

To manually update the Windows client:

1. **Open** the *Taegis NGAV GUI*
2. **Navigate** to the *Support* tab
3. **Select** *Update Now*
   Notes:

   - If *Update Now* is not selectable, the client is up-to-date.

- If a password is set, it must be entered to proceed. All attempts, successful or not, are logged to the Administrative Console.

Manually Register the Windows Client

If you received the Client installer from a source other than Management Console download option, or the client has been unregistered, you must register the client and key manually to activate or re-activate Taegis NGAV.

Register in the Client

To manually register the client and associated access key, perform the following:

1. If the client is launched without a completed registration, a dialog displays
2. Click **OK** to close the dialog and display the *Activation* page with field for the *Registration Key* and *Server URL*
3. Enter the *Registration Key* and *Web Server URL* values sent from Secureworks
4. Click the *Activate* button

   Upon successful registration, the *Taegis NGAV Dashboard* displays.

Register Through PowerShell

To manually register the client and associated access key through PowerShell, see the Install Windows Client - Use PowerShell Commands section for information.

The Windows Client Console

The client console enables viewing various information and performing tasks concerning this product and your system. Click the product icon on the task bar to display the client dashboard.

Note: Actions available to the user depend on the *client policy* set in the Management Console.

Windows Client Dashboard - Initial Display

The Windows client dashboard has 2 panes:

- Left tabs pane that selects information to display in the right-hand pane
- Right pane that displays various information depending upon selection.

The **Support** tab displays the icons that specify what to display in the right pane:

- **Current Status** (default)
- **Notifications** - displays alert Information
- **Settings** - displays current protection settings

- **Support** (currently selected) - includes:
  - current *version*
  - *Registration Key*
  - *Web Service URL*
  - **Check Updates** button
  - **Go to Support Portal** button
  - **Unregister** button

Windows Client - Malware Response

When a file is downloaded or copied to the computer, it is automatically scanned to detect potential malware. If a file is perceived to be malware, the detection is announced.

This product performs the following actions on the file:

- intercepts the file
- blocks execution
- moves the file to quarantine

Windows Client - View Malware Information

To view the file information:

1. Click on the pop-up message or click the icon to display the dashboard
2. Click the notification icon

Windows Client - Restore Quarantined File

Files that are mis-identified as malware can be retrieved from the quarantine and unblocked from execution. This process must be used with care because the restore process includes:

- Move the file back to its original directory, if available, see note below
- Unblock its execution
- Add the file to the Allow List so it will **NEVER TRIGGER A RESPONSE** going forward

Note: The restore functionality is not available when *Display End-User Notifications* or *Allow End-User Remediation* is disabled in the Agents policy.

To restore a quarantined file:

1. Click the product icon to display the dashboard
2. Click the notification icon
3. Click the *filename* of the file to restore to display the *Restore* dialog
4. Respond to the *Confirm Restore* dialog
   When the file has successfully restored, a confirmation notification displays in the console.
   Note: In the case where a file is restored but the original path is unavailable, the client restores the file to the *User Desktop* instead.

Linux Client

The following section describes installing, configuring and using the Linux client.

Linux Client Requirements

Supported Distributions

This product supports the following Linux Distributions:

- Debian: 9-11
- RHEL 7-9
- Ubuntu: 18.04, 20.04, 22.04

Notes:

- Enterprise Linux Client is currently supported on Linux Kernels up to 5.15, future releases will expand supported kernel versions.
- *Process Execution* is not supported on versions greater than 5.15.

Linux System Requirements

Shell:
The bash Linux shell must be installed on your Linux distribution

Depending on your Linux distribution:

RHEL

- RedHat package manager (RPM)
- The following packages or libraries installed (via `yum install`, for example):
  - `gcc`
  - `gcc-c++`
  - `make`
  - `kernel-devel`
  - `elfutils-libelf-devel`

Debian (only)

- The following package or library installed (via apt install, for example):
  - `linux-headers-amd64`

Debian/Ubuntu

- `gdebi` or `apt` package manager
- The following packages or libraries installed (via apt install, for example):
  - `gcc`

- `g++`
- `make`
- `build-essential`

Linux Prerequisites

- This product requires one of two files, depending on the installation:
  - A dalicense file for IT deployments is available on the *Deployment* page under the **Download a redistributable package** section. The product looks for this file to reference for setting the configuration file.

    Notes:
    - Only 1 `dalicense` file can be on the disk for successful installation and registration. If more than one file exists, the installation will fail.
    - If the `dalicense` file does not exist on the installation target disk, it is necessary to manually edit the config.json file to enter details. These details are available from the management console. See Linux Client Setup Issues for more information.
  - A `DAOTLICENSE` license file for Linux Industrial OT client deployments.
    Notes:
    - The *Registration Key* and *Server URL* are encrypted within the `DAOTLICENSE` license file for OT deployments
    - Instances of multiple users logged in on a system are not supported on the Industrial OT clients
- *Root* or *sudo* privileges are required to install the service.

Linux Client Options

The options available to install the Linux Client include various installation packages, depending on the Linux distribution.

Notes:

- Enterprise Linux Client is currently supported on Linux Kernels up to 5.15, future releases will expand supported kernel versions
- *Process Execution* is not supported on versions greater than 5.15.

The installation is performed through the various package installers:

- **Debian** package - for Ubuntu 18.04+ and Debian 9+
- **RPM** package - for RHEL 7, 8

Linux File Locations

The following files provide important information:

- **Linux client log file:**
  `/var/log/TaegisNGAV_linux_service.log`

- `config.json` **file:**
  `/etc/TaegisNGAV/config.json`

Install on Linux

The Linux client installation uses distribution-based packages. This means using the appropriate package manager and package for each supported Linux distribution.

Notes:

- Instances of multiple users logged in on a system are not supported on the Industrial client for Linux.
- For versions prior to *3.4.0/3.4.1* on RHEL, it was necessary to install the CentOS package on RHEL to install this product.

  To receive updates for RHEL (on a RHEL machine), uninstall the CentOS package and install the RHEL package.

Install Debian/Ubuntu Packages

Before beginning package installation, verify that the `bash` Linux shell is installed on your system.

Some examples require that `gdebi` be installed. If necessary, install it:

```
$ sudo apt-get install gdebi
```

Perform the following to install Debian/Ubuntu-based packages:

1. **Download the Package:**
   a. Use a web browser to navigate to the *management console*.
   See your welcome email for appropriate URL and credential information.
   b. Log into the management console
   c. Click **Deployment** to display the downloads pane.
   Note: download options are unavailable until a *Device Group* is selected for the linux machine
   d. Select a *Device Group* for the Linux machine
   e. Click to download the appropriate Linux package
   f. When the package download completes, move the package to an appropriate location
2. If this is an IT deployment, **Download the** `dalicense` **file**
   a. On the *Downloads* page, locate the *License File*

b. Click the **Download** button

c. Save the file -
Specify any convenient location, the file will be found during installation

Notes:

- The `dalicense` file is necessary to configure Taegis NGAV. The installation process consults this file to set the configuration file(s).
- If the `dalicense` file does not exist on the installation target disk, it is necessary to manually edit the `config.json` file to enter the details.
- Only 1 `dalicense` file can be on the disk for successful installation and registration. If more than one file exists, the installation will fail.

3. **Install the package**

To install the package, use a suggested package manager such as `gdebi` or `apt`.

For example, issue one of the following commands as a user with *sudo* authority:

```
$ sudo gdebi -n <Path_To_Package.deb>
```
or
```
$ sudo apt install <./Path_To_Package.deb>
```

Notes:

- If the `dalicense` file is present on the disk, the installation references it and the `config.json` configuration file is populated with the appropriate data. If this file is missing, the `config.json` file must be edited to manually add the appropriate data. The required configuration information is available from the management console. See Linux Client Setup Issues for more information.
- Only 1 `dalicense` file can be on the disk for successful installation and registration. If more than one file exists, the installation will fail.

Install RHEL Packages

Before beginning package installation, verify that the *bash* Linux shell is installed on your system.

Perform the following to install RHEL-based packages:

1. **Download Package:**
   a. Use a web browser to navigate to the *management console*.
   See your welcome email for appropriate URL and credential information.
   b. Log into the management console
   c. Click **Deployment** to display the downloads pane.
   Note: download options are unavailable until a *Device Group* is selected for the

Linux machine

d. Select a *Device Group* for the Linux machine

e. Click to download the appropriate Linux package

f. When the package download completes, move the package to an appropriate location

2. **Download `dalicense` file**

a. On the *Downloads* page, locate the *License File*

b. Click the **Download** button

c. Save the file -
Specify any convenient location, the file will be found during installation

The `dalicense` is necessary to configure Taegis NGAV. The installation process consults this file to set the configuration file(s).
Notes:

- If the `dalicense` file does not exist on the installation target disk, it is necessary to manually edit the config file to enter details
- Only 1 `dalicense` file can be on the disk for successful installation and registration. If more than one file exists, the installation will fail.

3. **Install package**
To install the package, use the yum package manager. For example, issue the following command as a user with *sudo* authority:

```
> sudo yum install <Path_To_Package.rpm>
```

Notes:

- If the `dalicense` file is present on disk, the configuration file is populated with the appropriate data extracted from the license file. If this file is missing, the *config* file must be edited to add the appropriate data manually. This information is available from the management console. See Linux Client Setup Issues for more information.
- Only 1 `dalicense` file can be on the disk for successful installation and registration. If more than one file exists, the installation will fail.

Adjust Logging Levels

Before starting the Linux service, consult and, if necessary, adjust the *logging* level. The logging level determines the granularity of logged events. This granularity directly affects the amount of data recorded. To view/adjust the logging values:

1. Navigate to the `/usr/bin` directory
2. Locate the `Nlog` file

3. Open the `Nlog` file to view/edit the logging settings.
   If you edit the file, save the changes and exit to apply the changes.

Linux Client Service Startup and Verification

When the Linux Client service is installed, the daemon is registered with the system and runs as a service. This means it starts automatically.

To verify the status of the service (daemon), issue the following command as a user with sudo authority:

```
$ sudo systemctl status taegisngav.service
```

Note: Because this product runs as a service, there is no visible output to the console because events are written to the service logs.

Stop the Client Service

To halt/stop the Client service, shut down the *Client* service.

Perform the following as a user with sudo authority:

1. Verify the service is running:
   ```
   $ sudo systemctl status taegisngav.service
   ```
2. Stop the service:
   ```
   $ sudo systemctl stop taegisngav.service
   ```
3. Verify the service is stopped:
   ```
   $ sudo ps -A | grep taegisngav
   ```
   The system returns a null answer if the service is stopped.

Disable the Client Service

To disable the Client service from automatically running/restarting, perform the following as a user with `sudo` authority:

```
$ sudo systemctl disable taegisngav.service
```

Note: If the service is disabled it will not start again until it is re-enabled. To re-enable the Client service, issue the following command:

```
$ sudo systemctl enable taegisngav.service
```

Restart the Client Service

To restart the Client service, perform the following as a user with `sudo` authority:

```
$ sudo systemctl restart taegisngav.service
```

Uninstall/Remove Linux Client

To uninstall and remove the Linux Client, perform the following as a user with sudo authority:

1. Verify the client service is stopped. Stop the service if necessary.
2. Use the appropriate package manger to remove the package:
   - For Debian/Ubuntu (.deb) packages:

     ```
     $ sudo dpkg -P <package_name>
     ```

     For additional information on using the dpkg (Debian) package manager, see the Debian dpkg documentation.

   - For RHEL (.rpm) packages:

     ```
     > sudo rpm -e <package_name>
     ```

     For additional information on using the RPM (RedHat) package manager, see the rpm.org documentation.

Update the Linux Client

Issue an appropriate command to update the client:

Debian/Ubuntu example:

Issue an upgrade command as a user with `sudo` authority.

```
$ sudo apt update    # update package index
$ sudo apt list | grep taegisngav
    # return current version and name of package
$ sudo apt install taegisngav
```

RHEL example:

Issue an update command as a user with `sudo` authority.

```
$ sudo yum list | grep taegisngav
    # return current version and name of Taegis NGAV package
$ sudo yum install taegisngav
```

Linux Client Differs from Windows

The Linux Client differs from Windows because there is no client GUI. This product alerts for the Linux client display on the management console.

To observe Linux client alerts on the management console, perform the following:

1. Use a web browser to navigate to the *management console*.
   See your welcome email for appropriate URL and credential information.

2. Log into the management console
3. Click **Devices** tab to display the *Devices* pane that lists all devices connected to that server.

   Note: Select filters to limit the number of devices that display and use the search option to discover a particular system. The filter options include:
   - Device Group(s)
   - Active Connection(s)
   - Device Risk(s)
   - Device Platform(s)
   - Device Version(s)
4. Locate your device
5. Click the device icon to display the *Details* pane.

   The pane includes any files that triggered alerts
6. To take a prescribed action against the file that triggered the alert, click the *File Name*. For additional information, see *Devices - Take Action*.

   Note: Because the Linux client functions as a headless agent, no popups or alert announcements display to the user. This means that if the automatic action is set to *quarantine*, files identified as malicious are automatically quarantined.

Linux Client Setup Issues

Service Does not Start

If the service is disabled it will not run until it is re-enabled. To re-enable the Client service, issue the following command as a user with `sudo` authority:

```
$ sudo systemctl enable taegisngav.service
```

Commands not Executed

If commands do not appear to work as expected, verify the following:

- The `bash` shell is installed
- Commands are run as a user with appropriate authority
- The appropriate package manager is used

Linux - Edit Configuration File

If the `dalicense` is not found on the target system, it is necessary to edit the configuration file to provide important details for the product to function:

1. Open a browser and navigate to the management console URL
2. Log into the management console

3. Navigate to the *Downloads* page
4. Locate and copy the *Registration key* and *Web Service URL* values, at the top of the page
5. As a user with appropriate authority on the client computer, change into the `/usr/bin/` directory
6. Open the `config.json` file for editing
7. Search for the following fields:
   - `Registration Key`
   - `Web Service URL`
8. Enter the *Registration key* and *Web Service URL* values from the management console into the config.json file:

```
Registration Key: "LicenseKeyValue"
Web Service URL: "https://YourWebServiceURL/"
```

9. Save the changes and exit the file
   - **Note**: Only 1 `dalicense` file can be on the disk for successful installation and registration. If more than one file exists, the installation will fail.

Alerts

This product alerts when untrusted applications whose cognitive threat confidence is above 50% attempt to run. This means any program with a score equal or less than 50% is considered to be *benign*.

The *cognitive threat confidence* is a percentage value that describes the likelihood an executable is malicious. This value is based on the calculated prediction result from the cloud-based cognitive and machine learning algorithms pipeline.

The algorithms enable machine learning to identify malware. The algorithms operate from pre-built training models based on example inputs from hundreds of thousands of malware and benign programs to learn how to differentiate both malware and benign programs.

This product enables various actions against identified threats:

- **Threat Trigger Threshold** Any program with a score equal or less than 50% is considered to be *benign*. This means untrusted/unverified programs with a predicted cognitive threat confidence greater than (>) 50% automatically trigger this product following a 30-second alert timeout period.
- **Allow a Threat**
  Select **Allow** to allow an application access to run. This is useful in the case where this product falsely identifies an application as a threat.
  Note: When an application is allowed, this product will no longer alert against that application because it has been added to the *allow* list.

Warning: Only allow trusted or known applications to run. Any application on the *Allow* list is ignored and will not trigger an alert.

False Positives

This section explains how the client can sometimes mistakenly block benign programs or applications that are not malware and guides you through the *teaching* process so you can train the product concerning applications that it alerts on by mistake.

Alerts on Benign Applications/Programs

This product is not signature-based. It is a trained program, using advanced mathematical algorithms against hundreds of thousands of malware and benign files. This enables it to build classifiers that attempt to predictively classify various file executables as either *malicious* or *benign*.

Although the cloud-based cognitive model is incrementally and continuously trained, sometimes the cognitive threat prediction for a benign application brings the file too close to that of a malware range. This causes the product to mistakenly alert on that application.

Common applications like program updaters, .dll files, and other executables can behave or present in potentially malicious ways; for example, they might alter files, touch protected system files, launch scripts, or alter permissions. This means their potential activities can be erroneously determined to be malicious and result in alerts. Because this product is designed to detect and react against such file activities, it will alert on their presence and activity. This alert is an indication that the production is active and on duty. Files known to be non-malicious can be allow listed by certificate to reduce the number of false positives.
See Allow and Deny Lists for more information.

Responding to Alerts on Benign Applications/Programs

To counteract an alert generated by a known benign program, clicking the alert dialog enables selecting the appropriate action for that alert. The file can be added to the allow list that designates the program as *benign* for Taegis NGAV. Because this product learns this particular program is benign, it no longer alerts on the program.

To respond to a particular alert for action:

1. Double-click the alert(s) associated with the file to be designated as *benign* and display the *Alert Details* pane
2. Click the **Action** button (top right) to display the *Take Action* drop-down dialog
3. Select the appropriate action from the drop-down options:
    - **Remote Remediate** - Choose to add the file(s) to the allow list so they are considered benign and no longer considered potential malware.
    - **Remote Restore** - Restore the quarantined file(s) to their original directory location.

Note: If a file is moved from an allow list to a deny list, the status for that file changes to a *Remediated* status.

- **External Remediation** - mark the file(s) as already handled by an external process

4. **Clear Selection**
   Select this option to clear the selected files and close the dialog.

Incident Investigation and Response

This product provides various tools and mechanisms for the administrator to investigate and respond to alerts and potential incidents.

The alerts generated by this product are deeply dependent on the fine tuning and testing that is performed during adoption and rollout across the enterprise. See Best Practice Recommendations for additional information.

This product provides logging and various statistics, identification, and information about files/processes that cause alerts. Analyzing the available data enables administrators to make informed response decisions and respond accordingly. See the following sections for additional information:

- Alerts Tab
- Devices Tab
- Audit Logs Tab

External Investigation Tools

In addition to the data this product provides concerning alerts, various external tools exist to assist in determining whether alerted files or processes are truly malicious. For example, the Google VirusTotal (https://www.virustotal.com/) tool enables administrators to submit suspicious files. VirusTotal analyzes and ranks the submitted files in terms of their potential as malware. The results of this analysis can inform the administrator decision to classify the file or process as either *malicious* (block/deny list) or *benign* (allow/allow list). See Allow and Deny Lists for additional information.

Investigative and Response Workflow

The investigative workflow for the Administrator consists of various tasks:

1. Receive the console alert
2. Consult the alert information on the *Alert Details* page to determine what data is provided and what action has been taken automatically. If necessary, specify immediate action though *Remote Remediation*
3. If necessary, perform a deep dive analysis on the threat to verify or classify it's severity
4. Verify that the action taken is appropriate. If necessary, click the T**ake Action** button on the *Alert Details* page to reverse it through *Remote Restore* and or *Remote Remediate*

5. Adjust allow and deny lists and automatic action as necessary to fine-tune the product alerts. See the Allow and Deny Lists section for additional information.

Incident Response

As part of responding to incidents/alerts, this product includes the ability for administrators to perform various response actions from the console, including *Remote Remediation*.

Remote Remediation Response

Incident responses (*Remote Remediation*) originating at the console can be tailored in granularity. Administrators can target responses at individual files, or large groups that can include every instance of a file across the network or device group. Additionally, responses can be targeted at an individual client machine, or all the machines within a network or device group.

Remote Remediate enables various options depending on the target:

- Device specific actions are quarantine of a malicious file or termination of a malicious process
- Global action is to add the SHA1 identifier for the file or process to the global deny list so it is identified as malicious and apply the information to all occurrences and/or use the generated certificate thumbprint to identify each file

  Action Failed Message

  Any downloaded threat that is moved to another location results in 2 occurrences of the threat. For example, moving the threat from the *Downloads* folder to the *Desktop* folder. If the *Remote Remediate* action is applied to the threat, the process is successful for the *Desktop* location but a failure for the *Downloads* location. This is because the file was moved from the original location and the remediation action could not be completed. This generates an **Action Failed** message that can safely be ignored. The threat is successfully mitigated.

Misidentification and Accidental Quarantine

This product marks and reports files identified as malicious and also moves them from their location into a special quarantine folder. This can be a source of problems for clients that cannot locate their file(s) due to the relocation. This means it is important that administrators can gracefully recover from accidental quarantine. Accidental quarantine can result from mis-identification and marking a file as malicious. The console provides administrators a mechanism to reclassify accidentally misclassified files. This mechanism is called *Remote Restoration*. This restoration changes the file classification to *benign* (*not* malicious) and restores it to its original location on the client machine(s).

Remote Restore can be performed with the **Take Action** button on the *Alert Details* page.

The various options depend on the target for the action:

- Device specific action is to restore the file. This means remove the file from quarantine and move it back to the original location.
- Global action is to add the SHA1 identifier for the file or process to the global allow list so it is considered benign and apply the information to all occurrences of the file or process.

  Action Failed Message

  Any threat that is moved to another location before it is accidentally quarantined and then restored can result in 2 occurrences of a file restoration. For example, moving a file from the *Downloads* folder to the *Desktop* folder and then (accidentally) quarantining the file. If the *Remote Restore* action is applied to the file, the process is successful for the *Desktop* location but a failure for the *Downloads* location. This is because the file was moved from the original location and the restoration action could not be completed. This generates an **Action Failed** message that can safely be ignored. Verify the file is correctly restored.

Files Remediated Outside Taegis NGAV

For the occasion when a potentially malicious file is already handled by the administrator or through a method outside of Taegis NGAV, the console provides the *External Remediation* option. This option enables the administrator to (re)classify a threat as resolved by some action external to Taegis NGAV. This action rescinds the alert as *Action Taken* and removes the active alert.

Using this product with Other Antivirus Products

Due to potential performance impacts and potential conflicts, it is not generally recommended to run multiple antivirus products simultaneously. If it becomes necessary to run another antivirus program in addition to Taegis NGAV, it might be necessary to add Taegis NGAV to the allow list for that antivirus program. This section provides generic instructions to add several common antivirus products to the Allow list. For products not listed in this section, consult the manufacturer documentation.

Directories/Folders to Allow List

To enable this product to work with other virus products, recursively allow the following folders/directories in the *Allow* list:

- Windows Clients (32-bit and 64-bit):
  - `C:\Program Files (x86)\SecureWorks\Taegis NGAV\*`
  - `C:\ProgramData\SecureWorks\Taegis_NGAV\system\quarantine\*`

Microsoft Windows Defender

Microsoft includes the Windows Defender antivirus program. If Windows Defender alerts on this product, allow list this product with Windows Defender. For example, on Windows 10:

1. Open *Windows Defender Security Center* from the *Start* menu
2. Click **Manage settings** under *Virus & Threat Protection Settings*
3. Scroll down to **Exclusions**
4. Click the **Add or remove exclusions**
5. Click the **Add an exclusion** button to display a drop-down list
6. Select **Folder**
7. Continue with the on-screen directions to add the new folder exclusion. Add a folder exclusion for each of the product folders listed in Windows Clients (32-bit and 64-bit)

   Note: To remove an exclusion, perform the same procedure and in the selection step, select the item to remove and click the Remove button.

McAfee Antivirus

McAfee for Windows Client

To exclude the files and application of this product:

1. Open McAfee Security suite
2. Click **Real-Time Scanning: On**
3. Click **Excluded Files**
4. Click **Add File**
5. Browse to and select the files located in the directories to exclude this product from scans. See Directories/Folders to Allow List for a list of folders.
   Note: At this time McAfee does not support folder exclusion from real-time scans.

Symantec Antivirus

For Enterprise customers, the *Symantec Software White-Listing* program offers an opportunity to reduce the possibility of false positives by adding your software to an allow list that Symantec maintains of known good software. See the Symantec White List submission site for additional information.

Enterprise - Use the Endpoint Protection Management Console (SEPMC)

SEPMC - Create Rule for this product

To allow this product to communicate and run on Symantec, perform the following:

1. Log in to the Symantec Endpoint Protection Management Console
2. On the Left side pane, select **Policies**
3. In the Center pane, select **Firewall**
4. Select and double-click the policy to modify

5. On the left, select **Rules**
6. At the bottom, click **Add Rule**
7. Click the **Next** button three times to display the *Define and Application* page
8. On the *Define an Application* page enter the full path to the product executable file, for example C:\Program Files\ABCDE*
9. Click the **Next**
10. Click **Finish**
11. Highlight the new rule for this product
12. click the **Move Up** button to move the rule to the top of the list

SEPMC - Exclude the Product Folders

Symantec Endpoint Protection Manager can be configured to allow the product directories:

1. In Symantec console, navigate *Policies Tab* > *Exceptions*
2. Right-click in the blank space within the right pane
3. Click **Add**
4. Enter a policy name, for example `MyPolicyName`
5. Navigate the drop-down selection: *Add Button* > *Windows Exceptions* > *Files or Folders*
6. In the *Folder Options* field enter the path for the product on the client machines, See Directories/Folders to Allow for a list of folders.
7. Test the policy and assign to appropriate groups

Symantec Client

Symantec Windows Client - Exclude Folder

To exclude the product folders from scans on Windows clients, repeat the following procedure for each folder:

1. On the *Exceptions Policy* page, click **Exceptions**
2. Under *Exceptions*, click *Add* > *Windows Exceptions* > *Folder*
3. In the *Prefix variable* drop-down box, select **NONE** to enter the absolute path to the product folder.
4. In the Folder text box, type the name of the folder. See Directories/Folders to Allow for a list of folders.

   Note: A path must be denoted with a backward slash
5. Under *Specify the type of scan that excludes this folder*, select **All** from the types of scan

(*Security Risk*, *SONAR*, *Application control*, or *All*).

6. Click **OK**

Taegis NGAV Support

The following resources enable you to research issues, create support tickets, or contact the Taegis NGAV support team:

- Visit the Taegis NGAV support portal to create a support ticket and log your issue at https://ctpx.secureworks.com/
- Send email to the support team at product_support@secureworks.com
- Contact your Taegis NGAV support team by phone: *855-525-7497*

Secureworks Privacy Policy and EULA

- The Secureworks Privacy Policy is located at *https://www.secureworks.com/~/media/Files/Corporate/privacy_saas.ashx*
- The product EULA is located at: *https://www.secureworks.com/~/media/Files/Corporate/privacy_saas.ashx*

Reference

Minimum Hardware Requirements

The following section describes the minimum hardware requirements for the various supported operating systems.

Windows Requirements

The following requirements must be met to successfully run the Windows client.

Windows Minimum OS Requirements

Supported Windows versions:

- Windows 7 SP1
- Windows 8.1
- Windows 10 1903 and above
- Windows 11

Windows Minimum Hardware Requirements

- **RAM**: Minimum *2 GB* reserved for client operation
- **Hard Drive Space**: *1GB* reserved for client operation
- **Processor**: Minimum *two-core* processor required

Linux Requirements

The following requirements must be met to successfully run the Linux client.

Linux Minimum OS Requirements

Supported Linux versions:

- Debian: 9-11
- RHEL: 7-9
- Ubuntu: 18.04, 20.04, 22.04

Linux Minimum Hardware Requirements

- **RAM**: Minimum *2 GB* reserved for client operation
- **Hard Drive Space**: *1GB* reserved for client operation
  Processor: Minimum *two-core* processor required

Supported File Types

The SDK currently supports the following file types:

File Types	Examples
Archives	.archive (macOS) TAR, .gz (gzip), .7z (7-Zip), .rar, .bz2, .zip
Executables	PE32/PE32+ .acm, .ax, .cpl, .dll, .drv, .efo, .exe, .mui, .ocx, .pyd, .scr, .sys, .tsp, Mach-o (32bit and 64bit x86)
Legacy Documents	.doc, .dot, .pot, .pps, .ppt, .wdk, .xlm, .xls, .xlt
Linux	.elf
macOS	.app, .dmg, .macho, .pkg
OpenXML Documents	.docb, .docm, .docx, .dotm, .dotx, .odp, .ods, .odt, .potm, .potx, .ppam, .ppsm, .ppsx, .pptm, .pptx, .sldm, .sldx, .xlsm,

	.xlsx, .xltm, .xltx,
PowerShell	.cdxml, .ps1xml, .psd1, .psrc, .pssc
VBScript	.asp , .hta, .htm, .html .vbe, .vbs, .wsc, .wsf

Notes on Email Attached Virus or Compressed Files

This product does not necessarily alert on email attached threats until they are downloaded, or in the case of compressed files, extracted. This economy of action enhances efficiency in terms of processing effort.

Note that:

1. Although this product does not usually alert on text files, an identified potentially malicious file is blocked when dragged, dropped or executed.
2. Because a compressed file must be extracted (unzipped, untarred, unpacked, etc.) before it can be executed, the file is not scanned until downloaded and extracted. This product immediately analyzes the extracted contents and alerts if appropriate.

SysLog Field & Event Descriptions

The following section shows an example syslog output and provides descriptions for the syslog fields and events.

Example syslog output

The following shows an example syslog output:

```
2021.6.0
New Device Registered
Message: Event:"Register" Account:"00000000-0000-0000-0000-000000000001" \
Partner:"111" DeviceName:"TCT-V0-1611" DeviceUsername:"jwick" \
DeviceGuid:"3e0a3f69-ce4d-4302-9606-8b41ba2f8746" \
DeviceOS:"Microsoft Windows 10 Pro 10.0.15063" DeviceAgent:"1.0.0.0" \
DeviceIP:"192.168.22.29" DeviceIPV4:"127.0.0.1" DeviceMac:"54AB3AC568D1" \
DeviceFqdn:"TCT-V0-1611.local" \
DeviceGroup:"Engineering Team - Windows" \
DevicePolicy:"IT Corporate Desktop Policy" \
DeviceCreated:"2021-06-23T12:26:23.365804+00:00" \
DeviceScore:"" Active:"True"
The sysLog fields and events are described below.
```

Syslog Field Descriptions

- **Account** -
  Description: Account identification number, with the form of
  8 digits-4 digits-4 digits-4 digits-12 digits
  Example: "00000000-0000-0000-0000-000000000001"

- **ActionTaken** -
  Description: The action taken against the file (could be QUARANTINED, BLOCKED or an empty string indicating no action)
  Example: "QUARANTINED"

- **AlertGuid** -
  Description: GUID identification of the alert (unique per alert)
  Example: "6aa77570-2f72-412a-9c85-bd1c99573860"

- **AlertType** -
  Description: Classification assigned to the alert (ABNORMAL, SUSPICIOUS and MALICIOUS - the later being the most confident of a malicious payload)
  Example: "MALICIOUS" Score:"1.0"
  Note: This value has a range from *0 to 1* where *1.0* indicates the highest risk. This value is converted to a percentage in the management console so the values in the GUI range from 0 to 100%.

- **AlertURL** -
  Description: Contains the URL to the Alert (if applicable), where the number (in the the following example) *222* is the *Alert ID*.
  Example: "https://ngav.taegis.secureworks.com/alerts/222"

- **DACloud** -
  Description: Connection status with the management console at the time of detection
  Example: "Connected"

- **DetectionMethod** -
  Description: Describes what type of detection was used
  Example: "FILE"

  Syslog Detection Type Mappings

  - BATCH_SCAN: 'Scan'

- DIRECTORY: 'Scan'
- FILE: 'Scan'
- FILEWATCHER: 'File'
- FULL_SYSTEM: 'Scan'
- OFFLINE_SCAN: 'Scan'
- PROCESSWATCHER: 'Process Execution'
- RTFM: 'Real-Time File Monitoring'

- **DeviceAgent** -
  Description: Version of the agent on the device
  Example: "1.0.0.0"

- **DeviceCreated** -
  Description: Date the device was originally created in the console
  Example: "2021-06-23T12:26:23.837786+00:00"

- **DeviceFqdn** -
  Description: Fully qualified domain name of the device
  Example: "FRT-V0-1611.mynewtech.local"

- **DeviceGroup** -
  Description: The device group the device is assigned to in the management console
  Example: "Engineering Team – Windows"

- **DeviceGuid** -
  Description: The device GUID ID information
  Example: "3e0a3f69-ce4d-nnnn-9606-8b41bxxxxxxx"
- **DeviceIP** -
  Description: IP address of the device
  Example: "192.168.nnn.nnn"

- **DeviceIPV4** -
  Description: IP address in IP4 notation of the device
  Example: "127.0.0.1"

- **DeviceMac** -
  Description: MAC address of the device
  Example: "54AB3AC5xxxx"

- **DeviceName** -
  Description: Host Name assigned to the device
  Example: "MyPC-V0-1611"

- **DeviceOS** -
  Description: Operating System information of the device, including version
  Example: "Microsoft Windows 10 Pro 10.0.15063"

- **DevicePolicy** -
  Description: If assigned, identifies the policy group the device is assigned to
  Example: "IT Corporate Desktop Policy"

- **DeviceScore** -
  Description: Measure of protection for the device. The range is *0* to *100*.
  A score of *0* means unprotected and absolutely at risk.
  A score of *100* means completely protected, not at risk.
  This means a higher score is better.
  Example: "70"

- **Active** -
  Description: Describes the current status of the device (True/False - indicating the protection status)
  Example: "True"

- **DeviceUsername** -
  Description: User name logged into the device
  Example: "jwick"

- **Event** -
  Description: Type of triggering event
  Example: "Detect"

- **EventTime** -
  Description: Time of the event trigger
  Example: "2021-06-23T12:38:18.002387+00:00"

- **FileCreated** -
  Description: Time file was created
  Example: FileCreated:"2017-08-08T12:16:01.766000+00:00"

- **FileModified** -
  Description: Time file was last modified
  Example: FileModified:"2017-08-08T05:45:25.496000+00:00"

- **FileName** -
  Description: File name that triggered the event
  Example: "P30.exe"

- **FilePath** -
  Description: Path to the file that triggered the event
  Example: "C:\temp\P30.exe"

- **FileSize** -
  Description: File size of file that triggered event
  Example: "10"

- **FileType** -
  Description: Type of file that triggered the event
  Example: "win32 exe"

- **First** -
  Description: Time and date the file that triggered the event was first detected
  Example: "2017-05-12T00:40:18.732000+00:00"

- **Network** -
  Description: Status of the network connectivity of the device at the time of the event
  Example: "Connected"

- **Partner** -
  Description: Partner identification value, if any
  Example: "Partner ID

- **RunningApps** -
  Description: List of applications running on the device at the time of the event
  Example: "Chrome.exe"

- **SHA1** -
  Description: SHA1 value of file that triggered the event Example:
  "DECB41EB5E523580EAC421570A79732FB9658DC6"

- **ThreatCategory** -
  Description: Category that the model classified the malware as being most like
  Example: "Generic"

- **ThreatLevel** -
  Description: The severity level or seriousness of the triggered event
  Example: "2"

- **ThreatName** -
  Description: Displays the threat name that was detected, if known
  Example: "Generic"

Syslog Events Descriptions

- **Agent Interruption** -
  Description: This announces that the agent's protection was interrupted
  Example (truncated): Message: Event:"Agent_interruption" Account:"...-12345" Partner:"111"…

- **Device Login** -
  Description: This occurs when the device checks in with the management console
  Example (truncated): Message: Event:"Login" Account:"...-12345" Partner:"111"…

- **Device Unregister** -
  Description: Message to communicate removal (de-registration) of a device from the console
  Example (truncated): Message: Event:"Unregister" Account:"...-12345" Partner:"111"…

- **Network Process Execution Attempted** (Requires Enabled Network File Control) -
  Description: Announces a detected attempt to run a suspect process through from a network share
  Example (truncated): Message: Event:"Network_file_control" Account:"...-12345" Partner:"111"…

- **New Application Event** (Requires Application Control to be Enabled) -
  Description: Announces a detected attempt to run a new suspect application
  Example (truncated): Message: Event:"New_application" Account:"...-12345" Partner:"111"…

- **New Device Registered** -
  Description:Announces addition (registration) of a device with the console
  Example (truncated): Message: Event:"Register"…

- **New USB Device Detected** -
  Description: Announces detection of a new USB device (Mass Storage devices only)
  Example (truncated): Message: Event:"New_usb" Account:"...-12345" Partner:"111"…

- **Policy Exception** -
  Description: Announces a policy exception detection by the end user
  Example (truncated): Message: Event:"Policy_exception" Account:"...-12345" Partner:"111"…

- **Script Event** (Requires Enabled Script Control) -
  Description: Announces a new script triggered event detection such as PowerShell, CSript or WScript
  Example (truncated): Message: Event:"New_script" Account:"...-12345" Partner:"111"…

- **Threat Action** (End User Remediation - Restore or Quarantine an alert) -
  Description: Announces a new threat action event initiated by the logged in user on the device

Example (truncated): Message: Event:"Action"…

- **Threat Detect** -
  Description: Announces a new threat event detection occurred, no remediation was performed
  Example (truncated): Message: Event:"Detect"…

- **Threat Prevent** -
  Description: Announces a new threat prevention triggered event, no additional remediation is required

  Example (truncated): Message: Event:"Prevent"…

Alert Timestamps

Timestamps for Alerts are based on alert detection times relative to the local time of the logged in Management Console user.

Because *Epoch Time* is used to show the absolute time an event occurred, this means the Alert timestamp will always be aligned to the timezone of the Management Console user. A console user logged in from a different timezone than the detected alert will see the threat detection time based on their local console time.

Best Practice Recommendations

To enhance your results with this product, consider the following best practice recommendations.

Policy Best Practices

- **Limit Initial Deployment**

  Before deploying this product across an organization, run a limited test pilot deployment.

- **Adjust Policy**

  Deploy this product initially to a small group of systems. Monitor the management console for alerts on applications or processes that are considered safe. Adjust the policy (Allow List) to enable these applications/processes to run on all systems without alerting.

- **Executable Detection First**

During the initial deployment, limit the product first to *executable detection only*. This enables identification and quarantine for malicious or abnormal processes and files that exist within your environment. Tighten protection policy in a phased manner to eventually include *document attack* vectors.

Group Best Practices

Establish initial device groups to organize devices for *pilot*, *policy*, and *user-role granularity* within the organization.

- **Policy Groups**

  Establish pilot groups to manage the initial rollout and test new agent updates

- **Device Differentiation**

  Establish policy based groups to differentiate between different types of devices, such as *workstations* and *servers*. This can include devices with exclusions.

- **Novel Groups/Roles**

  Various identifiers, limited only by imagination, can define groups. For example:

  - User-Roles like departmental association such as *sales*, *marketing*, or *engineering*
  - User locations such as *office number*, *geographical* or *floor* location

---

User Roles

This product supports several user roles, each with different levels of access, abilities and permissions. These user roles are defined within the management console:

- Administrator
- Manager
- Auditor

Administrator -

The *Administrator* role includes global permissions and complete access to product logs, tools and data. The Administrator has extensive modification powers. The *Administrator* permissions include:

- add, edit, or remove users
- assign/remove users to/from groups
- add/remove devices
- create, add/remove policies
- permanently delete users, devices, policies, groups from a site

Manager -

The *Manager* role includes permissions within any group they manage and partial access to product logs, tools, and data. The Group Manager has limited modification powers. Note that each device and device group requires a group manager. The Group Manager is displayed in the device data. The *Group Manager* permissions include:

- assign users to view their groups
- add/include other group managers with the group
- add/remove devices
- edit device and group names (within assigned group)

Notes:

- If a *group* is assigned to a user, that user becomes a group manager for that group with associated permission changes.
- There can be multiple group managers for a particular group.

Auditor -

The *Auditor* role includes limited permissions and ability to modify. Note that an Auditor must be assigned to a group by an Administrator or Group Manager, an Auditor cannot self-assign/join. The *Auditor* permissions include:

- view own profile
- view own system information, including logs, historical data, and actions
- modify own password
- quarantine or waive threat actions within assigned group

Policy Settings

The following sections explain the various policies, types and settings.

User Setting

Lock User -

- Default Value: On
- Recommended Value: **ON**
- Description: Prevents users from making changes on their client.

OS Protection Settings

Process Execution Monitoring & Control -

- Supported OS: Windows and Linux
- Default Value: On
- Recommended Value: **On**
- Description: Values = On/Off. Toggle run-time process execution activity monitoring. Policy settings are enforced on abnormal or malicious process activity.

Scanning of Network Share Processes -

- Supported OS: Windows
- Default Value: On
- Recommended Value: **On**
- Description: Values = On/Off. Toggle scanning of network share processes. When enabled, all network share Windows executables are blocked from execution. To exclude certain paths, add *Allow List* folders. Policy settings are enforced on abnormal or malicious process activity.

Application Control -

- Supported OS: Windows
- Default Value: Disabled
- Recommended Value: no recommended value
- Description: Values = Enabled/Disabled.
  Provides explicit control over running processes.
  Note: before enabling this feature, ensure all applications allowed to run are listed within the *Global Allow List* and *Certificate Allow List*.

Script Control -

- Supported OS: Windows & Linux
- Default Value: Disabled
- Recommended Value: no recommended value
- Description: Values = Enabled/Disabled
  - Windows:
    Provides flexibility to allow (*enable*) or block (*disable*) scripting processes on Windows such as `PowerShell` or `Wscript`.
    - When Script Control is *enabled*, fine grain control of script types is selectable. This means an administrator can individually block or allow scripts by file type.
    - When Script control is *disabled*, no script types are disabled. This means Taegis NGAV will not automatically allow or block scripts by file type.
    - If script types are allowed or Script Control is *disabled*, Taegis NGAV still scans scripts before allowing them to run.
  - Linux:
    Provides flexibility to allow (*enable*) or block (*disable*) scripting processes on Linux such as `Bash` or `Shell`.

USB Control -

- Supported OS: Windows
- Default Value: Disabled

- Recommended Value: Per user requirement
- Description: Values = Enable/Disable

  USB Control provides explicit control over USB Storage devices being able to be connected to endpoints. Use the Management Console to either *Allow* or *Block* a USB device when it has been detected.
  Taegis NGAV uses a *serial number* to uniquely identify USB devices. If the client fails to uniquely identify a USB device, that USB device is blocked and a notification is sent to the server. The most common reason for failing to uniquely identify a USB device is the device does not correctly report information to the operating system that is required by the USB specification.

Real-Time File Monitoring -

- Supported OS: Windows and Linux
- Default Value: On
- Recommended Value: **ON**
- Description: Values = On/Off. Toggle real-time file activity monitoring. Policy settings are enforced on abnormal or malicious files.

Personal Firewall -

- Supported OS: Windows
- Default Value: Enabled
- Recommended Value: **ON**
- Description: Values = On/Off. Monitor Trusted Software Verifications connections performed by applications and provides advanced network activity control to protect against hacking and malware.

User Access Control (UAC) -

- Supported OS: Windows
- Default Value: Enabled
- Recommended Value: **ON**
- Description: Values = On/Off. Toggle script execution activity monitoring in system memory at run-time. Policy settings are enforced on abnormal or malicious script activity.

Trusted Software Verification -

- Supported OS: Windows
- Default Value: Enabled
- Recommended Value: **ON**
- Description: Values = On/Off. Toggle validating the authenticity of new applications and

provides notifications when applications cannot be verified. This verification protects against malicious websites and malware downloaded from those sites.

Credential Guard -

- Supported OS: Windows
- Default Value: Enabled
- Recommended Value: **ON**
- Description: Values = On/Off. Toggle protection for sensitive documents stored within a virtual container that is only accessible by privileged system software.

Autonomous Restore Based Cloud Intelligence -

- Supported OS: Windows and Linux
- Default Value:
- Recommended Value: **ON**
- Description: Values = On/Off. Toggle Automatic restoration and Allow listing of files with a verified clean file reputation. This reputation is based on product cloud intelligence and file reputation services.

Agent Settings

Display User Interface -

- Default Value: On
- Recommended Value: Disabled
- Description: Values = On/Off. Toggle the User Interface visibility (GUI, System Tray Icon, Shortcuts). Disable for silent operation.

Display User Notifications -

- Default Value: On
- Recommended Value: Disabled
- Description: Values = On/Off. Toggle User alert notifications. Disable for silent operation.

Allow End User Remediation -

- Default Value: On
- Recommended Value: Enabled
- Description: Allows or denies the end user from being able to take action on the endpoint (restoring a file or quarantining a previously restored file)

Agent Administrator Password -

- Default Value: On
- Recommended Value: Enabled

- Description: The Agent Administrator password provides the ability to prevent an

unauthorized user from uninstalling the agent

Automatic Executable Sample Upload -

- Default Value: On
- Recommended Value: None
- Description: Values = On/Off. Toggle uploads. When an alert is generated, executable samples are automatically uploaded to the product. The files can be downloaded to the management console. Default sample retention time is 30 days.

Auto-Delete Quarantined Files -

- Default Value: 14 Days
- Recommended Value: None
- Description: Values = On/Off. Toggle automatic quarantined file deletion. The time to retain the files is configurable. If Auto-Delete is disabled, files must be manually deleted.

Automatic Client Update -

- Disabling this will cause the Client Updates to not occur automatically and will require manual work to update the software with an RMM tool or manually uninstalling and reinstalling the client.

Client Architecture Optimization Settings-

- Supported OS: Windows, Linux
- Default Value: On
- Recommended Value: On
- Description: Values = On/Off. Client architecture optimization enables loading only platform-relevant Machine Learning models. This improves system performance by lowering memory requirements.

Alert Actions Defined

This product provides various actions to respond to alerts. The possible alert actions include the following:

Alert Action	Description
Remote Remediate -	Remotely remediate an identified threat - actions include: • *Device Specific Actions*: **Quarantine** (file) or **Terminate** (execution) • *Global Actions:* **Add SHA1 to Global Deny List** and (optionally) **Apply to All Occurrences**
Remote Restore -	Restores the alerted file to its original directory and adds its

	information to the global allow list to mark it *benign*. **Note:** Any downloaded threat that is moved to another location results in 2 occurrences of the threat. For example, moving the threat from the *Downloads* folder to the *Desktop* folder. If the *Remote Remediate* action is applied to the threat, the process is successful for the *Desktop* location but a failure for the *Downloads* location. This is because the file was moved from the original location and the remediation action could not be completed. This generates an **Action Failed** message that can safely be ignored.
External Remediation -	This action clears the alert and marks the file as mediated through a means external to this application.

Windows Command Line Installation Parameters

The Windows PowerShell command line installation parameters for the Taegis NGAV Windows client:

- REGISTRATIONKEY -
  - Value - <Installation Token>
  - Description - Auto input the Installation Token

- WEBSERVICEURL -
  - Value - <Web Service URL>
  - Description - Web Service URL

- NOGUI -
  - Value - <0 or 1>
  - Description - Enables installing the Taegis NGAV package without the Graphical User Interface
    Notes:
    - Policy settings must be configured to ensure successful operation without a user interface
    - Turn off *Display User Interface* from the policy settings
    - The `NOGUI` parameter ensures Taegis NGAV is installed with the *Graphical User Interface* disabled
- q/ -
  - Value – none
  - Description - Enables installing the package in *quiet mode*; no user interaction requested/required

Command Usage

Note: commands that are displayed below as broken across multiple lines should be issued as a single command:

```
.\<version>_SecureWorks_EPP.msi WEBSERVICEURL=http:<YourWebServerUrl>
REGISTRATIONKEY=<YourRegKey> NOGUI=<0 or 1> /q
```