How to get a threat assessment report on customer endpoints

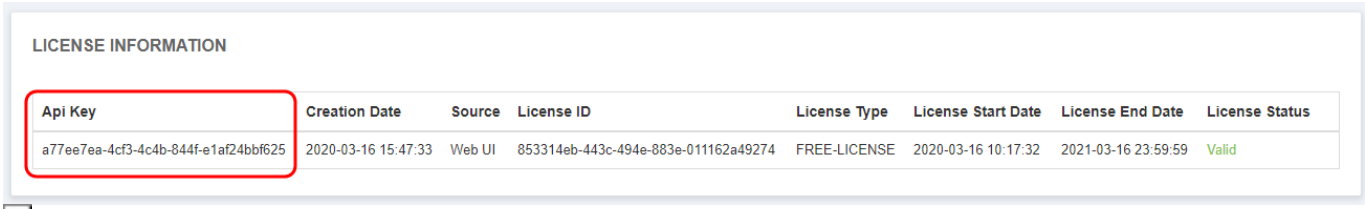
The customer assessment procedure lets you quickly evaluate the security of your managed Windows endpoints. The procedure generates a report which summarizes the following:

- **Device Vulnerability** – List of operating system and 3rd party patches that need to be installed
- **Endpoint Security** – Details of malware and unknown files found on devices.
- **Phishing and Internet Risks** – Tests whether your endpoints can connect to harmful websites.
- **Xcitium Agents** – An overview of which Xcitium agents are installed on your endpoints.

Prerequisites

You must login to Valkyrie and get the API key in order to run the scan. The scan itself is run by Valkyrie, our cloud-based threat analysis service.

- Login at https://valkyrie.xcitium.com with the same UN/PW as you use for Xcitium.
- Click ‘Settings’ > ‘Account’
- Copy the API key string from the ‘License Information’ table:



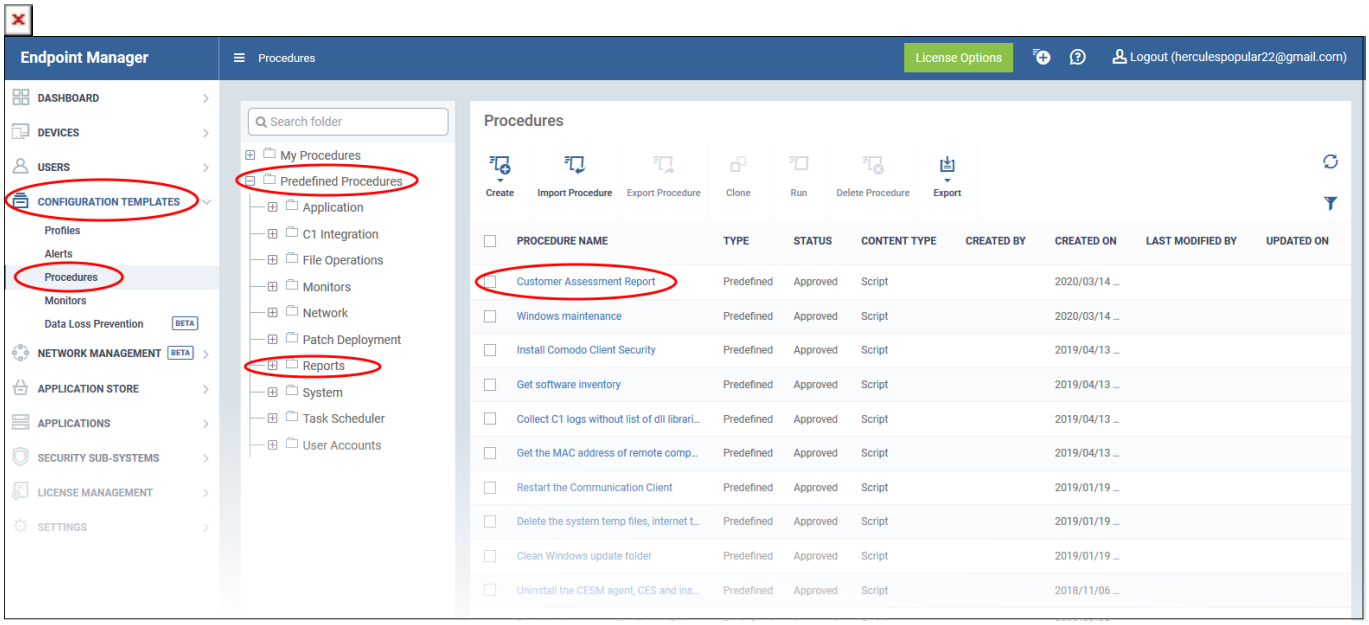
LICENSE INFORMATION

Api Key	Creation Date	Source	License ID	License Type	License Start Date	License End Date	License Status
a77ee7ea-4cf3-4c4b-844f-e1af24bbf625	2020-03-16 15:47:33	Web UI	853314eb-443c-494e-883e-011162a49274	FREE-LICENSE	2020-03-16 10:17:32	2021-03-16 23:59:59	Valid

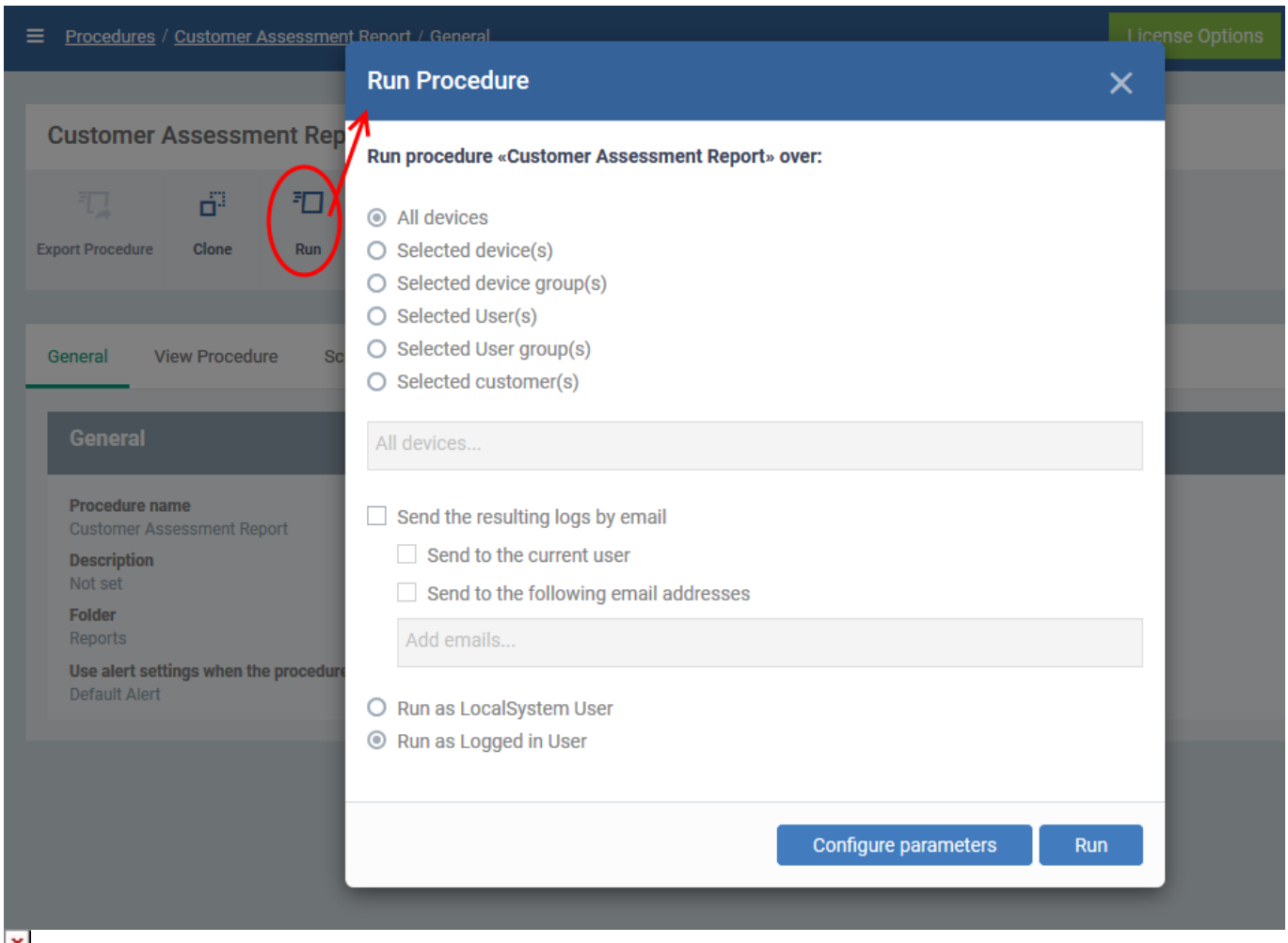
- You will need to paste the key into Endpoint Manager when setting up the scan.

Run a threat assessment report

- Login to Xcitium
- Click ‘Configuration Templates’ > ‘Procedures’
- Click ‘Predefined Procedures’ > ‘Reports’
- Click 'Customer Assessment Report'



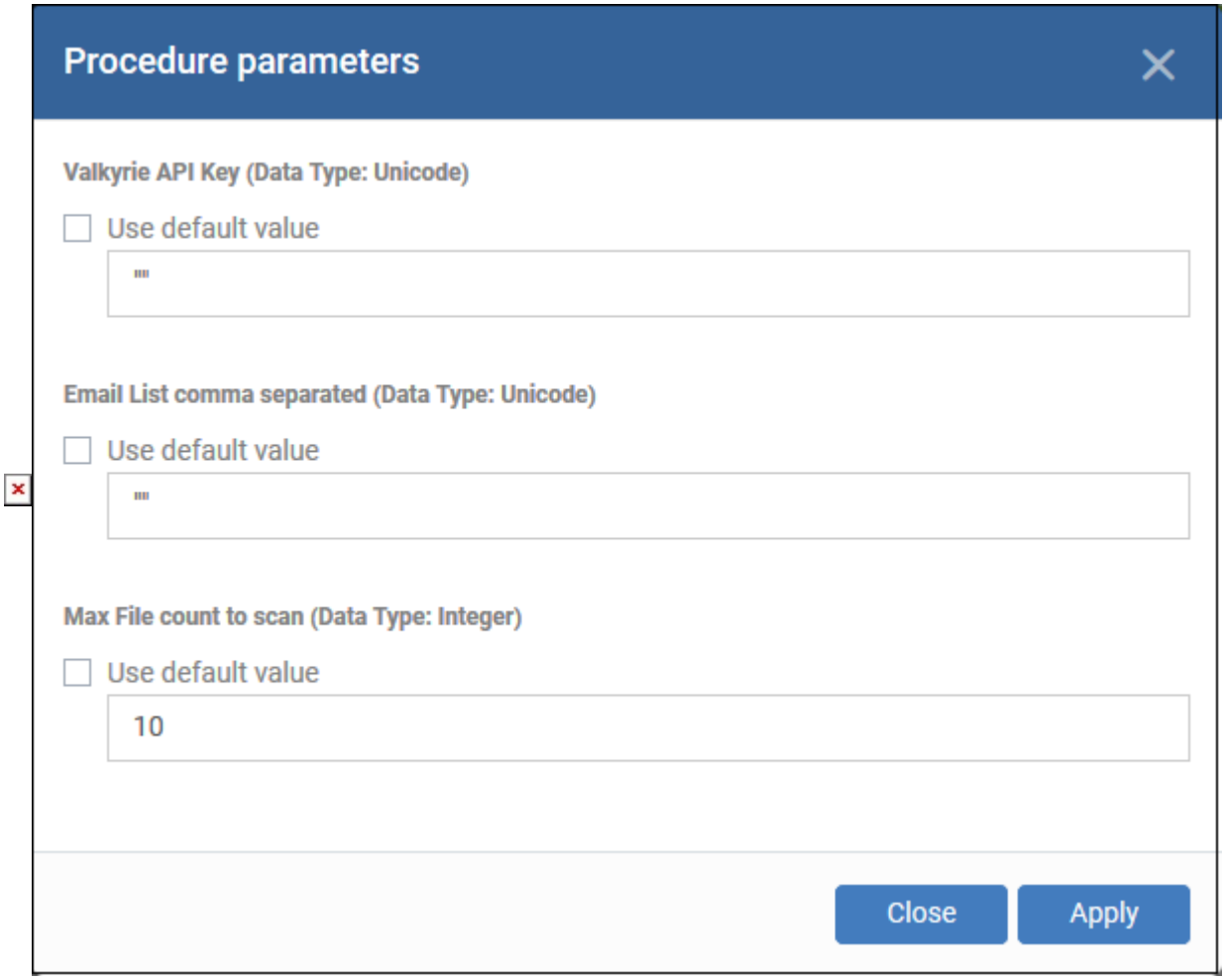
- Click 'Run' in the procedure screen



- Select the devices on which you want to run the procedure. You can also run the procedure on device groups, users, user groups, and customers.

- **Send to current user** - Procedure results are sent to the admin who is currently logged into Endpoint Manager.
- **Send to the following email addresses** - Add email addresses to whom log results should be sent.
- **Run as Local System User / Run as Logged in user** - Choose the user account under which the scan should run.

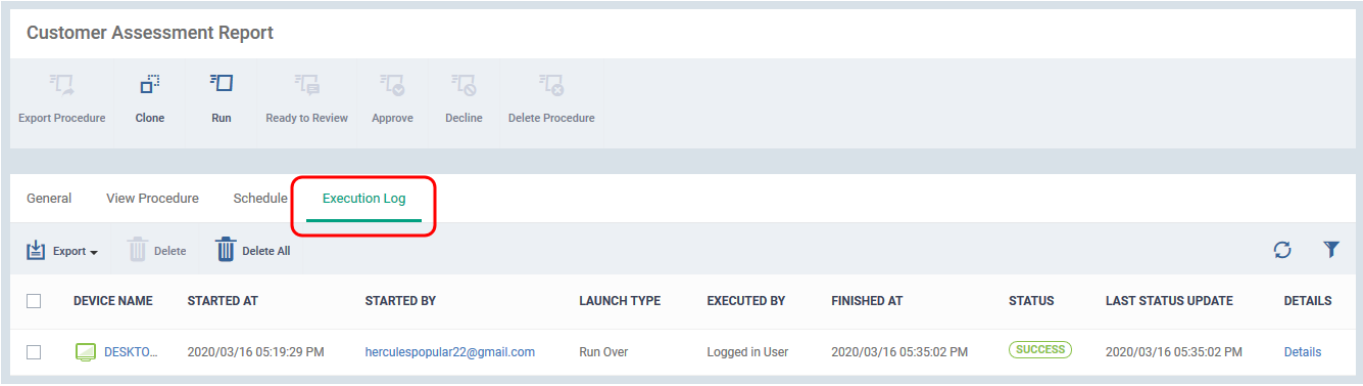
Configure parameters



- **Valkyrie API key** – Paste the API code from your Valkyrie account. See the prerequisites if you need help to get this code.
- **Email List** – Report recipients. Addresses you add here will receive a pdf version of the report over email. You can enter multiple addresses separated by a comma.
- **Max File count to scan** – The procedure scans executables in important locations on the target devices. Enter the total number of files you would like the scan to check. The max is 50.

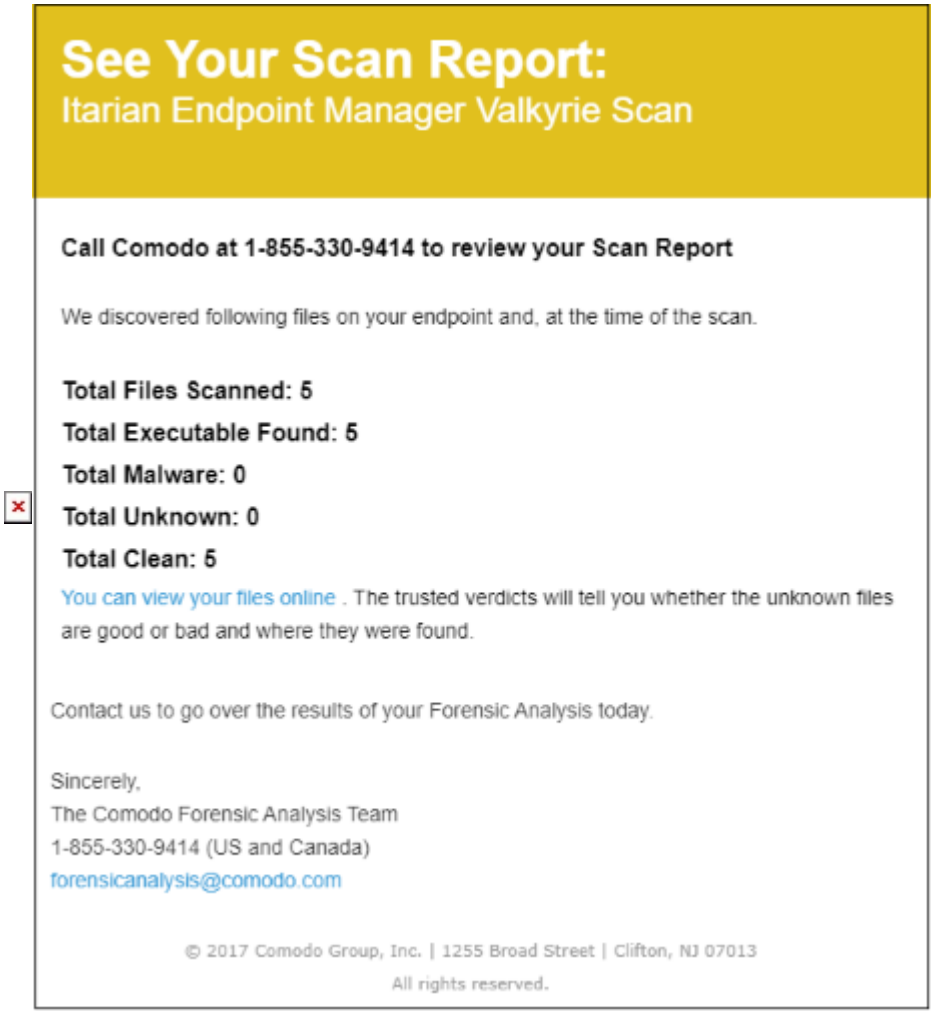
Click 'Apply' then 'Run' in the procedure dialog.

The command is immediately sent to the selected endpoints. Click 'customer assessment report' link in the procedures screen, then 'Execution Log' to view the status of the scan.



View scan results

A scan report is sent to the recipients you added to the email list:



See Your Scan Report:
Itarian Endpoint Manager Valkyrie Scan

Call Comodo at 1-855-330-9414 to review your Scan Report

We discovered following files on your endpoint and, at the time of the scan.

Total Files Scanned: 5
Total Executable Found: 5
Total Malware: 0
Total Unknown: 0
Total Clean: 5

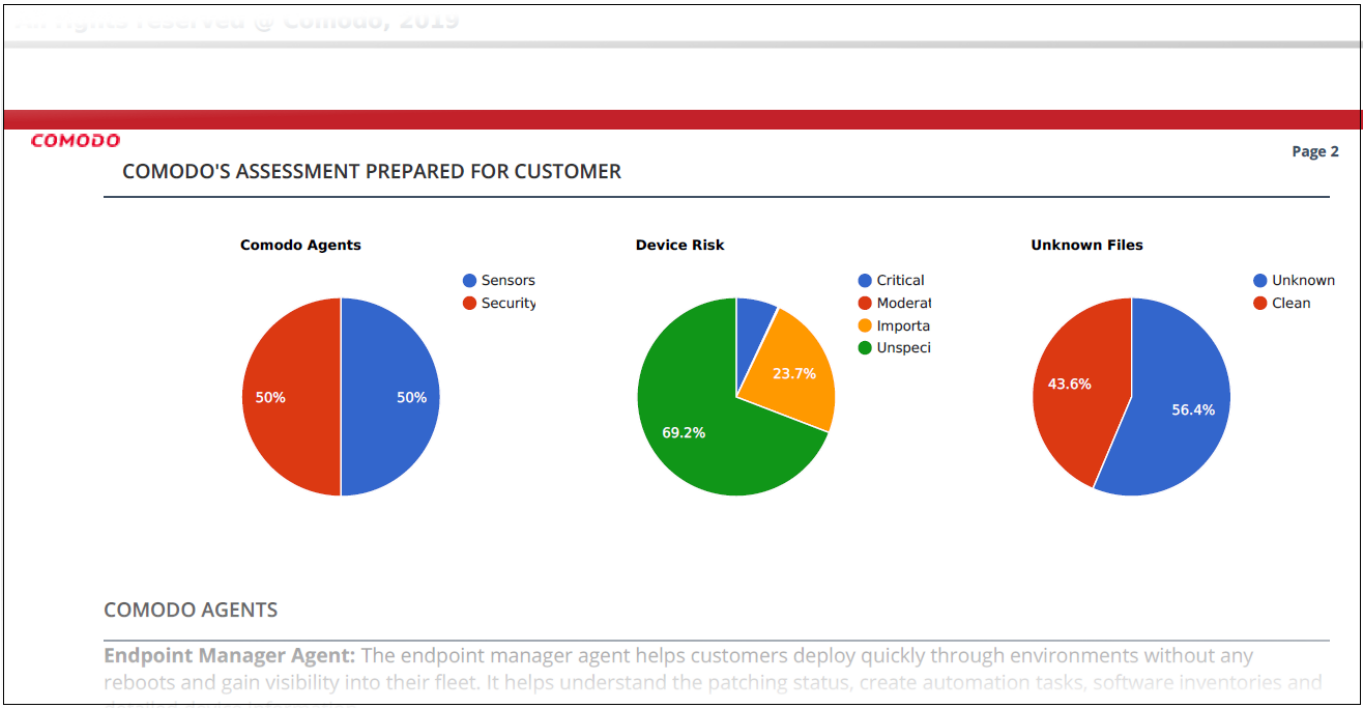
You can view your files online . The trusted verdicts will tell you whether the unknown files are good or bad and where they were found.

Contact us to go over the results of your Forensic Analysis today.

Sincerely,
The Comodo Forensic Analysis Team
1-855-330-9414 (US and Canada)
forensicanalysis@comodo.com

Click 'You can view your files online' to see results on the Valkyrie website. Click here if you want to learn more about Valkyrie.

Download the PDF report from the mail:



The report is divided into four sections:

Xcitium agents – The Xcitium clients installed on the endpoints.

- Sensors / Endpoint Manager agent = Xcitium Communication Client
- Security = Xcitium Client Security

Device Vulnerability Risk – Details about OS and third-party patches that should be installed on the devices.

Endpoint Security Risk – Details about malware and unknown file types found on scanned devices. Unknown files are those that do not yet have a trust rating of definitely safe nor definitely malware.

Phishing and Internet Risks – Shows whether your endpoints are protected from harmful websites in various categories. 'Not protected' means the scanner was able to make a connection to a site in the category from the endpoint.

Our Secure Internet Gateway product provides complete, DNS-based protection from harmful sites. Log into Xcitium > Click 'Applications' > 'Secure Internet Gateway' to get started.

Further reading

Configure and run procedures on managed devices

How to patch endpoints using Endpoint Manager

How to run virus scans on endpoints

How to manage unknown and malicious files on your devices

How to block harmful websites for your users

How to install the security client on devices