SMA User Interfaces

The Cisco Secure Malware Analytics platform provides a suite of user interfaces designed to accommodate the distinct needs of administrators and security analysts. Understanding the purpose of each interface is key to effectively managing the appliance and analyzing malware.

Interface	Description
Admin TUI (Text-based)	A text-based console interface accessible via a command-line connection (like SSH). It provides a more limited set of administrative functions compared to the OpAdmin, focusing on essential, low-level tasks such as initial setup, network troubleshooting, and password resets. It is often used when the web-based UI is unavailable or for more advanced troubleshooting. For more information, please refer to the Admin TUI.
OpAdmin (Web-based)	A comprehensive graphical interface for managing and configuring the Secure Malware Analytics appliance. It is used for tasks like system maintenance, network settings, and license management. This interface is accessed via a web browser and is the primary tool for most administrative tasks. For more information, please refer to the OpAdmin.
Portal UI (Web-based)	The primary user-facing portal where analysts and end-users submit files for analysis, view analysis reports, and manage their submitted samples. This is where users interact with the core functionality of the platform, such as viewing threat intelligence, searching for malware reports, and managing user accounts. This portal also provides robust APIs for automating tasks such as submitting samples for analysis, querying for malware intelligence, and retrieving curated threat intelligence feeds. The help for this interface, including API documentation, is available directly within the product and is not public.

Note LDAP authentication is available for Admin TUI and the OpAdmin. RADIUS authentication is available for the Secure Malware Analytics Application UI.

• Secure Malware Analytics Portal, on page 3

Admin TUI

The **Admin TUI** interface is used to configure the network interfaces. The Admin TUI is displayed when the Secure Malware Analytics Appliance successfully boots up.

Reconnecting to the Admin TUI

The Admin TUI remains open on the console and is accessed either by attaching a monitor to the appliance or, if CIMC is configured, via remote KVM.

Note CIMC is not supported on the Secure Malware Analytics M5 Appliance server.

To reconnect to the Admin TUI, ssh into the Admin IP address as the user **threatgrid**.

The required password is either the initial, randomly generated password, which is visible initially in the Admin TUI, or the new Admin password you create during the first step of the OpAdmin Configuration (see the *Cisco Secure Malware Analytics Appliance Getting Started Guide*).

Threat Grid Shell (tgsh)

The Threat Grid Shell (tgsh) is an administrator's interface that is used to execute commands (including destroy-data and forced backup), and for expert, low-level debugging. To access tgsh, choose **CONSOLE** in the Admin TUI.

Note The OpAdmin uses the same credentials as the Secure Malware Analytics user, so any password changes/updates made via tgsh will also impact the OpAdmin.

Caution Network configuration changes made with tgsh are not supported unless specifically directed by Secure Malware Analytics support; the OpAdmin or Admin TUI should be used instead. The Wipe Appliance operation is now activated within recovery mode tgsh rather than the bootloader menu.

OpAdmin

The OpAdmin is the Secure Malware Analytics Appliance administrator's main configuration interface. It is a Web portal that can be used once an IP address has been configured on the Secure Malware Analytics Appliance Admin interface.

Much of the Secure Malware Analytics Appliance configuration can ONLY be done via the OpAdmin, including licenses, email host, and SSL certificates.

Note The initial setup and configuration wizard is described in the Cisco Threat Grid Appliance Getting Started Guide.

Components of OpAdmin

The following sections provide you with the necessary details to configure using the OpAdmin.

- Home
- Configuration
- Status
- Operations
- Support

Secure Malware Analytics Portal

The Secure Malware Analytics user interface application is available as a cloud service, and is also installed on Secure Malware Analytics Appliances. There is no communication between Secure Malware Analytics Cloud service and the Secure Malware Analytics Portal that is included with a Secure Malware Analytics Appliance.

Figure 1: Secure Malware Analytics Portal UI