

# How to view security events on Windows endpoints

Click 'Security Sub-Systems' > 'Security Dashboards'

- The security dashboard is a list of all security-related events on managed Windows endpoints.
- Events are generated by different security modules in Xcitium Client Security. Events are generated by the antivirus, containment, application-control, auto-run control, and virtual desktop modules.
- Example events you will see in the security dashboard are:
  - When malware is blocked, quarantined or ignored
  - When someone changes the trust rating of a file or submits a false positive
  - When a file is run in the container
  - When files are added to, or removed from the client security file list
- There are three ways you can view the events:
  - **Event View** - Lists all events in chronological order.
  - **File View** - Groups all events by the file that generated the event.
  - **Device View** - Groups all events by the device on which they occurred.
- All views let you change the trust rating of a file, move files in or out of quarantine, and view file details and activity.

## Open and use the dashboard

- Log into Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-Systems' > 'Security Dashboards'

The actions that can be taken are similar in all three views. From here downward we use 'Event View' as the example.

<input type="checkbox"/>	DATE TIME	COMPONENTS	ACTION	OS	DEVICE NAME	FILE NAME	FILE PATH	FILE HASH	INITIAL COMODO RATING	CUR COM RATI
<input type="checkbox"/>	2019/09/04 02:01:29 PM	Containment	Run virtually	Windows	DESKTOP-K...	explorer.exe	C:\Prog...	08603B...	Trusted	Trus
<input type="checkbox"/>	2019/09/04 02:01:11 PM	Containment	Run virtually	Windows	DESKTOP-K...	rundll32.exe	C:\Wind...	2F34CC...	Trusted	Trus
<input type="checkbox"/>	2019/09/04 02:01:04 PM	Containment	Run virtually	Windows	DESKTOP-K...	explorer.exe	C:\Prog...	08603B...	Trusted	Trus
<input type="checkbox"/>	2019/09/04 02:00:58 PM	Containment	Run virtually	Windows	DESKTOP-K...	dllhost.exe	C:\Wind...	257815...	Trusted	Trus
<input type="checkbox"/>	2019/09/04 02:00:53 PM	Containment	Run virtually	Windows	DESKTOP-K...	explorer.exe	C:\Prog...	B1A662...	Trusted	Trus
<input type="checkbox"/>	2019/09/04 02:00:28 PM	Virtual Desk...	Session star...	Windows	DESKTOP-K...					
<input type="checkbox"/>	2019/09/04 02:00:24 PM	Virtual Desk...	Launched	Windows	DESKTOP-K...					
<input type="checkbox"/>	2019/09/04 02:00:24 PM	Virtual Desk...	Switched to ...	Windows	DESKTOP-K...					

## Columns

- **Date/Time** - The time at which the event occurred.
- **Components** - The CCS module that reported the event. This can be 'Antivirus', 'Containment', 'Application Control', 'Autorun Control' or 'Virtual Desktop'.
- **Action** - The response to the event. This shows how the file was handled by the component in the preceding column.
- **Severity** - The criticality of the event. The possible values are high, moderate and low.
- **File Name** - The label of the executable file affected by the action. Click the name of a file to view its details.
- **File Path** - The installation location of the executable file on the endpoint.
- **File Hash** - The SHA 1 hash value of the executable file. Hash values uniquely identify the file, even if the file name changes.
- **Initial Xcitium Rating** - The trust rating awarded by Xcitium File Lookup Service (FLS) to the file before the event.
- **Current Xcitium Rating** - The present trust rating of the file as per the Xcitium FLS.
- **Initial Admin Rating** - The trust rating of the file as manually set by the admin before the event, if any.
- **Current Admin Rating** - The most recent trust rating of the file as manually set by the admin after the event, if any.
- **Additional Info** - Provides the current status of the event or the action taken on the affected file.

## Actions

- **Action on Endpoints** - Delete the file, or restore it from quarantine on the endpoint. Applies to events where malware or auto-run items were quarantined.
- **Change rating** - Assign a new admin rating to a file. Possible ratings are:
  - **Trusted** - The file is safe and is allowed to run normally on the endpoint.

**Malicious** - The file is malware and is quarantined or deleted on the endpoint.

- **Unrecognized** - No trust rating is available for the file. Unrecognized files are automatically run in the container because there is the possibility they are malicious. Contained applications write to a virtual file system and registry, and cannot access other processes or user data. You have the option to auto-upload these files to Valkyrie for behavior testing. The tests will identify whether the file is trustworthy or malicious.

See [this wiki](#) if you want to learn more about file ratings.

- **File Details** - View complete information about the file that caused the event. You can also view a history of actions taken by the file.
- **Download Valkyrie Report** – Get a complete report on the file from Xcitium’s file analysis service, Valkyrie (pdf format).
  - Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks. The service helps Xcitium establish whether an unknown file is malicious or safe.
  - See this [help page](#) if you want to read more about Valkyrie.
- **Check Valkyrie Details** – View an online version of the Valkyrie report.
- **Export** - Save the list of events as a comma-separated values (CSV) file.

## Related topics

- [Add a Valkyrie section to a profile](#)