Troubleshoot SEG or SWA Factory Reset Using enablediag

Contents

Introduction

Prerequisites

Components Used

Problem

Solution

Related Information

Introduction

This document describes how to reset the SEG or SWA hardware appliances, if you use the **enablediag** authentication method.

Prerequisites

Components Used

- Cisco Secure Email Gateway (SEG) AsyncOS 14.2.2 or later versions
- Cisco Secure Web Appliance (SWA) AsyncOS 14.5.1-008 or later versions

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

The SEG/SWA is inaccessible through WebUI or network if an upgrade fails or services get corrupted, this leaves a RMA as the only option. This capability allows you to reset the appliance to factory default settings and avoid the need for an RMA.

Solution

1. Access the SEG/SWA through the console or an Ethernet terminal session.

2. Log in with these credentials:

- Username:enablediag
- Password: admin password

3. Run the **resetappliance** command.

4. Select the required previous version option from the displayed list.

5. Confirm the reset operation.

6. Wait for the appliance to clear all settings to system defaults, including removal of network IP settings.

7. Verify that the SEG/SWA is returned to a clean, unconfigured state and is ready for setup.

Complete sample output from the **resetappliance** process.

```
login: enablediag
> Log in with the enablediag account and provide the appropriate administrator credentials when prompte

AsyncOS 14.2.2 for Cisco C395 build 004

Welcome to the Cisco C395 Email Security Appliance

Available Commands:
help -- View this text.
quit -- Log out.
service -- Enable or disable access to the service system.
network -- Perform emergency configuration of the diagnostic network interface.
clearnet -- Resets configuration of the diagnostic network interface.
ssh -- Configure emergency SSH daemon on the diagnostic network interface.
clearssh -- Stop emergency SSH daemon on the diagnostic network interface.
tunnel -- Start up tech support tunnel to IronPort.
print -- Print status of the diagnostic network interface.
resetappliance -- Reset appliance reverts the appliance to chosen build with factory default settings w
reboot -- Reboot the appliance.

S/N ABC12345678-00000000
Service Access currently disabled.
ironport.example.com> resetappliance

This command will revert the appliance to a previous version of AsyncOS.

Warning: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process and should be backed up:
 - current system configuration file
 - all log files
 - all reporting data (including saved scheduled and archived reports)
 - any custom end user notification pages
 - current network settings

Reverting the device will cause a reboot to take place.
```

```
After rebooting, the appliance reinitializes itself and reboots
again to the desired version, with default system configuration.

Would you like to continue [Y/N]?
y
Are you sure you want to continue [Y/N] ?
y
This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all IronPort Spam Quarantine message and end-user safelist/blocklist data

Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords unmasked)
- exported the IronPort Spam Quarantine safelist/blocklist database
  to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots
again to the desired version.

    Available versions
    ==================
 1. 13.5.3-010
 2. 13.5.4-038
 3. 14.2.2-004
Please select an AsyncOS version [2]: 3
Do you want to continue? [N]> y

Are you sure you want to continue? [N]> y
You have selected "14.2.2-004".
mv: rename /data/pub/configuration/revert_netconfigwith_v6.xml to /data/pub/configuration/revert_netcon
Reverting to "shipping" preconfigure install mode.
ls: /data/db/features/*.revert: No such file or directory

AsyncOS Amnesiac (cuau0)

login: admin
> Log in with the admin account and provide the appropriate administrator credentials when prompted

AsyncOS 14.2.2 for Cisco C395 build 004
Welcome to the Cisco C395 Email Security Appliance

NOTE: This session will expire if left idle for 30 minutes. Any uncommitted
configuration changes will be lost. Commit the configuration changes as soon
as they are made.

Warning!
You are currently using a demonstration certificate(Cisco ESA Certificate)
which is not secure and is not recommended for general use. Create or import
a certificate using the certconfig > CERTIFICATE option.
The features/services currently using the demonstration certificate are:
default destination controls entry, LDAPS
Please run "systemsetup" or "sethostname" then "commit" before sending mail.
ironport.example.com>
```

Related Information

- Cisco Email Security
- Cisco Secure Email Gateway Launch Page to Support Guides
- Secure Web Appliance Launch Page