Field Installer

Using the Field Installer

This procedure details how to create a bootable USB drive, and use it to restore your Secure Malware Analytics Appliance to its factory condition.

Caution This process will automatically wipe all data and installed software on the appliance.

Before you begin

The Field Installer image is large, so it is broken into chunks for distribution. Downloading and re-assembling the image requires a specialized tool and an index file.

Note The Field Installer is a self-contained **ISO file** that contains the entire Secure Malware Analytics operating system.

Contact Cisco Support to obtain the Field Installer index file (with the `.caibx` extension) and the specific download instructions. Do not attempt to acquire this tool outside of the formal Cisco Support process.

Support will provide the following version-specific details:

- The current file name (e.g., `field-installer-X.Y.Z.iso`) and its corresponding index file (`.caibx` file).
- The required **SHA256 checksums** for verification.

Ensure you have the **desync tool** installed, which is used to download chunks and re-assemble the final ISO.

- The tool is available at `https://github.com/folbricht/desync`.

Procedure

Step 1 **Download and Assemble the ISO:** Execute the following command, replacing the bracketed placeholders with the current file names provided by Cisco Support:

Example:

```
$HOME/go/bin/desync extract -k \
  -s s3+https://s3.amazonaws.com/sma-appliance-airgap-update \
  [field-installer-X.Y.Z.iso.caibx] [field-installer-X.Y.Z.iso]
```

To resume an interrupted download, run the same command again.

Tip
Schedule the download during off-peak times (e.g., after office hours) to minimize bandwidth impact.

Step 2 **Prepare the Bootable USB Drive:** Use a USB device that is at least 46 GB in size, as the resulting ISO file is large (the 2.19.6 version is approximately 46 GB). Once the ISO is constructed, follow the same procedure used for airgap updates to write the image to a bootable USB device.

Step 3 **Reimage the Appliance:**

Action	Details
Shut Down the Appliance	Properly shut down the Secure Malware Analytics Appliance.
Insert USB Drive	Insert the prepared bootable USB drive into the appliance.
Access the Boot Menu	Power on or reboot the appliance. When the **BIOS screen** appears, press **F6** on the console to open the Boot Menu.
Boot from USB	Select the USB device from the boot menu and hit **Enter**.
Installation Starts	The system automatically executes the payload, beginning the **wiping and reimaging process**. The installer runs automatically without a UI.
Remove USB	The process is complete when the system prompts you to **remove the USB drive**.
Reboot	Confirm the prompt by pressing **Y** (or 'yes') and then **Enter**. The appliance will reboot and successfully boot into the newly installed operating system payload.

Once the appliance successfully reboots, it will be in its factory default state with a fresh operating system installation. All previous network settings, cluster configuration, and user data have been permanently erased.

What to do next

You must now proceed with the initial setup and configuration of the Secure Malware Analytics Appliance as outlined in this guide (starting from the network setup section) to return the appliance to a usable state.