CONNECTWISE

Absolute Resilience for ConnectWise

User Guide

Version 1.0

Absolute Resilience for ConnectWise – User Guide

Table of Contents

Absolute Resilience for ConnectWise – User Guide

Overview

Integrate Absolute® Secure Endpoint with the Asio™ platform to enable uncompromised monitoring of your endpoints and near real-time remediation of security breaches at the source.

This powerful integration allows you to manage device and data security, even if a device is off the network or in the hands of an unauthorized user. The persistent connection between Absolute's secure and patented agent and the Absolute Monitoring Center ensures you have protected access to up-to-date information about your entire device inventory. You can also track devices and initiate data and device security operations for the purposes of enforcing compliance policies, identifying at-risk computers, and taking preemptive and reactive measures if a security incident occurs.

Prerequisites

Before setting up the integration, you'll need an Absolute Secure Endpoint account configured specifically for Managed Service Providers (MSPs). You can register for this type of account by completing Absolute's registration form.

You can activate and subscribe to one or more Absolute product modules, depending on the needs of your client environments. For more information on the modules available within the integration and their pricing, see Absolute's website.

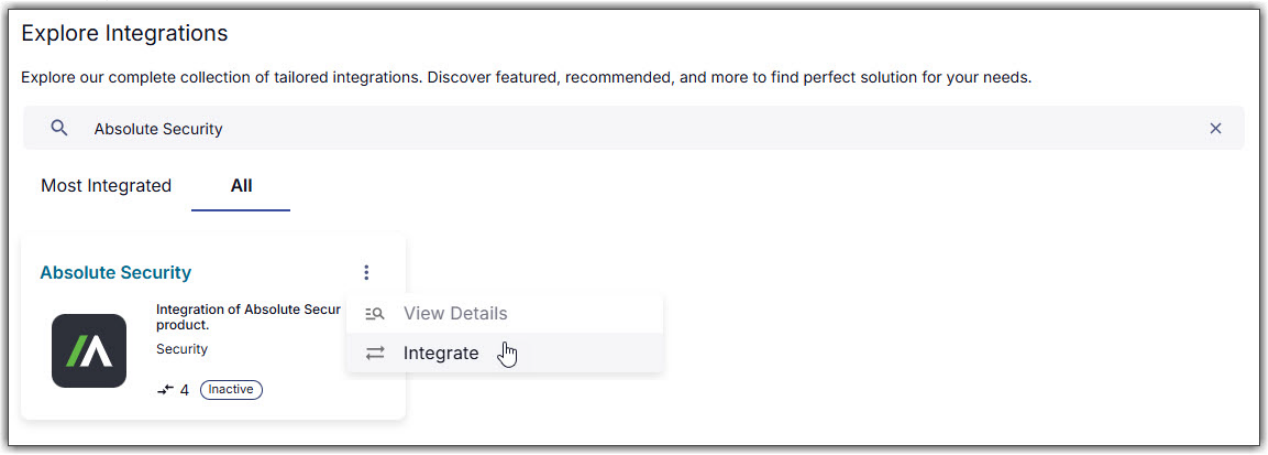
Setting up the integration

To successfully integrate Absolute Secure Endpoint with the Asio platform, you'll need to:

- Generate client credentials in the Asio platform
- Enable the integration in Secure Endpoint
- Generate an API token in Secure Endpoint
- Enable the integration in the Asio platform
- Map your Asio sites to Absolute Security

Generating client credentials in the Asio platform

1. Log in to the Asio platform. For more information, see the Asio platform documentation.
2. Navigate to **Integrations** > **Asio Integrations**.
3. In the Explore Integrations panel, search for *Absolute Security* and click on it.
4. Click **Integrate**.

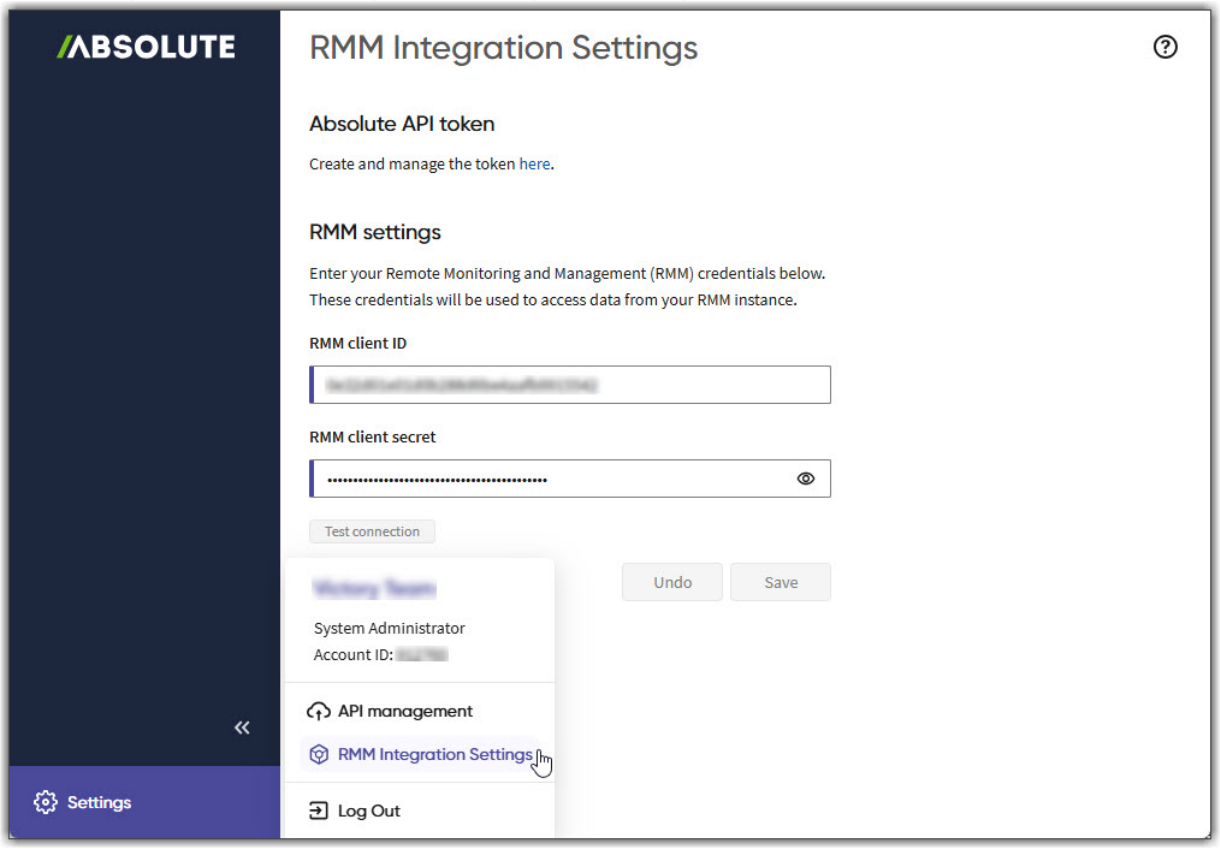


5. On the Asio API Credentials page, click **Generate**. A client ID and secret key are generated.
6. Leave the page open while you complete the next section.

Absolute Resilience for ConnectWise – User Guide

Enabling the integration in Secure Endpoint

1. Log in to the Secure Endpoint Console (use the URL in the registration confirmation email you received from Absolute Security). If this is your first time logging in, review and accept the Master Subscription Agreement (MSA).
2. On the navigation bar, click **Settings** > **RMM Integration Settings**.

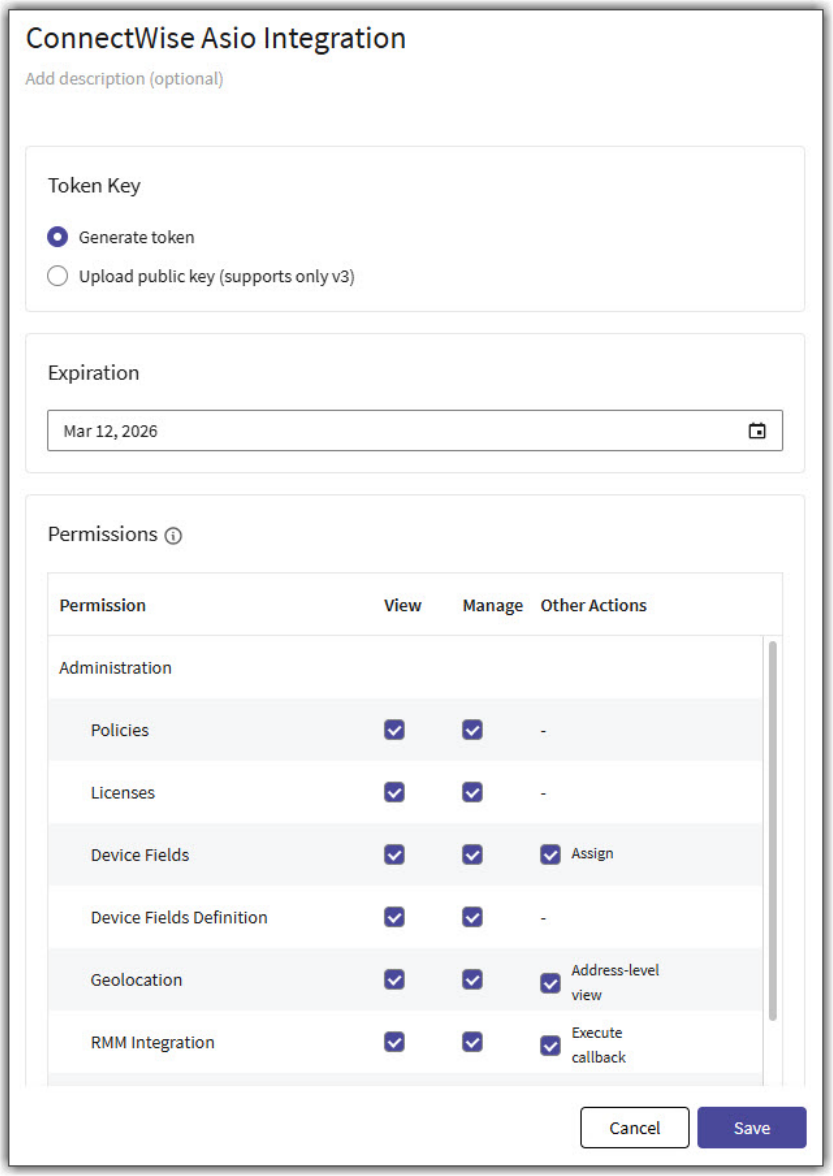


3. Copy the client ID and secret key you generated in step 5 of *Generating client credentials in the Asio platform* and paste them in their respective fields (**RMM client ID** and **RMM client secret)**.
4. Click **Test connection**. If Secure Endpoint can connect to the Asio platform with the credentials you entered, you'll see a "Connection success" message.
5. Click **Save**.
6. Leave the page open while you complete the next section.

Generating an API token in Secure Endpoint

1. Under Absolute API token on the RMM Integration Settings page, click **here**. Alternatively, you can click **Settings > API management** on the navigation bar.
2. On the API management page, click **Create API token**.
3. Click the title and enter a name for the API token.

4. Click the **Expiration** date field and set an expiration date for the API token.

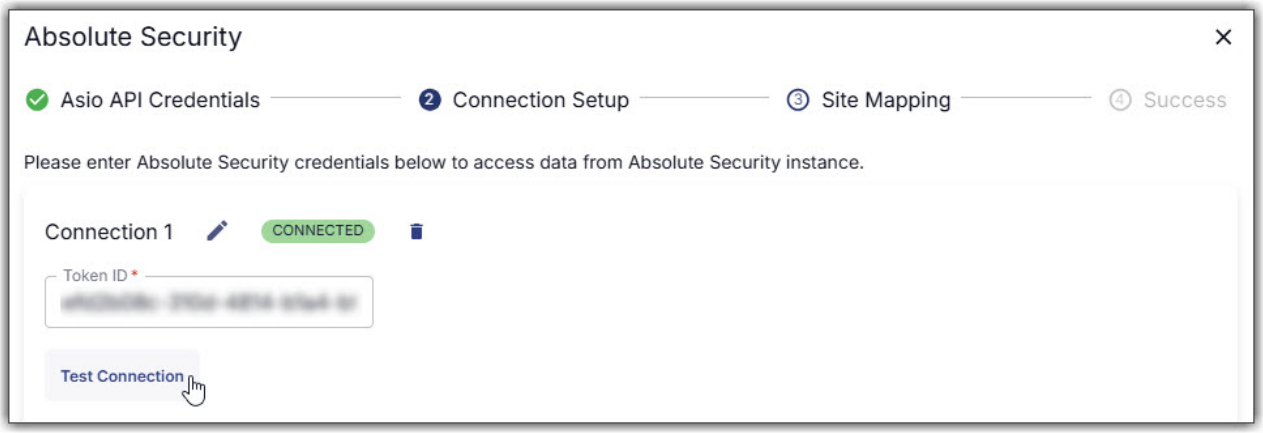


   By default, the expiry date is 90 days from the day the token is created. You can set the expiry date to be up to one year from the creation date.
5. Leave all other configurations set to their default settings and click **Save**.
   By default, all **RMM Integration** permissions are enabled for the token. These permissions are required to successfully integrate Absolute Secure Endpoint with the Asio platform.
6. Next to Token ID, click **Copy**.

NOTE: To avoid your token expiring (which will cause a "connection failed" error in the Asio platform), you can extend the token up to one year any time before it expires from the Secure Endpoint Console. If your token has expired, generate a new one by following the instructions above and add it to the Asio platform by following the instructions in the next section.

Enabling the integration in the Asio platform

1. From where you left off in *Generating client credentials in the Asio platform*, click **Proceed**.
2. In the **Token ID** field, paste the token ID that you copied in step 6 of *Generating an API token in Secure Endpoint*.
3. Click **Test Connection**.

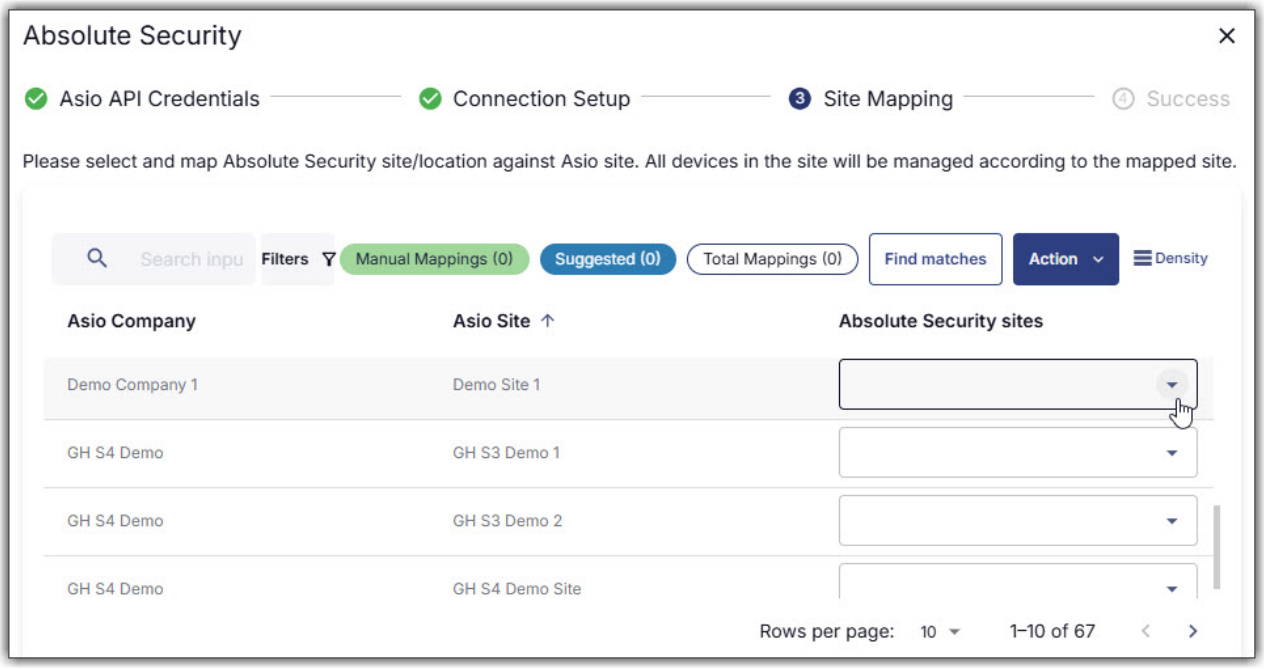


If the Asio platform can connect to Secure Endpoint with the token ID you entered, you'll see a "Connection established successfully" message.

4. Select the checkbox next to **Grant API Access to Absolute Secure Endpoint**.
5. Click **Save and Proceed**.
6. Leave the page open while you complete the next section.

Mapping your Asio sites to Absolute Security

1. From the list of your current Asio sites, find a site for which you want to enable the Secure Endpoint integration. If you have a large number of Asio sites, you can search by company name and filter by mapping status.
2. Next to the site, select your company name from the Absolute Security sites drop-down list.



3. Repeat steps 1 and 2 for each site you want to integrate. If you want to exclude a particular Asio site from the integration, leave the Absolute Security sites list blank.
4. Click **Save and Proceed**.
5. Click **Continue**.
6. Click **Complete Setup**.

NOTE: Applying Absolute-enabled policies to Asio sites that are not yet mapped to Absolute Security can produce unpredictable results. If this happens, move the site's devices to another site that is already mapped to Absolute Security.

Deploying the Secure Endpoint Agent to your devices

The Secure Endpoint Agent is a small software client you need to deploy to your devices before you can manage them through the Asio platform.

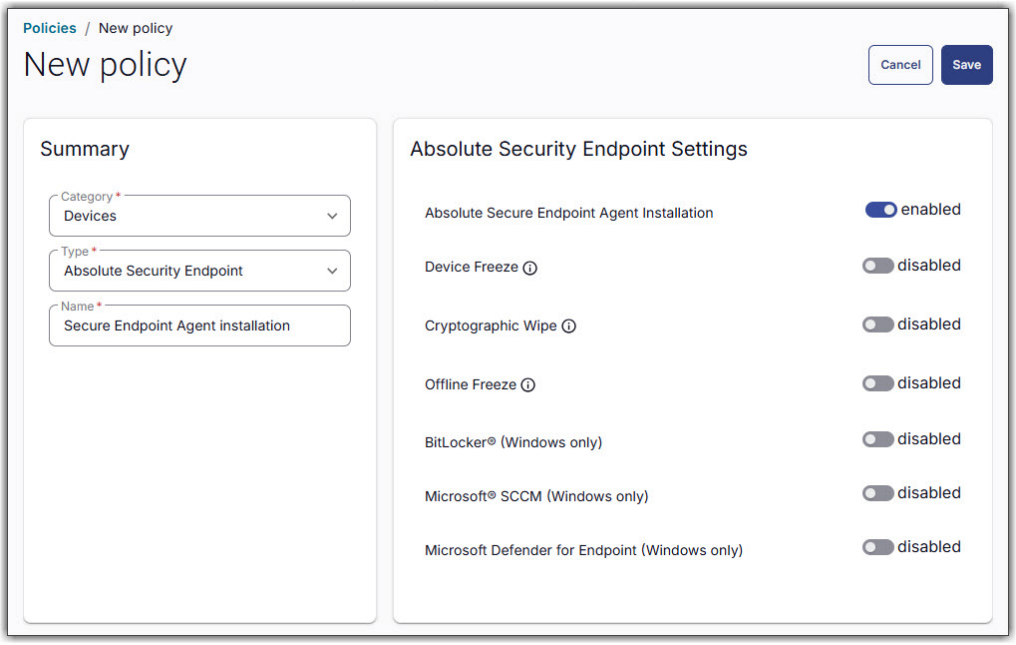
To deploy the Secure Endpoint Agent to your devices, you'll need to:

- Create a policy for agent deployment
- Create a package and assign the policy
- Assign the package to your sites

NOTE: You'll also need to deploy and install the ConnectWise RMM Agent to your devices if you haven't already done so. For more information, see the Asio platform documentation.

Creating a policy for agent deployment

1. Log in to the Asio platform. For more information, see the Asio platform documentation.
2. Navigate to **Endpoints > Policies** and click **Add Policy**.
3. Select **Devices** from the **Category** drop-down list and **Absolute Security Endpoint** from the **Type** drop-down list.
4. In the Name field, enter a name for your policy (for example, "Secure Endpoint Agent installation").
5. Enable the **Absolute Secure Endpoint Agent Installation** option.

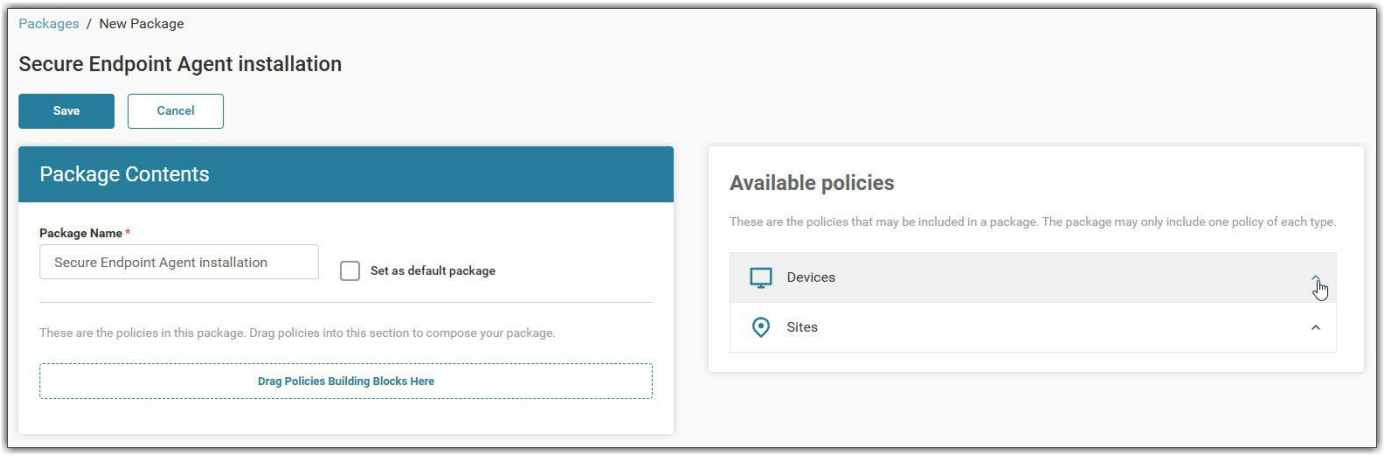


NOTE: You can enable multiple options within a single policy. For the purposes of this procedure, only one option is enabled.

6. Click **Save**.

Creating a package and assigning the policy

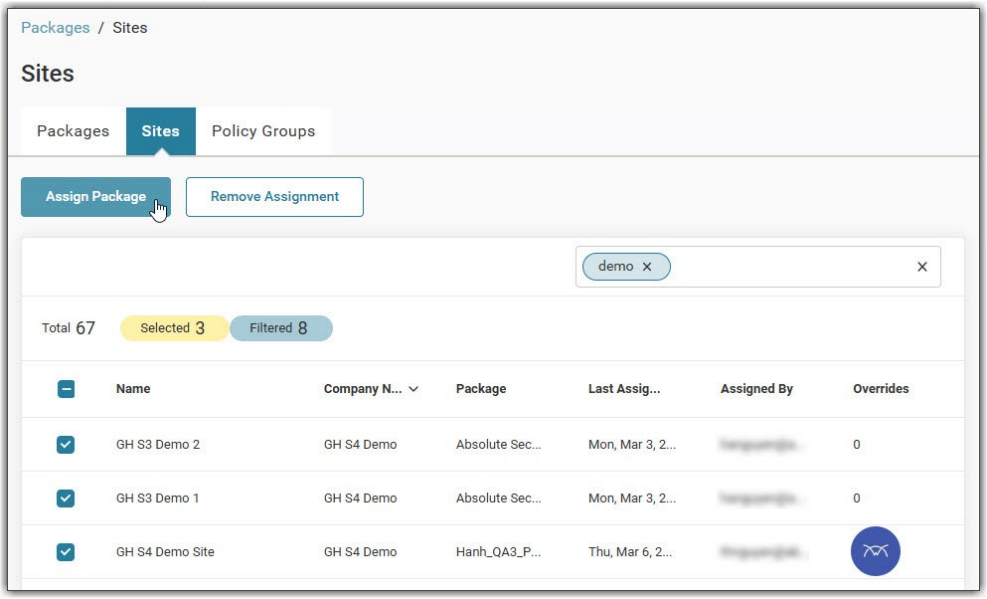
1. Navigate to **Endpoints > Packages** and click **Add Package**.
2. In the Package Name field, enter a name for your package (for example, "Secure Endpoint Agent installation").
3. Under Available policies, click the **Devices** drop-down and locate the policy you created in *Creating a policy for agent deployment*.



4. Drag and drop the policy to the Drag Policies Building Blocks Here section.
5. Click **Save**.

Assigning the package to your sites

1. In **Endpoints > Packages**, navigate to the **Sites** tab.
2. From the list of sites, select the checkbox next to each site you want to assign the package to.
3. Click **Assign Package**.



4. Select the package you created in *Creating a package and assigning the policy* and click **Assign**.
5. If you are asked to acknowledge that updating a package will update the policies for the site, click **Update** to proceed.

The Secure Endpoint Agent will now begin deploying to all devices associated with the sites you selected. You can navigate to **Endpoints > Devices** and select **Absolute Software** from the Integrations drop-down list to view the devices that have the agent installed.

Managing your devices

After you've successfully deployed the agent to your sites, it will begin collecting data from your devices and you can start leveraging the endpoint management capabilities of Absolute Secure Endpoint, including:

- Viewing the details of devices (location, app health, etc.)
- Freezing and unfreezing devices
- Wiping devices
- Monitoring and repairing critical applications on devices

How the agent works

After the Secure Endpoint Agent is initially installed on a device, it's activated with the device's first connection to the Absolute Monitoring Center, at which time it receives a unique identifier. A device record is then created in the database and the device information detected by the agent is made available in the Asio platform.

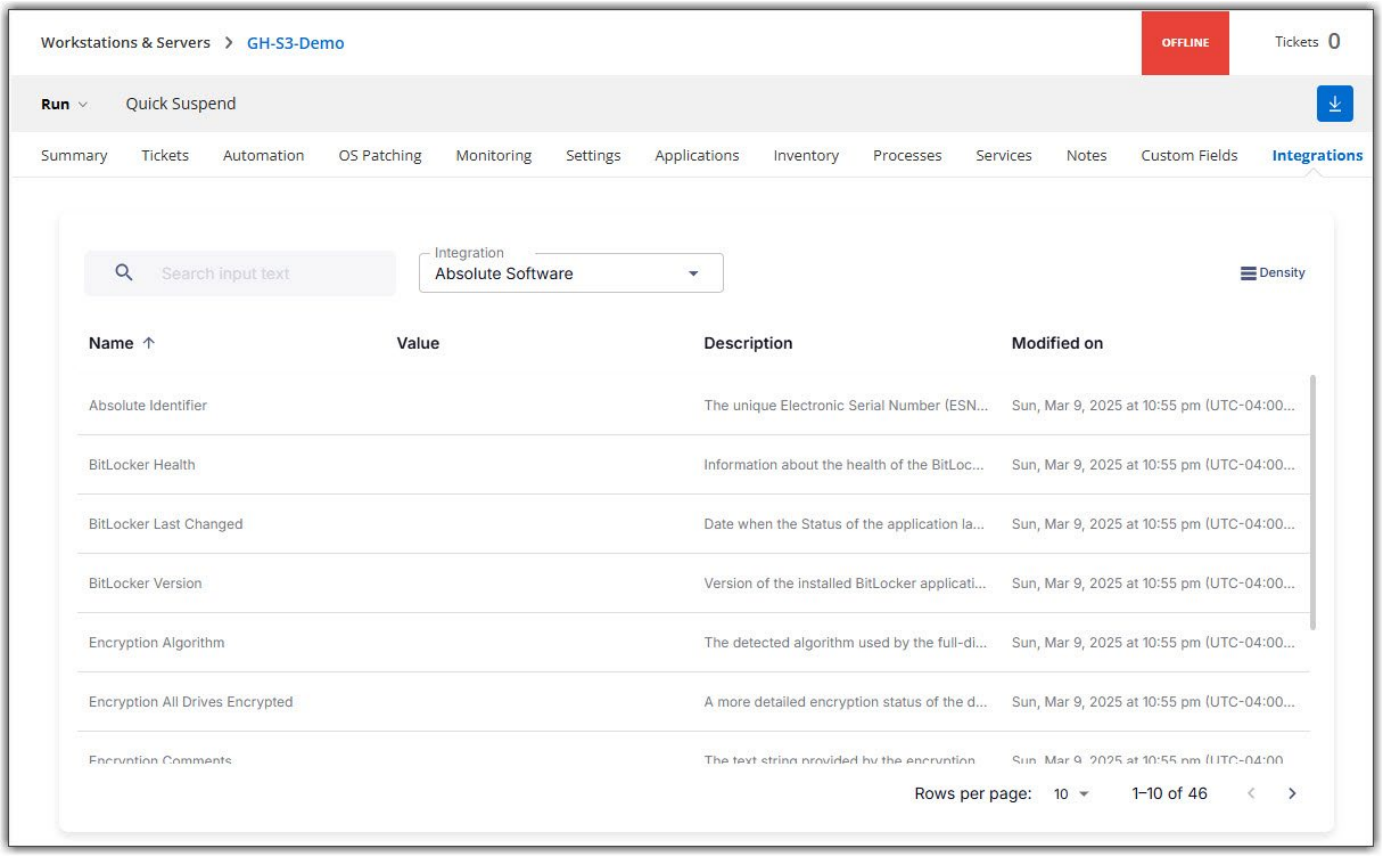
Going forward, the Secure Endpoint Agent maintains regular two-way communication with the Absolute Monitoring Center, monitoring the device's data points and uploading any changes in near real-time. The agent also receives and processes all device actions requested in the Asio platform, such as Wipe and Freeze requests.

The agent remains concealed on devices, and it does not affect system performance or interfere with internet activities. Absolute's Persistence® technology monitors the health of the agent and restores it if it's missing, damaged, or tampered with. Even if the firmware is flashed, the device is reimaged, or the hard drive is replaced, Absolute's Persistence technology ensures the agent will be reinstalled.

Viewing the details of devices

1. Navigate to **Endpoints > Devices**.
2. Under the Name column, click the device whose details you want to view.

3. From the menu at the top, click **Integrations** and ensure that **Absolute Software** is selected from the Integration drop-down list.



From this page you can see detailed device information, including when the information was last updated by the agent. Depending on the device's configuration and applied policies, the following details may be available.

Name	Description
Absolute Identifier	The unique Electronic Serial Number (ESN) assigned to the Secure Endpoint Agent installed on the device
BitLocker Health	The assessed health status of the BitLocker application installed on the device
BitLocker Last Changed	Date and time when BitLocker's health status last changed on the device
BitLocker Version	The version of BitLocker installed on the device
Encryption Algorithm	The detected algorithm used by the full-disk encryption software, if available. Most products use an Advanced Encryption Standard (AES) algorithm.
Encryption All Drives Encrypted	A more detailed encryption status of the device's drives
Encryption Comments	The text string provided by the encryption vendor that provides more information about the encryption status of the device's system drive
Encryption Key Size	The number of bits in a key used by the detected algorithm. For products that use an AES algorithm, the key size is typically 128 or 256 bits.
Encryption Last Updated	The date and time when a change in the device's encryption information was last detected

Encryption Product Name	The name of the full-disk encryption software detected on the device
Encryption SED Capable	Indicates whether the encryption product is hardware-based (i.e., it is an Opal compliant self encrypting drive [SED]) or software-based
Encryption Status	The summarized encryption status of the device
Encryption Version	The version number of the detected full-disk encryption software
Freeze Request Details	Information about the Freeze request submitted for the device
Freeze Request Status	The status of the Freeze request action submitted for the device. Possible values: • **Failed** – either the system or the device is unable to perform the action, the request was declined, or the request was auto declined **Pending –** the action hasn't been downloaded to the device or the request requires approval • **Canceled** – a user has canceled the action • **Processing** – the action is currently being performed on the device, but the action hasn't been completed yet • **Completed** – the action has run on the device
Freeze Requested Date	The date and time when the Freeze request was submitted
Freeze Status	The status of the Freeze request submitted for the device. Possible values: • **Pending** – a request has been submitted, but it has not been sent to the device yet • **Frozen** – the device is frozen and it has checked in to confirm its status
Freeze Unfreeze Code	The 4- to 8-digit passcode that a user can enter on the device to unfreeze it if it was frozen by a Freeze request
Freeze Updated Date	The date and time when the Freeze request changed status
Location Accuracy	The estimated accuracy of the technology used to locate the device in meters
Location City	The city the device was last reported in
Location Country	The country the device was last reported in
Location Last Data Received	The date and time when the device's location was last updated in the Asio platform
Location Lat and Long	The location coordinates (latitude and longitude) of the device
Location Link	Click the link to view the location of the device in Google Maps, based on the reported latitude and longitude
Location Policy Updated	The date and time when the Geolocation Tracking policy was activated or last updated
Location State	The state or province the device was last reported in
Location Status	The status of the Geolocation Tracking policy
Location Type	The type of geolocation technology used by the device
MS Defender Health	The assessed health status of Microsoft Defender for Endpoint on the device
MS Defender Last Changed	Date and time when Microsoft Defender for Endpoint's health status last changed on the device
MS Defender Version	The version of Microsoft Defender for Endpoint installed on the device
Offline Freeze Status	The status of the Offline Freeze rule. Possible values: • **Pending** – a rule has been activated, but it has not been sent to the device yet • **Set** – the rule has been sent to the device and it is waiting for the offline timer to expire • **Frozen - Timer Expired** – the offline timer has expired, but the device has not checked in to confirm its Frozen status • **Frozen** – the device is frozen and it has checked in to confirm its status

Offline Freeze Updated Date	The date and time when the Offline Freeze request changed status
Offline Unfreeze Code	The 4- to 8-digit passcode that a user can enter on the device to unfreeze it if it was frozen by an Offline Freeze rule
Remove Freeze Request Details	Information about the Remove Freeze request submitted for the device
Remove Freeze Request Status	The status of the Remove Freeze request submitted for the device. Possible values: • **Failed** – either the system or the device is unable to perform the action, the request was declined, or the request was auto declined • **Pending** – the action hasn't been downloaded to the device or the request requires approval • **Canceled** – a user has canceled the action • **Processing** – the action is currently being performed on the device, but the action hasn't been completed yet • **Completed** – the action has run on the device
Remove Freeze Requested Date	The date and time when the Remove Freeze request was submitted
Remove Freeze Updated Date	The date and time when the Remove Freeze request changed status
SCCM Health	The assessed health status of Microsoft System Center Configuration Manager on the device
SCCM Last Changed	Date and time when Microsoft System Center Configuration Manager's health status last changed on the device
SCCM Version	The version of Microsoft System Center Configuration Manager installed on the device
Wipe Requested Date	The date and time when the Crypto Wipe request was submitted
Wipe Status	The status of the Crypto Wipe request submitted for the device. Possible values: • **Failed** – either the system or the device is unable to perform the action, the request was declined, or the request was auto declined • **Pending** – the action hasn't been downloaded to the device or the request requires approval • **Canceled** – a user has canceled the action • **Processing** – the action is currently being performed on the device, but the action hasn't been completed yet • **Succeeded** – the action has run on the device, and the action was completed successfully
Wipe Status Details	Information about the Crypto Wipe request submitted for the device
Wipe Updated Date	The date and time when the Crypto Wipe request changed status

Freezing and unfreezing devices

You can prevent anyone from accessing an at-risk device by freezing it from the Asio platform. A frozen device displays a full-screen message in place of the login page. This message can't be closed or bypassed.

The device remains frozen until:

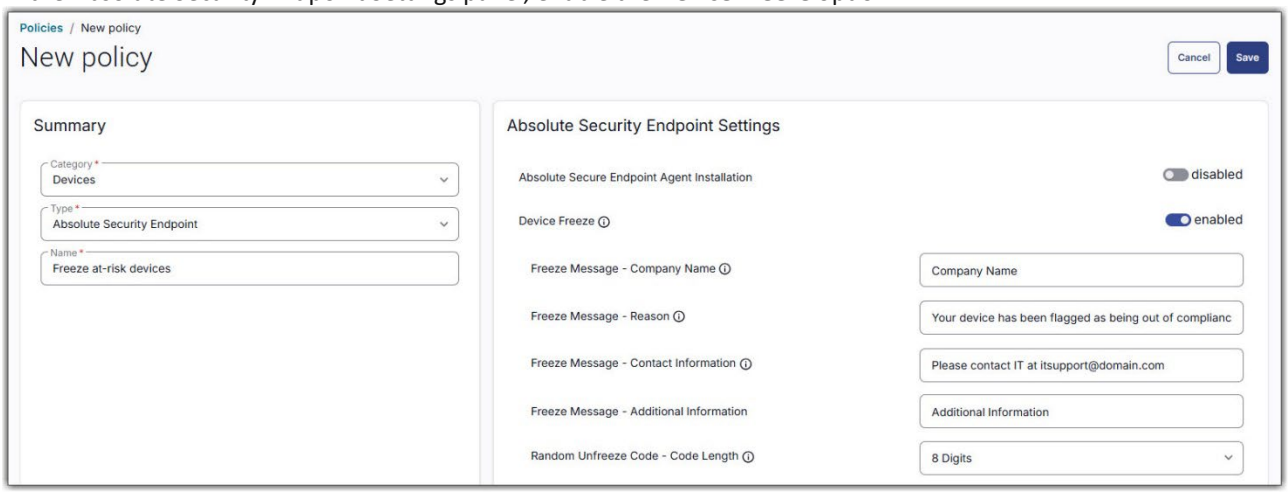
- The device's unfreeze code is entered on the frozen device, or
- You submit a Remove Freeze request in the Asio platform

As a preventative security measure, you can also configure an Offline Freeze rule for your sites, which freezes any device that goes offline and doesn't contact the Absolute Monitoring Center for a specified number of days. This action helps ensure your devices are protected even when they're powered off or a network connection isn't available.

Before you can freeze and unfreeze devices, you must set up a Freeze policy and deploy it to your sites.

Setting up and deploying a Freeze policy

1. Navigate to **Endpoints** > **Policies** and click **Add Policy**.
2. In the Summary panel:
    - From the Category drop-down, select **Devices**.
    - From the Type drop-down, select **Absolute Security Endpoint**.
    - In the Name field, enter a name for this Freeze policy (for example, “Freeze at-risk devices”).
3. In the Absolute Security Endpoint Settings panel, enable the **Device Freeze** option.



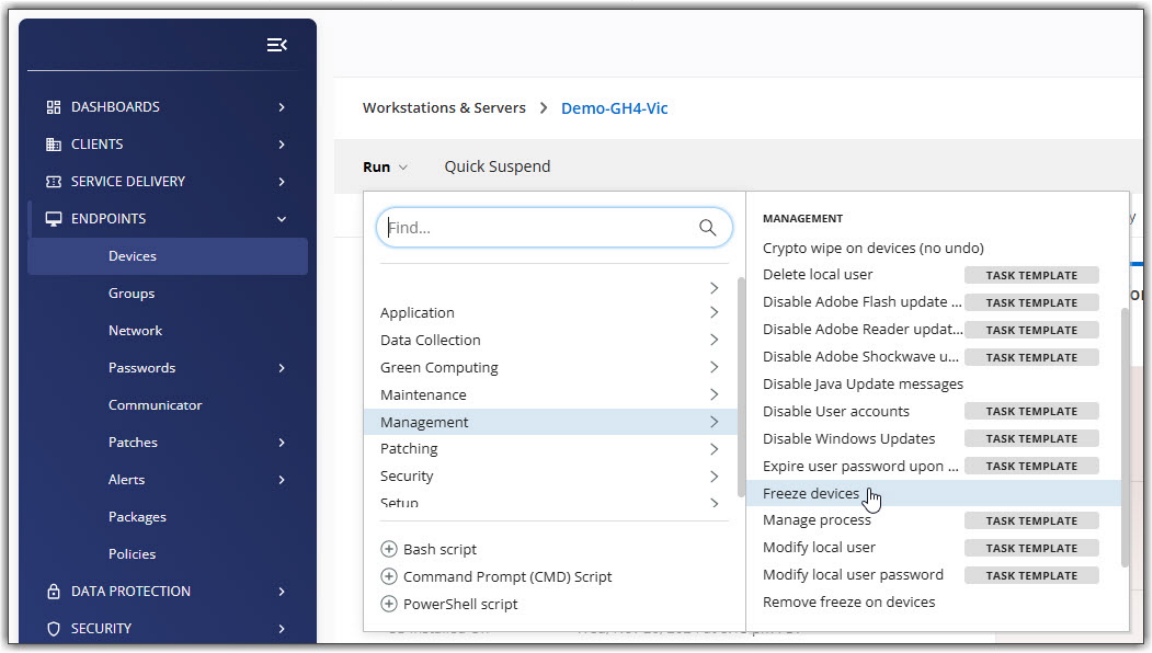
NOTE: You can enable multiple options within a single policy. For the purposes of this procedure, only one option is enabled.

4. Create a freeze message that users will be able to see on frozen devices:
    - In the Freeze Message - Company name field, enter your company name so users know where the message is coming from.
    - In the Freeze Message - Reason field, enter the reason why the device has been frozen.
    - In the Freeze Message - Contact Information field, enter your contact details so users can reach out to you if needed.
    - In the Freeze Message - Additional Information field, enter any additional information you want users to see in the freeze message.
5. From the Generate A Random Unfreeze Code - Code Length drop-down, select the number of digits for the unfreeze code, which can be entered directly on the frozen device to unfreeze it.
6. Click **Save**.
7. Navigate to **Endpoints > Packages** and click **Add Package**.
8. In the Package Name field, enter a name for your package (for example, “Freeze at-risk devices”).
9. Under Available policies, click the **Devices** drop-down and locate the Freeze policy you just created.
10. Drag and drop the policy to the Drag Policies Building Blocks Here section.
11. Click **Save**.
12. In **Endpoints > Packages**, navigate to the **Sites** tab.
13. From the list of sites, select the checkbox next to each site you want to apply your Freeze policy to. (Note that you are not freezing devices at this point, but simply deploying Freeze-related settings to your sites.)
14. Click **Assign Package**.
15. Select the package you just created for freezing devices and click **Assign**.

16. If you are asked to acknowledge that updating a package will update the policies for the site, click **Update** to proceed.

Freezing devices from the Workstations & Servers page

1. Navigate to **Endpoints > Devices**.
2. On the Workstations & Servers page, select the checkbox next to the device(s) you want to freeze.
   You can use the search bar to find specific devices or filter your device list by criteria like site and device group.
3. From the menu at the top of the page, select **Run > Management > Freeze devices**.



4. Indicate when you want to initiate the Freeze request by selecting one of the following options:
   - **Run now** – Devices are frozen on the next agent connection, which is typically within a few minutes (assuming the devices are online).
   - **Run later** – Devices are frozen at a future date and time. If you select this option, specify the date and time you want to freeze the devices.
   - **Run recurringly** – Devices are scheduled to be frozen on a regular basis at specific times and days. If you select this option, specify the date, time, and frequency to freeze the devices.
   - **Run on trigger** – Devices are frozen only when triggered by an action you specify. If you select this option, specify the trigger and a time range.
5. Click **Run Task**.

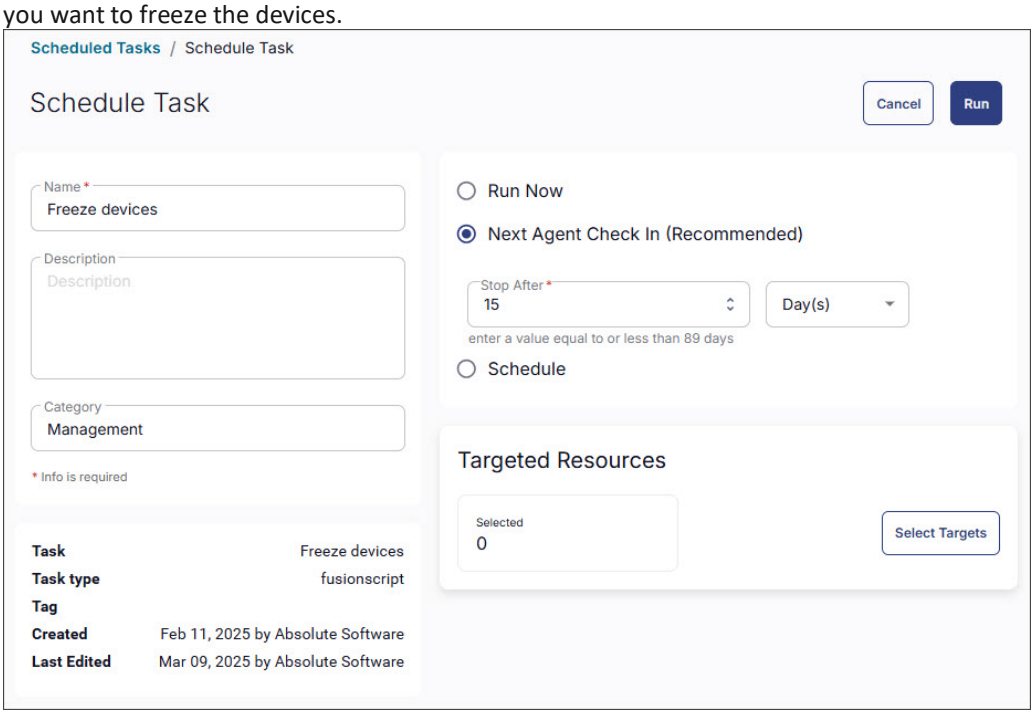
The Freeze request is submitted. You can track the status of your request in two ways:

- Navigate to **Endpoints > Devices**, select the device, and click the **Automation** tab.
- Navigate to **Automation > Scheduled Tasks**, select your request, and click **History**.

Freezing devices from the Tasks page

1. Navigate to **Automation > Tasks**.
2. In the search bar, enter **freeze** and click **Freeze devices** under the Name column.
3. Click **Schedule**.

4. In the Name field, enter a name that will help you identify and track your Freeze request on the Scheduled Tasks page. You can also enter an optional description for your Freeze request in the Description field.
5. Indicate when you want to initiate the Freeze request by selecting one of the following options:
    - **Run Now** – The task runs immediately and its status moves directly to "Running". Devices are frozen on the next agent connection, which is typically within a few minutes (assuming the devices are online).
    - **Next Agent Check In** – Devices are frozen on the next agent connection, which is typically within a few minutes (assuming the devices are online). If you select this option, specify the number of days or hours to cancel the request if the devices don't come online.
    - **Schedule** – Devices are frozen at a future date and time. If you select this option, specify the date and time you want to freeze the devices.



6. Click **Select Targets**.
7. Under Select Target Endpoints, specify which devices you want to freeze. You have the following options:
    - **Companies** – Freeze all devices associated with the companies you select.
    - **Sites** – Freeze all devices associated with the sites you select.
    - **Device Groups** – Freeze all devices associated with the device groups you select (for more information on device groups, see the Asio platform documentation).
    - **Devices** – Freeze the specific device or devices you select.
8. Click **Save Selection**.
9. Click **Run**.

The Freeze request is submitted. You can track the status of your request in two ways:

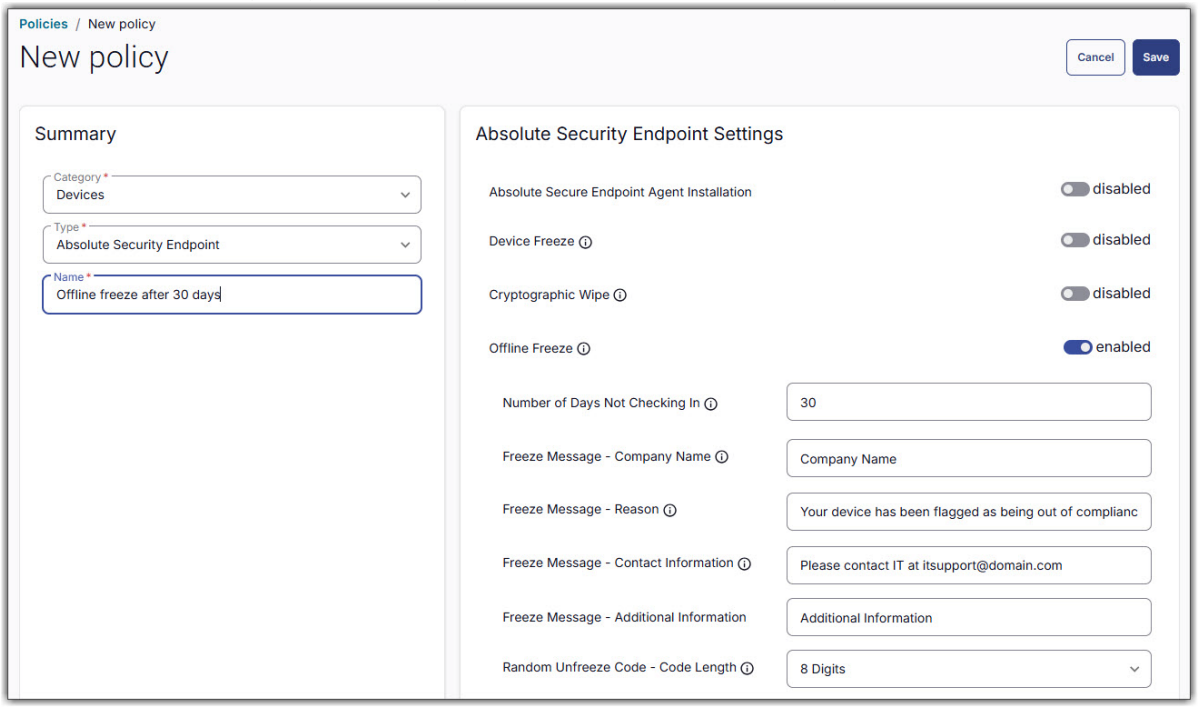
- Navigate to **Endpoints > Devices**, select the device, and click the **Automation** tab.
- Navigate to **Automation > Scheduled Tasks**, select your request, and click **History**.

Creating an Offline Freeze rule

1. Navigate to **Endpoints** > **Policies** and click **Add Policy**.
2. In the Summary panel:

- From the Category drop-down, select **Devices**.
- From the Type drop-down, select **Absolute Security Endpoint**.
- In the Name field, enter a name for this Offline Freeze policy.

3. In the Absolute Security Endpoint Settings panel, enable the **Offline Freeze** option.



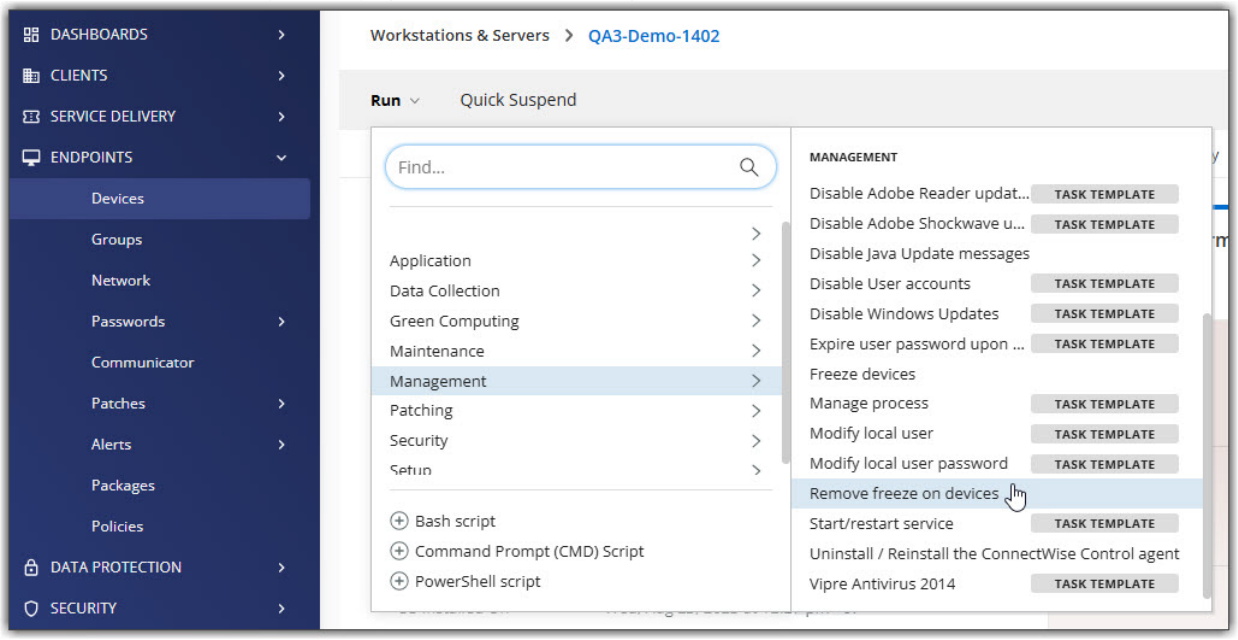
NOTE: You can enable multiple options within a single policy. For the purposes of this procedure, only one option is enabled.

4. In the Length of the timer in days field, enter the number of days a device can remain offline before it is frozen. The default value is 30 days, but any value from 4 to 2000 days is supported. If a device does not contact the Absolute Monitoring Center before the timer elapses, the Secure Endpoint Agent freezes the device.
5. Create a freeze message that users will be able to see on frozen devices:
   - In the Freeze Message - Company name field, enter your company name so users know where the message is coming from.
   - In the Freeze Message - Reason field, enter the reason why the device has been frozen.
   - In the Freeze Message - Contact Information field, enter your contact details so users can reach out to you if needed.
   - In the Freeze Message - Additional Information field, enter any additional information you want users to see in the freeze message.
6. From the Generate A Random Unfreeze Code - Code Length drop-down, select the number of digits for the unfreeze code, which can be entered directly on the frozen device to unfreeze it.
7. Click **Save**.
8. Navigate to **Endpoints > Packages** and click **Add Package**.
9. In the Package Name field, enter a name for your package.
10. Under Available policies, click the **Devices** drop-down and locate the Offline Freeze policy you just created.
11. Drag and drop the policy to the Drag Policies Building Blocks Here section.
12. Click **Save**.
13. In **Endpoints > Packages**, navigate to the **Sites** tab.

14. From the list of sites, select the checkbox next to each site you want to apply the Offline Freeze rule to.
15. Click **Assign Package**.
16. Select the package you created for the Offline Freeze rule and click **Assign**.
17. If you are asked to acknowledge that updating a package will update the policies for the site, click **Update** to proceed.

Unfreezing devices from the Workstations & Servers page

1. Navigate to **Endpoints > Devices**.
2. On the Workstations & Servers page, select the checkbox next to the device(s) you want to unfreeze.
   You can use the search bar to find specific devices or filter your device list by criteria like site and device group.
3. From the menu at the top of the page, select **Run > Management > Remove freeze on devices**.



4. Indicate when you want to initiate the Remove Freeze request by selecting one of the following options:
   a. **Run now** – Devices are unfrozen on the next agent connection, which is typically within a few minutes (assuming the devices are online).
   b. **Run later** – Devices are unfrozen at a future date and time. If you select this option, specify the date and time you want to unfreeze the devices.
   c. **Run recurringly** – Devices are scheduled to be unfrozen on a regular basis at specific times and days. If you select this option, specify the date, time, and frequency to unfreeze the devices.
   d. **Run on trigger** – Devices are unfrozen only when triggered by an action you specify. If you select this option, specify the trigger and a time range.
5. Click **Run Task**.

The Remove Freeze request is submitted. You can track the status of your request in two ways:

- Navigate to **Endpoints > Devices**, select the device, and click the **Automation** tab.
- Navigate to **Automation > Scheduled Tasks**, select your request, and click **History**.

Unfreezing a device immediately using its unfreeze code

1. Navigate to **Endpoints > Devices**.
2. Under the Name column, click the device you want to unfreeze.

3. From the menu at the top, click **Integrations** and ensure that **Absolute Software** is selected from the Integration drop-down list.
4. Under the Name column, find the Freeze Unfreeze Code (if the device was frozen by a Freeze request) or Offline Unfreeze Code (if the device was frozen by an Offline Freeze rule).
5. Provide the code to the device's user along with the following device-specific instructions for unfreezing the device:
    - For Windows devices
        i. Power on the frozen device. The full screen Device Freeze message shows.
        ii. Type the unfreeze code. You can use the keyboard's numeric keypad, if it exists. If you make a mistake, press **Esc** to clear your input and start again. Note that your typed code is not displayed on the screen – this is the expected behavior.
        iii. Press **Enter** or **Return** on your keyboard.
    - For Mac devices
        i. Power on the frozen device. The full screen Device Freeze message shows.
        ii. To enable the device to accept an unfreeze code, press the **Esc** key on your keyboard. Note that no new page or field opens.
        iii. Type the unfreeze code and press **Enter** or **Return** on your keyboard.

Wiping devices

You can use the Crypto Wipe feature to remotely remove all sensitive data from your devices before you reuse, resell, or dispose of them. This process is known as data sanitization.

How it works

The Crypto Wipe feature employs the cryptographic erase data sanitization process, which removes all encryption keys, effectively making all data on a device irretrievable, including the operating system.

This type of Crypto Wipe conforms to the *Purge* standard defined in NIST Special Publication 800-88, Guidelines for Media Sanitization, and it is HIPAA compliant. Although a Purge does not perform any data overwrites, it is recognized as a quick and effective method of data sanitization.

When a Crypto Wipe request is deployed to a device:

- The device's encryption keys are removed. The ciphertext remains on the device, but without an encryption key the encrypted data is unreadable.
- A Certificate of Sanitization is generated and made available after the Crypto Wipe is completed.
- The BitLocker recovery page shows when a user powers on a wiped device. Users cannot log in.

The Crypto Wipe feature is very destructive, and a request can't be canceled or undone after it's deployed to a device. To limit the impact of a Crypto Wipe request submitted in error or with malicious intent, a request can include a maximum of 100 devices only. To wipe additional devices, you must submit another request.

To learn more about how the Crypto Wipe feature works, see the Absolute Device Wipe datasheet.

Eligibility requirements

Crypto Wipe requests can be executed on supported Windows devices with the following attributes:

- Encrypted by BitLocker
- Encryption Status set to either Encrypted or Used Space Encrypted

Also note that devices must be regularly connecting to the Absolute Monitoring Center.

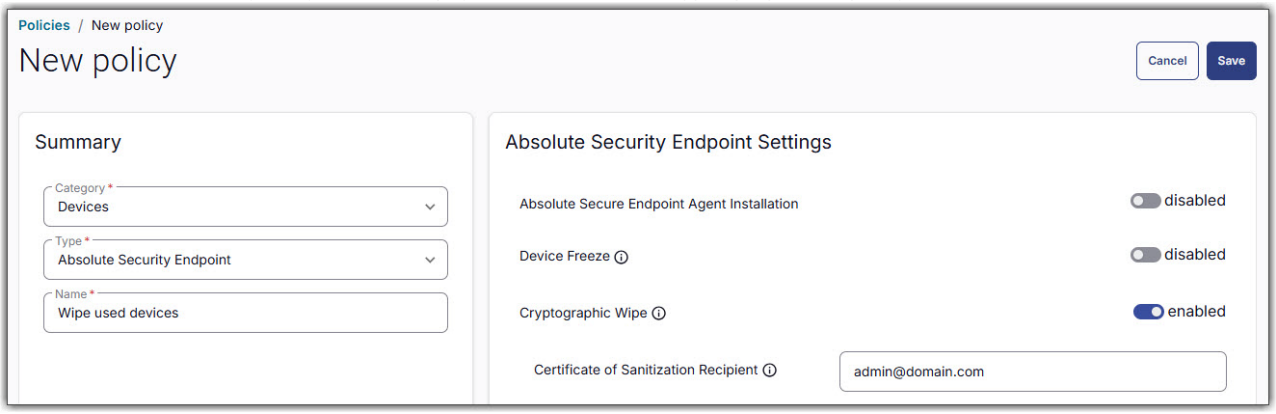
Crypto Wipe requests are not supported on the following devices:

- Mac devices
- Unencrypted or partially encrypted Windows devices
- Devices encrypted by a product other than BitLocker
- Devices with an outstanding Crypto Wipe request

Before you can wipe devices, you must set up a Crypto Wipe policy and deploy it to your sites.

Setting up and deploying a Crypto Wipe policy

1. Navigate to **Endpoints** > **Policies** and click **Add Policy**.
2. In the Summary panel:
    - From the Category drop-down, select **Devices**.
    - From the Type drop-down, select **Absolute Security Endpoint**.
    - In the Name field, enter a name for this Crypto Wipe policy (for example, “Wipe used devices”).
3. In the Absolute Security Endpoint Settings panel, enable the **Cryptographic Wipe** option.

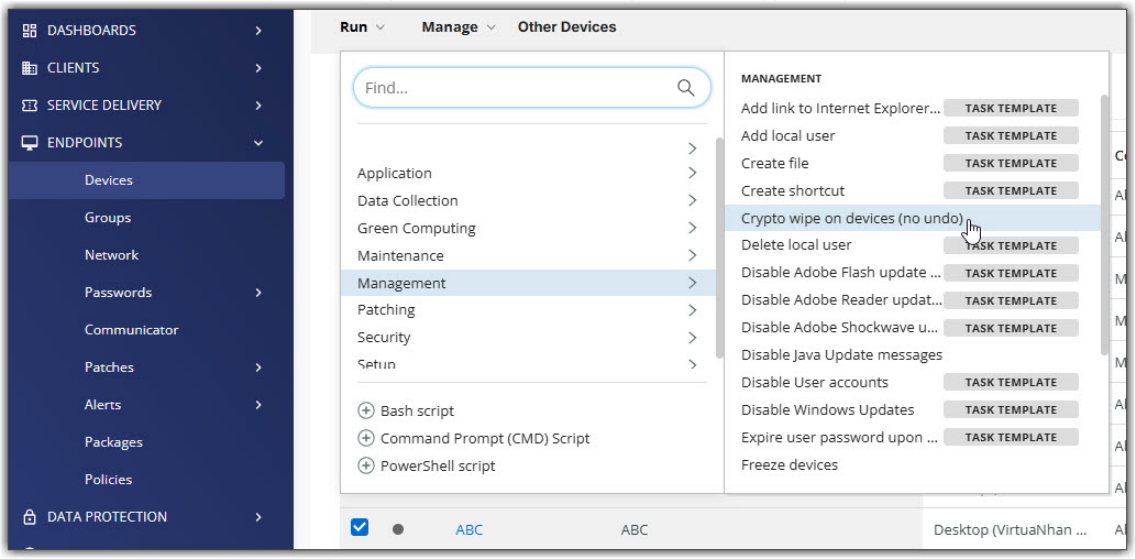


NOTE: You can enable multiple options within a single policy. For the purposes of this procedure, only one option is enabled.

4. In the Sanitization Certificate Recipient Email field, enter the email address that will receive Certificates of Sanitization after Crypto Wipe actions are completed. You can use this certificate to demonstrate to auditors that a device's data was successfully sanitized in compliance with NIST Special Publication 800-88, *Guidelines for Media Sanitization*.
5. Click **Save**.
6. Navigate to **Endpoints > Packages** and click **Add Package**.
7. In the Package Name field, enter a name for your package (for example, “Wipe used devices”).
8. Under Available policies, click the **Devices** drop-down and locate the Crypto Wipe policy you just created.
9. Drag and drop the policy to the Drag Policies Building Blocks Here section.
10. Click **Save**.
11. In **Endpoints > Packages**, navigate to the **Sites** tab.
12. From the list of sites, select the checkbox next to each site you want to apply your Crypto Wipe policy to. (Note that you are not wiping devices at this point, but simply deploying Crypto Wipe-related settings to your sites.)
13. Click **Assign Package**.
14. Select the package you just created for wiping devices and click **Assign**.
15. If you are asked to acknowledge that updating a package will update the policies for the site, click **Update** to proceed.

Wiping devices from the Workstations & Servers page

1. Navigate to **Endpoints > Devices**.
2. On the Workstations & Servers page, select the checkbox next to the device(s) you want to wipe.
   You can use the search bar to find specific devices or filter your device list by criteria like site and device group.
3. From the menu at the top of the page, select **Run > Management > Crypto wipe on devices (no undo)**.



4. Indicate when you want to initiate the Crypto Wipe request by selecting one of the following options:
   a. **Run now** – Devices are wiped on the next agent connection, which is typically within a few minutes (assuming the devices are online).
   b. **Run later** – Devices are wiped at a future date and time. If you select this option, specify the date and time you want to wipe the devices.
   c. **Run recurringly** – Devices are scheduled to be wiped on a regular basis at specific times and days. If you select this option, specify the date, time, and frequency to wipe the devices.
   d. **Run on trigger** – Devices are wiped only when triggered by an action you specify. If you select this option, specify the trigger and a time range.
5. Click **Run Task**.

The Crypto Wipe request is submitted. You can track the status of your request in two ways:

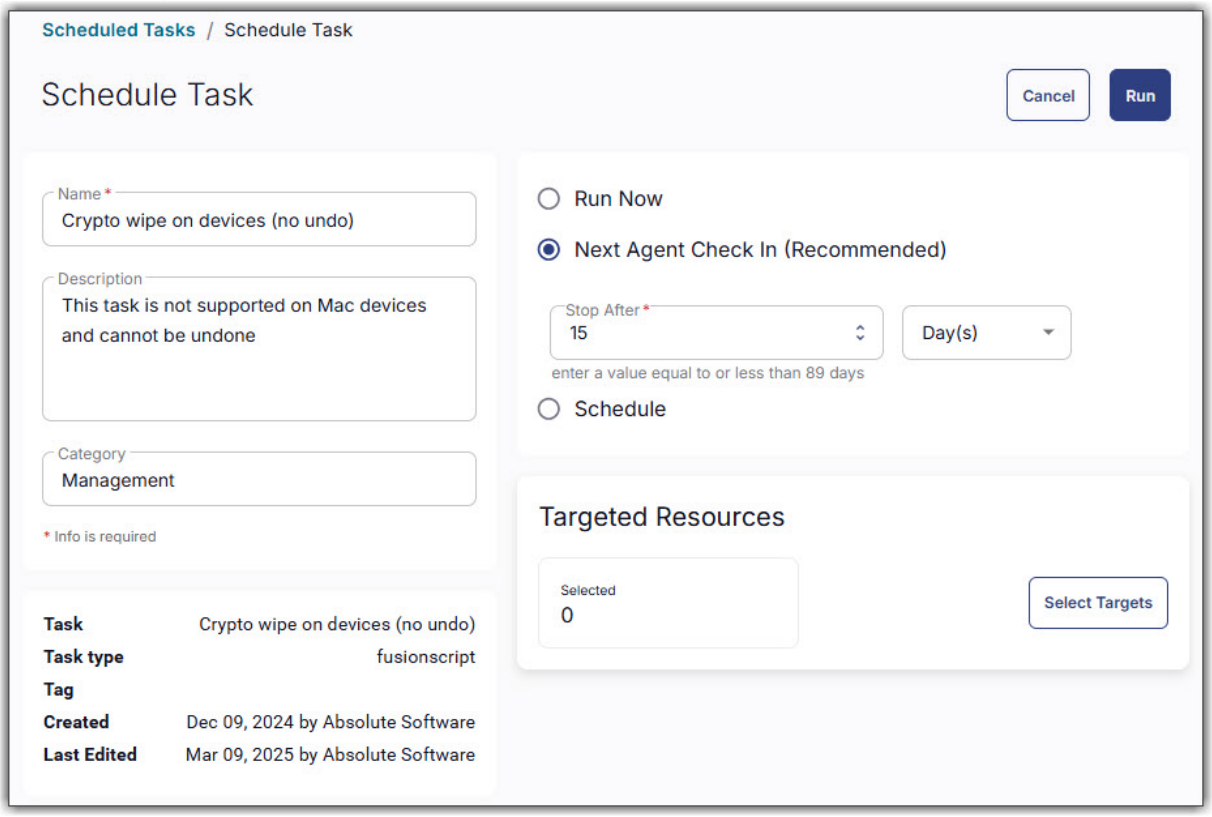
- Navigate to **Endpoints > Devices**, select the device, and click the **Automation** tab.
- Navigate to **Automation > Scheduled Tasks**, select your request, and click **History**.

After a Crypto Wipe action is completed on a device, a Certificate of Sanitization is emailed to the address specified in the Cypto Wipe policy. If you want to reuse a device after it's wiped, reimage the device.

Wiping devices from the Tasks page

1. Navigate to **Automation > Tasks**.
2. In the search bar, enter **wipe** and click **Crypto wipe on devices (no undo)** under the Name column.
3. Click **Schedule**.
4. In the Name field, enter a name that will help you identify and track your Crypto Wipe request on the Scheduled Tasks page. You can also enter an optional description for your Crypto Wipe request in the Description field.
5. Indicate when you want to initiate the Crypto Wipe request by selecting one of the following options:

- **Run Now** – The task runs immediately and its status moves directly to "Running". Devices are wiped on the next agent connection, which is typically within a few minutes (assuming the devices are online).
- **Next Agent Check In** – Devices are wiped on the next agent connection, which is typically within a few minutes (assuming the devices are online). If you select this option, specify the number of days or hours to cancel the request if the devices don't come online.
- **Schedule** – Devices are wiped at a future date and time. If you select this option, specify the date and time you want to wipe the devices.



6. Click **Select Targets**.
7. Under Select Target Endpoints, specify which devices you want to wipe. You have the following options:
    - **Sites** – Wipe all devices associated with the sites you select.
    - **Device Groups** – Wipe all devices associated with the device groups you select (for more information on device groups, see the Asio platform documentation).
    - **Devices** – Wipe the specific device or devices you select.
8. Click **Save Selection**.
9. Click **Run**.

The Crypto Wipe request is submitted. You can track the status of your request in two ways:

- Navigate to **Endpoints > Devices**, select the device, and click the **Automation** tab.
- Navigate to **Automation > Scheduled Tasks**, select your request, and click **History**.

After a Crypto Wipe action is completed on a device, a Certificate of Sanitization is emailed to the address specified in the Crypto Wipe policy. If you want to reuse a device after it's wiped, reimage the device.

Monitoring and repairing critical applications on devices

Organizations depend on a multitude of software applications to complete the critical business processes required in their day-to-day operations. Many of these applications are deployed to a fleet of devices with limited access to tools that make sure the devices are secure and comply with an organization's defined policies. Over time, these critical applications may become non-functional or non-compliant without your knowledge, potentially exposing your organization to data breaches, regulatory non-compliance, and a loss of employee productivity.

From the Asio platform, you can activate application policies for your sites to help validate and maintain the health of critical third-party applications in the following ways:

- Report on the functional status of the application's essential components
- Determine if the device is compliant by comparing the current state of the application with the desired state (as defined in the application policy configurations)
- Repair components that are non-functional or non-compliant

How it works

The Application Resilience (RAR) component of the Secure Endpoint Agent is responsible for collecting status information about third party agents, clients, services, and drivers installed on your devices.

When you activate an application policy, the RAR component is activated on each device after the next successful agent connection to the Absolute Monitoring Center. Going forward, the component checks the status of the application every 15 minutes. If the device is online, results are uploaded to the database using a secure connection. The upload occurs every 6 hours. An additional upload occurs immediately if an application's health status changes.

You can activate the application policy to enable the RAR component to report on the functional status and compliance of the third-party applications currently supported. Each application has a series of health checks that are tested by the RAR component when the application's policy is configured and activated. For most applications, the RAR component checks to make sure the version installed on the device matches the version configured in the policy. In addition, each application has its own set of health checks that the RAR component tests.

If the RAR component determines that the application is non-functional or non-compliant, the component can be configured to attempt to repair the application.

Supported applications

Currently, you can configure an application policy from the Asio platform for the following third-party applications:

- BitLocker
- Microsoft Defender for Endpoint
- Microsoft System Center Configuration Manager (SCCM)

Application policies are supported on devices running the Windows operating system only. Devices must also be running PowerShell version 5.1 or higher.

NOTE: Due to PowerShell restrictions imposed by Microsoft, application policies aren't supported on devices running Windows 11 SE.

Health checks

In addition to checking the application version, the following table describes the health checks performed on devices when an application policy is enabled.

Component	Test performed
BitLocker®	
Windows Management Instrumentation Service (Winmgmt.msc)	Installed and running
(BitLocker with MBAM integration only) BitLocker Management Client Service	Installed and running
Partitions	A valid partition is found
(BitLocker with MBAM integration only) MBAM service endpoint URLs: • MBAM Recovery and Hardware (CoreService.svc) • MBAM Status reporting (StatusReportingService.svc)	In the device's registry
Microsoft® SCCM	
Windows Management Instrumentation (WMI)	A connection can be established to the WMI and a simple query can be run
Admin share (checked only if selected in the policy configuration)	The admin share is present and enabled
Assigned site (checked only if selected in the policy configuration)	The assigned site can be retrieved
Domain attribute (checked only if selected in the policy configuration)	The domain attribute is reachable and the device is on the network
Client version	The version number of the installed SCCM client
Client variables	The SCCM client variables can be retrieved
CCM services	The SCCM client service and its dependent services are running: • SMS Agent Host (ccmexec) *NOTE: If Microsoft SCCM is using Task Sequence, the RAR component doesn't check to see if SMS Agent Host is running* • Windows Management Instrumentation (winmgmt) • Server (lanmanserver) (checked only if selected in the policy configuration) • Remote Procedure Call (rpcss)
Management point (checked only if selected in the policy configuration)	The management point can be retrieved
Registry setting for DCOM	DCOM is enabled and allows for remote client connections
Hardware inventory (checked only if selected in the policy configuration)	A hardware scan has been run and the last hardware inventory date and time can be retrieved
Software inventory (checked only if selected in the policy configuration)	A software scan has been run and the last software inventory data and time can be retrieved
Microsoft Defender for Endpoint	
Windows Defender Advanced Threat Protection Service (MsSense.exe)	Running and signed by one of the signers entered in the policy configuration
Registry key:	Exists; Value name = “OnboardingInfo”; Data = “<not parsed>”

HKLM:\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection	
Registry key: HKLM:\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection\Status	Exists; Value name = "OnboardingState"; Data = "1"

Configuring and deploying an application policy

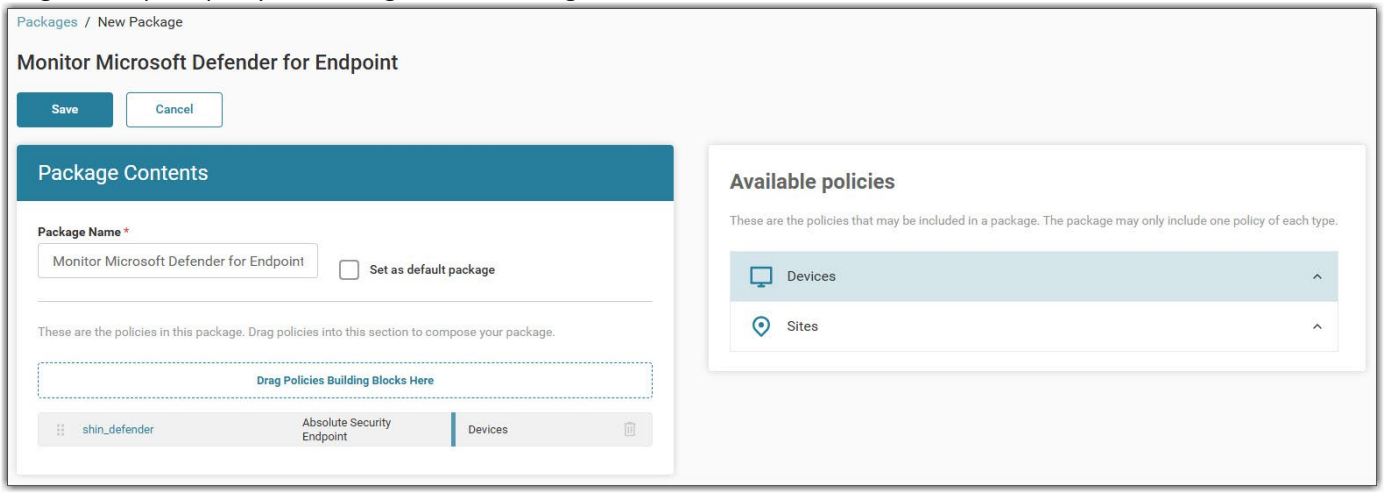
1. Navigate to **Endpoints** > **Policies** and click **Add Policy**.
2. In the Summary panel:
    a. From the Category drop-down, select **Devices**.
    b. From the Type drop-down, select **Absolute Security Endpoint**.
    c. In the Name field, enter a name for this application policy.
3. In the Absolute Security Endpoint Settings panel, enable the **BitLocker®**, **Microsoft® SCCM**, or **Microsoft Defender for Endpoint** options, depending on which applications you want to monitor.
4. Configure the options for each application you selected:

Option	Description
BitLocker®	
Application Version	Select the version of the application that you expect to be running on your devices. For some applications, only one version is available. *NOTE: Devices using Microsoft BitLocker To Go are not supported.*
BitLocker Setup	Select whether your organization is using Microsoft BitLocker Administration and Monitoring (MBAM) to manage BitLocker on your devices. If it does, you must specify the location of the MBAM service endpoints configured in your MBAM Group Policy settings (see the next two options below).
Location of the MBAM Recovery and Hardware service endpoint - URI	Enter the following URI: <protocol>://<hostname>:<port>/MBAMRecoveryAndHardwareService/CoreService.svc The variables are defined as follows: • <protocol> is http or https. • <hostname> is the MBAM Administration and Monitoring server name. • <port> is the port number used by the web service. [Optional]
Location of the MBAM Status reporting service endpoint - URI	Enter the following URI: <protocol>://<hostname>:<port>/MBAMComplianceStatusService/StatusReportingService.svc The variables are defined as follows: • <protocol> is http or https. • <hostname> is the MBAM Administration and Monitoring server name. • <port> is the port number used by the web service. [Optional]
Encrypted Drives	Select the drives that you expect to be encrypted on the devices.
Encryption Strength	Select which strength should have been used to encrypt the devices' drives.
Minimum System Partition Size (MB)	Enter the minimum size (in megabytes) that can be configured for the system partition drive.
Report and Repair Mode	Select one of the following options: • **Report Only** – Collect status information about the application and show it in the Asio platform. • **Report and Repair** – Collect status information about the application and show it in the Asio platform, AND attempt to repair the application if the Secure Endpoint Agent detects that the application is non-functional.

Microsoft® SCCM	
Microsoft SCCM Version	Enter the version of Microsoft SCCM you expect to be running on your devices. • The target version must be a sequence of digits separated by a period. • You can use wildcard "*" characters after the major version number; for example, *5.** or *5.00.** or *5.00.9068.**. • Make sure the version you are entering is consistent with version *5.** or higher.
Report Higher Versions as Compliant	Enable this option if you want higher versions than you entered to be reported as Compliant if the application's health checks still pass.
By default, the policy performs a number of health checks of Microsoft SCCM components. If a particular Microsoft SCCM component isn't applicable to your organization's Microsoft SCCM deployment, the health check may return a status of Not Compliant when Microsoft SCCM is, in fact, functioning correctly. To avoid false results, you can exclude one or more of the following components from the Microsoft SCCM health check.	
Admin Share	This health check tests that the admin share is present and enabled. The admin share is used to deploy the Microsoft SCCM software remotely by allowing administrative remote access to the disk volume over the network.
Assigned Site	This health check tests to see if the assigned site can be retrieved.
Domain Attribute	This health check tests to see if the domain attribute is reachable and the device is on the network.
Lanmanserver Service	This health check detects if the lanmanserver service is running. This service enables the sharing of file and print resources over the network.
Management Point	This health check tests to see if the management point can be retrieved.
Hardware Inventory Scan (Report And Repair Only)	This health check detects the date and time when the SCCM client last scanned a device's installed hardware.
Software Inventory Scan (Report And Repair Only)	This health check detects the date and time when the SCCM client last scanned a device's installed software.
Report and Repair Mode	Select one of the following options: • **Report Only** – Collect status information about the application and show it in the Asio platform. • **Report and Repair** – Collect status information about the application and show it in the Asio platform, AND attempt to repair the application if the Secure Endpoint Agent detects that the application is non-functional.
Microsoft Defender for Endpoint	
Microsoft Defender for Endpoint Version	Enter the version of Microsoft Defender for Endpoint you expect to be running on your devices. • The target version must be a sequence of digits separated by a period. • You can use wildcard "*" characters after the major version number; for example, *10.** or *10.8760.**.
Report Higher Versions as Compliant	Enable this option if you want higher versions than you entered to be reported as Compliant if the application's health checks still pass.

Signers	Enter the name of the signers for the application's files used in the health checks. Separate multiple signers with a ";" (semicolon). By default, **Signers** contains "*Microsoft Corporation*" and "*Microsoft Windows Publisher*".
Report and Repair Mode	Select one of the following options: • **Report Only** – Collect status information about the application and show it in the Asio platform. • **Report and Repair** – Collect status information about the application and show it in the Asio platform, AND attempt to repair the application if the Secure Endpoint Agent detects that the application is non-functional.

5. Click **Save**.
6. Navigate to **Endpoints > Packages** and click **Add Package**.
7. In the Package Name field, enter a name for your package.
8. Under Available policies, click the **Devices** drop-down and locate the application policy you just created.
9. Drag and drop the policy to the Drag Policies Building Blocks Here section.



10. Click **Save**.
11. In **Endpoints > Packages**, navigate to the **Sites** tab.
12. From the list of sites, select the checkbox next to each site you want to apply the application policy to.
13. Click **Assign Package**.
14. Select the package you created for the application policy and click **Assign**.
15. If you are asked to acknowledge that updating a package will update the policies for the site, click **Update** to proceed.

After you deploy an application policy, the agent begins to collect third-party application status information from the devices associated with the sites you selected. After you've allowed a day for the policy to be deployed and run on each Windows device, you can view the collected status information from the **Endpoints > Devices** area. See *Viewing the details of devices* for more information.

NOTE: To see information about third-party applications in the Asio platform, each device's Secure Endpoint Agent must be regularly connecting to the Absolute Monitoring Center.

Unenrolling devices from Absolute Secure Endpoint

At any point, you can unenroll devices from the Absolute Secure Endpoint integration. After a device is unenrolled, its device record remains visible in the Asio platform, but no further information is collected from the device, and no device actions can be requested.

Currently, there are two ways of unenrolling devices:

- To unenroll a device or group of devices, move them to a site not integrated with Absolute Secure Endpoint
- To unenroll all devices associated with a site, disconnect the site from the Absolute Secure Endpoint integration

NOTE: Performing actions like disabling Absolute-related policies, removing Absolute-related policies from packages, or removing these packages from a site are NOT sufficient to unenroll devices. To successfully unenroll devices from the Absolute Secure Endpoint integration, you must follow the instructions in this section.

How it works

Unenrolling a device has the following effect:

- Immediately after unenrollment, the Absolute product licenses are disassociated from the device.
- On the agent's next successful connection to the Absolute Monitoring Center, the component manager (CTES) and its components are automatically removed from the device. A connection typically occurs within a few minutes, assuming the device is online.
- If there are outstanding security actions pending on a device, such as a Freeze or Crypto Wipe request, these actions are canceled.
- After a 72-hour waiting period has elapsed, the Secure Endpoint Agent is removed on the next agent connection.
- The device's database record and device information are retained, but you no longer have the ability to manage the device from the Asio platform, and its device information is no longer updated.

These unenrollment actions occur automatically and do not require additional steps on your part.

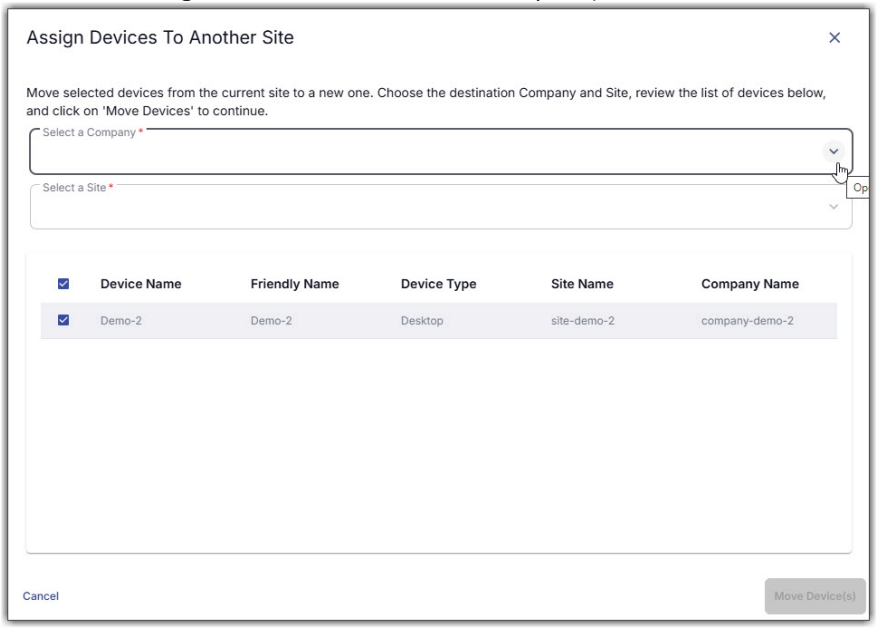
NOTE: To re-enroll devices that have previously been unenrolled from the Absolute Secure Endpoint integration, you must complete the following actions:

- *Move the devices to a site that is integrated with Absolute Secure Endpoint.*
- *Locate the site's policy for agent deployment, disable the **Absolute Secure Endpoint Agent Installation** option, enable the option again, then save the policy.*

Unenrolling a device or group of devices

1. Navigate to **Endpoints > Devices**.
2. On the Workstations & Servers page, select the checkbox next to the device(s) you want to unenroll.
   You can use the search bar to find specific devices or filter your device list by criteria like site and device group.
3. From the menu at the top of the page, select **Manage > Assign to Another Site**.

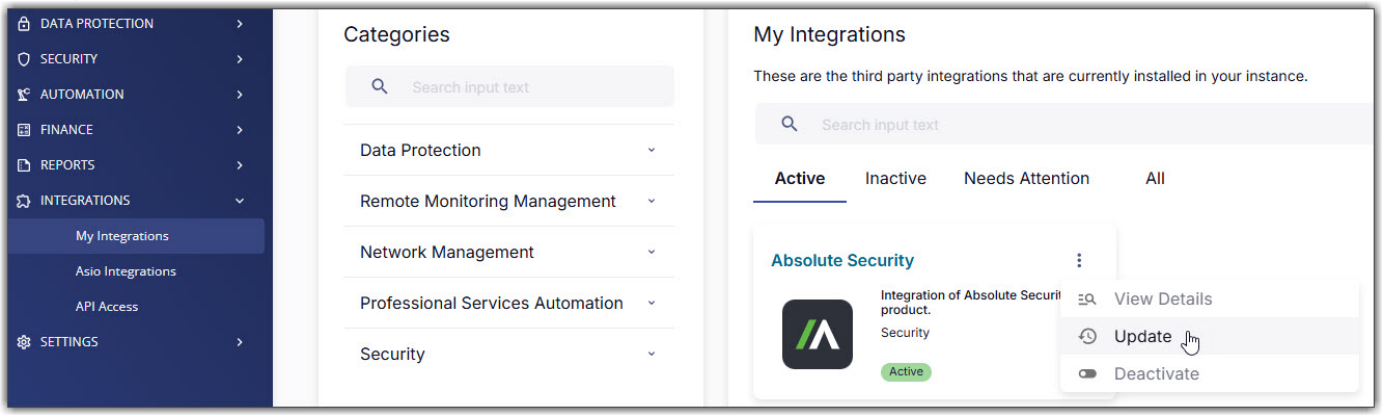
4. From the Select a Company list, choose the company containing the site you want to move the device(s) to (the site must not be integrated with Absolute Secure Endpoint).



5. From the Select a Site list, choose the destination site not integrated with Absolute Secure Endpoint.
6. Click **Move Device(s)**.
7. If you are asked to acknowledge that assigning devices to another site could take up to 5 minutes, click **Confirm** to proceed.

Unenrolling all devices associated with a site

1. Navigate to **Integrations > My Integrations**.
2. In the My Integrations panel, search for *Absolute Security* and click on it.
3. Click **Update**.



4. Click **Site Mapping**.
5. From the list of your current Asio sites, find the site containing the devices you want to unenroll. If you have a large number of Asio sites, you can search by company name and filter by mapping status.
6. Next to the site, click ✕ (Clear) to the right of your company name in the Absolute Security sites drop-down list.
7. Click **Save and Proceed**.

8. Click **Continue**.
9. Click **Complete Setup**.

Support information

For assistance with creating API members or integration setup, send an email to Help@ConnectWise.com and the ConnectWise support team can assist.

For questions or issues related to the Absolute Resilience for ConnectWise product, send an email to msp.support@absolute.com. Contacts need to be authorized contacts (either the person who registered or someone previously authorized by them) and must also provide the Absolute Account ID, which is provided in the Welcome Email sent to the registration contact and also visible to the registration contact in the Absolute Secure Endpoint Console.

Absolute Security performs routine infrastructure maintenance to ensure reliability, security, and functionality across its systems. During these periods, service may be temporarily interrupted. For detailed information on scheduled maintenance windows, refer to the Maintenance Schedule.