How to configure Valkyrie in Windows, MAC and Linux profiles

Click ‘Configuration Templates’ > ‘Profiles’ > open a Windows, Mac or Linux profile > Click ‘Add Profile Section’ > ‘Valkyrie’

- Valkyrie is a cloud-based service which tests unknown files to identify those that are malicious. Xcitium Client Security (CCS) can automatically submit to Valkyrie any unknown files found on your network. Valkyrie will test the file, award it a trust-rating, and send the results back to CCS on the endpoint.

- The software can then take actions on the file depending on its trust rating. Files rated as ‘Safe’ is allowed to run. Files rated as ‘Malware’ are, of course, quarantined or deleted.

    - Click 'Security Sub-Systems' > 'Valkyrie' to view unknown files found on your network, along with their Valkyrie trust-rating.

    - See this wiki for help to view Valkyrie results of unknown files identified on your managed devices

- The Valkyrie that comes with the free version of Endpoint Manager will only run automated tests on an unknown file. The Premium version also includes manual testing by Xcitium research technicians.
- You need to add a ‘Valkyrie’ section to an Endpoint Manager profile to activate the service on your endpoints.

- This article explains how to add and configure a Valkyrie section.

Valkyrie settings vary for Windows, MAC and Linux profiles. Use the links below to go the OS of the profile you need help with:

- Windows profile

- Mac OS and Linux profiles

Windows profile

- Log into Xcitium

- Click 'Applications’ > ‘Endpoint Manager’

- Click 'Configuration Templates' > 'Profiles'
- Open the Windows profile applied to your target devices

    - Open the 'Valkyrie' tab

      OR

    - Click 'Add Profile Section' > 'Valkyrie' (if it hasn't yet been added)

Lookup and submit files with Valkyrie - Select to enable managed devices to auto-submit unknown files to Valkyrie for analysis

Check Manual Analysis Interval – Frequency at which CCS should contact Valkyrie for the verdicts on files submitted for manual analysis. Default = every 1800 seconds (30 minutes).

Check Auto Analysis Interval - Frequency at which CCS should contact Valkyrie for the verdicts on files submitted for automatic analysis. Default = every 60 seconds.

Submit for – Select one of the following:

- **Automatic analysis** – Files are tested by Valkyrie's automated behaviour analysis systems.
- **Automatic and human-expert analysis** – Files are tested in-depth by human technicians, in addition to automatic analysis. Only available if you have Endpoint Manager Premium license. You can also obtain the service by subscribing for a stand-alone Valkyrie premium license and adding it to your EM.
    - Click 'Valkyrie Premium License' to purchase a Vallkyrie license
    - Click 'License Management' > 'License Management' > 'Licenses' > 'Add New License' and enter your Valkyrie license key to activate Valkyrie Premium on your EM portal
    - See this wiki for help to manage EM licenses

Enable Auto - Whitelisting if NO suspicious activities detected… - The files are added to your local white-list of trusted files if Valkyrie finds they are not malicious.

Do not lookup and submit files to Valkyrie if file lookup service returns an error - When an unknown file is detected, Xcitium Client Security first checks the file lookup server (FLS) to see if there is a 'Safe' or 'Malicious' verdict on the file. If not, then it is confirmed as unknown and submitted to Valkyrie for testing. This option will abort the Valkyrie submission if there is an issue with the initial FLS check, meaning no verdict is provided. CCS will keep retrying the FLS to get the initial verdict.

Submit Metadata - Metadata is general information about the file, including file source, author, and date of creation. Select this option to send metadata along with the file itself.

Submit When – Choose between:

- **Immediately** – Unknown files are submitted to Valkyrie as soon as they are discovered.
- **Schedule Analysis** – Set a date and time when you want to submit all unknown files. All unknown files are submitted as a batch on the date/time you specify.
- Click 'Save' for your settings to take effect.

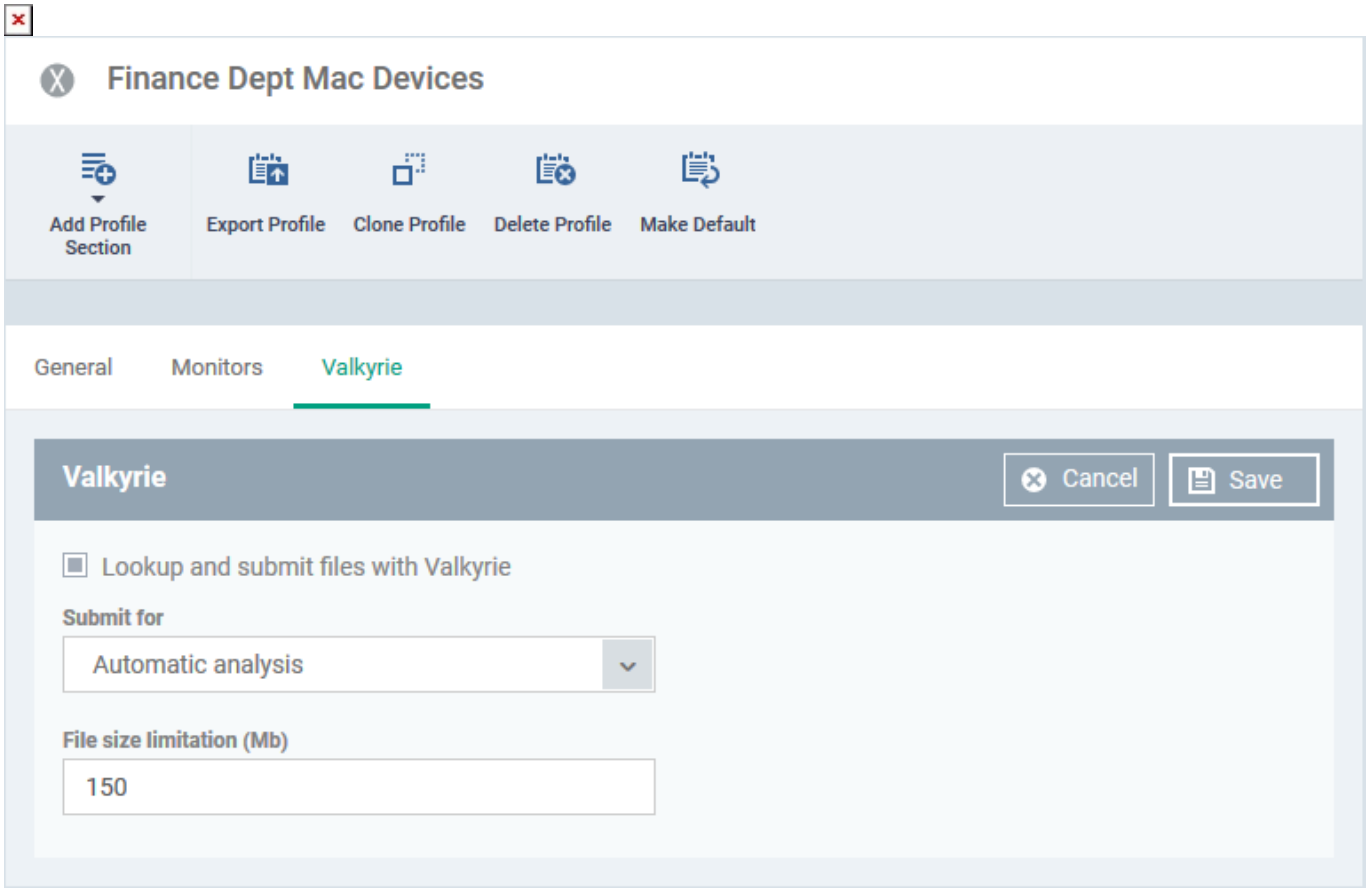
Mac OS and Linux profiles

The options are similar in Mac OS and Linux profiles

- Click 'Configuration Templates' > 'Profiles'
- Open the Mac or Linux profile applied to your target devices
    - Open the 'Valkyrie' tab

      OR

- Click 'Add Profile Section' > 'Valkyrie' (if it hasn't yet been added)

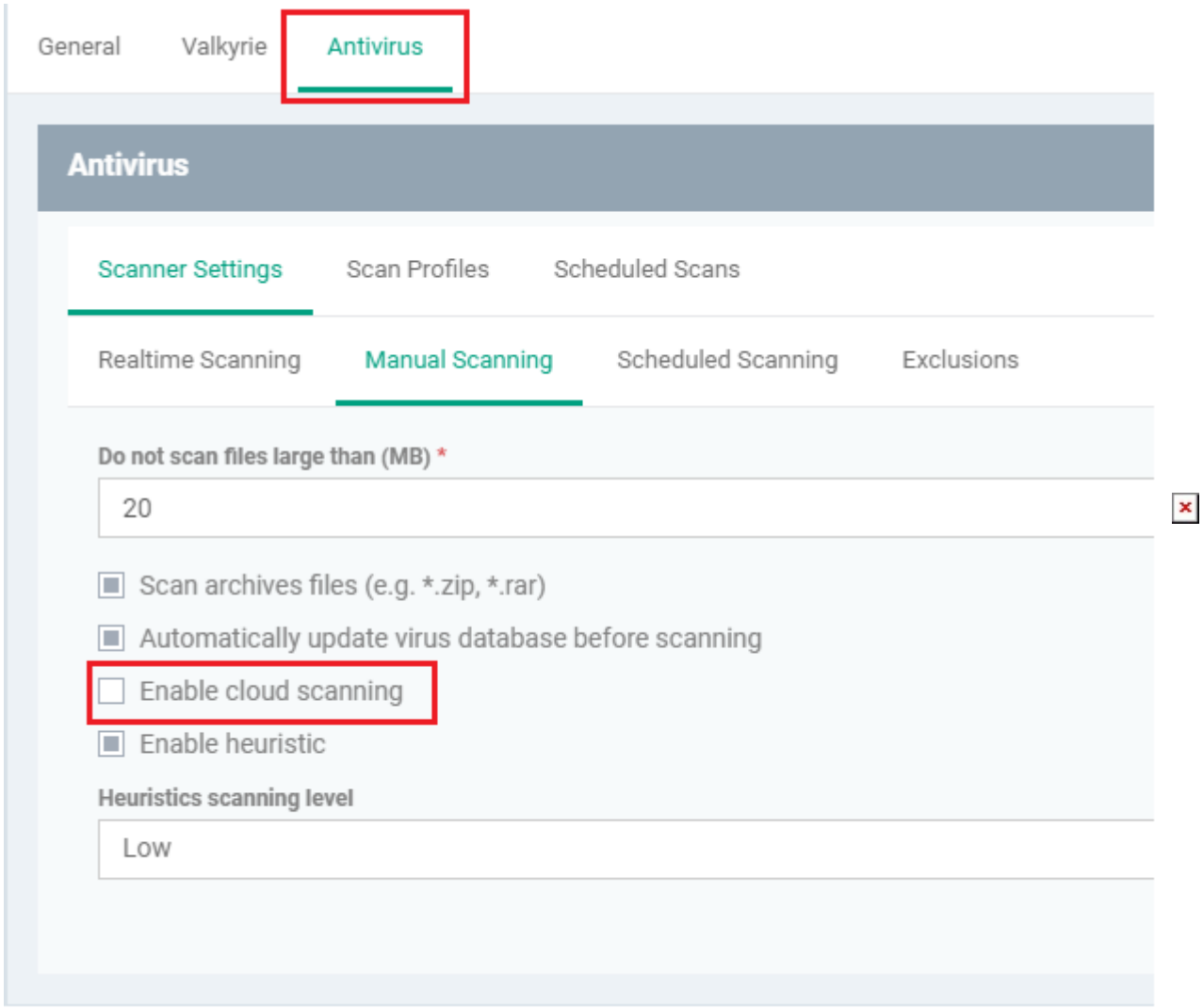


Lookup and submit files with Valkyrie - Select to enable managed devices to auto-submit unknown files to Valkyrie for analysis

Submit for – Select one of the following:

- **Automatic analysis** – Files are tested by Valkyrie's automated behaviour analysis systems.
- **Automatic and human-expert analysis** – Files are tested in-depth by a human technician. Only available if you have Endpoint Manager Premium license. You can also obtain the service by subscribing for a stand-alone Valkyrie premium license and adding it to your EM.
    - Click 'License Management' > 'License Management' > 'Licenses' > 'Add New License' and enter your Valkyrie license key to activate Valkyrie Premium on your EM portal
    - See this wiki for help to manage EM licenses
- **File Size Limitations (MB)** – Specify the maximum file size that should be uploaded to Valkyrie. Default = 150 MB.
- Click 'Save' for your settings to take effect.

Note for Linux devices. You also need to enable cloud scanning in the antivirus section of the profile for Valkyrie to work:


General
Valkyrie
Antivirus
Antivirus
Scanner Settings
Scan Profiles
Scheduled Scans
Realtime Scanning
Manual Scanning
Scheduled Scanning
Exclusions
Do not scan files large than (MB) *
20
Scan archives files (e.g. *.zip, *.rar)
Automatically update virus database before scanning
Enable cloud scanning
Enable heuristic
Heuristics scanning level
Low