ReversingLabs A1000

This app supports using ReversingLabs Advanced File Analysis to 'detonate file' on the A1000 Advanced Malware Analysis Appliance.

The A1000 appliance is a powerful threat detection and file analysis platform that integrates other ReversingLabs technologies (TitaniumCore - the automated static analysis solution, and TitaniumCloud File Reputation Service) to provide detailed information on each file's status and threat capabilities.

The A1000 makes it easy to upload multiple samples for analysis. It can process, unpack, and classify them in a matter of milliseconds, and display detailed analysis reports. Historical analysis results are preserved in a database to enable in-depth searching, and malware samples are continually reanalyzed to ensure the most up-to-date file reputation status.

The A1000 relies on several threat classification methods, including YARA rules and ReversingLabs hashing algorithm (RHA) that classifies files based on their functional similarity.

For more information, consult the official product website.

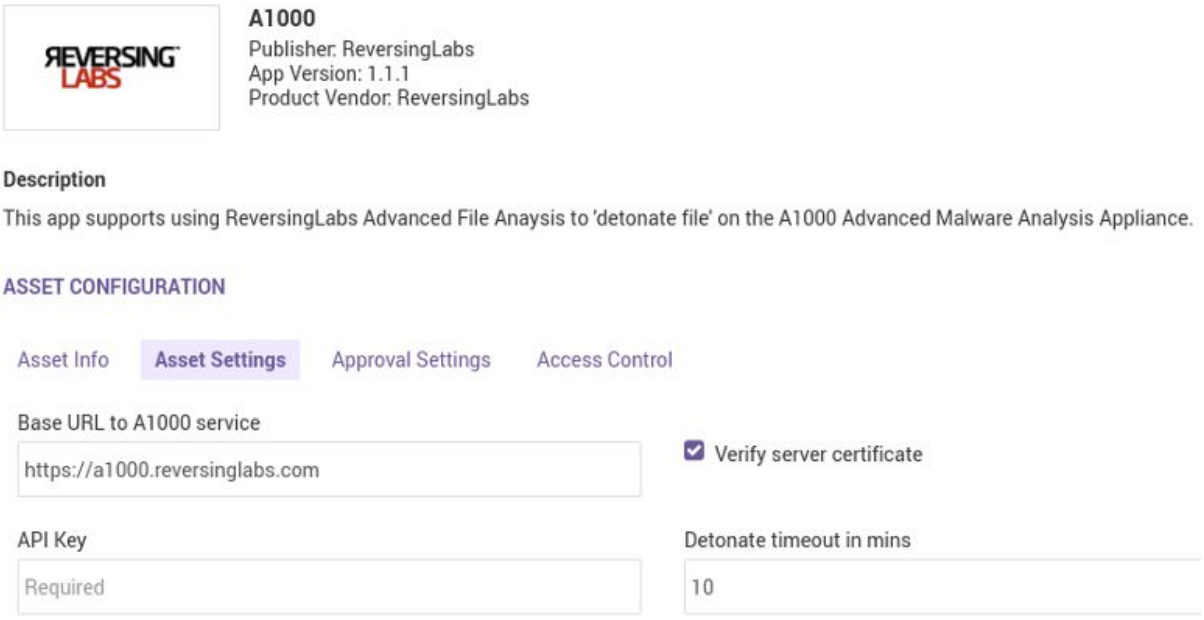
Configuration Variables

The configuration variables in the table below are required for this app to operate on A1000. These are specified when configuring an asset in Phantom.

VARIABLE	REQUIRED	TYPE	DESCRIPTION
verify_server_cert	required	boolean	If selected, plugin will accept self-signed certificates.
api_key	required	string	API Key obtained from A1000 used for authentication.
base_url	required	string	Base URL to A1000 instance.
timeout	required	numeric	Analysis timeout in minutes.

How to Configure the App

Access the Asset Settings tab on the Asset Configuration page. The variables described in the previous section are displayed in this tab.



The "Base URL" field requires the host address of the A1000 appliance. Select the "Verify server certificate" checkbox to allow only commercial certificates, not the self-signed certificates.

The "API Key" contains the the authentication token obtained from an A1000 instance used for accessing the A1000 REST API.

The "Detonate timeout" variable defines how long the app should wait for the results from the A1000 appliance.

Supported Actions

detonate file - Analyze the file in the A1000 Advanced Malware Analysis Appliance and retrieve the analysis results.

test connectivity - Validate the asset configuration for connectivity. This action logs into the device to check the connection and credentials.