

Setzen Sie die ESA/SMA/WSA auf die werkseitige Standardkonfiguration zurück.

Inhalt

[Einführung](#)

[Setzen Sie die ESA/SMA/WSA auf die werkseitige Standardkonfiguration zurück.](#)

[ESA/SMA](#)

[WSA](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie eine Cisco E-Mail Security Appliance (ESA), Cisco Security Management Appliance (SMA) oder Cisco Web Security Appliance (WSA) auf die werkseitige Standardkonfiguration zurückgesetzt wird.

Setzen Sie die ESA/SMA/WSA auf die werkseitige Standardkonfiguration zurück.

Manchmal kann ein Kunde verlangen, dass die Appliance auf die werkseitige Standardkonfiguration zurückgesetzt wird. In der Regel wird dies angefordert, nachdem eine Appliance-Evaluierung abgeschlossen ist oder ein Kunde eine ersetzte Appliance aus Gründen der Retouren genehmigung (Return Material Authorization, RMA) oder eines Upgrades zurückgibt. Es kann daher erforderlich sein, die Appliance auf die werkseitige Standardkonfiguration zurückzusetzen, um Kundeninformationen zu entfernen.

Vorsicht: Die in diesem Dokument beschriebenen Befehle geben alle Netzwerkeinstellungen auf die Werkseinstellungen zurück. Dadurch wird die Verbindung möglicherweise von der CLI getrennt, Dienste, die Sie für die Verbindung mit der Appliance verwendet haben (z. B. File Transfer Protocol (FTP), Telnet, Secure Shell (SSH), HTTP und HTTPS), werden deaktiviert und die zusätzlichen Benutzerkonten, die Sie mit dem Befehl **userconfig** erstellt haben, werden sogar entfernt. Verwenden Sie diese Befehle nicht, wenn Sie über die serielle Schnittstelle oder die Standardeinstellungen des Verwaltungsports über das Standard-Benutzerkonto "Admin" keine Verbindung zur CLI herstellen können.

Durch die Verwendung dieser Befehle werden auch alle verfügbaren Versionen von AsyncOS entfernt, auf die noch mit dem Befehl **zurücksetzen** zugegriffen werden kann. Die einzige Version von AsyncOS, die verbleibt, ist die Version, die derzeit ausgeführt wird. **WICHTIG: Mit dem Befehl "Revert" wird alles von der Appliance gelöscht: Der Befehl REVERT der ESA setzt die Appliance auf eine frühere Version von AsyncOS zurück.**

WARNUNG: Es ist äußerst destruktiv, das Gerät zurückzusetzen.

Diese Daten werden dabei zerstört:

- alle Konfigurationseinstellungen (einschließlich Listener)
- alle Protokolldateien

- alle Datenbanken (einschließlich Nachrichten in Virus-Outbreak- und Policy-Quarantäne)
- alle Berichtsdaten (einschließlich gespeicherter geplanter Berichte)
- alle Nachrichtenverfolgungsdaten
- alle IronPort Spam Quarantine-Nachrichten und Endbenutzer-Daten zu Listen sicherer Absender/Sperrlisten

Nur die Netzwerkeinstellungen bleiben erhalten.

Bevor Sie diesen Befehl ausführen, stellen Sie Folgendes sicher:

- die Konfigurationsdatei dieser Appliance (mit nicht maskierten Kennwörtern) gespeichert
- exportiert die Datenbank der IronPort Spam Quarantine Safelist/Sperrliste auf einen anderen Computer (falls zutreffend)
- Warten Sie, bis die Mailwarteschlange leer ist.

Wenn Sie das Gerät zurücksetzen, wird das Gerät sofort neu gestartet. Nach einem Neustart wird die Einheit neu initialisiert und wieder zur gewünschten Version neu gestartet.

Vorsicht: WSA Revert-Befehl

Mit diesem Befehl wird die Appliance auf eine frühere Version von AsyncOS zurückgesetzt.

WARNUNG: Es ist äußerst destruktiv, das Gerät zurückzusetzen.

Diese Daten werden während des Prozesses vernichtet und sollten gesichert werden:

- aktuelle Systemkonfigurationsdatei
- alle Protokolldateien
- alle Berichtsdaten (einschließlich gespeicherter geplanter und archivierter Berichte)
- alle benutzerdefinierten Endbenutzer-Benachrichtigungsseiten

Mit diesem Befehl werden die aktuellen Netzwerkeinstellungen beibehalten.

Wenn Sie das Gerät zurücksetzen, wird das Gerät sofort neu gestartet. Nach einem Neustart initialisiert sich die Appliance selbst neu und startet erneut mit der vorherigen Systemkonfiguration zur gewünschten Version.

Tipp: Bevor Sie fortfahren, empfiehlt Cisco, den Befehl **saveconfig** oder **mailconfig** auszuführen, um gegebenenfalls eine Kopie der aktuellen Appliance-Konfiguration beizubehalten. Die Appliance-Konfiguration wird nach einem erfolgreichen Zurücksetzen entfernt und kann nicht wiederhergestellt werden.

ESA/SMA

Gehen Sie wie folgt vor, um eine Cisco ESA oder SMA auf die werksseitige Standardkonfiguration zurückzusetzen:

Hinweis: Cisco empfiehlt, dass Sie über Konsolenzugriff auf die Appliance verfügen, bevor Sie den Befehl **systemsetup** ausführen, um Netzwerkkonfigurationen zu entfernen.

1. Geben Sie den **diagnostischen** Befehl auf der ESA oder SMA ein, und wählen Sie dann den **RELOAD**-Vorgang aus.

2. Geben Sie **Y** ein, wenn Sie gefragt werden, ob Sie fortfahren möchten, und geben Sie dann **Y** erneut ein, um den Vorgang abzuschließen.

Bei diesem Prozess wird die Appliance-Konfiguration zurückgesetzt, und alle Kundendaten (z. B. Konfiguration, Protokolle, Berichte und Benutzerinformationen) werden entfernt. Zu diesem Zeitpunkt wird das Admin-Kennwort auf den Standard-*Ironport* zurückgesetzt:

```
myesa.local> diagnostic
```

```
Choose the operation you want to perform:
```

- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.

```
[ ]> RELOAD
```

```
This command will remove all user settings and reset the entire device.
```

```
If this is a Virtual Appliance, all feature keys will be removed,  
and the license must be reapplied.
```

```
Are you sure you want to continue? [N]> y
```

```
Are you *really* sure you want to continue? [N]> y
```

```
Reverting to "testing" preconfigure install mode.
```

Die Appliance schließt zu diesem Zeitpunkt die aktuelle Verbindung und startet neu.

3. Um die Netzwerkkonfiguration zu entfernen, müssen Sie den Systemeinstellungsassistenten erneut mit dem Befehl **systemsetup** ausführen. Gehen Sie durch den Assistenten, und geben Sie bei Bedarf generische Informationen ein (z. B. *192.168.42.42* für die Management-IP-Adresse, einen generischen Hostnamen und eine generische *admin@example.com* für die E-Mail-Adresse).
4. Geben Sie nach Abschluss des Setup-Assistenten **Y ein**, wenn Sie dazu aufgefordert werden, die Änderungen zu bestätigen:

```
*****
```

```
Would you like to commit these changes at this time? [Y]> Y
```

```
Congratulations! System setup is complete.
```

An diesem Punkt werden die zuvor festgelegten Konfigurationswerte für Ihre Appliance gelöscht, und die Kundendaten sollten aus der Appliance entfernt werden.

Wenn die Konfiguration auf die ursprünglichen Herstellerwerte zurückgesetzt wird, werden die Feature-Schlüssel entfernt und auf den 30-Tage-Demo-Schlüssel für die *Bearbeitung eingehender E-Mails* zurückgesetzt. Die Feature-Schlüssel der ESA-Hardware sind direkt an die Seriennummer einer Appliance gebunden. Wenn die Appliance mit dem Aktualisierungsdienst kommuniziert, ruft sie alle gültigen zugewiesenen Feature-Schlüssel zurück. Für die virtuellen ESA-Appliances werden die Feature-Schlüssel entfernt, da diese an die Virtual License Number (VLN) gebunden sind, die in die Konfiguration selbst eingebettet ist. Bei den virtuellen Appliances muss die Option

loadlicense erneut ausgeführt werden, und das VLN muss neu geladen werden.

Hinweis: Wenn dieser Prozess für eine Demo-Appliance abgeschlossen werden muss und mehr Zeit erforderlich ist, müssen Sie sich an die Cisco Global Licensing Operations (GLO) wenden, um eine Durchwahlnummer oder neue Feature-Schlüssel anzufordern.

WSA

Gehen Sie wie folgt vor, um eine Cisco WSA auf die werksseitige Standardkonfiguration zurückzusetzen:

Hinweis: Cisco empfiehlt, dass Sie Konsolenzugriff auf die Appliance haben, bevor Sie den Befehl **resetconfig** oder **reload** ausführen, um eine Netzwerkkonfiguration zu entfernen.

1. Geben Sie in der Appliance-CLI den **diagnostischen** Befehl ein, und wählen Sie **REPORTING > DELETEDB** aus.
2. Geben Sie den Befehl **resetconfig** in die CLI ein.

Bei diesem Vorgang wird die Konfiguration vollständig neu installiert, d. h. alle Einstellungen gehen verloren. Die Management-IP-Adresse wird auf **192.168.42.42** zurückgesetzt, und das Admin-Kennwort wird auf den *IronPort*-Standard zurückgesetzt:

```
mywsa.local> resetconfig
```

```
Are you sure you want to reset all configuration values? [N]> y
```

```
All settings have been restored to the factory defaults.  
Please run System Setup Wizard at http://192.168.42.42:8080
```

3. Ein erweiterter Befehl kann auch auf der ESA eingegeben werden. Geben Sie den Befehl für das versteckte **Neuladen** in die ESA-CLI ein, geben Sie **Y** ein, und geben Sie dann **JA** ein, um den Vorgang abzuschließen. Mit diesem Befehl werden alle Kundendaten gelöscht (z. B. alle Konfigurations- und Netzwerkeinstellungen, Protokolle, archivierte geplante Berichte und Benutzerinformationen):

```
mywsa.local> reload
```

```
WARNING !!
```

```
This command will erase customer data, reporting and log files,  
erase proxy cache, reset to factory configuration (shipping mode),  
including network settings and IP addresses and reboot the machine.
```

```
This command does NOT extend the feature keys.  
Those must be applied separately.
```

```
If this is a Virtual Appliance, all feature keys will be removed,  
and the license must be reapplied.
```

WARNING !!

This command is primarily intended for Cisco IronPort Field Engineers and may delete valuable data. Administrators should normally use 'resetconfig' instead.

Are you sure you want to continue? [y|n] **y**

Are you **really** sure you want to continue? If so, type 'YES': **yes**

Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Cisco Security Management Appliance - Benutzerhandbücher](#)
- [Cisco Web Security Appliance - Benutzerhandbücher](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)