FIREEYE TECHNISCHE DOKUMENTATION

# NETWORK SECURITY

## SYSTEMADMINISTRATIONSHANDBUCH

## VERSION 9.1

Network Security Systemadministrationshandbuch

Software Ausgabe 9.1.0

Revision 1

**FireEye Kontaktinformation:**

Website: www.fireeye.com/company/contact-us.html

Technischer Support: https://csportal.fireeye.com

**Telefon (USA):**

1.408.321.6300

1.877.FIREEYE

# Inhalt

# TEIL I: Overview

# KAPITEL 1: Die Network Security Appliance

Fortgeschrittene gezielte Angriffe nutzen das Internet als primären Bedrohungsfaktor, um wichtige Systeme zu gefährden, bestehende Abwehrmechanismen auszukundschaften, langfristige Kontrolle über und Zugriff auf vernetzte Systeme zu erlangen und Daten zu extrahieren. Die FireEyeNetwork Security Appliance stoppt webbasierte Angriffe, die herkömmliche Firewalls und Firewalls der nächsten Generation (NGFW), IPS-, AV- und Webgateways verpassen. Die Network Security schützt vor Zero-Day Web-Exploits und Multi-Protokoll Rückrufen, um vertrauliche Daten und Systeme sicher zu verwahren.

## Deploymentmodi

Sie können die Network Security Appliance auf Ihrem Netzwerk entweder im inline oder out-of-band Modus bereitstellen. Jeder Modus liefert unterschiedliche Optionen und bietet festgelegte Kosten und Vorteile. FireEye empfiehlt dringend, einen der inline Deploymentmodi zu verwenden. Eine inline bereitgestellte Appliance kann automatisch Angriffe und Rückrufe an Command and Control (CnC) Server blockieren. Mit Inline-Bereitstellung ist die Wiederherstellung nach einem Malware-Angriff schneller und weniger ressourcenintensiv. Informationen über die Bereitstellung der Network Security Appliance in Ihrem Netzwerk finden Sie im *Network Security Hardware Administrationshandbuch* für Ihr Appliance Modell und Betriebsmodi auf Seite 115.

# Network Security Produktausgaben und SmartVision

Auf Network Security Appliances, die in Version 8.1.2 oder später lizenziert sind, ist die SmartVision Technologie in zwei Produktausgaben auf der Appliance verfügbar: Classic und SmartVision. Network Security Appliances, die vor Version 8.1.2 lizenziert wurden, können SmartVision in der Classic Produktversion auf der Appliance aktivieren.

- **Classic Produktausgabe**—Eine Network Security Appliance mit einer Classic Edition Appliance Lizenz bietet die vollständige Palette von SmartVision Funktionen und Standard Network Security Appliance Funktionen. Diese Art von SmartVision Appliance kann ein **SmartVision-fähiger Network Security Sensor** oder eine **SmartVision-fähige Network Security integrierte Appliance** sein.
- **SmartVision product edition**—Ein **SMartVision Edition Sensor** (dies ist eine Komponente der *FireEye Network Security, SmartVision Edition* Lösung) ist eine Network Security Hardware oder virtuelle Appliance mit einer SmartVision Edition FIREEYE_APPLIANCE Lizenz. Diese Art einer SmartVision Appliance bietet eine einfache, leichtere Version der vollfunktionalen Classic Network Security Appliance.

Die Network Security Appliance Produktausgabe wird von ihrer FIREEYE_APPLIANCE Lizenz bestimmt und nicht von dem installierten Software Image. Sie können die Ausgabe in den Appliance Lizenzdetails und anderen Bereichen der Network Security Web-UI und CLI anzeigen und für verwaltete Network Security Appliances in der Central Management Web-UI und CLI.

Weitere Informationen über die Verwendung der SmartVision Funktionen finden Sie im *Network Security SmartVison Funktionshandbuch*. Einen Überblick über die Unterschiede zwischen den Classic und den SmartVision Produktausgaben von Network Security Appliances erhalten Sie von Ihrem FireEye Verkaufsvertreter.

# Network Security High Availability

Zwei mit einer Network Security Appliance verbundene Central Management Appliances können jetzt als ein hoch-verfügbares Paar zur Erkennungsredundanz konfiguriert werden. Das Network Security Paar arbeitet im aktive-aktive Modus. Im active-active Modus können beide Appliances allen Verkehr empfangen und verarbeiten. Die beiden Appliances in dem Paar kommunizieren fortlaufend miteinander über einen dedizierten Steuerungs- und einen Datenlink. Der Steuerungslink wird zum Austauschen von Steuerungsnachrichten verwendet. Der Datenlink wird verwendet, um den Netzwerk-Verkehr von den Überwachungsports auf einer Appliance auf die andere Appliance zu replizieren.

Beide Appliances überwachen aktiv den Status des Netzwerks. Der Datenlink behält genau den gleichen Status zwischen beiden Appliances bei - jedes auf den Überwachungsport empfangene Paket wird auf die Peer Appliance durch den Datenport repliziert. Auf den Überwachungsports empfangener Verkehr generiert aktive Warnungen, die auf der Central Management Appliance aggregiert und in der Web-UI angezeigt werden. Auf den Datenports empfangener Verkehr generiert Standby-Warnungen, die nicht aggregiert oder angezeigt werden. Wenn eine Appliance ausfällt, wird die Erkennungsaktivität auf die Peer-Appliance übertragen, die alle neuen Ereignisse und Übermittlungen als "aktiv" erstellt.

Details finden Sie im *Network Security High-Availability Handbuch*.

# MVX-Cluster Deployment

Eine Standard (oder integrierte) Appliance führt sowohl Überwachung als auch Analyse aus. FireEye Distributed Network Security trennt diese beiden Funktionen. Appliances, die als Sensoren fungieren, extrahieren Objekte und URLs aus dem Datenverkehr, den sie überwachen und senden Eingaben an ein MVX-Cluster zur Inspektion und Analyse. Sensoren und integrierte Appliances haben identische Funktionen und Erkennungswirksamkeit.

Eine Appliance, die im MVX-Hybrid Modus läuft, kann Eingaben an ein MVX-Cluster senden, aber nur, wenn ein vordefinierter Kapazitätsschwellenwert erreicht ist. Dies entlagert die Analysefunktion von der Appliance auf das MVX-Cluster, wodurch Verzögerungen und verminderte Wirksamkeit verhindert werden, wenn das Volumen und andere Verarbeitungsanforderungen hoch sind. Wenn die Kapazität unter diesen Schwellenwert fällt, nimmt die Appliance das Senden von Eingaben an ihre integrierte Analyseengine wieder auf.

Sensoren können von der Central Management Appliance verwaltet werden, die das MVX-Cluster verwaltet oder von einer anderen Central Management Appliance. Die Sensoren können auch eine eigenständige Appliance sein, die nicht von einer Central Management Appliance verwaltet wird.

Hybrid Appliances müssen von der Central Management Appliance verwaltet werden, die das MVX-Cluster verwaltet. Dies können keine eigenständige Appliances sein.

Das MVX-Cluster enthält Rechenknoten, bei denen es sich um Virtual Execution Appliances mit MVX-Analyseengines handelt. Rechenknoten sind als Broker designiert. Die Broker empfangen die Eingaben von den Sensoren und verwalten sie in einer Warteschlange, die über die Broker in dem Cluster verteilt ist. Die Rechenknoten ziehen Eingaben aus der Warteschlange, führen die Analyse durch und senden das Ergebnis an die Sensoren durch die Broker.

Die Sensoren generieren auf dem Ergebnis basierende Alarme. Ein verwalteter Sensor sendet die Alarme an seine verwaltende Central Management Appliance, die die Alarme

aggregiert und sie auf einer einzigen Oberfläche anzeigt. Ein eigenständiger Sensor zeigt seine eigenen Alarme an.

In einem MVX Smart Grid Deployment wird das Cluster on-Premises im Netzwerk des Kunden gehostet. In einem Cloud MVX-Deployment wird das Cluster in der FireEye Cloud gehostet.

Eine Liste der Appliances, die als Sensoren oder Hybrid-Appliances fungieren und Details für das Deployment finden Sie im *MVX Smart Grid Handbuch* und *Cloud MVX Handbuch*.

# Management-Pfad

Network Security Appliances können Sicherheitsinhalte und Softwareaktualisierungen vom FireEye Dynamic Threat Intelligence (DTI) Netzwerk herunterladen. Mit einer zweiweg Inhaltslizenz kann die Appliance auch Threat Intelligence Informationen auf das DTI-Netzwerk hochladen.

## Eigenständige Network Security Appliances, die DTI Updates empfangen

Die Central Management Appliance und eigenständigen Appliances verwenden den ether1 Port, um mit dem DTI Netzwerk zu kommunizieren. Die Standardkonfiguration, in der Sie Aktualisierungen vom DTI empfangen (**cloud fireeye.com**) gestattet Ihnen ausgehenden Zugriff auf alle IP-Adressen auf den folgenden Ports:

- DNS (UDP/53)
- HTTPS (TCP/443)

Die Management Schnittstelle ether 1 erfordert eine statische IP-Adresse oder reservierte DHCP Adresse und Subnetzmaske.

## Umgebungen, die ausgehenden Zugriff auf bestimmte IP-Adressen beschränken

Wenn Ihre Sicherheitsrichtlinie den ausgehenden Zugriff auf bestimmte IP-Adressen einschränken, können Sie das DTI-Netzwerk nicht verwenden. Stattdessen zeigen Sie auf **Staticcloud.fireeye.com** für DTI-Aktualisierungen und gestatten den Zugriff auf die ***Incapdns.net** Domain.

Für Appliances, die Bedrohungsinformationen von der DTI-Cloud erhalten, müssen Sie Zugriff auf die Amazon Web Services (AWS) Cloud für ATI-Kommunikation aktivieren. Der Intel-Kontextservice wird in mehreren AWS-Regionen gehostet und wird auf mehreren IP-Adressen, je nach geografischem Standort, aufgelöst.

**Um staticcloud.fireeye.com zu konfigurieren und aufzurufen:**

1. Aktivieren Sie den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Geben Sie den folgenden Befehl von der Appliance CLI ein:

   ```
   hostname (config) # fenet dti source default DTI
   ```

3. Speichern Sie Ihre Konfiguration.

   ```
   hostname (config) # write mem
   ```

4. Fügen Sie IP-Adressen hier zur Firewall hinzu.

**Um Zugriff auf *incapdns.net zu gestatten:**

1. Fügen Sie den Block von unter https://incapsula.zendesk.com/hc/en-us/articles/200627570-Restricting-direct-access-to-your-website-Incapsula-s-IP-addresses- gefundenen IP-Adressen zu der Firewall hinzu.
2. Gestatten Sie Zugriff auf die ***.incapdns.net** Domain auf dem Proxy Gerät.

**Um Zugriff auf die AWS-Cloud für Bedrohungsinformationen zu gestatten:**

1. Gehen Sie auf https://dnschecker.org/#A/context.fireeye.com, um die IP-Adressen für Ihren Standort zu ermitteln.
2. Weitere Informationen über die Whiteliste der IP-Adressen finden Sie in der Dokumentation zum IP-Adressbereich von AWS.

## Network Security Appliances mit Domain-basierten Proxy ACL Regeln

Wenn Ihre Konfiguration Domain-basierte Proxy ACL Regeln einschließt, gestatten Sie Zugriff auf ***.fireeye.com**.

## Mit der Central Management Appliance verbundene Network Security Appliances

Für mit der Central Management Appliance verbundene Network Security Appliances benutzen Sie nur eine statische IP-Adresse und Subnetzmaske. Die Appliance sollte den ether1 Port für die Kommunication mit der Central Management Appliance verwenden.

**HINWEIS:** Verwenden Sie ZeroConf nicht auf der primären Schnittstelle.

Um IPv6 Routing für das Management Netzwerk zu aktivieren, verwenden Sie den Konfigurationsassistenten, oder lesen Sie die *CLI Befehlsreferenz* für Informationen über den **ipv6 enable** Befehl, **interface ipv6** Befehl oder **configuration jump-start** Befehl.

## Integriertes CM Kommunikationsprotokoll und Port Konfiguration

Erstellen Sie SSH Konnektivität zwischen der Central Management Appliance und jeder verwalteten  Network Security Appliance her. Details über Port- und Protokollkonfiguration finden Sie im *Network Security Hardware Administrationshandbuch*.

# Central Management Integration

Die Central Management Appliance ist eine einfach bereitzustellende, Netzwerk-basierte Plattform, die sowohl als Speicherhaus für ein Sicherheitsereignis als auch ein zentrales Management-Gerät für FireEye Appliances dient. Die Central Management Web-UI oder CLI wird benutzt, um ihre verwalteten Geräte zu konfigurieren, verwalten und aktualisieren.

Für Objekte, die als bösartig eingestuft sind, generiert die verwaltete Network Security Appliance automatisch Regeln in Echtzeit. Die automatisch generierten Regeln werden automatisch an die Central Management Appliance zur Verteilung an alle anderen verwalteten Appliances geleitet. Die "Submit to MAS" Central Management Funktion ermöglicht Analysten, einen Vorfall auf einer beliebigen verwalteten Appliance auszuwählen und an eine verwaltete Malware Analysis Appliance zur weiteren Forensik einzureichen.

Die Verbindung zwischen der verwalteten Appliance und der Central Management Appliance kann entweder von der Appliance (eine Client-initiierte Verbindung) oder der Central Management Appliance (eine Server-initiierte Verbindung) initiiert werden. Informationen über Client-initiierte Verbindungen finden Sie unter Management durch eine Central Management Appliance beantragen auf Seite 413. Informationen über Server-initiierte Verbindungen und die Annahme einer Client-initiierten Verbindungsanfrage finden Sie im *Central Management Administrationshandbuch*.

Standardmäßig verwendet eine verwaltete Appliance die Central Management Plattform als ihren Quellserver für Software-Downloads vom DTI-Netzwerk. In dieser Konfiguration verwenden sowohl der Management- als auch der DTI-Netzwerkverkehr einen einzigen Port. Sie können diese Konfiguration ändern, wie unter Den Adresstyp für DTI-Network Serviceanfragen ändern auf Seite 423 beschrieben.

**WICHTIG:** Wenn die Network Security Appliance von der Central Management Appliance verwaltet wird, sollten Sie im Allgemeinen vermeiden, geteilte Konfigurationseinstellungen von der Network Security Appliance Web-UI oder CLI zu ändern. Wenn Sie dies tun, könnten die Änderungen von Befehlen und Aktionen überschrieben werden, die von der Central Management Appliance ausgegeben wurden. FireEye empfiehlt, dass Sie verwaltete Appliances mit Hilfe der Central Management Web-UI konfigurieren. Informationen über die Verwendung der Central Management Web-UI für die Konfigurierung von verwalteten Appliances finden Sie im "Verwaltete Appliances konfigurieren" Abschnitt des *Central ManagementAdministrationshandbuchs*.

**HINWEIS.** Zusätzliche Informationen und Implementierungsdetails finden Sie unter CM Integration auf Seite 411.

# FIPS 140-2 und Common Criteria Konformität

Verwenden Sie die **Compliance Settings** Seite, um Konformitätsfunktionen auf der Network Security Appliance zu konfigurieren.

Sie können stattdessen die folgenden CLI Befehle verwenden, um Konformitätsfunktionen auf der Appliance zu konfigurieren.

- `compliance apply standard`
- `compliance declassify zeroize`
- `compliance options`
- `show compliance`
- `show compliance options`
- `show compliance standard`

Details finden Sie unter *FIPS 140-2 und Common Criteria Anhang*. sowie der *CLI Befehlsreferenz*.

# KAPITEL 2: Benutzerschnittstellen

Dieses Thema behandelt die folgenden Informationen:

# IPMI Überblick über Network Security Benutzerschnittstellen

FireEye Helix ermöglicht Ihnen den Zugriff auf alle Ihre FireEye on-Premises und Cloud-basierten Dienste von einer einzigen Ansicht.aus.

Die Network Security Appliance hat die folgenden Benutzerschnittstellen:

- **Web-UI**—Eine Web-basierte Benutzerschnittstelle, die zum Konfigurieren und Verwalten der Appliance verwendet wird. Dies ist in Die Network Security Appliance Web-UI auf der nächsten Seite beschrieben. Die Appliance Web-UI enthält ein in Das Network Security Appliance Dashboard auf Seite 33 beschriebenes **Dashboard**.
- **CLI**—Eine Befehlszeilenschnittstelle, die zum Konfigurieren und Verwalten der Network Security Appliance verwendet wird. Um auf die Appliance CLI zuzugreifen, sehen Sie Die Network Security Appliance Befehlszeilenschnittstelle auf Seite 36.
- **LCD Display**—Das LCD-Display und die zugehörigen Steuerelemente (bei einigen Modellen verfügbar) können für die Ersteinstellung der Network Security Appliance verwendet werden. Es kann auch benutzt werden, um den Systemstatus zu überprüfen und bestimmte Konfigurationsänderungen vorzunehmen. Dies ist in Das Network Security Appliance LCD Display auf Seite 36 beschrieben.
- **IPMI Interface**—Die IPMI Schnittstelle ermöglicht Ihnen, auf die Network Security Appliance über das Netzwerk zuzugreifen und Wiederherstellungsaktivitäten auszuführen, selbst wenn das System heruntergefahren ist oder auf andere Weise nicht reagiert. Dies ist in Die Network Security Appliance IPMI (Intelligent Platform Management Interface) Schnittstelle auf Seite 41 beschrieben.

Zwei externe Benutzerschnittstellen auf der Network Security Appliance beziehen sich auf die Verwendung der Network Security Appliance in einer FireEye Helix-Umgebung:

- **FireEye Helix Web-UI**—Eine Schnittstelle, die eine einzelne Ansicht der Alarme von allen Helix Appliances auf Ihrem Netzwerk bietet. Weitere Informationen finden Sie in der *Helix Bedienungsanleitung*.

- **FireEye Cloud IAM Web-UI**—Eine Schnittstelle auf dem Cloud IAM Server. Sie wird hauptsächlich von dem Administrator Ihrer IAM Organisation verwendet (einem Userkonto, das FireEye für Sie zusammen mit Ihrer IAM Organisation bietet). Der Administrator erstellt FireEye Cloud Konten für Benutzer und wendet rollenbasierte und regelbasierte Zugriffssteuerungen an. Dies ist in "FireEye Cloud IAM Userkonten" im *System-Sicherheitshandbuch* beschrieben.

  Die Eigentümer dieser Userkonten können sich auch auf der FireEye Cloud IAM Web-UI anmelden. Ihre Zugriffsrechte in der FireEye Cloud IAM Web-UI sind in der Regel auf Aktualisierung ihrer Kontovorgaben und Änderung Ihrer Passwörter begeschränkt. Die wird unter "Ihr FireEye Cloud IAM Userkonto" im *System-Sicherheitshandbuch* beschrieben.

Zugriff auf die FireEye Cloud IAM Web-UI ist erforderlich, damit Sie Unterstützung für Single Sign-On (SSO) Authentifizierung konfigurieren können. Wenn die SSO-Authentifizierung aktiviert ist und der Helix-Modus auf FireEye Appliances aktiviert ist, können Benutzer sich einmal anmelden, um sich auf ihrem FireEye Cloud Konto zu authentifizieren und dann zwischen den Komponenten zu navigieren, ohne sich lokal bei jeder Appliance anmelden zu müssen. Dies wird unter "Single Sign-On Authentifizierung" im *System-Sicherheitshandbuch* beschrieben.

Ändern Sie das Passwort für das permanente **api_analyst** Userkonto auf dem Endpoint Security Server nicht. Wenn Sie dies tun könnte die Verbindung zwischen dem Endpoint Security Server und Helix abbrechen. Wenn Sie eine API-Verbindung zwischen dem Endpoint Security Server und einem Drittanbieter-Produkt benötigen, fügen Sie ein weiteres Userkonto mit der api_analyst Rolle hinzu.

# Die Network Security Appliance Web-UI

Die Network Security Appliance Web-UI verwendet HTTPS, um eine sichere Verbindung für die Konfigurierung der Appliance zu liefern. Die Web-UI Funktionen, auf die Sie Zugriff haben, hängen von den Ihrer Rolle zugestandenen Berechtigungen ab.

Sie greifen auf die Network Security Appliance Web-UI zu, indem ein Browser mithilfe von HTTPS an die IP-Adresse oder den Hostnamen des Management-Ports geleitet wird. Die IP-Adresse und der Hostname werden während der Erstkonfiguration der Appliance festgelegt. Der Hostname muss von einem DNS-Server aufgelöst werden, wenn Sie ihn für den Zugriff auf die Web-UI verwenden.

Die Network Security Appliance Web-UI enthält Steuerelemente für die An- und Abmeldung mit Hilfe von lokalen, Appliance-spezifischen Berechtigungen. Die Web-UI zeigt außerdem an, ob der Helix Modus aktiviert ist und ob es sich bei den Alarmen um Helix Alarme handelt.

## Browser Support

Verwenden Sie eine neue Version eines der folgenden Browser, um auf die Network Security Appliance Web-UI zuzugreifen.

- Microsoft Edge auf unterstützten Versionen von Windows
- Firefox auf unterstützten Versionen von Windows und Mac
- Google Chrome auf unterstützten Versionen von Windows und Mac

## Erfordernisse für Bildschirmauflösung

Die Network Security Web-UI unterstützt die Verwendung der folgenden Bildschirmauflösungen:

| | |
|---|---|
| 1152 x 864 Pixel | 1440 x 900 Pixel |
| 1280 x 800 Pixel | 1600 x 900 Pixel |
| 1280 x 1024 Pixel | 1680 x 1050 Pixel |
| 1360 x 768 Pixel | 1920 x 1080 Pixel |
| 1366 x 768 Pixel | 1920 x 1200 Pixel |

## Lokal auf der Helix Appliance Web-UI anmelden

Um sich lokal auf der Helix Network Security Appliance Web-UI anzumelden, benötigen Sie die IP-Adresse oder den Hostnamen der Appliance und den lokalen Benutzernamen und Passwort, das der Appliance Administrator für Sie erstellt hat.

## Voraussetzungen

- Bevor sich der Standard Admin Benutzer auf der Appliance Web-UI anmelden und andere Benutzerkonten erstellen kann, muss das Standard-Herstellungspasswort (`admin`) auf ein neues Passwort geändert werden, das 8 bis 32 Zeichen lang ist. Dieser Schritt ist in Erstkonfiguration auf Seite 97 enthalten.

**Um sich lokal auf der Helix Network Security Appliance Web-UI anzumelden:**

1. Öffnen Sie einen Webbrowser und geben Sie **`https://<appliance>`** in der Adressenzeile ein, wobei `appliance` die IP- Adresse oder der Hostname der Appliance ist. Wenn zum Beispiel die konfigurierte IP-Adresse der Appliance 10.1.0.1 ist, geben Sie **`https://10.1.0.1`** ein.

2. Auf der Appliance Web-UI Login Seite geben Sie den lokalen Benutzernamen und das Passwort für diese Appliance ein, das Ihnen von Ihrem Administrator geliefert wurde.

## Benachrichtigung über ein Erkennungsproblem

Eine Warnmeldung wird angezeigt, wenn Probleme mit den Prozessen der Erkennungs-Engine bei der Anmeldung auf der Web-UI auftreten.

Um die Warnmeldung abzubrechen, klicken Sie auf das rote **X**. Die Warnung wird nicht länger auf der Seite angezeigt. Der Alarm wird weiterhin angezeigt, wenn Sie auf andere Seiten in der Web-UI gehen.

Um die Alarmmeldung während dieser Sitzung zu bestätigen, wählen Sie das **Acknowledge** Kontrollkästchen. Eine Bestätigungsnachricht wird angezeigt:

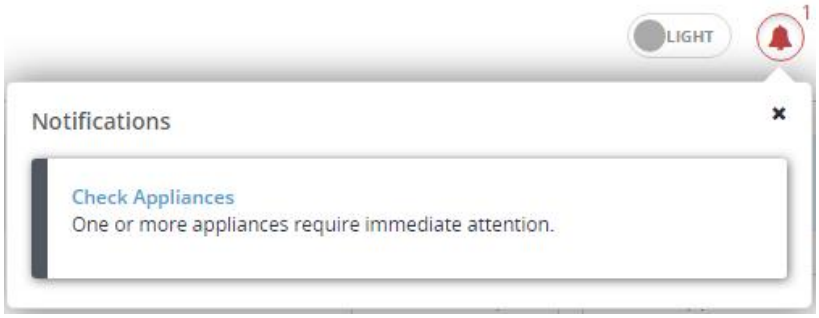
Klicken Sie auf **Yes**, um die Alarmmeldung zu bestätigen. Die Warnung wird nicht länger auf irgendeiner Seite in der Web-UI angezeigt. Der Alarm wird bei Ihrer nächsten Anmeldung angezeigt.

Um falsch positive zu übersteuern, kann die Alarmmeldung global durch ein Update des Sicherheitsinhalts deaktiviert werden.

## Benachrichtigungen über Appliance Integritätsprobleme

Die Glocke oben rechts auf der Web-UI zeigt die Anzahl der Appliance Integritätsprobleme an, die behoben werden müssen. Wenn Sie auf die Glocke klicken, werden die Benachrichtigungen mit Links auf die relevanten Web-UI Seiten angezeigt. Die Glocke wird nicht angezeigt, wenn keine Benachrichtigungen vorhanden sind.

Die folgende Abbildung zeigt, dass ein Problem behoben werden muss.




## Das Network Security Appliance Dashboard

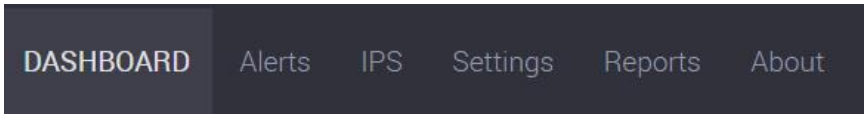
Die **Dashboard** Seite auf der Network Security Web-UI bietet eine hochgradige Ansicht der durch die Appliance gesammelten Bedrohungsintelligenz. Auf vielen Tafeln auf dem

Dashboard können Sie blaue Schaltflächen und Textlinks anklicken, um ein Drilldown auf kritische Bedrohungsinformationen auszuführen, die das Netzwerk betreffen.

Details über das Dashboard finden Sie in der *Network Security Bedienungsanleitung*.

## Network Security Web-UI Tabs

Dieser Abschnitt beschreibt die Network Security Web-UI Register.



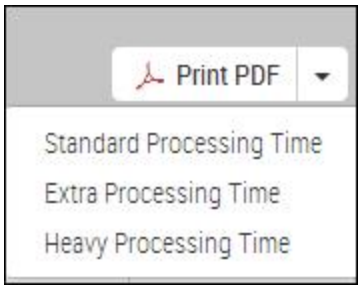

- **Dashboard**—Zeigt einen hochgradigen Überblick über die von der Network Security Appliance gesammelten Bedrohungsinformationen. Auf vielen Tafeln auf dem Dashboard können Sie blaue Schaltflächen und Textlinks anklicken, um ein Drilldown auf kritische Bedrohungsinformationen auszuführen, die das Netzwerk betreffen.
- **Alerts**—Zeigt erweiterbare Ebenen detaillierter Informationen über die Hosts an, die im Netzwerk infiziert sind, sowie Rückruf-Aktivität (botnet Server) und Malware Angriffe.
- **IPS Events**—Zeigt alle IPS-Ereignisse und IPS-Warnungen an (MVX-korrelierte IPS-Ereignisse), die von der IPS-fähigen Appliance entdeckt wurden.
- Summaries—Zeigt Zusammenfassungen erkannter Infektionen, Malware, Diagramme und Webanalyse-Prioritäten an.
- **Filter**—Ermöglicht das Filtern von Ereignissen je nach Quell- und Ziel-IP-Adressen, Datum und Auftrittsbereich. Diese Filter gestatten Ihnen, die Auflistung von Ereignissen zu vereinfachen, indem nur die Ereignisse von Interesse auf den Alerts und Summaries Seiten angezeigt werden.
- **Settings**—Bietet Optionen für die Konfigurierung der Appliance.
- **Reports**—Ermöglicht Ihnen die Erstellung oder Planung von konsolidierten Zusammenfassungsberichten, Rückrufserverberichten, Berichte zu infizierten Hosttrends, Berichte zu Warnungsdetails und Berichte zu Malware Aktivitäten.

- **About**—Netzwerk-Administration Informationen und Steuerungen:
  - **Summary**—Zeigt allgemeine Statusinformationen über Systemzustand und Appliance-Leistung an. Siehe Ergebnisse von Systemintegrität- und Leistungsüberprüfung anzeigen auf Seite 339.
  - **Supported Features** — Zeigt die für die Appliance verfügbaren Funktionen an, und ob sie aktiviert oder deaktiviert sind. Siehe Unterstützte Funktionen auf Seite 385.
  - **Health Check**—Zeigt Informationen über Appliance- und Systemzustand an. Siehe Systemintegrität und Leistung auf Seite 335.
  - **Deployment Check**—Bietet Netzwerkkonnektivität, Erkennungsprüfung und Netzwerk-Deploymentchecks.
  - **Log Manager**—Ermöglicht Ihnen, Protokollarchive zu erstellen, herunterzuladen, hochzuladen und zu löschen.
  - **Upgrade**—Ermöglicht Ihnen, Sicherheitsinhalte, Software Image und Guest Image Versionen anzuzeigen und zu aktualisieren.

## PDF Erstellung

Einige Web-UI Seiten, wie zum Beispiel die, die Analyseergebnisse anzeigen, haben eine **Print PDF** Schaltfläche in der oberen rechten Ecke der Seite, die Ihnen gestattet, den Inhalt der Seite auf PDF zu speichern, so dass er gedruckt oder gespeichert werden kann. Nur der auf der Seite sichtbare Inhalt ist in der PDF Ausgabe eingeschlossen. Wenn zum Beispiel ein Element auf der Seite nicht erweitert ist, werden die Einzelheiten über dieses Element nicht angezeigt und sind nicht in der PDF-Ausgabe enthalten. Je nach Ihren Webbrowser Einstellungen wird das erstellte PDF in dem Webbrowser geöffnet oder wird auf Ihren Computer heruntergeladen.

Die Zeit, die zum Erstellen des PDFs erforderlich ist, hängt von der aktuellen Belastung des Systems ab. Standardmäßig versucht das System, das PDF mit Hilfe von **Standard Processing** Time, der schnellsten möglichen Methode, zu erstellen. Wenn der Zeitintervall der Erstellung des PDFs abläuft, können Sie es erneut mit Hilfe anderer Optionen versuchen, indem Sie auf den Pfeil am Ende klicken und dann **Extra Processing Time** oder **Heavy Processing Time** auswählen, wobei Heavy Processing Time am längsten dauert.



# Die Network Security Appliance Befehlszeilenschnittstelle

Die Network Security Appliance enthält eine Standard Befehlszeilenschnittstelle (CLI), die zum Konfigurieren, Verwalten und Überwachen des Network Security Systems

**Um sich auf der CLI mit Hilfe eines Terminalfensters oder SSH Client einzuloggen:**

1. Melden Sie sich mit Hilfe des SSH Protokolls auf der Appliance über die IP-Adresse oder den Hostnamen der Management-Schnittstelle an,

   ```
   $ ssh <username>@<ipAddress> | <hostName>
   ```

   wobei `ipAddress` die IPv4 oder IPv6 Adresse der Management-Schnittstelle angibt.

2. Wenn Sie aufgefordert werden, geben Sie Ihr Passwort ein.

   ```
   Password: <password>
   ```

   Die `hostname` > Aufforderung wird angezeigt, nachdem Sie angemeldet sind.

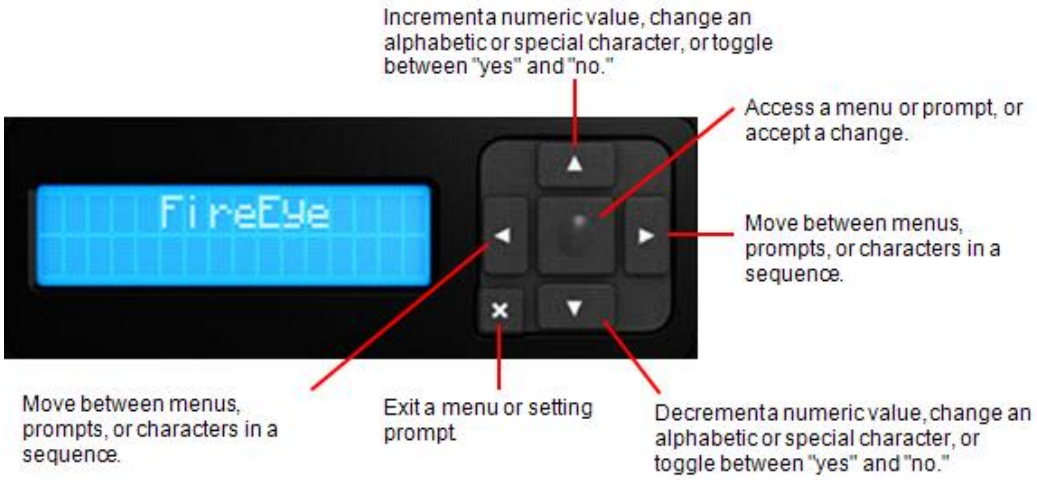
# Das Network Security Appliance LCD Display

Auf der Vorderseite einiger Appliance Modelle befindet sich ein LCD-Anzeige. Sie können die Erstkonfiguration der Appliance mit Hilfe des LCD Displays durchführen, wie unter Ersteinstellungen mit Hilfe der LCD Anzeige konfigurieren auf Seite 108 beschrieben. Sie können die LCD Anzeige verwenden, um auch andere allgemeinen Konfigurationsaufgaben auszuführen.

## Die LCD-Menüs navigieren

Die folgende Illustration der LCD Anzeige zeigt die Benutzung der Navigationsschaltflächen für die Konfigurierung der Einstellungen. Details über die Menüs finden Sie auf dem LCD Menu auf Seite 40.




Auf einigen Modellen müssen Sie die Frontplatte entfernen, um Zugriff auf die Navigationsschaltflächen der LCD Anzeige zu erhalten.

**Um die Vorderplatte zu entfernen:**

1. Schrauben Sie die Frontplatte ab, um sie zu entriegeln.

2. Entfernen Sie die Frontplatte.

# LCD Anzeige-Menüs

Die LCD Anzeige hat vier Menüs: Network Menü unten, Config Options Menu auf der nächsten Seite, LCD Menu auf Seite 40 und Restart Options Menü auf Seite 40.

Informationen über die Navigation durch die Menüs und Auswahl von Optionen finden Sie unter Die LCD-Menüs navigieren auf Seite 36.

## Network Menü

Die folgende Tabelle bietet Informationen über das **Network** Menü.

| Eingabeaufforderung | Beschreibung |
|---|---|
| Hostname | Hostname für die Appliance. |
| DHCP enabled | Geben Sie "yes" ein, um DHCP auf dem ether1 (Management-Schnittstelle) Port zu verwenden. Geben Sie "no" ein, um Ihre IP-Adresse und Netzwerkeinstellungen manuell zu konfigurieren. |
| Static IP address | Die Eingabeaufforderung ist verfügbar, wenn DHCP deaktiviert ist. Geben Sie die IP-Adresse für den ether1 (Management-Schnittstelle) Port ein. |
| Netmask | Die Eingabeaufforderung ist verfügbar, wenn DHCP deaktiviert ist. Geben Sie die Netzwerkmaske ein. |

| Eingabeaufforderung | Beschreibung |
|---|---|
| Default gateway | Die Eingabeaufforderung ist verfügbar, wenn DHCP deaktiviert ist. Geben Sie die Gateway IP-Adresse für die Management-Schnittstelle ein. |
| Primary DNS | Die Eingabeaufforderung ist verfügbar, wenn DHCP deaktiviert ist. Geben Sie die IP-Adresse des primären DNS-Servers ein. |
| Domain name | Die Eingabeaufforderung ist verfügbar, wenn DHCP deaktiviert ist. Geben Sie den Domainnamen für die Management-Schnittstelle ein, z.B. **it.acme.com**. |
| IPv6 enabled | Geben Sie "yes" ein, um IPv6 Protokoll zu aktivieren, wodurch das Netzwerk IP-Routing von IPv4 auf IPv6 geändert wird. |
| SLAAC enabled | Diese Aufforderung ist verfügbar, wenn IPv6 aktiviert ist. Geben Sie "yes" ein, um IPv6 autoconfig auf dem ether 1 (Management-Schnittstelle) Port zu aktivieren. Geben Sie "no" ein, um die IPv6 autoconfig auf dem ether1 (Management-Schnittstelle) Port zu deaktivieren. |
| Admin net login | Geben Sie "yes" ein, um dem Administrator zu gestatten, sich entfernt auf der Appliance anzumelden. Geben Sie "no" ein, um entfernten Zugriff zu deaktivieren. |

## Config Options Menu

Die folgende Tabelle liefert Informationen über das **Config Options** Menü.

| Eingabeaufforderung | Description |
|---|---|
| Save settings | Speichert die während dieser Sitzung vorgenommenen Änderungen, so dass Sie nach einem Neustart bestehen bleiben. |
| Revert to factory defaults | Setzt die Appliance auf Ihre Standard Werkseinstellungen zurück, einschließlich Benutzernamen, Kennwort und Informationen über die Netzwerkskonfiguration. |

| Eingabeaufforderung | Description |
|---|---|
| Reset admin password | Setzt das admin Kennwort für den Zugriff auf die Appliance selbst zurück. (Dies stellt nicht das Kennwort für den Zugriff auf das LCD Display ein.) Das neue Kennwort wird willkürlich generiert. Die LCD wird das Kennwort anzeigen. Wenn Sie es sich gemerkt haben, drücken Sie eine Schaltfläche, um auf die nächste Aufforderung oder Menü zu wechseln. Sie können auf ein Kennwort Ihrer Wahl mit Hilfe der Appliance CLI oder Web-UI wechseln, nachdem die allgemeine Konfiguration abgeschlossen ist. |

## LCD Menu

Die folgende Tabelle liefert Informationen über das **LCD**-Menü.

| Eingabeaufforderung | Beschreibung |
|---|---|
| Password | Stellt ein Passwort für den Zugriff auf die LCD Anzeige ein. (Dadurch wird kein Kennwort für Zugriff auf die Appliance eingestellt.) |
| Brightness | Stellt die Helligkeitsstufe der LCD Anzeige von 0 bis 9 ein, wobei 9 die hellste Stufe ist. |
| Contrast | Stellt die Kontraststufe der LCD Anzeige zwischen dem Hintergrund und Text von 0 bis 9 ein, wobei 9 die größte Kontraststufe ist. |

## Restart Options Menü

Die folgende Tabelle bietet Informationen über das **Restart Options** Menü.

| Eingabeaufforderung | Description |
|---|---|
| Reboot system | Startet das System erneut. |
| Halt system | Bringt das System auf den niedrigsten Status herunter, während es weiterhin eingeschaltet bleibt. |
| Next boot loc | Legt die Festplattenpartition (1 oder 2) fest, von der beim nächsten Neustart gebootet werden soll. |

# Die Network Security Appliance IPMI (Intelligent Platform Management Interface) Schnittstelle

Die FireEye Intelligent Platform Management Interface (IPMI) gestattet Ihnen, die folgenden Aufgaben entfernt von einem Web Browser auszuführen.

- Schalten Sie Ihre Appliance wieder ein, wenn sie nicht mehr reagiert.

  **HINWEIS:**Das IPMI ist aktiv, selbst wenn die Appliance über die Appliance CLI oder den Netzschalter an der Frontplatte ausgeschaltet wurde, solange die Hauptstromversorgung eingeschaltet ist.

- Setzen Sie den Server zurück.
- Greifen Sie auf die Serielle Konsole zu, wenn die Management Schnittstelle nicht verfügbar ist oder nicht reagiert.
- Überprüfen Sie den Status von Serversensoren.

Informationen über die Konfiguration der IPMI Schnittstelle finden Sie unter Die IPMI Schnittstelle konfigurieren auf Seite 109.

Die IPMI Schnittstelle verwendet eine Netzwerkverbindung mit dem IPMI Port der Appliance und wird durch eine sichere Web Browser Sitzung abgerufen. (Die Standard IPMI Schnittstelle ermöglicht Verbindungen mit Hilfe von Drittparteien Tools, wie z.B. Supermicro IPMI View. Allerdings ist jeder externe Zugriff auf die IPMI Schnittstelle von der Appliance deaktiviert.)

**WICHTIG!** Die IPMI Fernbedienung kann keine normale Ausschaltung auf der Appliance durchführen.

## IPMI Browsersupport

Verwenden Sie eine aktuelle Version der folgenden Webbrowser für den Zugriff auf die Web-UI:

- Microsoft Edge auf unterstützten Versionen von Windows
- Google Chrome auf unterstützten Versionen von Windows und Macintosh

**WICHTIG!** Firefox kann nicht für den Zugriff auf den IPMI Port benutzt werden. Der Firefox Browser interpretiert ein neuerstelltes HTTPS-Zertifikat als einen möglichen Angriff und erstellt einen Invalid Certificate Error Code ("sec_error_reused_issuer_and_serial"). Anstatt die Verbindung herzustellen, zeigt Firefox eine "Secure Connection Failed" Seite an.

## Auf der IPMI Schnittstelle anmelden

Dieser Vorgang beschreibt, wie Sie sich auf der Network Security Appliance IPMI Schnittstelle von einem Webbrowser anmelden.

## Voraussetzungen

- Der 100BASE-T IPMI Port auf der Rückseite der Appliance ist verkabelt und wie unter Die IPMI Schnittstelle konfigurieren auf Seite 109 beschrieben konfiguriert.
- Die IP-Adresse, die für den IPM Port konfiguriert wurde, ist bekannt.
- Sie verwenden einen Webbrowser, der in IPMI Browsersupport auf der vorherigen Seite aufgeführt ist.

**Um sich auf der IPMI Schnittstelle anzumelden:**

1. Greifen Sie auf den IPMI Port mit Hilfe eines Webbrowsers über eine sichere Webbrowsersitzung zu. In der Adresszeile des Browsers geben Sie **`https://`**, gefolgt von der IP-Adresse des IPMI Ports ein.
2. Melden Sie sich auf der IPMI Web-UI mit Hilfe von ADMIN als Benutzernamen und dem Passwort an, das für den IPMI Benutzer konfiguriert wurde.

## Das Gerät aus- und einschalten und zurücksetzen

Dieser Vorgang beschreibt die Verwendung der IPMI Schnittstelle zum Aus- und Einschalten der Network Security Appliance.

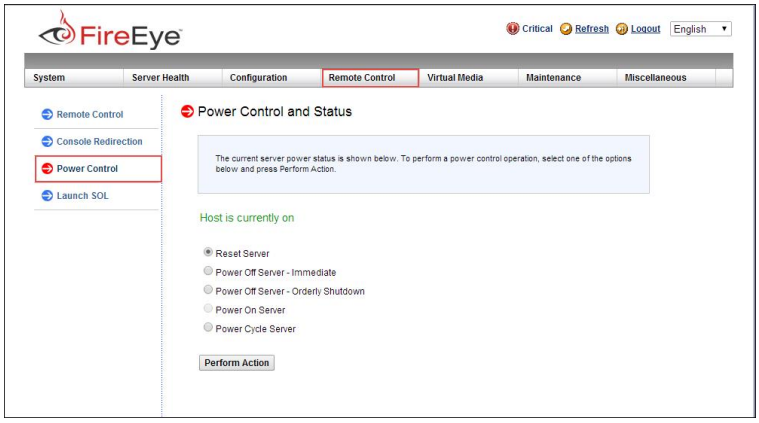
## Voraussetzungen

- Sie sind auf der Appliance IPMI angemeldet.

**Um wieder aus- und einzuschalten oder den Server zurückzusetzen:**

1. Klicken Sie auf den **Remote Control** Tab.
2. Klicken Sie auf der Seitenleiste auf **Power Control**.




3. Wählen Sie die gewünschte Option.
   - **Reset Server (Server zurücksetzen)**
   - **Power Off Server – Immediate (Server ausschalten - sofort)**
   - **Power Off Server – Orderly Shutdown (Server ausschalten - ordnungsgemäßes Herunterfahren)**
   - **Power On Server (Server einschalten)**
   - **Power Cycle Server (Server aus- und einschalten)**
4. Klicken Sie auf **Perform Action**.

# Die serielle Gerätekonsole abrufen

Dieser Vorgang beschreibt die Verwendung der IPMI Schnittstelle für den Zugriff auf die Network Security Appliance über eine serielle Konsole.

**WICHTIG!** Verwenden Sie die IPMI Web-UI für den Zugriff auf die serielle Konsole des Rechenknotens nur während einer Strom-oder Systemzurücksetzung oder wenn das System ansonsten nicht auf der Management-Schnittstelle reagiert.

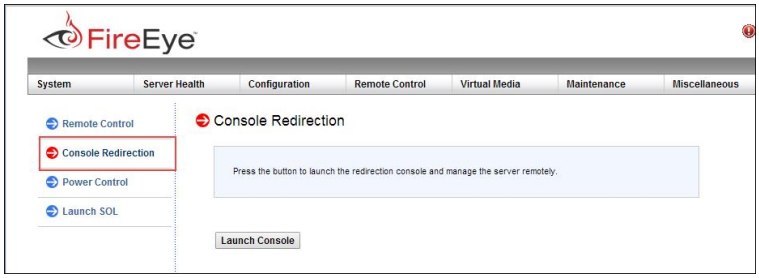
# Voraussetzungen

- Sie sind auf der Appliance IPMI angemeldet.
- Die Appliance benutzt ihre Management-Schnittstelle nicht.

**Um auf die serielle Konsole zuzugreifen:**

**WICHTIG!** Verwenden Sie die IPMI Web-UI, um nur während einer Strom- oder Systemzurücksetzung auf die serielle Konsole zuzugreifen oder wenn das System ansonsten nicht auf die Management-Schnittstelle reagiert.

1. Klicken Sie auf den **Remote Control** Tab.
2. Klicken Sie auf **Console Redirection** auf der Seitenleiste.




3. Klicken Sie auf **Launch Console**.

   Sie könnten aufgefordert werden, ein Java Programm zu installieren, um die Konsole zu starten. Dies könnte Änderungen Ihren Java Sicherheitseinstellungen erfordern. Wenn Ihre Sicherheitsrichtlinien dies nicht zulassen und Ihre Appliance eine neuere IPMI Firmwareversion benutzt, können Sie stattdessen Ports auf der Firewall öffnen. Um die installierten und verfügbaren Firmwareversionen anzuzeigen, klicken Sie auf **System** und dann auf **System Information** oder folgen Sie den Anleitungen unter IPMI und BIOS Firmware Aktualisierungen auf Seite 289.

# Den Status von Gerätesensoren überprüfen

Die Vorgang beschreibt die Verwendung der IPMI Schnittstelle für die Statusüberprüfung der Network Security Appliance Sensoren.

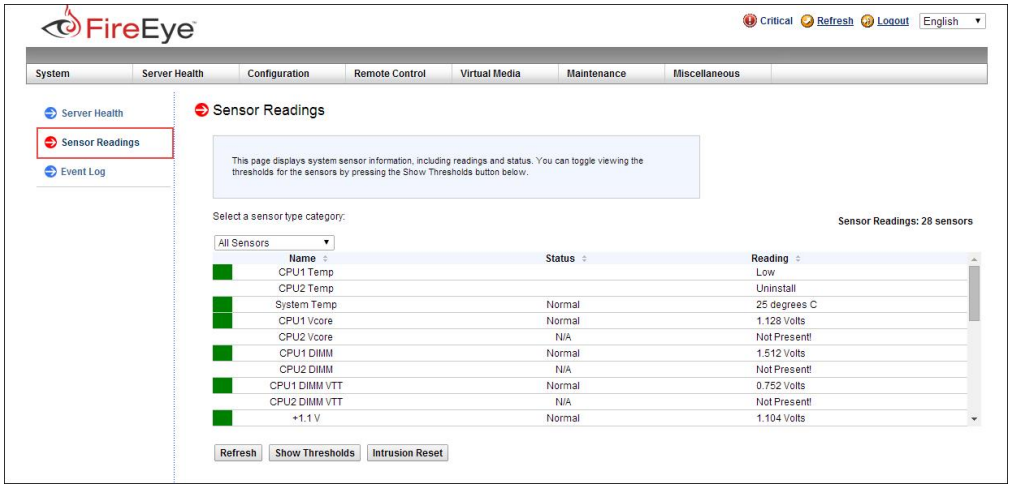
# Voraussetzungen

- Sie sind auf der Appliance IPMI angemeldet.

**Um den Status von Serversensoren zu überprüfen:**

1. Klicken Sie auf das **Server Health** Register.
2. Klicken Sie auf der Seitenleiste auf **Sensor Readings**.




3. Klicken Sie bei Bedarf am Ende der Seite auf Optionen:
   - **Refresh (Aktualisieren)**
   - **Show Thresholds (Schwellenwerte anzeigen)**
   - **Intrusion Reset (Angriffszurücksetzung)**

# Die IPMI Schnittstelle mit Hilfe der CLI zurücksetzen

Dieser Vorgang beschreibt die Zurücksetzung der IPMI Schnittstelle.

# Voraussetzungen

- Adminzugriff auf die Network Security Appliance.

Wenn die IPMI Schnittstelle nicht mehr funktioniert, führen Sie die folgenden Schritte aus, um sie zurückzusetzen. Möglicherweise müssen Sie dazu ein Wartungsfenster planen.

**Um die IPMI Schnittstelle zurückzusetzen:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Laden Sie die IPMI Firmware neu:

   ```
   hostname (config) # ipmi firmware reload cold
   ```

4. Warten Sie fünf Minuten.

5. Überprüfen Sie, ob die IPMI Schnittstelle aktiv ist.
   ```
   hostname (config) # show ipmi
   ```
6. Wenn die IPMI Schnittstelle nicht aktiv ist:
   a. Fahren Sie die Appliance herunter:
      ```
      hostname (config) # reload halt
      ```
   b. Ziehen Sie alle Netzkabel ab.
   c. Warten Sie 90 Sekunden.
   d. Stecken Sie das Netzkabel ein.
   e. Drücken Sie auf den Netzschalter, um die Appliance neu zu starten.

# KAPITEL 3: Das Appliance Dashboard

Das Dashboard zeigt eine Sammlung von Widgets an, die allgemeine Ansichten der von der Appliance oder dem Sensor gesammelten Bedrohungsinformationen bietet.

**HINWEIS:** Auf einer Network Security Appliance oder Sensor zeigt das Dashboard lokale Daten von der Appliance oder dem Sensor.

Auf einer Central Management Appliance zeigt das Dashboard konsolidierte Daten für mehrere Appliances oder Sensoren in der gleichen Gruppe an.

In diesem Kapitel werden die folgenden Informationen behandelt.

Network Security Dashboard Widgets

Die Web-UI wird auf dem Dashboards Tab geöffnet. Das vordefinierte Dashboard **FireEye Dashboard** zeigt alle für die Appliance verfügbaren Widgets an. Widgets werden als Analysis, Operational oder Detection kategorisiert. Verwenden Sie das Category Dropdown-Menü, um das **FireEye Dashboard** zu filtern, um alle Widgets in der ausgewählten Kategorie anzuzeigen. Sie können ein Widget im Vollbildmodus anzeigen und dann die Standard Dashboard Ansicht wiederherstellen. Die Dashboard Widgets werden in Network Security Dashboard-Widgets auf der nächsten Seite vorgestellt.

Benutzerdefinierte Dashboards

Sie können **benutzerdefinierte Dashboards** erstellen, indem Sie Network Security Dashboard Widgets auswählen und sie in einem gewünschten Layout anordnen. Jedes Dashboard kann als das **Standard Dashboard** designiert werden, das angezeigt wird, wenn Sie sich auf der Appliance Web-UI anmelden. Sie können auch die Reihenfolge der Dashboard Namen am oberen Seitenrand ändern. Diese Web-UI Vorgänge werden unter Benutzerdefinierte Dashboards auf Seite 79 beschrieben.

Dashboards und Widgets konfigurieren

Sie können das **auto-refresh Interval** konfigurieren, das sich auf alle Widgets in allen Dashboards bezieht. Sie können auch eine **einmalige Aktualisierung** der in allen aktuellen Dashboard-Widgets oder nur für ein einziges Widget angezeigten Daten anwenden. Sie können den abgedeckten **Zeitraum** von allen aktuellen Dashboard Widgets oder nur für ein einziges Widget festlegen. Diese Web-UI Vorgänge werden unter Dashboard- und Widget-Verwaltung auf Seite 85 beschrieben.

Dashboard-Berichte erstellen und planen

Sie können einen einzelnen Bericht generieren und Berichte planen, die stündlich, täglich, wöchentlich oder monatlich ausgeführt werden sollen. Wählen Sie das CSV, JSON oder XML Format. Berichte enthalten Daten über alle Widgets auf dem Dashboard. Weitere Informationen finden Sie unter Dashboard-Berichte generieren und planen auf Seite 89.

# Network Security Dashboard-Widgets

Das Network Security Dashboard zeigt Widgets an, die Ihnen eine Zusammenfassungsansicht der Web-Bedrohungsprävention und der von der Appliance oder dem Sensor bereitgestellten Bedrohungsinformationen geben.

Das Dashboard ist für die Admin, Analyst, Monitor und Operator Rollen zugänglich.

| Rolle | Zugängliche Network Security Dashboard-Widgets |
|---|---|
| Admin | Alle Widgets |
| Analyst | Alle Widgets, mit Ausnahme von Cluster Connection Status und Appliance Utilization |
| Monitor | Alle Widgets, mit Ausnahme von Cluster Connection Status |
| Operator | Nur Appliance Utilization |

Die folgenden Absätze fassen die Network Security Dashboard-Widgets zusammen:

**Threat Level**

Zeigt die allgemeine Bedrohungsstufe (Niedrig, Mittel, Hoch oder Kritisch) an, je nach den von der Appliance oder Sensor erkannten Bedrohungen und FireEyes Messungen der Bedrohungsstufe in der angegebenen Branche und geografischem Standort. Details finden Sie unter Threat Level auf Seite 52.

**Alerts Summary**

Zeigt die Anzahl der in jeder Angriffskategorie entdeckten Alarme an. Details finden Sie unter Alerts Summary auf Seite 53.

**Recent Alerts (25)**

Zeigt eine Tabelle der 25 zuletzt entdeckten Alarme an. Details finden Sie unter Recent Alerts (25) auf Seite 56.

**Cluster Connection Status**

Wenn eine Network Security Appliance im Sensor Modus arbeitet, zeigt das Cluster Connection Widets Statusinformationen über die Eingabeverbindung des Sensors mit seinem MVX-Cluster an. Details finden Sie unter Cluster Connection Status auf Seite 57.

**Critical Malware Detection**

Zeigt die Anzahl der mit bösartigen Infektionen verbundene Hosts an, die von FireEye entdeckt wurden.

- Hosts, die Malware Objektalarme ausgelöst haben
- Hosts, die Web-Infektionsalarme ausgelöst haben
- Hosts, die versucht haben, mit einem botnet Server zu kommunizieren

Details finden Sie unter Critical Malware Detection auf Seite 58.

**Threat Attacks**

Zeigt die top zehn Threat Attack Typen in dem überwachten Netzwerk an. In jeder Kategorie wird die Anzahl der Alarme als ein Prozentsatz der Gesamtzahl der Warnungen ausgedrückt. Details finden Sie unter Threat Attacks auf Seite 59.

**Callback Events (Top 25)**

Führt die top 25 Subnetze in dem überwachten Netzwerk auf, gemäß der Anzahl der entdeckten Rückrufereignisse und der Anzahl der infizierten Hosts. Details finden Sie unter Callback Events (Top 25) auf Seite 61.

**Infected Subnets (Top 25)**

Führt die top 25 Subnetze in dem überwachten Netzwerk auf, gemäß der Anzahl der Malware Ereignisse, einzigartigen Malware Typen und infizierten Hosts für jedes Subnetz bewertet. Details finden Sie unter Infected Subnets (Top 25) auf Seite 62.

**Analysis Statistics**

Zeigt den Prozentsatz der gescannten bösartigen und nicht-bösartigen Dateien an, sowie die Anzahl der bösartigen und nicht-bösartigen URLs, die gescannt wurden. Details finden Sie unter Analysis Statistics auf Seite 63.

**File Analysis Statistics**

Zeigt die Dateitypen als Prozentsätze an, die zur Analyse eingegeben wurden. Sie können alle übermittelten Dateitypen anzeigen oder die Daten nur für schädliche Dateien nach Prozentsätzen filtern. Details finden Sie unter File Analysis Statistics auf Seite 64.

**Supported Features**

Zeigt alle unterstützten Funktion einschließlich Status (aktiviert oder deaktiviert), Name, Kategorie und Beschreibung an. Details finden Sie unter Supported Features auf Seite 65.

**Malware Detection Trend (6 Months)**

Zeigt den von der Appliance oder dem Sensor erkannten Malware Trend an, verglichen mit der Malware, die innerhalb der angegebenen Branche oder geografischem Standort erkannt wurde. Details finden Sie unter Malware Detection Trend (6 Months) auf Seite 66.

**Infection Type Trend**

Zeigt Trends für Infektionsalarmtypen über den letzten Tag, Woche oder Monat an. Details finden Sie unter Infection Type Trend auf Seite 67.

**Top Malware by Host and Activity**

Zeigt das Verhalten der top Malware Kategorien an, die dem überwachten Netzwerk erkannt wurden. Siehe Top Malware by Host and Activity auf Seite 68.

**Monitored Traffic**

Enthält ein mehrzeiliges Diagramm der im überwachten Netzwerk erkannten Verkehrstypen. Siehe Monitored Traffic auf Seite 69.

**IPS Trend**

Zeigt ein Diagramm der Anzahl der MVX-korrelierten IPS-Ereignisse und der Anzahl der stündlich erkannten kritischen IPS-Ereignisse an. Details finden Sie unter IPS Trend auf Seite 70.

**Service Health Statistiktrend**

Zeigt ein Diagramm der aggregierten Integritätsstufe (Healthy, Warning oder Critical) im Zeitverlauf für die von Ihnen ausgewählten Servicekategorien an. Details finden Sie unter Service Health Statistics Trend auf Seite 71.

**Appliance Utilization**

Zeigt vier Diagramme an, die zeigen, wie die Appliance Ressourcen verwendet werden und wann die Belastung Warnstufen oder kritische Stufen erreicht. Details finden Sie unter Appliance Utilization auf Seite 72.

**Submission Statistics Trend (Top 20)**

Zeigt die Anzahl der Malware Übermittlungen an, die am letzten Tag oder in der letzten Woche analysiert wurden. Statistiken werden für jede Domain, Quell-IP-Adresse und Ziel-IP-Adresse geboten. Details finden Sie unter Submission Statistics Trend (Top 20) auf Seite 74.

**SSL URL Categorization Trends (MB)**

Zeigt die Diagramme des SSL-Verkehrs an, der basierend auf URL-Kategorien und Kategoriegruppen umgangen, in die Whitelist aufgenommen, nicht kategorisiert oder abgefangen wurde. Siehe SSL URL Categorization Trends (MB) auf Seite 75.

**Asymmetric Traffic**

Zeigt das Diagramm von asymmetrischem oder Syn-only Verkehr in Bytes oder die Gesamtzahl der Datenflüsse für den angegebenen Zeitraum an. Details finden Sie unter Asymmetric Traffic auf Seite 77.

**Application Visibility (Top 25)**

Zeigt die Top 25 Anwendungen je nach ihrer Netzwerknutzung an. Der Sitzungszähler und die Bandbreite sind zwei der angezeigten Metriken. Details finden Sie unter Application Visibility (Top 25) auf Seite 78.

# Threat Level

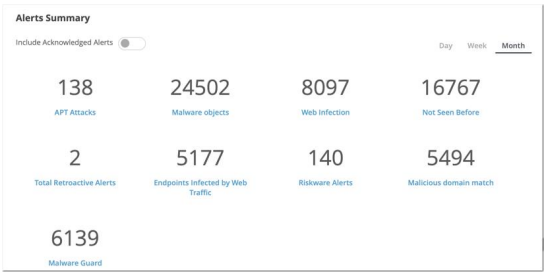
Das Threat Level Widget zeigt einen farbcodierte Zähler mit der Gesamtbedrohungsstufe für das überwachte Netzwerk an. Um die Bedrohungsstufe festzustellen—Low, Medium, High, or Critical—vergleicht die Appliance oder der Sensor Bedrohungen, die in den letzten zwei Monaten entdeckt wurden mit FireEyes Messungen der Bedrohungsstufe in der Branche und dem von Ihnen ausgewählten geografischen Standort.

**HINWEIS:** Das Widget zeigt keine Daten an, wenn die Appliance oder der Sensor nicht mit der FireEye Dynamic Threat Intelligence (DTI) Cloud verbunden ist.

Dieses Beispiel zeigt eine 45% oder "mittlere" Bedrohungsstufe für das überwachte Netzwerk. In diesem Fall wurden die Bedrohungsdaten für das überwachte Netzwerk mit FireEyes Bedrohungsdaten für Netzwerke in der Bank- und Finanzbranche in Nordamerika verglichen.

# Alerts Summary

Das Alerts Summary Widget führt die Anzahl der Alarme in jeder Angriffskategorie auf, die während des letzten Tages, Woche oder Monats entdeckt wurden. Sie können wählen, bestätigte Alarme ein- oder auszuschließen.




Die Namen der Angriffskategorien sind Shortcuts auf den Alerts Tab, die Riskware Alerts Seite oder die Smart Vision Alerts Seite.

**HINWEIS:** Informationen über die Widgets auf einem SmartVision Edition Sensor oder Appliance Dashboard finden Sie unter "SmartVision Alerts verwalten" im *Network Security SmartVision Funktionshandbuch*.

Die folgende Tabelle beschreibt Angriffskategorien, die auf dem Alerts Summary Widget des Dashboards gezählt werden können. Auf dem Widget können Sie auf den Namen einer Angriffskategorie klicken und die individuellen Alarme in dieser Kategorie über den ausgewählten Zeitraum hinweg anzeigen.

| Attack Category Counted | Um individuelle MVX-korrelierte Alarme anzuzeigen |
|---|---|
| Advanced Persistent Threats | Klicken Sie auf **APT Attacks**, um den Alerts Tab zu öffnen, der nach Alarmen in der Malware gefiltert ist, die einen der folgenden Werte enthalten:<br>• .APT.<br>• _APT_ |
| Attacks not seen before | Klicken Sie auf **Not Seen Before**, um den Alerts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die einen der folgenden Werte in der Malware Spalte enthalten:<br>• Exploit.Browser<br>• Malware.ZerodayMatch<br>• Malware.Binary<br>• Malware.ZerodayCallback<br>• ^DTI.Callback |

| Attack Category Counted | Um individuelle MVX-korrelierte Alarme anzuzeigen |
|---|---|
| Clients infected | Klicken Sie auf **Hosts Infected by Web Traffic**, um den Alerts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die einen der folgenden Werte in der Alert Type Spalte enthalten:<br>• Web Infection |
| Malicious domain matches | Klicken Sie auf **Malicious domain match**, um den Alerts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die einen der folgenden Werte in der Alert Type Spalte enthalten:<br>• Domain Match |
| Malware objects downloaded | Klicken Sie auf **Malware Objects**, um den Alerts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die einen der folgenden Werte in der Alert Type Spalte enthalten:<br>• Malware Object |
| Riskware Alerts | Klicken Sie auf **Riskware Alerts**, um die Riskware Alerts Seite zu öffnen. Die Seite führt Einträge auf, den folgenden Wert in der Riskware Type Spalte enthält:<br>• Riskware Object<br>• Riskware Callback<br>• Riskware Infection |
| SmartVision Alerts | Klicken Sie auf **SmartVision Alerts**, um die SmartVision Alerts Seite zu öffnen.<br>Diese Angriffskategorie tilt nur für SmartVision Appliances:<br>• SmartVision Edition Sensor<br>• SmartVision-fähiger Network Security Sensor<br>• SmartVision-fähige Network Security integrierte Appliance |
| SSL Intercepts | Klicken Sie auf **SSL Intercepts**. Der **Alerts** Tab führt Einträge auf, die den folgenden Wert in der **Alert Type** Spalte enthält:<br>• Malware Object<br>• Infection Match |
| Malware Guard | Klicken Sie auf **Malware Guard**, um den Alerts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die einen der folgenden Werte in der Alert Type Spalte enthalten:<br>• Malware Object<br>• Malware Callback |

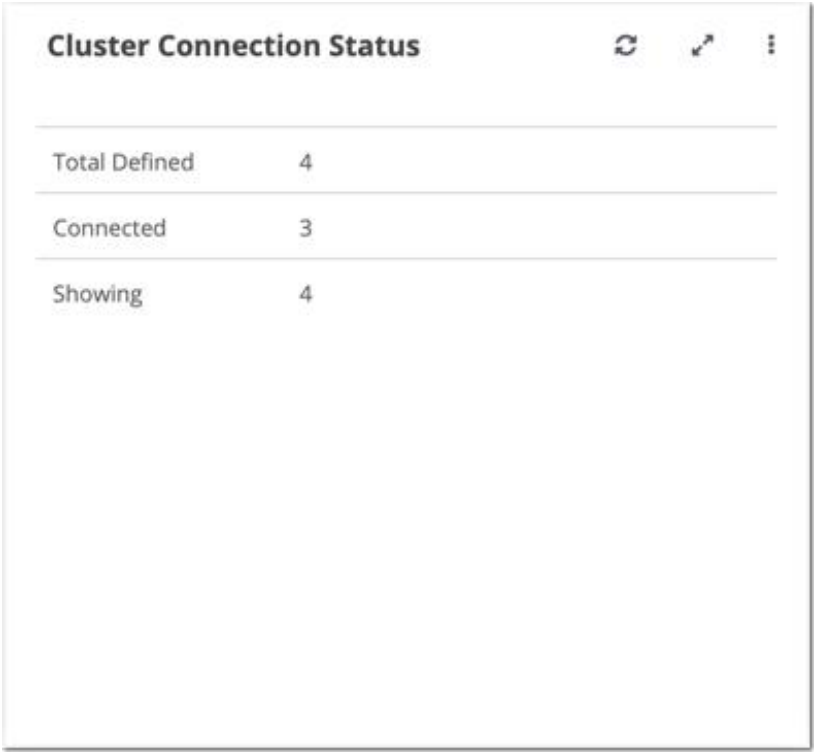
| Attack Category Counted | Um individuelle MVX-korrelierte Alarme anzuzeigen |
|---|---|
| ICAP Alerts | Klicken Sie auf **ICAP Alerts**, um den Alerts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die einen der folgenden Werte in der Alert Type Spalte enthalten:<br>• Web Infection<br>• Infection Match<br>• Malware Callback<br>• Malware Object |

## Recent Alerts (25)

Das Recent Alerts (25) Widget zeigt eine Tabelle der 25 letzten Alarme an, die von der Network Security Appliance entdeckt wurden. Das Widget zeigt Type, Malware, Victim IP, Attacker IP, Severity und Time (Typ, Malware, Opfer-IP, Angreifer IP, Schweregrad und Uhrzeit) an. Sie können die Tabelle filtern, um Alarme in einer der folgenden Kategorien anzuzeigen: Malware Object, Malware Callback, Infection Match, Web Infection, Domain Match, Riskware, IPS oder Smartvision. Klicken Sie auf einen Alarm, um genauere Einzelheiten anzuzeigen.

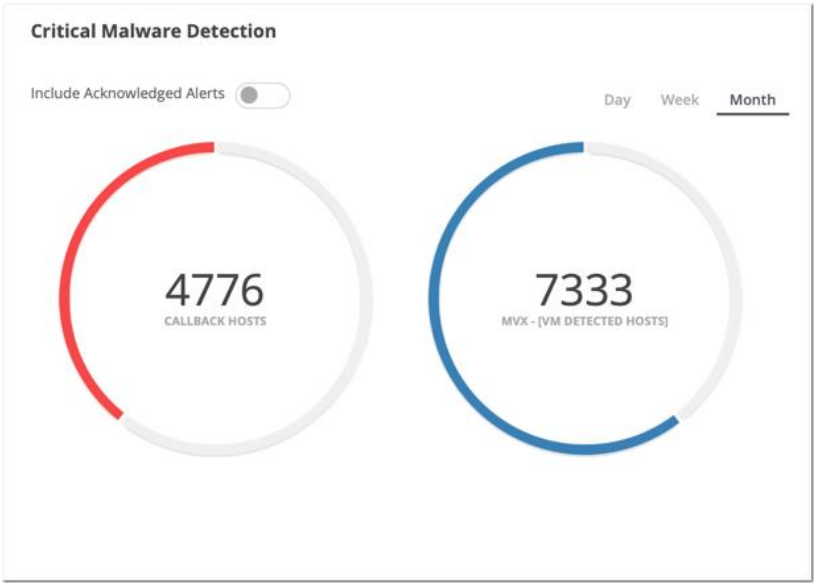
# Cluster Connection Status

Wenn verwaltete Network Security Appliances im Sensor Modus arbeiten, zeigt das Cluster Connection Widget auf der Central Management Appliance Statusinformationen über alle Eingabeverbindungen des Sensors mit Ihren entsprechenden Clustern an.



# Critical Malware Detection

Das Critical Malware Detection Widget zeigt die Anzahl der Hosts an, die kritische Malware Warnungen ausgelöst haben. Kritische Malware Alarme bestehen aus Malware Object, Web Infection und Malware Callback Alarmen. Sie können bestätigte Alarme in den Statistiken ein- und ausschließen.



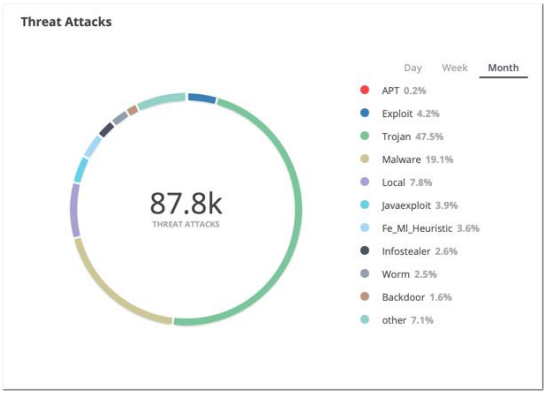

Jedes Kreisdiagramm enthält eine Verknüpfung mit dem Alerts Tab, wo Sie individuelle Alarmgruppen anzeigen können.

- Klicken Sie auf den roten Bogen im **Callback Hosts** Kreis, um den Alerts Tab zu öffnen, der gefiltert ist, Alarme auf kritischer Ebene anzuzeigen, die "Malware Object" in der Alert Type Spalte enthalten
- Klicken Sie auf den blauen Bogen im **MVX – [VM-Detected Hosts]** Kreis, um den Alerts Tab zu öffnen, der gefiltert ist, Alarme auf kritischer Ebene anzuzeigen, die “Malware Object” oder “Web Infection” in der Alert Type Spalte enthalten.

**HINWEIS:** Informationen über die Widgets auf einem SmartVision Edition Sensor oder Appliance Dashboard finden Sie unter "SmartVision Alerts verwalten" im *Network Security SmartVision Funktionshandbuch*.

# Threat Attacks

Das Threat Attacks Widget zeigt die Top Threat Attack Typen als Prozentsätze an. Die Gesamtzahl der Angriffe erscheint in der Mitte des Diagramms. Um die Anzahl der Angriffe eines bestimmten Typs anzuzeigen, ziehen Sie den Mauszeiger über den Legendeneintrag.



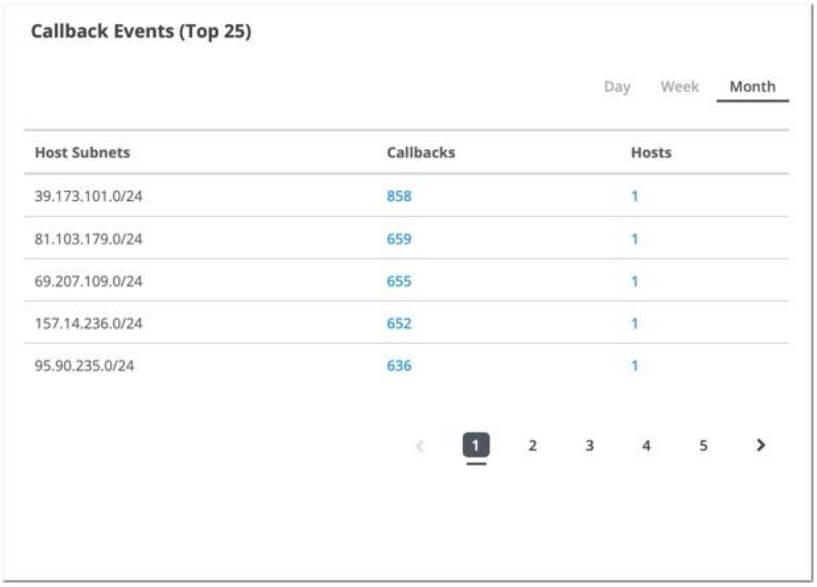

Um die von einem Threat Attack Typen repräsentierten Alarme anzuzeigen, klicken Sie auf den Legendeneintrag, um auf den nach ausgewählten Angriffstypen gefilterten Alerts Tab zu gehen.

| Threat Attack Type | Übereinstimmungswert für das Malware Feld auf der Alerts Seite |
|---|---|
| APT | APT |
| Exploit | ^Exploit$\|^Exploit.\|^Win.Exploit. |
| Fe_Heuristic_Malware_ Reflection_Jar_3 | ^Fe_Heuristic_Malware_Reflection_Jar_3$\| ^Fe_Heuristic_Malware_Reflection_Jar_3.\| ^Win.Fe_Heuristic_Malware_Reflection_Jar_3. |
| Fe_Heuristic_Malware_ Reflection_Jar_6 | ^Fe_Heuristic_Malware_Reflection_Jar_6$\| ^Fe_Heuristic_Malware_Reflection_Jar_6.\| ^Win.Fe_Heuristic_Malware_Reflection_Jar_6. |
| Fe_Packer_Upx | ^Fe_Packer_Upx$\|^Fe_Packer_Upx.\| ^Win.Fe_Packer_Upx. |
| Infostealer | ^Infostealer$\|^Infostealer.\|^Win.Infostealer. |
| Javaexploit | ^Javaexploit$\|^Javaexploit.\|^Win.Javaexploit. |
| Local | ^Local$\|^Local.\|^Win.Local. |
| Malicious | ^Malicious$\|^Malicious.\|^Win.Malicious. |
| Malware | ^Malware$\|^Malware.\|^Win.Malware. |

| Threat Attack Type | Übereinstimmungswert für das Malware Feld auf der Alerts Seite |
|---|---|
| Pua | `^Pua$\|^Pua.\|^Win.Pua.` |
| Trojan | `^Trojan$\|^Trojan.\|^Win.Trojan.` |

# Callback Events (Top 25)

Das Callback Events (Top 25) Widget führt die Top 25 Subnetzein Ihrem überwachten Netzwerk auf, gemäß der Anzahl der Rückrufereignisse, die am letzten Tag, Woche oder Monat Callback Ereignisse entdeckt wurden, einschließlich Signatur-Übereinstimmungen und Kommunikationen mit einem Botnet-Server.




Für jedes aufgeführte Subnetz zeigt das Widget die folgenden Informationen an:

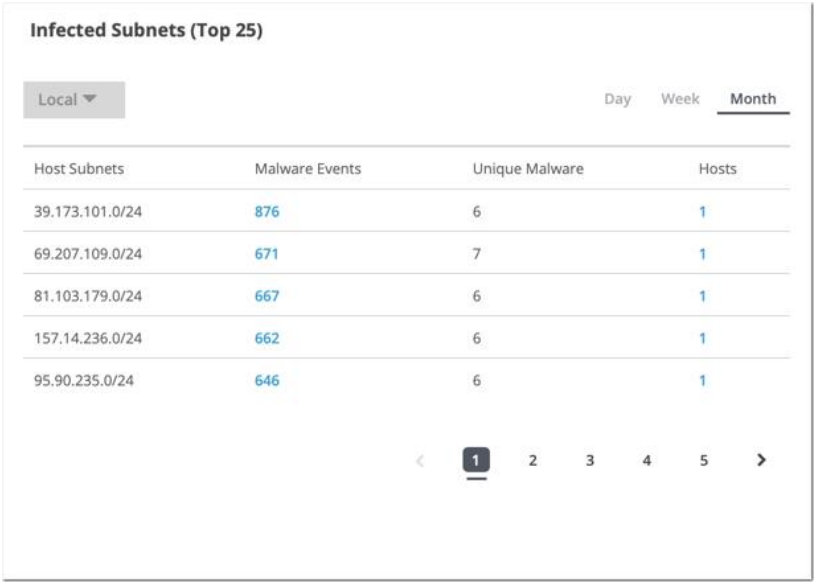
- Die Anzahl der erkannten Rückrufereignisse
- Die Anzahl der infizierten Hosts

Um Details über ein infiziertes Subnetz anzuzeigen, klicken Sie auf die Zahl in der Callbacks Spalte oder in der Hosts Spalte. Der Alerts Tab wird geöffnet, der gefiltert ist, um wichtige und kritische Alarme anzuzeigen, nach Angriffsregelnamen gruppiert, die den folgenden Kriterien entsprechen:

- Type enthält `Malware Callback`
- Source IP = IP-Adresse des infizierten Subnetzes.
- Der Zeitraum ist der gleiche wie im Callback Events (Top 25) Widget.

# Infected Subnets (Top 25)

Das Infected Subnets (Top 25) Widget führt die Top 25 Subnetze im überwachten Netzwerk auf, gemäß der Gesamtzahl von Malware Ereignissen, die am letzten Tag, in der letzten Woche oder im letzten Monat entdeckt wurden.




Für jedes aufgeführte Subnetz zeigt das Widget die folgenden Informationen an:

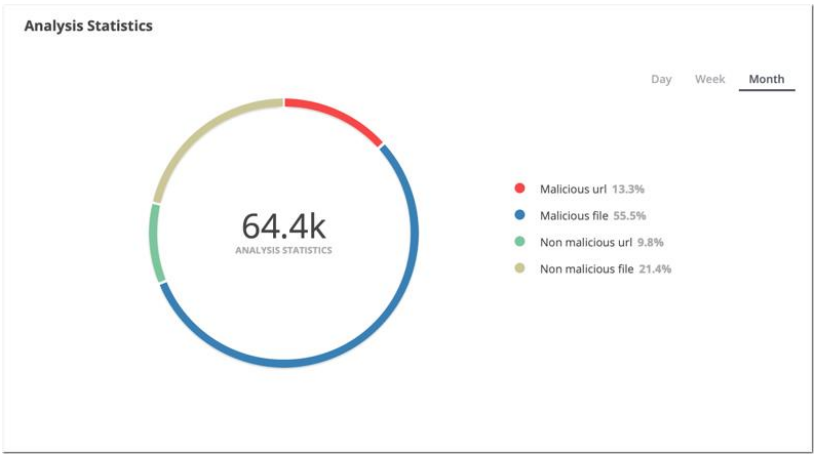
- Anzahl der entdeckten Malware Ereignisse
- Anzahl der einzigartigen Malware Ereignisse
- Anzahl der betroffenen Hosts (einzigartige IP-Adressen in der Source IP Spalte)

Zwei Spalten in der Liste enthalten Verknüpfungen zu Alarmlisten:

- Klicken Sie auf eine Zahl in der Malware Events Spalte auf dem Widget, um den Alerts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die die IP-Adresse des infizierten Subnetzes in der Source IP Spalte auf dem Alerts Tab enthalten.
- Klicken Sie auf die Zahl in der Hosts Spalte auf dem Widget, um den Hosts Tab zu öffnen, der gefiltert ist, um Alarme anzuzeigen, die die IP-Adresse des infizierten Subnetzes in der Source IP Spalte des Hosts Tab enthält.

# Analysis Statistics

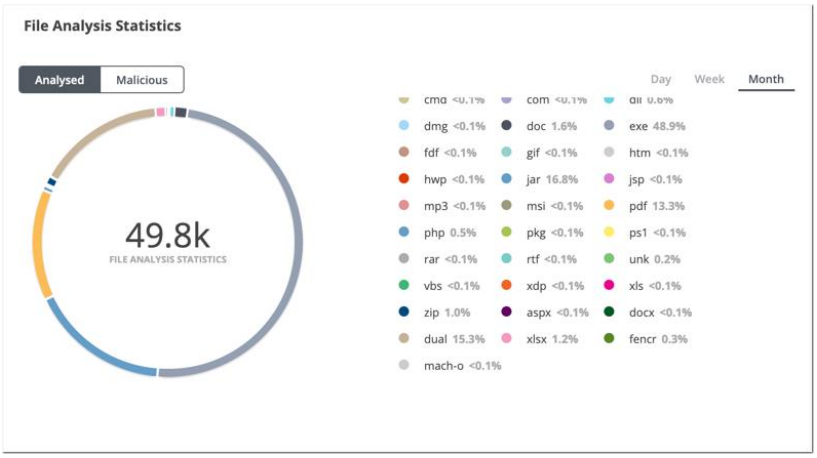
Das Analysis Statistics Widget zeigt den Prozentsatz bösartiger und nicht-bösartiger Dateien und URLs an, die gescannt wurden.




Die Gesamtzahl der gescannten bösartigen und nicht-bösartigen Dateien und URLs wird in der Mitte des Diagramms angezeigt. Um die Anzahl der gescannten bösartigen oder nicht-bösartigen Dateien oder die Anzahl der gescannten bösartigen oder nicht bösartigen URLs anzuzeigen, ziehen Sie den Mauszeiger über den entsprechenden Legendeneintrag.

# File Analysis Statistics

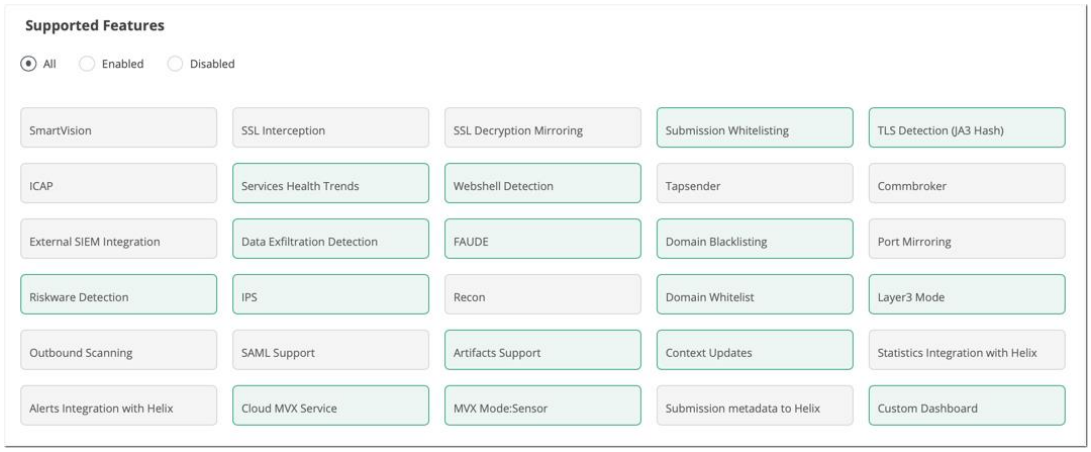
Das File Analysis Statistics Widget zeigt die Dateitypen, die zur Analyse eingegeben wurden, als Prozentsätze an. Sie können Daten für alle analysierten Dateitypen oder nur für bösartige Dateien anzeigen.




Die Gesamtzahl der analysierten Dateien (oder analysierten bösartigen Dateien) wird in der Mitte des Diagramms angezeigt. Um die Anzahl der eingegebenen Dateien eines bestimmten Typs anzuzeigen, ziehen Sie den Mauszeiger über den Legendeneintrag.

# Supported Features

Die Supported Features Widget führt alle unterstützten Funktionen auf. Die Namen der aktivierten Funktionen werden durch schattierte Karten angezeigt. Um die Beschreibung und Kategorie einer Funktion anzuzeigen, schieben Sie den Mauszeiger über die Karte.

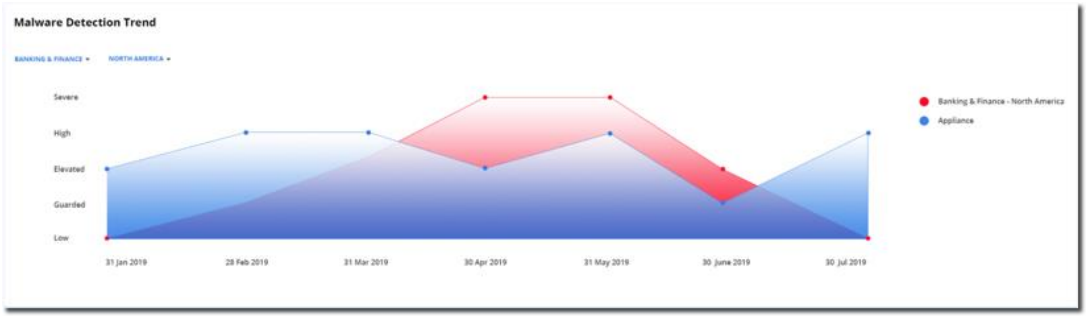



Sie können die Anzeige Filtern, um nur aktivierte oder deaktivierte Funktionen anzuzeigen.

Diese Informationen sind auch im About Tab verfügbar.

# Malware Detection Trend (6 Months)

Das Malware Detection Trend (6 Months) Widget zeigt den von Ihrer FireEye Appliance oder Sensor erkannten Malware Trend im Vergleich mit der innerhalb einer bestimmten Branche und geografischem Standort in den letzten 6 Monaten entdeckten Malware an,




**HINWEIS:** Das Widget zeigt keine Daten an, wenn die Appliance oder der Sensor nicht mit der FireEye Dynamic Threat Intelligence (DTI) Cloud verbunden ist.

**Um einen der Malware Erkennungstrends auszufiltern:**

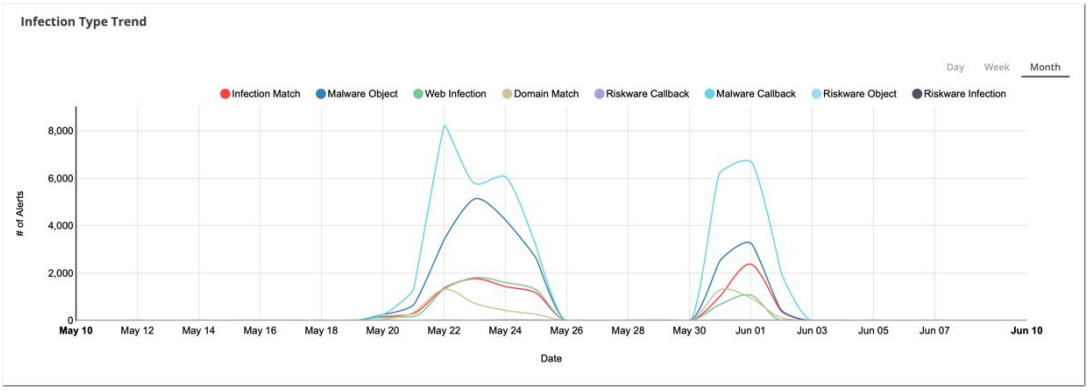
- Klicken Sie auf seine farbige Scheibe in der Legende. Die Scheibe wird zu einem Kreis.

**Um das Herausfiltern eines Malware Trends zu stoppen:**

- Klicken Sie auf die entsprechende farbige Scheibe in der Legende.

# Infection Type Trend

Das Infection Type Trend Widget deckt Trends von Infektionsalarmtypen auf, indem es die Anzahl der Warnungen jedes Typs für jeden Tag grafisch darstellt.




Um die Anzahl der Alarme anzuzeigen, die an einem bestimmten Tag aufgetreten sind, zeihen Sie den Mauszeiger über das Diagramm.

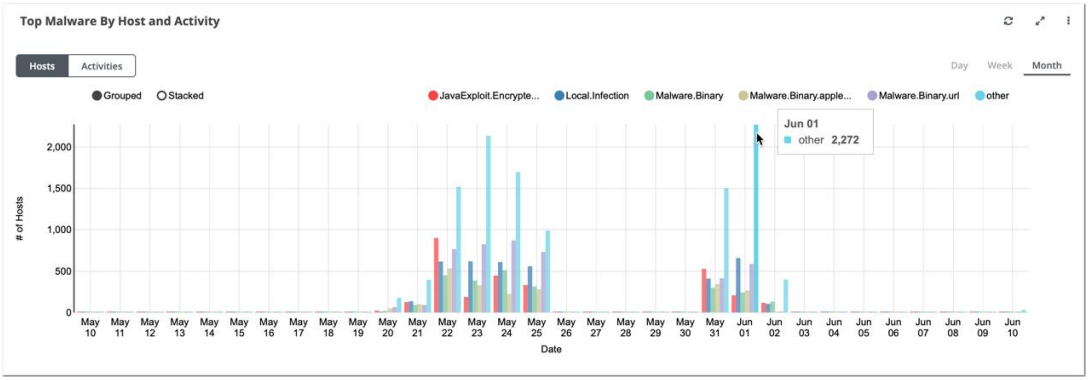
Um einen Alarmtyp von dem Diagramm auszuschließen, klicken Sie auf das farblich kodierte Symbol in der Legende. Um die Daten auf dem Diagramm wiederherzustellen, klicken Sie erneut auf das Symbol.

# Top Malware by Host and Activity

Das Top Malware by Host and Activity Widget zeigt das Verhalten der Top Malware Kategorien, die in dem überwachten Netzwerk am letzten Tag, der letzten Woche oder dem letzten Monat entdeckt wurden.

**HINWEIS:** Durch Ändern des Zeitraums können die Top Malware Kategorien geändert werden.

Für jede Malware Kategorie zeigt das Diagramm entweder die Anzahl der Hosts (**Hosts**) an, die mit dem Malware Typ infiziert sind oder die Anzahl der Erkennungen (**Activities**) für den Malware Typ.

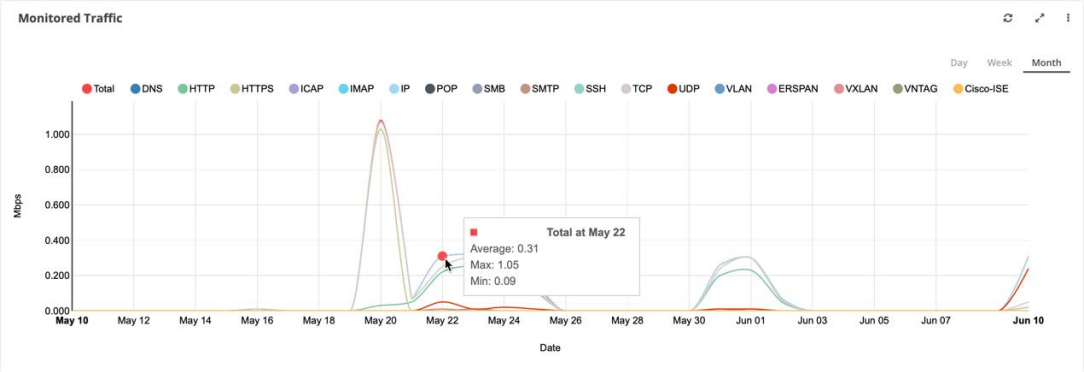



Bewegen Sie den Mauszeiger über das Diagramm, um die durchschnittliche, maximale und minimale Anzahl von Hosts oder Angriffen für eine Malware Kategorie an einem bestimmten Tag anzuzeigen.

Um eine Malware Infektionskategorie von den Daten in dem Diagramm auszuschließen, klicken Sie auf das farblich kodierte Symbol in der Legende. Um die Daten auf dem Diagramm wiederherzustellen, klicken Sie erneut auf das Symbol.

# Monitored Traffic

Das Monitored Traffic Widget zeigt ein Diagramm an, das die Rate (in Mbps bemessen) des überwachten Verkehrs zeichnet. Das Diagramm zeigt den gesamten überwachten Datenverkehr in rot und individuelle Verkehrstypen in anderen Farben an.




Um die Anzahl der Hosts anzuzeigen, die mit einer Malware Kategorie an einem bestimmten Tag infiziert wurden, ziehen Sie den Mauszeiger über das Diagramm.

Um einen Malware Typ von den Daten in dem Diagramm auszuschließen, klicken Sie auf das farblich kodierte Symbol in der Legende. Um die Daten auf dem Diagramm wiederherzustellen, klicken Sie erneut auf das Symbol.

# IPS Trend

Das IPS Trend Widget zeigt die Anzahl der MVX-korrelierten IPS-Ereignisse und die Anzahl der stündlich erkannten kritischen IPS-Ereignisse an.

Um die Anzahl der Ereignisse anzuzeigen, die zu einer bestimmten Zeit angezeigt werden, ziehen Sie den Mauszeiger über das Diagramm.

# Service Health Statistics Trend

Das Service Health Statistics Trend Widget zeichnet die aggregierte Integritätsstufe (Healthy, Warning oder Critical) im Zeitverlauf für die von Ihnen ausgewählten Servicekategorien. Sie können Integritätsverfolgung für eine oder jede Kombination der folgenden Servicekategorien aktivieren:

- Cloud-Erkennung
- Metadaten-Streaming
- Analyse
- System
- Netzwerk-Verarbeitung
- DTI

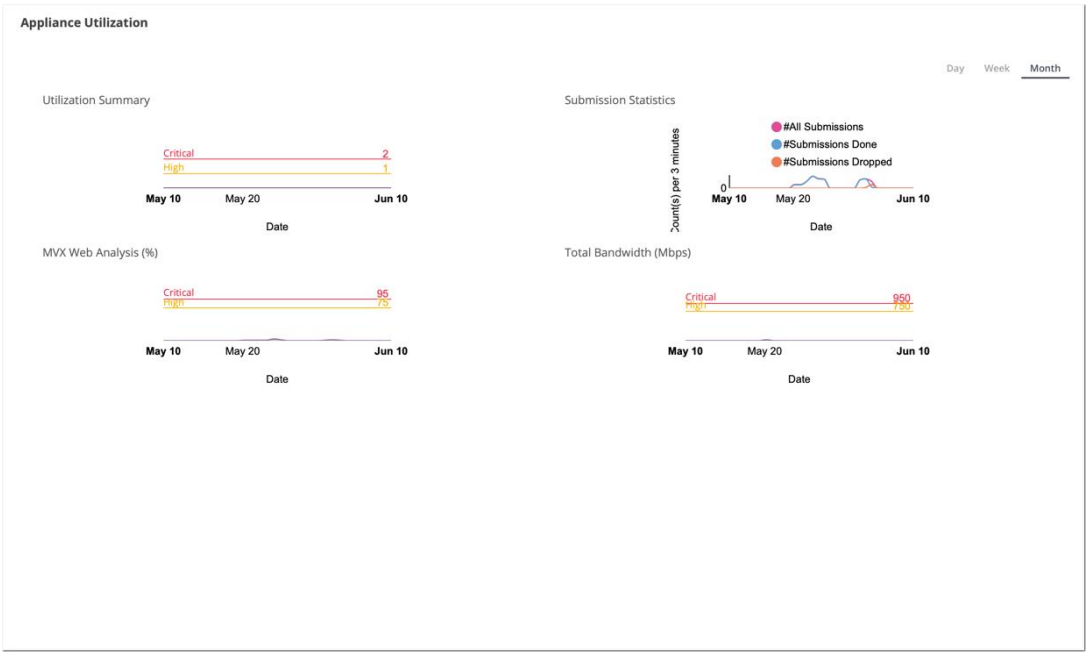
Jeder Kategorieschaltfläche zeigt entweder die aktuelle Integritätsstufe oder "Disabled" an.


Um die Aufgliederung von Service-Integritätsstufen zu einem beliebigen Zeitpunkt anzuzeigen, ziehen Sie den Mauszeiger über das Diagramm.

# Appliance Utilization

Das Appliance Utilization Widget enthält vier Diagramme, die anzeigen, wie die Ressourcen der Appliances genutzt werden.

**HINWEIS:** Die Operator Rolle kann nur auf das Appliance Utilization Widget zugreifen und die Analyst Rolle hat keinen Zugriff auf die Appliance Utilization Widget.




Utilization Summary

Dieses Diagramm zeichnet die Nutzungsebene der Appliance über einen Zeitraum hinweg auf: Normal (0), High (1) oder Critical (2).
Eine Hohe oder Kritische Benutzerstufe kann bedeuten, dass die Appliance überzeichnet ist.

Submission Statistics

Dieses Diagramm zeichnet die Anzahl der Dateien oder URLs auf, die zur Analyse über einen Zeitraum hinweg eingegeben wurden. Gesamtzahl der Eingaben, analysierte Eingaben und abgelegte Eingaben werden getrennt aufgezeichnet.

MVX Web Analysis (%)

Dieses Diagramm zeichnet den Prozentsatz der Eingaben auf, die über einen Zeitraum hinweg zu Web Infection Alarmen geführt haben. Die High Nutzungsebene (75%) und die Critical Nutzungsebene (95%) sind markiert.

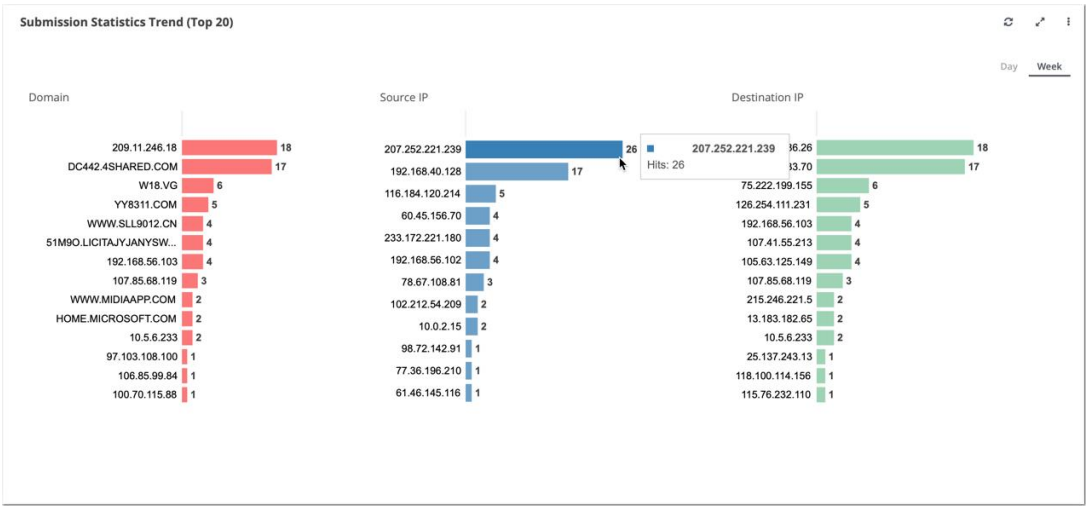
Total Bandwidth (Mbps)

Dieses Diagramm zeichnet die gesamte Bandbreitennutzung in Mbps über einen Zeitraum hinweg auf. Die High Nutzungsstufe (750 Mbit / s) und die Critical Nutzungsstufe (950 Mbit / s) sind markiert.

# Submission Statistics Trend (Top 20)

Das Submission Statistics Trend (Top 20) Widget zeigt die Anzahl der Malware Eingaben an, die am letzten Tag oder in der letzten Woche analysiert wurden. Statistiken werden für jede Domain, Quell-IP-Adresse und Ziel-IP-Adresse geboten.

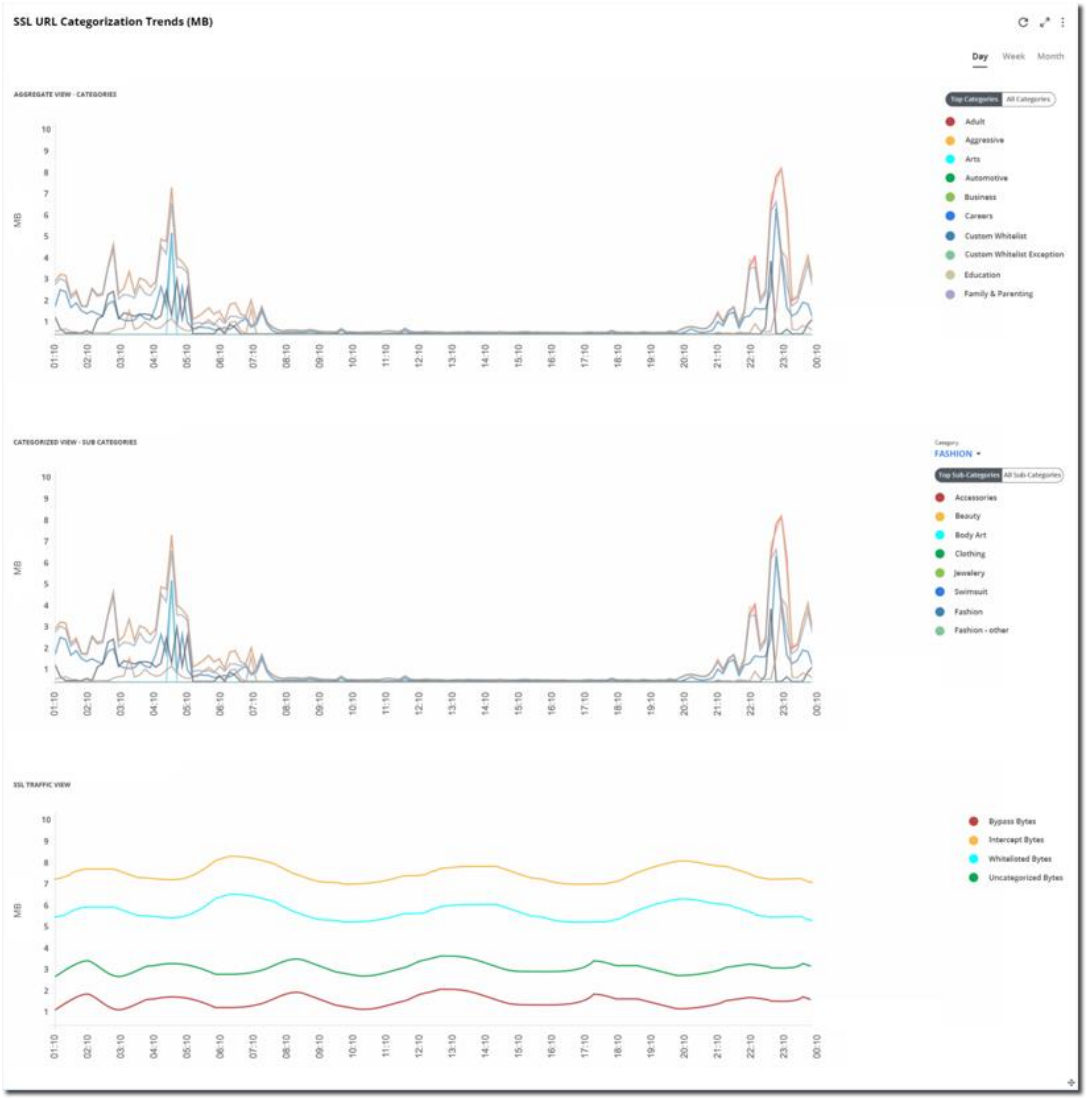



Bewegen Sie den Mauszeiger über die Leiste im Diagramm, um die Anzahl der MVX-Clusterübermittlungen für eine bestimmte Domain, Quell-IP-Adresse oder Ziel-IP-Adresse anzuzeigen.

# SSL URL Categorization Trends (MB)

Das SSL URL Categorization Trends (MB) Widget zeichnet URL Kategorisierungsstatistiken an, die am letzten Tag, in der letzten Woche oder im letzten Monat für die vordefinierte FireEye Whitelist, benutzerdefinierte Whitelist und benutzerdefinierte Whitelist Ausnahme-URL Kategorien gesammelt wurden.

**HINWEIS:** Sie müssen die SSL-Kategorisierungstrend Funktion aktivieren, um die Diagramme von SSL-Verkehr je nach URL-Kategorien und Kategoriegruppen anzuzeigen. Weitere Informationen finden Sie unter "Die Anzeige der URL Categorization Trend Statistics aktivieren oder deaktivieren" in der *Network Security Bedienungsanleitung*.



**Um eine URL-Kategorie, Subkategorie oder SSL-Verkehrstyp herauszufiltern:**

- Klicken Sie auf seine farbige Scheibe in der Legende. Die Scheibe wird zu einem Kreis.

Das SSL Categorization Trend Statistics Widget enthält drei Diagramme:

**Aggregate View – Categories**

Das erste Diagramm zeigt die gesammelten Statistiken für Verkehrsdurchsatz für die Top 10 URL Kategorien oder für alle URL Kategorien an.

**Categorized View – Sub Categories**

Das zweite Diagramm zeigt die gesammelten Statistiken für Verkehrsdurchsatz für die Top 10 URL-Kategorien oder für alle URL-Subkategorien an.

**SSL Traffic View**

Wenn SSL-Interception auf mindestens einem Netzwerkportpaar aktiviert ist, zeigt das dritte Diagramm die gesammelten Statistiken für Verkehrsdurchsatz an, der übergangen, auf die Whitelist gesetzt, abgefangen und (falls aktiviert) nicht kategorisiert wurde.

Wenn SSL-Interception auf einem Netzwerkportpaar deaktiviert ist, zeigt das dritte Diagramm nur die gesammelten Statistiken für Verkehrsdurchsatz an, der von der FireEye Unified Mulitflow Engine (FUME) nicht kategorisiert wurde.

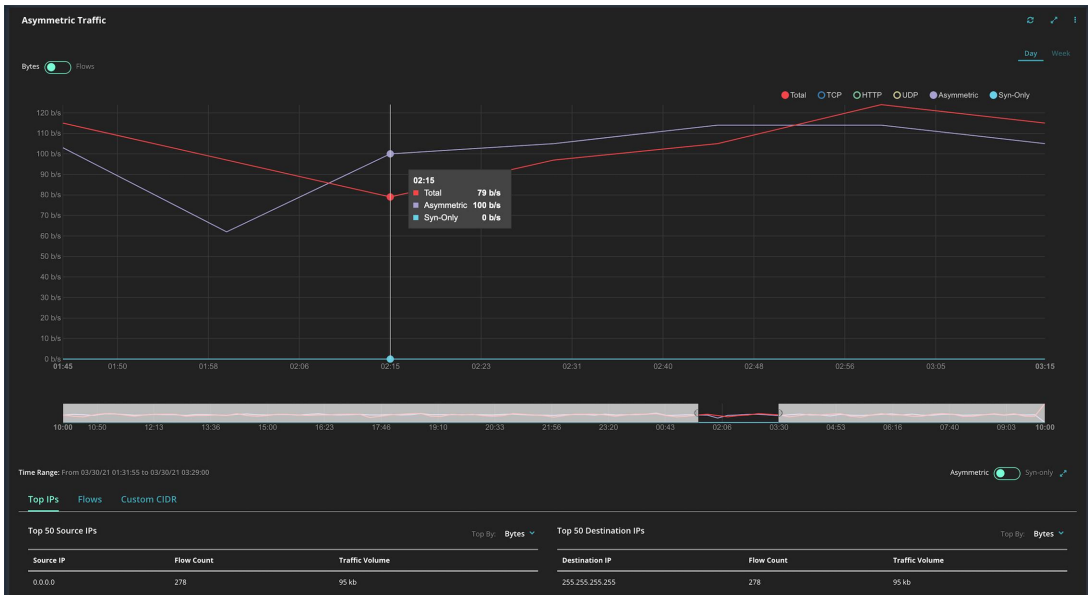
# Asymmetric Traffic

Das Asymmetric Traffic Widget zeigt Informationen über die folgenden Verkehrstypen an:

- TCP
- HTTP
- UDP
- Asymmetric
- SYN-only

Für jeden Verkehrstyp zeigt das Diagramm entweder das Verkehrsvolumen in Bytes oder die Anzahl der Verkehrsflüsse an. Um das Verkehrsvolumen in Bytes oder die Anzahl der Datenflüsse zu einem bestimmten Zeitpunkt anzuzeigen, bewegen Sie den Mauszeiger über das Diagramm. Klicken Sie auf den Namen des Verkehrstyps in der Legende, um ihn auf dem Diagramm anzuzeigen.

Um das Diagramm in größerem Detail anzuzeigen, klicken und ziehen Sie den Mauszeiger im Fokusdiagramm. Um diese Ansicht zu beenden, klicken Sie in dem grauen Bereich.




Die Tabelle zeigt detaillierte Informationen zu den Top-IPs und Flows für die Netzwerke an, die asymmetrischen und SYN-only-Verkehr erzeugen. Sie können benutzerdefinierte Classless Inter-Domain Routing (CIDR) Adressen definieren, um das asymmetrische Verkehrsvolumen und die Anzahl der Datenflüsse für jede CIDR-Adresse anzuzeigen.

## Eine benutzerdefinierte CIDR-Adresse hinzufügen oder entfernen

Um eine benutzerdefinierte CIDR-Adresse hinzuzufügen:

1. Klicken Sie auf Custom CIDR > Add.
2. Unter Type wählen Sie Source oder Destination.
3. Geben Sie das CIDR ein und klicken Sie auf Add.

Um eine benutzerdefinierte CIDR-Adresse zu löschen:

1. Klicken Sie auf Custom CIDR.
2. Klicken Sie in der Action Spalte auf den Papierkorb und dann auf DELETE.

## Application Visibility (Top 25)

Das Application Visibility (Top 25) Widget führt die Top 25 auf dem Netzwerk überwachten Anwendungen auf, geordnet nach der Anzahl der Sitzungen und dem Verkehrsvolumen des letzten Tages, der letzten Woche oder des letzten Monats. Die folgenden Tabs führen die Anwendungen je nach ihrem Typ auf:

- Client
- Payload
- Service

Das Diagramm zeigt die Netzwerknutzung für jede Anwendung über die Anwendungstypen hinweg an. Wählen Sie die Metrik von der Liste:

- Sessions
- Traffic Volume

# Benutzerdefinierte Dashboards

Sie können persönliche benannte Dashboards erstellen, in denen nur die von Ihnen ausgewählten Dashboard-Widgets angezeigt werden und die von Ihnen konfigurierten Zeiträume abgedeckt werden.

**HINWEIS:** Auf die von Ihnen erstellten benutzerdefinierten Dashboards können von Ihrem Benutzerkonto zugegriffen werden.

Jede der unter Dashboard- und Widget-Verwaltung auf Seite 85 beschriebenen Vorgänge kann sowohl auf benutzerdefinierten Dashboards als auch dem vordefinierten FireEye Dashboard ausgeführt werden.

Sie können ein neues Dashboard erstellen, indem Sie ein vorhandenes Dashboard klonen, oder Sie können mit einem leeren Dashboard beginnen. Die Dashboard-Namen werden oben auf dem Dashboard Tab angezeigt, und Sie können die Reihenfolge ändern, in der die Namen angezeigt werden.

- Ein Dashboard klonen auf der nächsten Seite
- Ein neues Dashboard erstellen auf Seite 81
- Dashboard-Namen neu anordnen auf Seite 81

Die folgenden Vorgänge treffen auf das aktuelle benutzerdefinierte Dashboard zu:

- Ein benutzerdefiniertes Dashboard umbenennen auf Seite 81
- Das Standard Dashboard festlegen auf Seite 82
- Ein benutzerdefiniertes Dashboard löschen auf Seite 82

Die folgenden Vorgänge treffen auf Widgets im aktuellen benutzerdefinierten Dashboard zu:

- Widgets zu einem benutzerdefinierten Dashboard hinzufügen auf Seite 82
- Die Größe eines Widgets in einem benutzerdefinierten Dashboard ändern auf Seite 83
- Ein Widget in ein benutzerdefiniertes Dashboard verschieben auf Seite 83
- Ein Widget von einem benutzerdefinierten Dashboard entfernen auf Seite 84

### Voraussetzungen

- Admin, Analyst, Monitor oder Operator Zugriff auf die Appliance.
- Sie sind auf der Appliance Web -UI angemeldet.

## Ein Dashboard klonen

Durch Klonen wird eine Kopie eines Dashboards erstellt, das nur für Ihr Benutzerkonto zugänglich ist.

**Um ein Dashboard zu klonen:**

1. Klicken Sie auf **Dashboard** und wählen Sie das Dashboard, das Sie klonen wollen.
2. Klicken Sie auf das More Options Menü auf Dashboard-Ebene (⋮) und wählen Sie **Clone**.
3. Geben Sie einen Namen für das neue Dashboard ein.
4. Klicken Sie auf **Clone**.
5. Um ein Widget hinzuzufügen—klicken Sie auf **Widget Libraries** und dann auf **Add** für dieses Widget.

   Einige Widgets enthalten Konfigurationsoptionen. Sie können diese Einstellungen jetzt konfigurieren und jederzeit ändern:

   - Vergleichsoptionen für die Bedrohungsintelligenz (z.B. **Region** und **Industry**)
   - Optionen für den Zeitraum (z.B. **Day**, **Week**, **Month**)
   - Datenfilterungsoptionen (z.B. ob bestätigte Alarme eingeschlossen werden sollen)
6. Um Widgets neu anzuordnen—Ziehen Sie ein Widget an der Titelleiste auf eine neue Position auf dem Dashboard.
7. Um ein Widget zu entfernen—Klicken Sie auf das More Options Widgetmenü (⋮) und wählen Sie **Remove**.

# Ein neues Dashboard erstellen

Verwenden Sie die **+Add** Option auf der Dashboard Seite, um ein neues, leeres Dashboard zu erstellen, das nur für Ihr Benutzerkonto zugänglich ist.

**Um ein neues Dashboard zu erstellen:**

1. Klicken Sie auf **Dashboard** und dann auf **+Add**.
2. Geben Sie einen Namen für das neue Dashboard ein und klicken Sie dann auf das Häkchen.
3. Um ein Widget hinzuzufügen—klicken Sie auf **Widget Libraries** und dann auf **Add** für dieses Widget.

   Einige Widgets enthalten Konfigurationsoptionen. Sie können diese Einstellungen jetzt konfigurieren und jederzeit ändern:

   - Vergleichsoptionen für die Bedrohungsintelligenz (z.B. **Region** und **Industry**)
   - Optionen für den Zeitraum (z.B. **Day**, **Week**, **Month**)
   - Datenfilterungsoptionen (z.B. ob bestätigte Alarme eingeschlossen werden sollen)
4. Um Widgets neu anzuordnen—Ziehen Sie ein Widget an der Titelleiste auf eine neue Position auf dem Dashboard.
5. Um ein Widget zu entfernen—Klicken Sie auf das More Options Widgetmenü (⋮) und wählen Sie **Remove**.

# Dashboard-Namen neu anordnen

Um die Dashboard-Namen oben auf der Dashboard Seite neu anzuordnen, ziehen Sie die Dashboard-Namen.

# Ein benutzerdefiniertes Dashboard umbenennen

Folgen Sie diesen Schritten, um ein benutzerdefiniertes Dashboard umzubenennen. Das vordefinierte FireEye Dashboard kann nicht umbenannt werden.

**Um ein benutzerdefiniertes Dashboard umzubenennen:**

1. Greifen Sie auf das benutzerdefinierte Dashboard zu, das Sie umbenennen wollen.
2. Klicken Sie das More Options Menü (⋮) auf der Dashboard-Ebene und wählen Sie **Rename**.

3. Tippen Sie den neuen Namen für das Dashboard und klicken Sie dann auf das Häkchen.

## Das Standard Dashboard festlegen

Folgen Sie diesen Schritten um ein beliebiges Dashboard als das Standard Dashboard festzulegen. Das Standard Dashboard wird angezeigt, wenn Sie sich auf der Appliance Web-UI anmelden.

**Um das Standard Dashboard festzulegen.**

1. Rufen Sie das Dashboard auf, das Sie als Standard festlegen wollen.
2. Klicken Sie auf der Dashboard-Ebene auf das More Options Menü (⋮) und wählen Sie **Mark as Default**.

## Ein benutzerdefiniertes Dashboard löschen

Folgen Sie diesen Schritten, um ein benutzerdefiniertes Dashboard zu entfernen. Das vordefinierte FireEye Dashboard kann nicht gelöscht werden.

**Um ein benutzerdefiniertes Dashboard zu löschen:**

1. Greifen Sie auf das benutzerdefinierte Dashboard zu, das Sie entfernen wollen.
2. Klicken Sie auf der Dashboard-Ebene auf das More Options Menü (⋮) und wählen Sie **Delete**.
3. Klicken Sie auf **Yes, Delete**.

## Widgets zu einem benutzerdefinierten Dashboard hinzufügen

Folgen Sie diesen Schritten, um Widgets zu einem benutzerdefinierten Dashboard hinzuzufügen. Sie können keine Widgets zu dem vordefinierten FireEye Dashboard hinzufügen.

**Um Widgets zu einem benutzerdefinierten Dashboard hinzuzufügen:**

1. Klicken Sie auf **Dashboard** und wählen Sie das Dashboard, das Sie bearbeiten wollen.
2. Klicken Sie auf **Widgets Library**.
3. Klicken Sie auf **Add**, um ein Widget zu dem Dashboard hinzuzufügen.

# Die Größe eines Widgets in einem benutzerdefinierten Dashboard ändern

Folgen Sie diesen Schritten, um die Größe von Widgets in einem benutzerdefinierten Dashboard zu ändern. Im vordefinierten FireEye Dashboard kann die Größe von Widget nicht geändert werden.

**Um die Größe eines Widgets in einem benutzerdefinierten Dashboard zu ändern.**

1. Greifen Sie auf das benutzerdefinierte Dashboard zu, dessen Größe Sie ändern wollen.
2. Bewegen Sie den Mauszeiger über die untere rechte Ecke des Widgets, um den Cursor in einen kleinen diagonalen nach unten Pfeil zu verändern. 
3. Klicken und ziehen Sie die Ecke, um die Breite, Höhe oder beides des Widgets zu vergrößern oder zu verkleinern.

# Ein Widget in ein benutzerdefiniertes Dashboard verschieben

Folgen Sie diesen Schritten, um die Reihenfolge der Widgets in einem benutzerdefinierten Dashboard neu anzuordnen. In dem vordefinierten FireEye Dashboard können Widgets nicht neu angeordnet werden.

**Um Widgets in einem benutzerdefinierten Dashboard neu anzuordnen:**

1. Klicken Sie auf **Dashboard** und wählen Sie das Dashboard, das Sie bearbeiten wollen.
2. Ziehen Sie individuelle Widgets innerhalb des Dashboards.

# Ein Widget von einem benutzerdefinierten Dashboard entfernen

Folgen Sie diesen Schritten, um ein Widget von einem benutzerdefinierten Dashboard zu entfernen. Vom vordefinierten FireEye Dashboard können Widgets nicht entfernt werden.

**Um ein Widget von einem benutzerdefinierten Widget zu entfernen:**

1. Klicken Sie auf **Dashboard** und wählen Sie das Dashboard, das Sie bearbeiten wollen.
2. Bewegen Sie den Mauszeiger über der oberen rechten Ecke des Widgets.
3. Klicken Sie auf der Widget-Ebene auf das More Options Menü (⋮) und wählen Sie **Remove**.

# Dashboard- und Widget-Verwaltung

Sie können die Widgets anzeigen und verwalten, die nur für Ihr Benutzerkonto zugänglich sind. Alle Benutzerkonten haben Zugriff auf das vordefinierte Dashboard mit dem Namen **FireEye Dashboard**.

**HINWEIS:** Ein Benutzerkonto hat Zugriff auf die benutzerdefinierten Dashboards, die nur von diesem Konto erstellt wurden. Weitere Informationen finden Sie unter Benutzerdefinierte Dashboards auf Seite 79.

Der folgende Vorgang gilt für alle Dashboards, die für Ihr Benutzerkonto zugänglich sind.

- Das automatische Aktualisierungsintervall konfigurieren auf der nächsten Seite

Die folgenden Vorgänge gelten für das aktuelle Dashboard:

- Die in All Widgets angezeigten Daten aktualisieren auf der nächsten Seite
- Den von allen Widgets abgedeckten Zeitraum konfigurieren auf Seite 87
- Ein Dashboard speichern oder drucken auf Seite 87

Die folgenden Vorgänge gelten für ein einzelnes Widget im aktuellen Dashboard:

- Die in einem einzigen Widget angezeigten Daten aktualisieren auf Seite 88
- Den von einem einzelnen Widget abgedeckten Zeitraum konfigurieren auf Seite 88
- Ein einzelnes Widget im Vollbildmodus anzeigen auf Seite 89

## Voraussetzungen

- Admin, Analyst, Monitor oder Operator Zugriff auf die Appliance.
- Sie sind auf der Appliance Web -UI angemeldet.

# Das automatische Aktualisierungsintervall konfigurieren

Folgen Sie diesen Schritten, um das Intervall zu konfigurieren, in dem das System automatisch die Daten in allen Widgets in jedem für Ihr Benutzerkonto zugänglichen Dashboard aktualisiert. Standardmäßig werden die in den Dashboard-Widgets angezeigten Daten alle 10 Minuten automatisch aktualisiert.

Die Appliance behält diese kontoweite Einstellung bei, bis Sie sie ändern.

**Um den automatischen Aktualisierungsintervall anzuzeigen und zu ändern:**

1. Klicken Sie auf das Settings Menü ( ) der Seite und wählen Sie **Set Refresh interval**.
2. Wählen Sie den neuen automatischen Aktualisierungsintervall: 5 Minuten, 10 Minuten, 15 Minuten oder Custom (benutzerdefiniert).
   Wenn Sie Custom wählen, bestimmen Sie einen Intervall von 1 bis 60 Minuten.
3. Klicken Sie auf **Yes, Proceed**.

# Die in All Widgets angezeigten Daten aktualisieren

Folgen Sie diesen Schritten für eine einmalige Aktualisierung der in allen Widgets des aktuellen Dashboards angezeigten Daten. Dieser Vorgang wirkt sich nicht auf den globalen automatischen Aktualisierungsintervall aus.

**Um die in allen Widgets des aktuellen Dashboards angezeigten Daten zu aktualisieren:**

1. Greifen Sie auf das Dashboard zu, das Sie aktualisieren möchten.
2. Klicken Sie auf der Dashboard-Ebene auf das More Menü ( ) und wählen Sie **Refresh**.

# Den von allen Widgets abgedeckten Zeitraum konfigurieren

Für viele Dashboard-Widgets können Sie den Zeitraum konfigurieren, für den das Widget Daten anzeigt. Typische Optionen für Zeiträume sind täglich, wöchentlich und monatlich. Folgen Sie diesen Schritten, um den Zeitraum für alle Widgets im aktuellen Dashboard zu konfigurieren.

Die Appliance behält die Dashboard-weite Einstellung für Ihre Benutzerkonto bei, bis Sie sie ändern. Sie können diese Einstellung für ein individuelles Widget im Dashboard übersteuern.

**Um den von allen Widgets im aktuellen Dashboard abgedeckten Zeitraum zu konfigurieren:**

1. Greifen Sie auf das Dashboard zu, das Sie bearbeiten möchten.
2. Klicken Sie auf der Dashboard-Ebene auf das More Menü (⋮) und wählen Sie **Set Time Period**.
3. Wählen Sie die neue Aktualisierungsrate für die Dashboard-Widgets, Day, Week oder Month (Tag, Woche oder Monat).
4. Klicken Sie auf **Yes, Proceed**.

# Ein Dashboard speichern oder drucken

Folgen Sie diesen Schritten, um das aktuelle Dashboard auf eine PDF-Datei zu speichern. Sie können das Dashboard direkt auf einem Drucker drucken.

**Um das aktuelle Dashboard zu drucken oder zu speichern:**

1. Klicken Sie auf Dashboard, um wählen Sie das Dashboard, das Sie drucken oder speichern wollen.
2. Klicken Sie auf der Dashboard-Ebene auf das More Menü (⋮) und wählen Sie **Print PDF**.
3. Um eine Kopie des Dashboards zu drucken, wählen Sie die Druckereinstellungen und klicken Sie dann auf **Print**.
4. Um eine Kopie des Dashboards zu speichern, wählen Sie **Save as PDF**, legen Sie den Datei-Speicherort fest und klicken Sie dann auf **Save**.

# Die in einem einzigen Widget angezeigten Daten aktualisieren

Folgen Sie diesen Schritten für eine einmalige Aktualisierung der in einem einzelnen Widget des aktuellen Dashboards angezeigten Daten. Dieser Vorgang wirkt sich nicht auf den globalen automatischen Aktualisierungsintervall aus.

**Um die in einem einzelnen Widget im aktuellen Dashboard angezeigten Daten zu aktualisieren:**

1. Klicken Sie auf **Dashboard** und wählen Sie das Dashboard, das ein Widget enthält, das aktualisiert werden soll.
2. Bewegen Sie den Mauszeiger über der oberen rechten Ecke des Widgets.
3. Klicken Sie auf das Aktualisieren Symbol ( ).

# Den von einem einzelnen Widget abgedeckten Zeitraum konfigurieren

Für viele Dashboard-Widgets können Sie den Zeitraum konfigurieren, für den das Widget Daten anzeigt. Typische Optionen für Zeiträume sind täglich, wöchentlich und monatlich. Folgen Sie diesen Schritten, um den Zeitraum für ein einzelnes Widgets im aktuellen Dashboard zu konfigurieren.

Die Appliance behält diese Widget-spezifische Einstellung für Ihr Benutzerkonto bei, bis Sie diese oder den Dashboard-weiten Zeitraum ändern.

**Um den von einem einzigen Widget im aktuellen Dashboard abgedeckten Zeitraum zu konfigurieren:**

1. Klicken Sie auf **Dashboard** und wählen Sie das Dashboard, das das Widget enthält, dessen Zeitraum Sie ändern wollen.
2. Wählen Sie den Zeitraum, für den Daten angezeigt werden sollen.

## Ein einzelnes Widget im Vollbildmodus anzeigen

Folgen Sie diesen Schritten, um ein einzelnes Widget zu erweitern und im Vollbildmodus anzuzeigen.

**Um ein einzelnes Widget im Vollbildmodus anzuzeigen:**

1. Klicken Sie auf **Dashboard** und wählen Sie das Dashboard, das Sie im Vollbildmodus anzeigen wollen.
2. Bewegen Sie den Mauszeiger über der oberen rechten Ecke des Widgets.
3. Klicken Sie auf das Vollbild Symbol ( ).

# Dashboard-Berichte generieren und planen

Für jedes Dashboard auf der Network Security Appliance Web-UI können Sie einen einzelnen Bericht erstellen oder Berichte für eine regelmäßige Ausführung planen. Der Bericht enthält Daten über alle Widgets auf dem Dashboard. Sie können die erstellten Berichte auf der Reports > Static Reports Seite anzeigen und geplante Berichte auf der Reports > Schedule Reports Seite. Um den Bericht zu löschen oder herunterzuladen, klicken Sie auf das Action Symbol in der Action Spalte.

**HINWEIS:** Einige Widgets speichern Daten für höchstens einen Monat. Wenn Sie einen längeren Zeitraum als diesen festlegen, hebt der Bericht hervor, dass nur Daten von einem Monat für diese Widgets enthalten sind.

**Um einen Bericht von dem Dashboard zu generieren:**

1. Klicken Sie auf das More Options Menü und dann auf **Generate Report**.
2. Wählen Sie das Berichtsformat. Sie können CSV, JSON oder XML auswählen.
3. Wählen Sie den Zeitraum, den der Bericht umfassen soll und klicken Sie auf **Apply**.

Sie können auch einen Bericht von der Report > Static Reports Seite generieren.

**Um einen Bericht von dem Dashboard zu planen:**

1. Klicken Sie auf das More Options Menü und dann auf **Schedule Report**.
2. Unter Scheduled wählen Sie, wie oft Sie einen Bericht generieren wollen. Sie können stündlich, täglich, wöchentlich oder monatlich wählen.

3. Geben Sie die Tageszeit, den Wochentag, und gegebenenfalls den Tag des Monats an.
4. Wählen Sie die Zustellungsmethode, das Berichtsformat und den Zeitraum, den der Bericht abdecken soll.
5. Klicken Sie auf **Schedule**.

Sie können auch einen Bericht von der Report > Schedule Reports Seite planen.

# TEIL II: Konfiguration

# KAPITEL 4: Zugriff auf die physische oder serielle Konsole

Verwenden Sie eine der Methoden in diesem Abschnitt, um eine Verbindung mit der physischen oder seriellen Konsole herzustellen.

## Physische Konsolenmethode

Sie können Tastatur- und Videokabel mit der Appliance verbinden und sich dann auf der Network Security CLI anmelden. Die Positionen der Ports finden Sie im *Handware Administrationshandbuch*

**Um auf die physische Konsole zuzugreifen:**

- Schließen Sie eine Tastatur und einen VGA-Monitor an.

## Serielle Konsolenmethoden

Wenn Sie keinen Terminalserver verwenden, müssen Sie sich in der Nähe der Network Security Appliance befinden, um den seriellen Port zu verwenden. Der serielle Port befindet sich auf der Rückseite der Appliance. Lesen Sie Ihr *Hardware Administrationshandbuch*, um den Portstandort anzuzeigen.

Der serielle Port verwendet die folgenden Einstellungen:

- Baudrate: 115200
- Datenbits: 8
- Stopp-Bits: 1
- Parität: keine
- Datenflusssteuerung: XON/XOFF

**HINWEIS:** Wenn die Appliance beim Start nicht mehr reagiert, ohne das eine Fehlernachricht angezeigt wird, könnte der serielle Port oder die Verbindung fehlerhaft sein. Wenn dies geschieht, tun Sie folgendes:

1. Drücken und halten Sie die Starttaste auf der Vorderseite der Appliance ein paar Sekunden lang gedrückt, bis die Appliance abschaltet.
2. Ziehen alle Netzkabel vom Server ab und warten Sie ungefähr 5 Minuten um sicherzustellen, dass das Herunterfahren abgeschlossen ist.
3. Verbinden Sie ein anderes serielles Kabel.
4. Stecken Sie das Netzkabel ein.
5. Wenn der Server nicht automatisch neu startet, drücken Sie auf die Starttaste.

Sie können auf den seriellen Port, wie in den folgenden Themen beschrieben, zugreifen:

- PC oder Mac unten
- Linux auf der nächsten Seite
- Terminal Server auf der nächsten Seite

# PC oder Mac

Da Laptops normalerweise keinen seriellen Port haben, benötigen Sie ein USB nach Seriell Kabel, um den Laptop mit dem DB-9 der Network Security Appliance zu verbinden. FireEye verwendet Prolific Technology Inc. Adapter.

**WICHTIG!** Ein USB-zu-Seriell-Kabel ist nicht im Lieferumfang des Geräts enthalten.

**Um auf die serielle Konsole von einem PC oder Mac Laptop zuzugreifen:**

1. Verbinden Sie das USB-nach-seriell Kabel mit dem USB Port des Laptops.
2. Verbinden Sie ein Ende des mit der Appliance gelieferten Nullmodemkabels mit dem USB-nach-seriell-Kabel.
3. Verbinden Sie das andere Ende des Nullmodemkabels mit dem seriellen Port der Appliance.
4. Verwenden Sie eine serielle Anwendung (wie zum Beispiel PuTTY), um eine Verbindung zu erstellen. Bestimmen Sie den COM-Port, der dem USB-nach-Seriell-Kabel zugeordnet ist.

# Linux

Sie können ein serielles Kabel oder ein USB-nach-Seriell-Kabel für die Verbindung der Linux Maschine mit dem seriellen Port der Network Security Appliance zu verbinden. FireEye verwendet Prolific Technology Inc. Adapter.

**WICHTIG!** Ein USB-zu-Seriell-Kabel ist nicht im Lieferumfang des Geräts enthalten.

**Um auf die serielle Konsole von einem Linux Gerät zuzugreifen:**

1. Verbinden Sie das Kabel mit dem seriellen Port der Appliance und der Linux Maschine.
2. Erstellen Sie eine Verbindung von einer Eingabeaufforderung. Wenn Sie ein USB-nach-Seriell-Kabel verwenden, bestimmten Sie den COM-Port, der ihm zugewiesen ist.

# Terminal Server

**Um auf die serielle Konsole von einem Terminalserver zuzugreifen:**

1. Stellen Sie den Terminalserver auf eine Baudrate von 115200 ein.
2. Stöpseln Sie ein Ende des seriellen Kabels in den DB-9 seriellen Port auf der Network Security Appliance ein und das andere Ende in den Terminal Server.
3. In einer Telnet Anwendung (z.B. PuTTY) geben Sie den Hostnamen oder die Terminalserver IP-Adresse, die Terminalserver Portnummer, die die Appliance verwendet und die Appliance Portnummer ein.

# KAPITEL 5: Erstkonfiguration

Dieses Thema behandelt die folgenden Informationen:

- Überblick über Erstkonfiguration auf der nächsten Seite
- Voraussetzungen für Erstkonfigurationen auf Seite 99
- Verwenden Sie eine der folgenden Methoden, um Ersteinstellungen zu konfigurieren:
    - Ersteinstellungen mit Hilfe einer Tastatur und eines Monitors konfigurieren auf Seite 99
    - Ersteinstellungen mit Hilfe des seriellen Konsolenports konfigurieren auf Seite 100
    - Ersteinstellungen mit Hilfe der LCD Anzeige konfigurieren auf Seite 108

  Informationen zum Beantworten der Eingabeaufforderungen des Konfigurationsassistenten finden Sie unter Schritte des Konfigurationsassistenten auf Seite 102.
- Die IPMI Schnittstelle konfigurieren auf Seite 109

# Überblick über Erstkonfiguration

Die Management-Schnittstelle ist der Port, durch den die Network Security Appliance verwaltet wird. Dies ist auch der Port, durch den eine Appliance von der Central Management Appliance verwaltet wird. Bei einem single-Port Adresstypen (unter Den Adresstyp für DTI-Network Serviceanfragen ändern auf Seite 423 beschrieben) ist die Management-Schnittstelle auch der Port, durch den eine verwaltete Appliance Software-Updates vom DTI Netzwerk anfordert und herunterlädt.

Ersteinstellungen müssen konfiguriert werden, die Management-Schnittstelle einzustellen und Zugriff auf das Netzwerk zu gestatten, das Standard Administratorkennwort zu ändern und so weiter. Die folgenden Methoden für die Erstkonfiguration sind verfügbar:

Verwenden Sie eine der folgenden Methoden, um sich auf der Network Security CLI anzumelden und Ersteinstellungen zu konfigurieren:

- **Tastatur und Monitor**—Verbinden Sie eine USB Tastatur und einen VGA Monitor direkt mit den USB 3.0 Ports und einem Video Port auf der Rückseite der Appliance. Dies die einfachste Art, die Ersteinstellungen zu konfigurieren, wenn Sie sich in der Nähe der Appliance befinden.
- **Serieller Port**—Schließen Sie einen Windows Laptop, ein Mac Laptop, ein Linux System oder einen Terminalserver an den seriellen Port der Appliance an. Die serielle Port befindet sich auf der Rückseite.
- **LCD Anzeige**—Verwenden Sie die Navigationstasten und Menüs auf dem LCD-Dislplay, um Ersteinstellungen auszuwählen. Das LCD-Display befindet sich bei den meisten Appliance Modellen auf der Vorderseite.

Denken Sie daran, die IPMI-Schnittstelle so zu verkabeln und zu konfigurieren, dass Sie Zugriff auf die Appliance haben, wenn sie auf Netzwerk- oder seriellen Portzugriff nicht mehr reagieren sollte.

**HINWEIS:** Sie müssen über die serielle Schnittstelle auf die Appliance zugreifen, um die Startaktivitäten der Appliance zu überwachen. Sie können CLI Befehle nur über direkte Tastatur- und Monitorverbindung eingeben, bevor der Bootloader mit dem Laden des Kernels beginnt, z.B. um die Ausgabe zu veröffentlichen und nachdem der Bootvorgang abgeschlossen ist.

# Voraussetzungen für Erstkonfigurationen

Bevor Sie die Appliance konfigurieren:

- Lesen Sie die *Versionshinweise* für die aktuelle Ausgabe.
- Sammeln Sie die folgenden Informationen von Ihrem Netzwerk Administrator:
    - Statische IP-Adresse, Subnetzmaske und Standard Gateway Adresse für die Appliance Management-Schnittstelle. (Sie benötigen diese Informationen nicht, wenn Dynamic Host Configuration Protocol (DHCP) auf der Management-Schnittstelle verwendet werden soll.)
    - IP-Adresse für jeden Domain Name System (DNS) Server (wenn DNS Namensauflösung benutzt werden soll).
    - IP-Adresse für jeden Network Time Protocol (NTP) Server (wenn NTP Synchronisierung benutzt werden soll).
    - Telnet oder SSH Client auf dem remote System (wenn die Appliance remote verwaltet werden soll).

**WICHTIG:** Der Endpoint Security Server muss sowohl eine IPv4 als auch eine IPv6 Adresse haben, um mit dem FireEye DTI-Server zu kommunizieren. Dies ist für Lizenzüberprüfung, Downloads von Agent Installer-Paketen, Downloads von Server-Paketen und IOC-Inhalten erforderlich.

- Wenn Sie die Ersteinstellungen über den seriellen Konsolenport und einen Windows- oder Mac Laptop konfigurieren möchten, besorgen Sie sich ein USB-zu-Seriell-Kabel.

# Ersteinstellungen mit Hilfe einer Tastatur und eines Monitors konfigurieren

Sie können Tastatur- und Videokabel mit der Appliance verbinden und sich dann auf der Network Security CLI anmelden, um die Erstkonfiguration durchzuführen. Die Positionen der Ports finden Sie in Ihrem *Handware Administrationshandbuch*.

**Um Ersteinstellungen mit Hilfe einer Tastatur und eines Monitors zu konfigurieren:**

1. Schließen Sie eine Tastatur und einen VGA-Monitor an.

2. Wenn Sie dazu aufgefordert werden, geben Sie den Standard Benutzernamen (`admin`) und Kennwort (`admin`) für den permanenten "admin" Benutzer ein.
3. Sie werden aufgefordert, die Endbenutzer Lizenzvereinbarung (EULA) anzunehmen. Geben Sie **y** ein, um die Vertragsbedingungen anzunehmen.
4. Geben Sie **y** ein, wenn Sie aufgefordert werden, den Konfigurationsassistenten für die Erstkonfiguration zu verwenden. Reagieren Sie dann auf die Aufforderungen, wie unter Schritte des Konfigurationsassistenten auf Seite 102 beschrieben.
5. Nachdem Sie die Fragen beantwortet haben, fasst der Assistent Ihre Antworten zusammen. Um eine Antwort zu ändern, geben Sie die Schrittnummer ein. Drücken Sie Eingabe, um die Änderungen zu speichern.

# Ersteinstellungen mit Hilfe des seriellen Konsolenports konfigurieren

Wenn Sie keinen Terminalserver verwenden, müssen Sie sich in der Nähe der Network Security Appliance befinden, um den seriellen Port zu verwenden. Der serielle Port befindet sich auf der Rückseite der Appliance. Lesen Sie Ihr *Hardware Administrationshandbuch*, um den Portstandort anzuzeigen.

Der serielle Port verwendet die folgenden Einstellungen:

- Baudrate: 115200
- Datenbits: 8
- Stopp-Bits: 1
- Parität: keine
- Datenflusssteuerung: XON/XOFF

**HINWEIS:** Wenn die Appliance beim Start nicht mehr reagiert, ohne das eine Fehlernachricht angezeigt wird, könnte der serielle Port oder die Verbindung fehlerhaft sein. Wenn dies geschieht, tun Sie folgendes:

1. Drücken und halten Sie die Starttaste auf der Vorderseite der Appliance ein paar Sekunden lang gedrückt, bis die Appliance abschaltet.
2. Ziehen alle Netzkabel vom Server ab und warten Sie ungefähr 5 Minuten um sicherzustellen, dass das Herunterfahren abgeschlossen ist.
3. Verbinden Sie ein anderes serielles Kabel.
4. Stecken Sie das Netzkabel ein.
5. Wenn der Server nicht automatisch neu startet, drücken Sie auf die Starttaste.

Konfigurieren Sie Ersteinstellungen, wie in den folgenden Themen beschrieben:

- Einen Windows oder Mac Laptop verwenden unten
- Ein Linux System verwenden unten
- Einen Terminalserver verwenden auf der nächsten Seite

## Einen Windows oder Mac Laptop verwenden

Verwenden Sie den Vorgang in diesem Abschnitt, um Ersteinstellungen auf einem Windows oder Mac Laptop zu konfigurieren.

**Um Ersteinstellungen von einem Windows oder Mac Laptop zu konfigurieren:**

1. Stellen Sie eine Verbindung mit der seriellen Konsole her, wie unter PC oder Mac auf Seite 94 beschrieben .
2. Wenn Sie dazu aufgefordert werden, geben Sie den Standard Benutzernamen (`admin`) und Passwort (`admin`) für den Administrator ein.
3. Sie werden aufgefordert, die Endbenutzer Lizenzvereinbarung (EULA) anzunehmen. Geben Sie `y` ein, um die Vertragsbedingungen anzunehmen
4. Wenn Sie dazu aufgefordert werden, geben Sie `y` ein, um den Konfigurationsassistenten für die Erstkonfiguration zu verwenden. Reagieren Sie dann auf die Aufforderungen, wie unter Schritte des Konfigurationsassistenten auf der nächsten Seite beschrieben.
5. Nachdem Sie die Fragen beantwortet haben, fasst der Assistent Ihre Antworten zusammen. Um eine Antwort zu ändern, geben Sie die Schrittnummer ein. Drücken Sie Eingabe, um die Änderungen zu speichern.

## Ein Linux System verwenden

Verwenden Sie den Vorgang in diesem Abschnitt, um Ersteinstellungen auf einem Linux System zu konfigurieren.

**Um Ersteinstellungen auf einem Linux System zu konfigurieren:**

1. Stellen Sie eine Verbindung mit der seriellen Konsole her, wie unter Linux auf Seite 95 beschrieben .
2. Wenn Sie dazu aufgefordert werden, geben Sie den Standard Benutzernamen (`admin`) und Passwort (`admin`) für den Administrator ein.
3. Sie werden aufgefordert, die Endbenutzer Lizenzvereinbarung (EULA) anzunehmen. Geben Sie `y` ein, um die Vertragsbedingungen anzunehmen

4. Wenn Sie dazu aufgefordert werden, geben Sie `y` ein, um den Konfigurationsassistenten für die Erstkonfiguration zu verwenden. Reagieren Sie dann auf die Aufforderungen, wie unter Schritte des Konfigurationsassistenten unten beschrieben.
5. Nachdem Sie die Fragen beantwortet haben, fasst der Assistent Ihre Antworten zusammen. Um eine Antwort zu ändern, geben Sie die Schrittnummer ein. Drücken Sie Eingabe, um die Änderungen zu speichern.

## Einen Terminalserver verwenden

Verwenden Sie den Vorgang in diesem Abschnitt, um Ersteinstellungen auf einem Terminalserver zu konfigurieren.

**Um Ersteinstellungen von einem Terminalserver zu konfigurieren:**

1. Stellen Sie eine Verbindung mit der seriellen Konsole her, wie unter Terminal Server auf Seite 95 beschrieben .
2. Wenn Sie dazu aufgefordert werden, geben Sie den Standard Benutzernamen (`admin`) und Passwort (`admin`) für den Administrator ein.
3. Sie werden aufgefordert, die Endbenutzer Lizenzvereinbarung (EULA) anzunehmen. Geben Sie `y` ein, um die Vertragsbedingungen anzunehmen
4. Wenn Sie dazu aufgefordert werden, geben Sie `y` ein, um den Konfigurationsassistenten für die Erstkonfiguration zu verwenden. Reagieren Sie dann auf die Aufforderungen, wie unter Schritte des Konfigurationsassistenten unten beschrieben.
5. Nachdem Sie die Fragen beantwortet haben, fasst der Assistent Ihre Antworten zusammen. Um eine Antwort zu ändern, geben Sie die Schrittnummer ein. Drücken Sie Eingabe, um die Änderungen zu speichern.

# Schritte des Konfigurationsassistenten

Der Konfigurationsassistent wird normalerweise benutzt, um die Erstkonfiguration des Systems durchzuführen. Informationen über die Ausführung des Assistenten, bevor die Managment-Schnittstelle konfiguriert ist, finden Sie unter Erstkonfiguration auf Seite 97. Nachdem die Management-Schnittstelle konfiguriert ist, kann ein Administrator den `configuration jump-start`CLI Befehl verwenden, um den Assistenten auszuführen.

Die folgende Tabelle beschreibt die Fragen, die der Konfigurationsassistent Sie auffordert, zu beantworten, während er sich durch die Assistentenschritte bewegt. Wie in der Tabelle vermerkt, überspringt der Assistent einige Schritte, je nach Ihren Antworten auf die vorherigen Schritte.

**HINWEIS:** Um den Konfigurationsassistenten zu beenden, drücken Sie STRG+C. Um ihn erneut zu starten, verwenden Sie den `configuration jump-start` Befehl.

| Schritt | Antwort |
|---|---|
| Hostname? | Geben Sie den Hostnamen für die Appliance ein. |
| Admin password? | Geben Sie ein neues Administratorkennwort ein. Das neue Passwort muss zwischen 8 und 32 Zeichen lang sein. Wenn Sie das Kennwort nicht ändern, kann der Administrator sich nicht auf der Appliance anmelden. |
| Confirm admin password? | Geben Sie das neue Adminstratorkennwort erneut ein. |
| Enable remote access for 'admin' user? | Geben Sie **yes** ein, um dem Administrator zu gestatten, sich auf der Appliance entfernt anzumelden. Geben Sie **no** ein, um entfernten Zugriff zu deaktivieren. |
| 2. Use DHCP on ether1 interface? | Geben Sie **yes** ein, um Dynamic Host Configuration Protocol (DHCP) zum Konfigurieren der Appliance IP-Adresse und anderer Netzwerk Parameter zu verwenden. Geben Sie **no** ein, um ihre IP-Adresse und Netzwerkeinstellungen manuell zu konfigurieren. (Wenn Sie **yes** eingeben, werden die zeroconf und static IP-Adressierung Schritte übersprungen.) |
| Use zeroconf on ether1 interface? | Geben Sie **yes** ein, um zero configuration Networking (zeroconf) zu verwenden. Geben Sie **no** ein, um eine statische IP Adrese und Netzwerkmaske festzulegen. (Wenn Sie **yes** festlegen, wird der nächste Schritt übersprungen.) **HINWEIS**: Verwenden Sie zeroconf nicht auf der primären Schnittstelle. |
| Primary IP address and masklen? | Geben Sie die IP-Adresse für die Management-Schnittstelle in A.B.C.D Format und die Netzwerkmaske zum Beispiel als 1.1.1.2/12 ein. |
| Default gateway? | Geben Sie die Gateway IP-Adresse für die Management-Schnittstelle ein. |
| Primary DNS server? | Geben Sie die IP-Adresse des DNS Servers ein. |
| Domain name? | Geben Sie die Domäne für die Management-Schnittstelle ein, zum Beispiel: **it.acme.com.** |

| Schritt | Antwort |
|---|---|
| Enable Incident Response or Compromise Assessment? | Geben Sie **yes** ein, um ein Incident Response oder Compromise Assessment Deployment zu konfigurieren. (Wenn Sie **yes** eingeben, werden die vier nächsten Schritte automatisch ausgeführt und die "Enable NTP?" und "Enable IPv6" Schritte werden übersprungen.) |
| Enable fenet service? | Geben Sie **yes** ein, um Zugriff auf das DTI Netzwerk zu aktivieren. (Wenn Sie **no** eingeben, werden die nächsten Schritte übersprungen.) |
| Enable fenet license update service? | Geben Sie **yes** ein, um den Lizenzierungsdienst zu aktivieren, Ihre Lizenzen automatisch vom DTI Netzwerk herunterzuladen und zu installieren. (Wenn Lizenzen erfolgreich heruntergeladen und installiert werden, überspringt der Assistent den Schritt zur Eingabe des Produktlizenzschlüssels und den Schritt zur Eingabe des Aktualisierungsschlüssels für Sicherheitsinhalte.) |
| Sync appliance time with fenet? | Geben Sie **yes** ein, um die Appliance Zeit mit der DTI Server Zeit zu synchronisieren. Wenn Sie den Lizenzierungsdienst aktiviert haben, verhindert Synchronisation, dass eine Funktion zeitweilig auf Grund von Zeitunterscheiden nicht lizenziert ist. Der Assistent unternimmt drei Versuche, diesen Schritt auszuführen, bevor er aufgibt und auf den nächsten Schritt weitergeht. |
| Update licenses from fenet? | Geben Sie **yes** ein, um Ihre Lizenzen herunterzuladen und zu installieren. Der Assistent unternimmt drei Versuche, um diesen Schritt auszuführen, bevor er aufgibt und auf den nächsten Schritt weitergeht. |
| Enable NTP? | Geben Sie **yes** ein, um automatische Zeitsynchronisation mit einem oder mehreren Network Time Protokcol (NTP) Server zu aktivieren. Geben Sie **no** ein, um die Zeit und das Datum auf der Appliance manuell einzustellen. (Dieser Schritt wird übersprungen, wenn Sie **yes** unter "Sync appliance time with fenet?" oder "Enable Incident Response or Compromise Assessment?" eingegeben haben Schritt eingegeben haben.) Wenn Sie **no** eingegeben haben, legen Sie die Uhrzeit und das Datum in Greenwich-Zeit (GMT) fest. |

| Schritt | Antwort |
|---|---|
| Enable FaaS VPN? | Geben Sie **yes** ein, um der Appliance zu ermöglichen, sich mit Managed Defense (FireEye as a Service) über das Internet mit Hilfe einer sicheren SSL VPN-Verbindung zu verbinden. (Dieser Schritt wird übersprungen, wenn keine MD_ACCESS Lizenz installiert ist. Dieser Schritt wird automatisch ausgeführt, wenn Sie **yes** im "Enable Incident Response or Compromise Assessment?" Schritt eingegeben haben.) |
| Set time (<hh>:<mm>:<ss>)? | Geben Sie die Systemzeit für die Appliance ein. (Dieser Schritt und der nächste Schritt wird übersprungen, wenn Sie **yes** im "Sync appliance time with fenet?" oder "Enable NTP?" Schritt eingegeben haben.) |
| Set date (<yyyy>/<mm>/<dd>)? | Geben Sie das Datum ein, das der Systemzeit für die Appliance entspricht. |
| Enable IPv6? | Geben Sie **yes** ein, um IPv6 Protokoll zu aktivieren, wodurch das Netzwerk IP-Routing von IPv4 auf IPv6 geändert wird. Sowie dieser als auch die nächsten zwei Schritte werden übersprungen, wenn Sie **yes** im "Enable Incident Response or Compromise Assessment?" Schritt eingegeben haben. Dieser Schritt sowie die nächsten zwei Schritte werden automatisch ausgeführt, wenn Sie **yes** im Schritt "Enable FaaS VPN" eingegeben haben. |
| Enable IPv6 autoconfig (SLAAC) on ether1 interface? | Geben Sie **yes** ein, um IPv6 autoconfig auf dem ether 1 (Management-Schnittstelle) Port zu aktivieren. (Dieser Schritt wird übersprungen, wenn Sie **no** im "Enable IPv6?" Schritt eingegeben haben.) |
| Enable DHCPv6 on ether1 interface? | Geben Sie **yes** ein, um DHCPv6 für die Konfigurierung von IPv6 Hosts mit IP-Adressen zu verwenden. (Dieser Schritt wird übersprungen, wenn Sie **no** im "Enable DHCP?" oder "Enable IPV6?" Schritt eingegeben haben.) |

| Schritt | Antwort |
|---|---|
| Submission: Interface? | Drücken Sie Eingabe, um ether1 als die Schnittstelle zu akzeptieren, durch die Sensoren und Broker kommunizieren. Andernfalls geben Sie den Namen der anderen Schnittstelle ein. (Wenn Sie ether1 akzeptieren, werden die nächsten drei Schritte übersprungen.)<br>**HINWEIS**: Um Management und Datenverkehr getrennt zu halten, empfiehlt FireEye, dass Sie eine andere Schnittstelle als either2 und keine Überwachungsschnittstelle verwenden. |
| Submission: Use DHCP on <name> interface? | DHCP ist derzeit nicht auf der Eingabeschnittstelle unterstützt. Geben Sie **no** ein, um die Adresseneinstellungen manuell zu konfigurieren. |
| Submission: IP address and masklen? | Geben Sie die IP-Adresse für die Eingabeschnittstelle im A.B.C.D. Format ein und geben Sie die Netzwerkmaske ein, z.B. 10.1.1.1 /24. |
| Submission: Default Ipv4 gateway? | Geben Sie die Gateway IP-Adresse für die Übermittlungsschnittstelle ein. |
| Mirror traffic to a PX appliance? | Geben Sie **yes** ein, um Portspiegelung für die Weiterleitung von Network Security Verkehr auf die Packet Capture Appliance in einem Incident Response Deployment zu verwenden. Wenn Sie **no** eingeben, müssen Sie Ihre Packet Capture Appliance manuell konfigurieren, um den richtigen Verkehr zu erhalten. (Dieser Schritt wird übersprungen, wenn Sie **no** im "Enable Incident Response oder Compromise Assessment?" Schritt eingegeben haben.)<br>**WICHTIG!** :FireEye empfiehlt die Verwendung der Portspiegelung in einem Incident Response Deployment. |

| Schritt | Antwort |
|---|---|
| Interface pair to mirror traffic to PX? | Geben Sie das Network Security Schnittstellenpaar oder -paare ein, deren Verkehr an die Packet Capture Appliance weitergeleitet werden soll.<br>Wenn mehrere Spiegelungsports bereits konfiguriert sind, werden dieser und der nächste Schritt übersprungen. Wenn bereits ein einziger Spiegelport für ein oder mehrere Paare konfiguriert wurde, wird dieses Paar oder diese Paare als Standard für diesen Schritt bereitgestellt.<br>**WICHTIG!** FireEye empfiehlt die Verwendung des Standardpaars **(A)**, wenn Sie eine neue Appliance konfigurieren. Andernfalls sind möglicherweise manuelle Konfigurationsschritte erforderlich. |
| Interface to mirror traffic to PX? | Geben Sie den Network Security Port ein, der den Verkehr auf den Packet Capture Erfassungsport weiterleiten soll. Bestimmen Sie keinen Port, der zu einem Schnittstellenpaar gehört, das Sie im vorherigen Schritt eingegeben haben.<br>Wenn bereits ein einzelner Spiegelport konfiguriert ist, wird er als Standard für diesen Schritt bereitgestellt.<br>**WICHTIG!** FireEye empfiehlt die Verwendung des Standard Ports **(pether6)**, wenn Sie eine neue Appliance konfigurieren. Andernfalls sind möglicherweise manuelle Konfigurationsschritte erforderlich. |
| Enable forensic analysis? | Geben Sie **yes** ein, um eine vollständige Paketerfassung und Analyse auf dem gespiegelten Verkehr auszuführen. |
| IP address of PX | Geben Sie die IP-Adresse der Packet Capture Appliance ein. (Dieser Schritt wird übersprungen, wenn Sie **no** bei der "Enable forensic analysis?" Schritt eingegeben haben.) |
| Product license key? | Geben Sie den Produktlizenzschlüssel ein, den Sie von FireEye erhalten haben oder drücken Sie Eingabe, um eine 15-tägige Auswertungslizenz zu installieren. (Dieser Schritt und der nächste Schritt wird übersprungen, wenn Sie **yes** im "Enable fenet license update service?" Schritt eingegeben haben und wenn Lizenzen als Ergebnis erfolgreich installiert wurden.) |
| Security-content updates key? | Geben Sie den Security-Content Lizenzschlüssel ein, den Sie von FireEye erhalten haben oder drücken Sie Eingabe, um diesen Schritt zu überspringen und die Lizenz später zu installieren. |

# Ersteinstellungen mit Hilfe der LCD Anzeige konfigurieren

Auf der Vorderseite einiger Appliance Modelle befindet sich eine LCD-Anzeige.

**Um Ersteinstellungen von der LCD Anzeige zu konfigurieren.**

1. Drücken Sie auf die Mitteltaste, um auf das **Network** Menü zuzugreifen und antworten Sie auf die Aufforderungen:
    a. **Hostname**—Bestimmen Sie den Hostnamen für das System.
    b. **DHCP enabled**—Geben Sie **yes** ein, um dynamic host configuration protocol (DHCP) zu verwenden. Geben Sie **no** ein, um Ihre IP-Adresse und Netzwerkeinstellungen manuell zu konfigurieren. Wenn Sie **yes** eingegeben haben, fahren Sie mit dem **IPv6 enabled** Schritt fort.
    c. **Static IP address**—Geben Sie die IP-Adresse für den Ethernet 1 (Management-Schnittstelle) Port ein.
    d. **Netmask**—Geben Sie die Netzwerkmaske ein.
    e. **Default gateway**—Geben Sie die Gateway IP-Adresse für die Management-Schnittstelle ein.
    f. **Primary DNS**—Geben Sie die primäre DNS-Server IP-Adresse ein.
    g. **Domain name**—Geben Sie den Domainnamen für die Management-Schnittstelle ein; z.B. **it.acme.com**.
    h. **IPv6 enabled**—Geben Sie **yes** ein, um IPv6 Protokoll zu aktivieren, wodurch Network IP-Routing von IPv4 auf IPv6 geändert wird. Wenn Sie **no** eingeben, fahren Sie mit dem **Admin net login** Schritt fort.
    i. **SLAAC enabled**—Geben Sie **yes** ein, um IPv6 autoconfig auf dem ether1 (Management-Schnittstelle) Port zu aktivieren. Geben Sie **no** ein, um IPv6 autoconfig auf der ether1 (Management-Schnittstelle) Port zu deaktivieren.
    j. **Admin net login**—Geben Sie **yes** ein, um dem Administrator zu genehmigen, sich auf dem System entfernt anzumelden. Geben Sie **no** ein, um remote Zugriff zu deaktivieren.
2. Drücken Sie auf die linke oder rechte Pfeilschaltfläche, bis Sie das **LCD** Menü erreichen. Bei der **Password** Aufforderung, geben Sie ein Kennwort ein, das für den Zugriff auf das LCD-Display verwendet wird. (Dies ist nicht das Passwort, das für den Zugriff auf die Appliance Web-UI oder CLI verwendet wird.)

3. Drücken Sie auf die linke oder rechte Pfeilschaltfläche, bis Sie das **Config Options** Menü erreichen. Auf der **Reset admin password** Aufforderung:

   a. Drücken Sie die Mitteltaste, um das Passwort zurückzusetzen, dass der permanente Admin Benutzer verwendet, um sich auf der Appliance Web-UI oder CLI anzumelden. (Dies ist nicht das Passwort, das für den Zugriff auf das LCD-Display verwendet wird.)

   b. Ein zufällig generiertes Passwort wird angezeigt. Nachdem Sie es sich gemerkt haben, drücken Sie die mittlere oder Schließen Schaltfläche, um die Anzeige zu schließen.

   Nach Abschluss der Erstkonfiguration können Sie auf das Passwort Ihrer Wahl mithilfe der Web-UI oder CLI wechseln.

# Die IPMI Schnittstelle konfigurieren

Verwenden Sie die Befehle in diesem Abschnitt, um die IPMI Schnittstelle zu konfigurieren. Informationen über die Verwendung der IPMI Schnittstelle nach ihrer Konfigurierung finden Sie unter Die Network Security Appliance IPMI (Intelligent Platform Management Interface) Schnittstelle auf Seite 41.

## Voraussetzungen

- Ein Ende des Ethernet Kabels ist an den IPMI Port angeschlossen und das andere Ende an einen Computer oder Terminalserver.

## Die IPMI Konfiguration anzeigen

Dieser Vorgang beschreibt die Verwendung der CLI für die Anzeige der IPMI Konfiguration.

**Um die IPMI Konfiguration anzuzeigen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie die Konfiguration an. Zum Beispiel:

   ```
   hostname (config) # show ipmi interface
   IPMI LAN Settings
   ----------------------------------------
   Admin Shut Down          : no
   Shut Down                : no
   IP Address Source        : Static Address
   IP Address               : 192.168.42.27
   Subnet Mask              : 0.0.0.0
   Default Gateway IP       : 0.0.0.0
   ```

# Den IPMI Port konfigurieren

Dieser Vorgang beschreibt die Verwendung von CLI Befehlen für die Konfigurierung der IPMI Schnittstelle.

**Um den IPMI Port zu konfigurieren:**

1. Wenn Sie eine statische IP-Adresse für die IPMI Schnittstelle konfigurieren wollen, gehen Sie folgendermaßen vor:
    a. Melden Sie sich bei der Appliance CLI an.
    b. Gehen Sie auf den CLI-Konfigurationsmodus.

    ```
    hostname > enable
    hostname # configure terminal
    ```

    c. Wenn DHCP zuvor für IPMI konfiguriert wurde, wechseln Sie auf die statische Methode:

    ```
    hostname (config) # ipmi lan ipsrc static
    ```

    d. Konfigurieren Sie die IP-Adresse für die IPMI Schnittstelle:

    ```
    hostname (config) # ipmi lan ipaddr <ipAddress>
    ```

    e. Konfigurieren Sie die Netzmaske für die IPMI Schnittstelle:

    ```
    hostname (config) # ipmi lan netmask <netMask>
    ```

    f. Konfigurieren Sie das Standard Gateway für die IPMI Schnittstelle:

    ```
    hostname (config) # ipmi lan defgw <ipAddress>
    ```

2. Wenn Sie DHCP konfigurieren wollen:
    a. Stellen Sie sicher, dass DHCP auf Ihrem Netzwerk aktiviert ist.

    ```
    hostname (config) # show ip dhcp
    ```

    b. Aktivieren Sie DHCP:

    ```
    hostname (config) # ipmi lan ipsrc dhcp
    ```

3. Der Standard Benutzername für die Anmeldung auf der IPMI Web-UI ist ADMIN. Konfigurieren Sie das Passwort. Das Passwort muss aus mindestens fünf und maximal 20 Zeichen bestehen.

    ```
    hostname (config) # ipmi user set password <password>
    ```

4. Speichern Sie Ihre Änderungen:

    ```
    hostname (config) # write memory
    ```

**Um auf die Standard Konfiguration zurückzugehen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

    ```
    hostname > enable
    hostname # configure terminal
    ```

2. Um auf die Standard Konfiguration zurückzugehen:

   ```
   hostname (config) # ipmi lan ipsrc static
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**HINWEIS:** Es ist wichtig, die neueste, für Ihr System verfügbare IPMI-Firmware zu verwenden. Details finden Sie unter IPMI und BIOS Firmware Aktualisierungen auf Seite 289.

# IPv6 Adressen für die IPMI-Schnittstelle konfigurieren

**WICHTIG:** Sie können IPv6-Adressen für die IPMI-Schnittstelle nur für NX 3500, NX 4500 und NX 5500 Appliances konfigurieren.

Verwenden Sie die Anweisungen in diesem Abschnitt, um eine IPv6 Adresse für die IPMI-Schnittstelle mit Hilfe der CLI zu konfigurieren. Informationen über die Verwendung der IPMI-Schnittstelle finden Sie unter Die Network Security Appliance IPMI (Intelligent Platform Management Interface) Schnittstelle auf Seite 41.

## Voraussetzungen

- Ein Ende des Ethernet Kabels ist an den IPMI Port angeschlossen und das andere Ende an einen Computer oder Terminalserver.
- Aktualisieren Sie die IPMI Firmwareversion auf 2.37. Details finden Sie unter IPMI und BIOS Firmware aktualisieren auf Seite 290.

**Um eine IPv6 Adresse für die IPMI-Schnittstelle mit Hilfe der CLI zu konfigurieren:**

1. Melden Sie sich bei der Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Konfigurieren Sie die statische IPv6 Adresse für die IPMI-Schnittstelle:

   ```
   hostname (config) # ipmi lan6 ipaddr <valid IPv6 Address> prefix <1-128>
   ```

4. Um DHCP auf Ihrem Netzwerk zu aktivieren:

   ```
   hostname (config) # ipmi lan6 dhcp enable
   ```

5. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

6. Zeigen Sie die Konfiguration an. Zum Beispiel:

```
hostname (config) # show ipmi interface
IPMI LAN Settings
----------------------------------------
Admin Shut Down         : no
Shut Down               : (n/a)
Set in Progress         : Set in Progress
IP Address Source       : DHCP Address
IPMI LAN6 Settings
----------------------------------------
Static ipv6 Address     : 2015:9:19:ffff::da7/64
Dhcp ipv6 Address       : 2015:9:19:ffff::da7/64
```

# KAPITEL 6: Virtuelle Appliances

Virtuelle Network Security Appliances werden als Sensoren in einem FireEye Network Security oder FireEye Helix Deployment verwendet. Informationen über die Bereitstellung und Arbeit mit virtuellen Appliances finden Sie im *FireEye Geräte- Deploymenthandbuch* auf dem FireEye Dokumentationsportal unter https://docs.fireeye.com/.

# KAPITEL 7: Betriebsmodi

Nach der Bereitstellung der Network Security Appliance in Ihrem Netzwerk müssen Sie das System konfigurieren, entsprechend zu funktionieren. Sie können Ihr System für jeden der folgenden Deploymenttypen entweder von der Web-UI oder der CLI konfigurieren.

**Inline**

- Inline-Modus über die Web-UI konfigurieren unten
- Inline-Modus über die CLI konfigurieren auf Seite 117

**Inline Proxy**

- Inline Proxy-Modus über die Web-UI konfigurieren auf Seite 120
- Inline Proxy-Modus über die CLI konfigurieren auf Seite 123

**Inline mit mehreren Proxys**

- Inline-Multi-Proxy-Modus mit Hilfe der Web-UI konfigurieren auf Seite 127
- Inline-Multi-Proxy-Modus mithilfe der CLI konfigurieren auf Seite 131

**Test Access Point (TAP)**

- TAP-Modus mit Hilfe der Web-UI konfigurieren auf Seite 136
- TAP-Modus mit Hilfe der CLI konfigurieren auf Seite 137

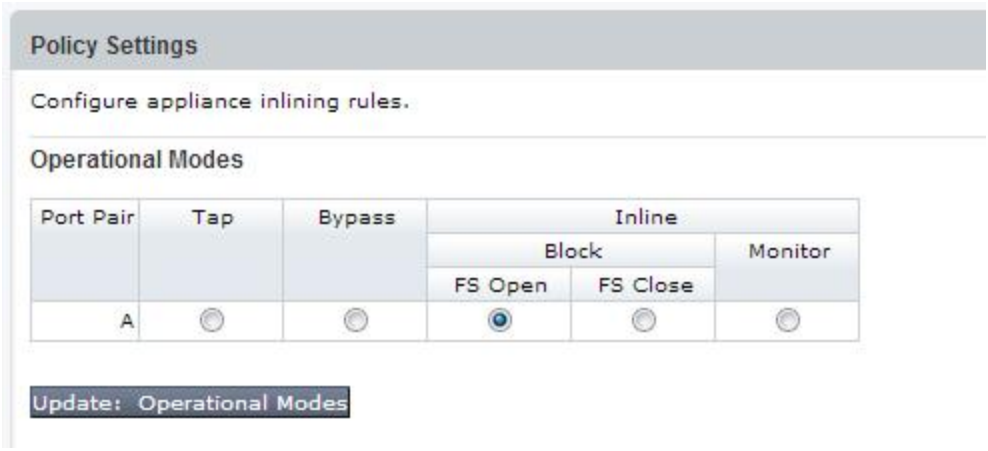
**Switch Port Analyzer (SPAN)**

- SPAN-Modus mit Hilfe der Web-UI konfigurieren auf Seite 138
- SPAN-Modus mit Hilfe der CLI konfigurieren auf Seite 140

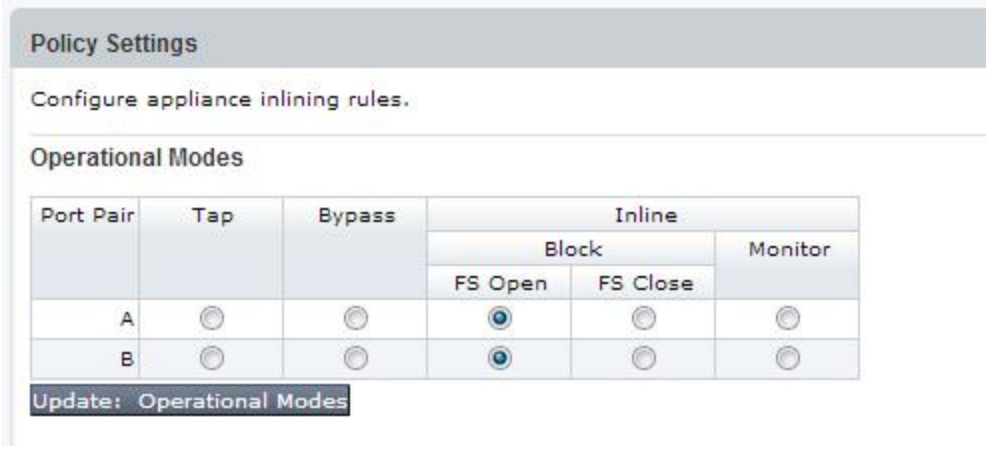
# Inline-Modus über die Web-UI konfigurieren

Verwenden Sie die **Policy Settings** Seite, um inline Modus zu konfigurieren.

In Inline-Modus können Sie die Appliance mit einem oder zwei Netzwerk-Portpaaren konfigurieren. Das folgende Beispiel zeigt ein Netzwerk-Portpaar.




Das folgende Beispiel zeigt zwei Netzwerk-Portpaare.




Die Betriebsmodi für die Inline-Bereitstellung werden in der folgenden Tabelle beschrieben.

| Modus | Beschreibung |
|---|---|
| Block | Blockiert böswilligen Datenverkehr (empfohlen).<br>• FS Open—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>• FS Close—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie diese Einstellung nur, wenn das Gerät aktiv überwacht wird). |
| Monitor | Überwacht den Verkehr und generiert Alarme für bösartige Ereignisse. |

| Modus | Beschreibung |
|---|---|
| Bypass | Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert.<br><br>**HINWEIS:** Beginnend mit Version 7.1.0 umgehen NX Appliances Pakete mit mehr als 1650 Bytes anstatt diese abzulegen. |

Details über inline Deployment finden Sie im *Hardware Administrationshandbuch* für Ihr Appliance Modell.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um inline Modus zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie für jedes verfügbare Portpaar eine Blockierungsoption aus. (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.

# Inline-Modus über die CLI konfigurieren

Verwenden Sie die CLI Befehle in diesem Thema, um die folgenden Optionen für die Konfigurierung des inline-Blockierungsmodus einzustellen.

| Einstellung | Beschreibung |
|---|---|
| Betriebsmodus | Das inline Deployment verfügt über drei optionale Modi: Es wird dringend empfohlen, dass Sie Ihre Appliance auf inline-Blockierungsmodus einstellen.<br><br>**HINWEIS**: Wenn Sie den Betriebsmodus auf Verkehr blockieren einstellen, geben Sie eine ausfallsichere Einstellung ein (**block open** oder **block close**)<br><br>• **block**—Blockiert bösartigen Verkehr (empfohlen).<br>  • **open**—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>  • **close**—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie die Einstellung nur, wenn das Gerät aktiv überwacht wird).<br>• **monitor**—Überwacht den Verkehr und erstellt Alarme über bösartige Ereignisse.<br>• **bypass**—Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert.<br><br>**HINWEIS:** Beginnend mit Version 7.1.0 umgehen NX Appliances Pakete mit mehr als 1650 Bytes anstatt diese abzulegen. |
| Richtlinientyp | Die folgenden Richtlinientypen werden unterstützt:<br><br>• **mixed**—Wendet sowohl lokale als auch globale Richtlinien an und die lokale Richtlinie hat Vorrang vor der globalen Richtlinie (empfohlen).<br>• **global**—Wendet FireEye-definierte globale Richtlinie auf die angegebene Schnittstelle an.<br>• **local**—Wendet benutzerdefinierte lokale Richtlinie auf die festgelegte Schnittstelle an.<br>• **none**—Wendet keine Richtlinie an. Es wird keine Richtlinie verwendet. |

Details über inline Deployment finden Sie im *Hardware Administrationshandbuch* für Ihr Appliance Modell.

# Voraussetzungen

- Operator oder Admin Zugriff

**Um inline Modus zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) im inline Blockiermodus:

   ```
   hostname (config) # policymgr interface A op-mode block fail-safe open
   policy-type mixed

   hostname (config) # policymgr interface A re-configure
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

4. (Optional) Konfigurieren Sie Paar B (Schnittstellen B1 und B2) im inline Blockiermodus:

   ```
   hostname (config) # policymgr interface B op-mode block fail-safe open
   policy-type mixed

   hostname (config) # policymgr interface B re-configure
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

6. Überprüfen Sie Ihre Konfiguration:

   ```
   hostname (config) # show policymgr interfaces

   Policy enabled: yes

   Interface A

     Active   : yes
     op mode  : block (blocking)
     fail-safe: open
     policy   : mixed
     tolerance: 1

     Ports    : pether3  pether4


   Interface B
     Active   : yes
     op mode  : block (blocking)
     fail-safe: open

     policy   : mixed
     tolerance: 1
     Ports    : pether5  pether6
   ```

# Inline Proxy-Modus über die Web-UI konfigurieren

Inline Proxy-Deployment benötigt zwei Netzwerk-Portpaare. Dies kann mit einer Network Security Appliance mit zwei Portpaaren oder einem Portpaar von jeweils zwei Network Security Appliances erreicht werden.

Details über inline-Proxy-Deployment finden Sie im *Hardware Administrationshandbuch* für Ihr Appliance Modell.

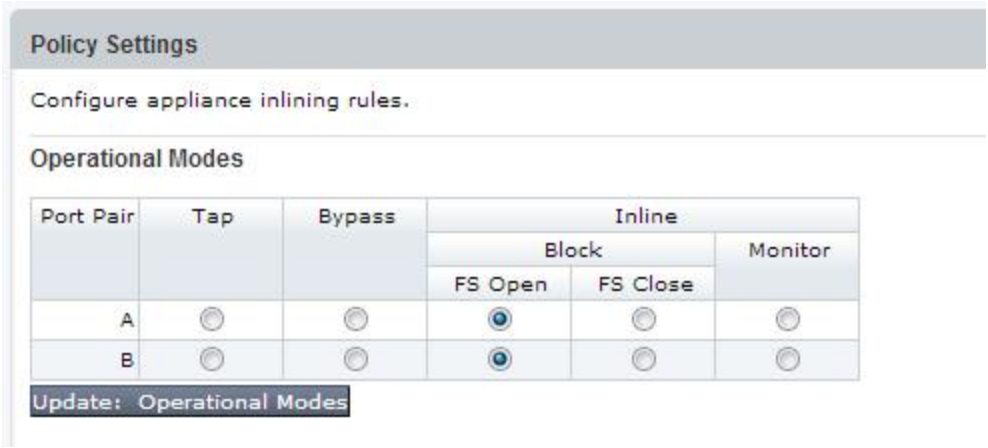
**HINWEIS:** Beginnend mit Version 7.1.0 umgehen NX Appliances Pakete mit mehr als 1650 Bytes anstatt diese abzulegen.

## Voraussetzungen

- Operator oder Admin Zugriff

## Inline Multi-Proxy-Modus mit einer Network Security Appliance konfigurieren

Verwenden Sie die **Policy Settings** Seite für inline Proxy Modus, um eine Bereitstellung mit einer Network Security Appliance mit zwei Netzwerk Port Paaren zu konfigurieren. Schnittstelle A verbindet den-LAN-zugewandten Switch oder Router (A1) mit dem Proxyserver (A2). Schnittstelle B verbindet den LAN-zugewandten Switch oder Router (B1) mit dem Internet-zugewandten Switch oder Router (B2).




Die Betriebsmodi für das Inline-Deployment werden in der folgenden Tabelle beschrieben.

| Modus | Beschreibung |
|---|---|
| Block | Blockiert böswilligen Datenverkehr (empfohlen).<br>• FS Open—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>• FS Close—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie diese Einstellung nur, wenn das Gerät aktiv überwacht wird). |
| Monitor | Überwacht den Verkehr und generiert Alarme für bösartige Ereignisse. |
| Bypass | Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert. |

Verwenden Sie die **Settings: Interfaces - Whitelists** Seite für inline Whitelisten, um Schnittstelle A2 zu konfigurieren, eingehendem Datenverkehr vom Proxyserver ungehinderte Passage zu ermöglichen.


**Um Schnittstelle A und Schnittstelle B zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie eine Blockierungsoption für Paar A und Paar B (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.
5. Wählen Sie **Inline-Whitelists** in der Seitenleiste. Geben Sie die Informationen für den Proxyserver ein und klicken Sie dann auf **Add Whitelist**.

# Inline Multi-Proxy-Modus mit zwei Network Security Appliances konfigurieren

Verwenden Sie die **Policy Settings** Seite für inline Proxy Modus, um Bereitstellung mit zwei Network Security Appliances mit jeweils einem Netzwerk Port Paar zu konfigurieren. NX Appliance1 verbindet mit dem Proxy Offline, und NX Appliance2 befindet sich zwischen einem LAN-zugewandten Switch oder Router und einem Internet-zugewandten Switch oder Router.


Die Betriebsmodi für das Inline-Deployment werden in der folgenden Tabelle beschrieben.

| Modus | Beschreibung |
|---|---|
| Block | Blockiert böswilligen Datenverkehr (empfohlen).<br>• FS Open—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>• FS Close—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie diese Einstellung nur, wenn das Gerät aktiv überwacht wird). |
| Monitor | Überwacht den Verkehr und generiert Alarme für bösartige Ereignisse. |
| Bypass | Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert. |

Verwenden Sie die **Policy Settings** Seite für inline Whitelisten, um Schnittstelle A2 zu konfigurieren zuzulassen, dass eingehender Verkehr vom Proxy Server unbehindert durchlaufen kann.


**Um NX Appliance1 zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie eine Blockierungsoption für Paar A. (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.
5. Wählen Sie **Inline-Whitelists** in der Seitenleiste. Geben Sie die Informationen für den Proxyserver ein und klicken Sie dann auf **Add Whitelist**.

**Um NX Appliance2 zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie eine Blockierungsoption für Paar A. (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.

# Inline Proxy-Modus über die CLI konfigurieren

Inline Proxy-Deployment benötigt zwei Netzwerk-Portpaare. Dies kann mit einer Network Security Appliance mit zwei Portpaaren oder einem Portpaar von jeweils zwei Network Security Appliances erreicht werden.

Verwenden Sie die CLI-Befehle in diesem Thema, um die folgenden Optionen für die Konfigurierung des Inline-Blockierungsmodus für ein Proxy-Deployment einzustellen.

| Einstellung | Beschreibung |
|---|---|
| Betriebsmodus | Das inline Deployment verfügt über drei Betriebsmodi: Es wird dringend empfohlen, dass Sie Ihre Appliance auf inline-Blockierungsmodus einstellen.<br><br>**HINWEIS**: Wenn Sie den Betriebsmodus auf Verkehr blockieren einstellen, geben Sie eine ausfallsichere Einstellung ein (**block open** oder **block close**)<br><br>• **block**—Blockiert bösartigen Verkehr (empfohlen).<br>  • **open**—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>  • **close**—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie die Einstellung nur, wenn das Gerät aktiv überwacht wird).<br>• **monitor**—Überwacht den Verkehr und erstellt Alarme über bösartige Ereignisse.<br>• **bypass**—Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert.<br><br>**HINWEIS:** Beginnend mit Version 7.1.0 umgehen NX Appliances Pakete mit mehr als 1650 Bytes anstatt diese abzulegen. |
| Richtlinientyp | Die folgenden Richtlinientypen werden unterstützt:<br><br>• **mixed**—Wendet sowohl lokale als auch globale Richtlinien an und die lokale Richtlinie hat Vorrang vor der globalen Richtlinie (empfohlen).<br>• **global**—Wendet FireEye-definierte globale Richtlinie auf die festgelegte Schnittstelle an.<br>• **local**—Wendet benutzerdefinierte lokale Richtlinie auf die festgelegte Schnittstelle an.<br>• **none**—Wendet keine Richtlinie an. Es wird keine Richtlinie verwendet. |

Details über inline-Proxy-Deployment finden Sie im *Hardware Administrationshandbuch* für Ihr Appliance Modell.

## Voraussetzungen

- Operator oder Admin Zugriff

## Inline Multi-Proxy-Modus mit einer Network Security Appliance konfigurieren

Verwenden Sie die CLI-Befehle in diesem Thema, um Deployment mit einer Network Security Appliance mit zwei Netzwerk-Portpaaren zu konfigurieren. Schnittstelle A verbindet den-LAN-zugewandten Switch oder Router (A1) mit dem Proxyserver (A2). Schnittstelle B verbindet den LAN-zugewandten Switch oder Router (B1) mit dem Internet-zugewandten Switch oder Router (B2).

**Um Schnittstelle A und Schnittstelle B zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) und Paar B (B1 und B2) im inline Blockiermodus:

   ```
   hostname (config) # policymgr interface A op-mode block fail-safe open
   policy-type mixed
   hostname (config) # policymgr interface A re-configure
   hostname (config) # policymgr interface B op-mode block fail-safe open
   policy-type mixed
   hostname (config) # policymgr interface B re-configure
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

4. Konfigurieren Sie Schnittstelle A2, um eingehendem Verkehr vom Proxy Server zu gestatten, ohne Blockierung durchzulaufen:

   ```
   hostname (config) # policymgr network host <Proxy_IP_address> interface
   A2 allow
   ```

   wobei `Proxy_IP_address` die IP-Adresse des Servers ist.

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

6. Überprüfen Sie Ihre Konfiguration:

   ```
   hostname (config) # show policymgr interfaces
   Policy enabled: yes
   Interface A
     Active   : yes
     op mode  : block (blocking)
   ```

```
  fail-safe: open
  policy   : mixed
  tolerance: 1
  Ports    : pether3  pether4

Interface B
  Active   : yes
  op mode  : block (blocking)
  fail-safe: open
  policy   : mixed
  tolerance: 1
  Ports    : pether5  pether6
```

## Inline Multi-Proxy-Modus mit zwei Network Security Appliances konfigurieren

Verwenden Sie die CLI-Befehle in diesem Thema, um ein Deployment mit zwei Network Security Appliance mit jeweils einem Netzwerk-Portpaar zu konfigurieren. NX Appliance1 verbindet mit dem Proxy Offline, und NX Appliance2 befindet sich zwischen einem LAN-zugewandten Switch oder Router und einem Internet-zugewandten Switch oder Router.

**Um NX Appliance1 zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname1 > enable
   hostname1 # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) im inline Blockiermodus auf der NX Appliance1:

   ```
   hostname1 (config) # policymgr interface A op-mode block fail-safe open
   policy-type mixed
   hostname1 (config) # policymgr interface A re-configure
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname1 (config) # write memory
   ```

4. Konfigurieren Sie Schnittstelle A2, um eingehendem Verkehr vom Proxy Server zu gestatten, ohne Blockierung durchzulaufen:

   ```
   hostname1 (config) # policymgr network host <Proxy_IP_address>
   interface A2 allow
   ```

   wobei `Proxy_IP_address` die IP-Adresse des Servers ist.

5. Speichern Sie Ihre Änderungen:

   ```
   hostname1 (config) # write memory
   ```

6. Überprüfen Sie Ihre Konfiguration:

   ```
   hostname1 (config) # show policymgr interfaces
   Policy enabled: yes
   Interface A
     Active   : yes
   ```

```
  op mode  : block (blocking)
  fail-safe: open
  policy   : mixed
  tolerance: 1
  Ports    : pether3  pether4
```

**Um NX Appliance2 zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname2 > enable
   ```

   ```
   hostname2 # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) im inline Blockiermodus:

   ```
   hostname2 (config) # policymgr interface A op-mode block fail-safe open
   policy-type mixed
   ```

   ```
   hostname2 (config) # policymgr interface A re-configure
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname2 (config) # write memory
   ```

4. Überprüfen Sie Ihre Konfiguration:

   ```
   hostname2 (config) # show policymgr interfaces
   ```

   ```
   Policy enabled: yes
   ```

   ```
   Interface A
     Active   : yes
     op mode  : block (blocking)
     fail-safe: open
     policy   : mixed
     tolerance: 1
     Ports    : pether3  pether4
   ```

# Inline-Multi-Proxy-Modus mit Hilfe der Web-UI konfigurieren

Inline-Multi-Proxy Deployment benötigt zwei Netzwerk-Portpaare. Dies kann mit einer Network Security Appliance mit zwei Portpaaren oder einem Portpaar von jeweils zwei Network Security Appliances erreicht werden.

Einzelheiten über inline-Deployment mit mehreren Proxy-Servern finden Sie im *Hardware Administrationshandbuch* für Ihr Appliance Modell.

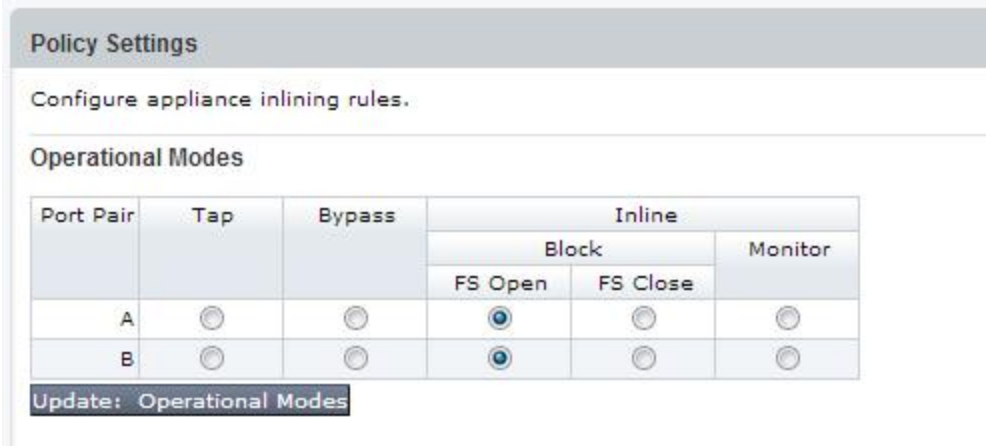
**HINWEIS:** Beginnend mit Version 7.1.0 umgehen NX Appliances Pakete mit mehr als 1650 Bytes anstatt diese abzulegen.

## Voraussetzungen

- Operator oder Admin Zugriff

## Inline Multi-Proxy-Modus mit einer Network Security Appliance konfigurieren

Verwenden Sie die **Policy Settings** Seite, für inline Multi-Proxy Modus, um eine Bereitstellung mit einer Network Security Appliance mit zwei Netzwerk Port Paaren zu konfigurieren. Schnittstelle A verbindet den-LAN-zugewandten Switch oder Router (A1) mit dem Proxyserver (A2). Schnittstelle B verbindet den LAN-zugewandten Switch oder Router (B1) mit dem Internet-zugewandten Switch oder Router (B2). Zusätzliche Network Security Appliances werden mit einem oder mehreren zusätzlichen Proxy Servern verbunden.




Die Betriebsmodi für die Inline-Deployment werden in der folgenden Tabelle beschrieben.

| Modus | Beschreibung |
|---|---|
| Block | Blockiert böswilligen Datenverkehr (empfohlen).<br>• FS Open—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>• FS Close—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie diese Einstellung nur, wenn das Gerät aktiv überwacht wird). |
| Monitor | Überwacht den Verkehr und generiert Alarme für bösartige Ereignisse. |
| Bypass | Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert. |

Verwenden Sie die **Policy Settings** Seite für inline Whitelisten, um Schnittstelle A2 zu konfigurieren zuzulassen, dass eingehender Verkehr vom Proxy Server unbehindert durchlaufen kann.


**Um Schnittstelle A und Schnittstelle B auf NX Appliance1 zu konfigurieren:**

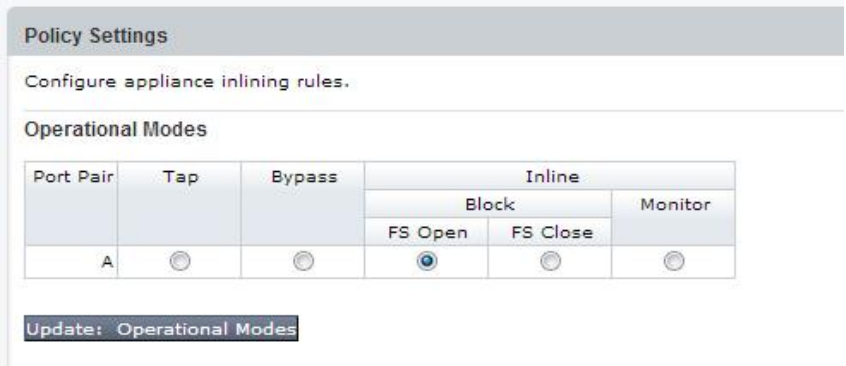
1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie eine Blockierungsoption für Paar A und Paar B (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.
5. Wählen **Inline-Whitelists** in der Seitenleiste. Geben Sie die Informationen für den Proxyserver ein und klicken Sie dann auf **Add Whitelist**.

**Um NX Appliance2 - NX Appliance *n* zu konfigurieren, mit einem oder mehreren Proxy Servern zu verbinden:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie eine Blockierungsoption für Paar A und Paar B (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.
5. Wählen **Inline-Whitelists** in der Seitenleiste. Geben Sie die Informationen für den Proxyserver ein und klicken Sie dann auf **Add Whitelist**.
6. Wiederholen Sie die Schritte 1 bis 5 für jede weitere Network Security Appliance.

# Inline Multi-Proxy-Modus mit zwei Network Security Appliances konfigurieren

Verwenden Sie die **Policy Settings** Seite für inline Multi-Proxy Modus, um Deployment mit zwei Network Security Appliances mit jeweils einem Netzwerk Port Paar zu konfigurieren. NX Appliance1 befindet sich inline zwischen einem LAN-zugewandten Switch oder Router und einem Internet-zugewandten Switch oder Router. Die Network Security Appliances NX Appliance2—NX Appliance *n* verbinden mit mehreren Proxyservern offline.




Die Betriebsmodi für die Inline-Deployment werden in der folgenden Tabelle beschrieben.

| Modus | Beschreibung |
|---|---|
| Block | Blockiert böswilligen Datenverkehr (empfohlen).<br>• FS Open—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>• FS Close—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie diese Einstellung nur, wenn das Gerät aktiv überwacht wird). |
| Monitor | Überwacht den Verkehr und generiert Alarme für bösartige Ereignisse. |
| Bypass | Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert. |

Für jede mit einem Proxy Server verbundene Appliance verwenden Sie die **Proxy Settings** Seite, um Schnittstelle A2 zu konfigurieren, eingehendem Verkehr von dem Proxy Server zu gestatten, ungehindert durch den Proxy Server zu durchlaufen.


**Um NX Appliance1 zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie eine Blockierungsoption für Paar A. (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.
5. Wählen Sie **Inline-Whitelists** in der Seitenleiste. Geben Sie die Informationen für den Proxyserver ein und klicken Sie dann auf **Add Whitelist**.

**Um NX Appliance2 - NX Appliance *n* zu konfigurieren, mit einem oder mehreren Proxy Servern zu verbinden:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie eine Blockierungsoption für Paar A. (Inline Block FS Open ist empfohlen).
4. Klicken Sie auf **Update: Operational Modes**.
5. Wählen Sie **Inline-Whitelists** in der Seitenleiste. Geben Sie die Informationen für den Proxyserver ein und klicken Sie dann auf **Add Whitelist**.
6. Wiederholen Sie diese Schritte auf jeder zusätzlichen Network Security Appliance.

# Inline-Multi-Proxy-Modus mithilfe der CLI konfigurieren

Inline-Multi-Proxy Deployment benötigt zwei Netzwerk-Portpaare. Dies kann mit einer Network Security Appliance mit zwei Portpaaren oder einem Portpaar von jeweils zwei Network Security Appliances erreicht werden.

Verwenden Sie die CLI Befehle in den folgenden Themen, um inline Blockiermodus für ein inline Deployment mit mehreren Proxys zu konfigurieren.

| | |
|---|---|
| Operational Mode | Das inline Deployment verfügt über drei optionale Modi: Es wird dringend empfohlen, dass Sie Ihre Appliance auf inline-Blockierungsmodus einstellen.<br><br>**HINWEIS**: Wenn Sie den Betriebsmodus auf Verkehr blockieren einstellen, geben Sie eine ausfallsichere Einstellung ein (**block open** oder **block close**)<br><br>• **block**—Blockiert bösartigen Verkehr (empfohlen).<br>  • **open**—Im Störfall wird aller Verkehr durchgeleitet (empfohlen).<br>  • **close**—Im Störfall wird aller Verkehr blockiert. (Benutzen Sie die Einstellung nur, wenn das Gerät aktiv überwacht wird).<br>• **monitor**—Überwacht den Verkehr und erstellt Alarme über bösartige Ereignisse.<br>• **bypass**—Erzwungene Überbrückung, wobei die Network Security Appliance Datenverkehr weder blockiert noch analysiert.<br><br>**HINWEIS:** Beginnend mit Version 7.1.0 umgehen NX Appliances Pakete mit mehr als 1650 Bytes anstatt diese abzulegen. |
| Richtlinientyp | Die folgenden Richtlinientypen werden unterstützt:<br><br>• **mixed**—Wendet sowohl lokale als auch globale Richtlinien an und die lokale Richtlinie hat Vorrang vor der globalen Richtlinie (empfohlen).<br>• **global**—Wendet FireEye-definierte globale Richtlinie auf die festgelegte Schnittstelle an.<br>• **local**—Wendet benutzerdefinierte lokale Richtlinie auf die festgelegte Schnittstelle an.<br>• **none**—Wendet keine Richtlinie an. Es wird keine Richtlinie verwendet. |

Einzelheiten über inline-Deployment mit mehreren Proxy-Servern finden Sie im *Hardware Administrationshandbuch* für Ihr Appliance Modell.

## Voraussetzungen

- Operator oder Admin Zugriff

## Inline Multi-Proxy-Modus mit einer Network Security Appliance konfigurieren

Verwenden Sie die CLI Befehle in diesem Thema, um Network Security Appliances mit mehreren Netzwerk-Portpaaren zu konfigurieren. Schnittstelle A verbindet den-LAN-zugewandten Switch oder Router (A1) mit dem Proxyserver (A2). Schnittstelle B verbindet den LAN-zugewandten Switch oder Router (B1) mit dem Internet-zugewandten Switch oder Router (B2). Zusätzliche Network Security Appliances werden mit einem oder mehreren zusätzlichen Proxy Servern verbunden.

**Um Schnittstelle A und Schnittstelle B auf NX Appliance1 zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname1 > enable
   hostname1 # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) und Paar B (B1 und B2) im inline Blockiermodus:

   ```
   hostname1 (config) # policymgr interface A op-mode block fail-safe open
   policy-type mixed
   hostname1 (config) # policymgr interface A re-configure
   hostname1 (config) # policymgr interface B op-mode block fail-safe open
   policy-type mixed
   hostname1 (config) # policymgr interface B re-configure
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname1 (config) # write memory
   ```

4. Konfigurieren Sie Schnittstelle A2, um eingehendem Verkehr vom Proxy Server zu gestatten ungehindert zu passieren:

   ```
   hostname1 (config) # policymgr network host <Proxy_IP_address>
   interface A2 allow
   ```

   wobei `Proxy_IP_address` die IP-Adresse des Servers ist.

5. Speichern Sie Ihre Änderungen:

   ```
   hostname1 (config) # write memory
   ```

**Um NX Appliance2 - NX Appliance *n* zu konfigurieren, mit einem oder mehreren Proxy Servern zu verbinden:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) im inline Blockiermodus auf jeder NX Appliance2-NX Appliance*n*:

   ```
   hostname (config) # policymgr interface A op-mode block fail-safe open policy-type mixed
   hostname (config) # policymgr interface A re-configure
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

4. Konfigurieren Sie Schnittstelle A2 , um eingehendem Verkehr vom Proxy Server zu gestatten, ohne Blockierung auf jeder Appliance durchzulaufen, die mit einem Proxy Server verbunden ist:

   ```
   hostname (config) # policymgr network host <Proxy_IP_address> interface A2 allow
   ```

   wobei `Proxy_IP_address` die IP-Adresse des Servers ist.

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

6. Überprüfen Sie Ihre Konfiguration:

   ```
   hostname (config) # show policymgr interfaces
   Policy enabled: yes
   Interface A
     Active   : yes
     op mode  : block (blocking)
     fail-safe: open
     policy   : mixed
     tolerance: 1
     Ports    : pether3  pether4

   Interface B
     Active   : yes
     op mode  : block (blocking)
     fail-safe: open
     policy   : mixed
     tolerance: 1
     Ports    : pether5  pether6
   ```

## Inline Multi-Proxy-Modus mit zwei Network Security Appliances konfigurieren

Verwenden Sie die CLI-Befehle in diesem Thema, um Deployment mit zwei Network Security Appliance mit jeweils einem Netzwerk-Portpaar zu konfigurieren. NX Appliance1 befindet sich inline zwischen einem LAN-zugewandten Switch oder Router und einem Internet-zugewandten Switch oder Router. NX Appliance2—NX Appliance *n* verbomde

**Um NX Appliance1 zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname1 > enable
   ```

```
hostname1 # configure terminal
```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) im inline Blockiermodus:

```
hostname1 (config) # policymgr interface A op-mode block fail-safe open
policy-type mixed
hostname1 (config) # policymgr interface A re-configure
```

3. Speichern Sie Ihre Änderungen:

```
hostname1 (config) # write memory
```

4. Überprüfen Sie Ihre Konfiguration:

```
hostname1 (config) # show policymgr interfaces
Policy enabled: yes
Interface A
  Active   : yes
  op mode  : block (blocking)
  fail-safe: open
  policy   : mixed
  tolerance: 1
  Ports    : pether3  pether4
```

**Um NX Appliance2 - NX Appliance *n* zu konfigurieren, mit einem oder mehreren Proxy Servern zu verbinden:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

```
hostname > enable
hostname # configure terminal
```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) im inline Blockiermodus auf jeder NX Appliance2-NX Appliance*n*:

```
hostname (config) # policymgr interface A op-mode block fail-safe open
policy-type mixed
hostname (config) # policymgr interface A re-configure
```

3. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

4. Konfigurieren Sie Schnittstelle A2 , um eingehendem Verkehr vom Proxy Server zu gestatten, ohne Blockierung auf jeder Appliance durchzulaufen, die mit einem Proxy Server verbunden ist:

```
hostname (config) # policymgr network host <Proxy_IP_address> interface
A2 allow
```

wobei `Proxy_IP_address` die IP-Adresse des Servers ist.

5. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

6. Überprüfen Sie Ihre Konfiguration:

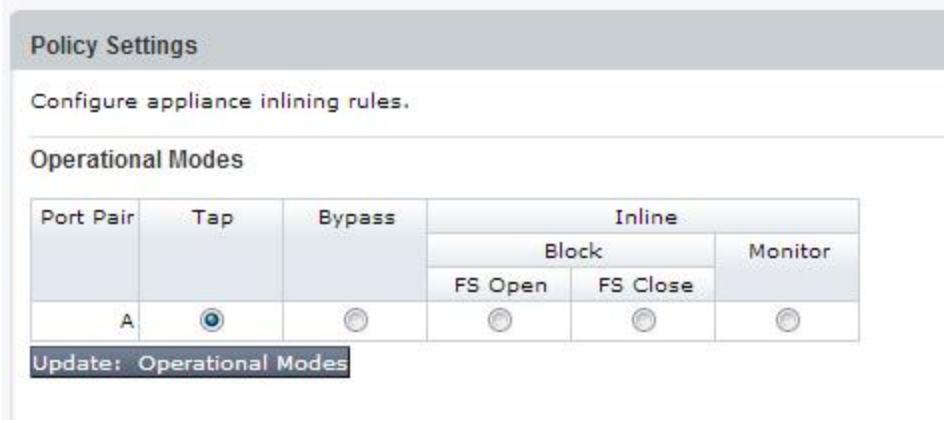
```
hostname (config) # show policymgr interfaces
Policy enabled: yes
```

```
Interface A
  Active   : yes
  op mode  : block (blocking)
  fail-safe: open
  policy   : mixed
  tolerance: 1
  Ports    : pether3  pether4
```

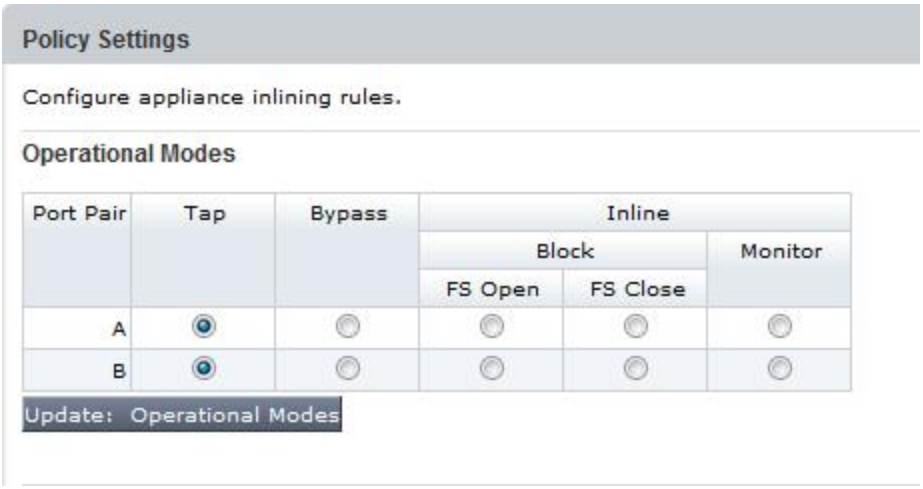
# TAP-Modus mit Hilfe der Web-UI konfigurieren

Verwenden Sie die **Policy Settings** Seite, um Test Access Point (TAP) Modus zu konfigurieren.

Im TAP-Modus können Sie Appliance mit einem oder zwei Netzwerk-Portpaaren konfigurieren. Das folgende Beispiel zeigt ein Netzwerk-Portpaar.




Das folgende Beispiel zeigt zwei Netzwerk-Portpaare.



Details über das TAP-Deployment finden Sie in der *Bedienungsanleitung* für Ihr Appliance Modell.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um TAP-Modus zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie den **TAP** Betriebsmodus für alle verfügbaren Port Paare.
4. Klicken Sie auf **Update: Operational Modes**.

# TAP-Modus mit Hilfe der CLI konfigurieren

Verwenden Sie die CLI-Befehle in diesem Thema, um die folgenden Optionen für die Konfigurierung der Appliance für Test Access Point (TAP) Modus einzustellen.

| Einstellung | Beschreibung |
|---|---|
| Betriebsmodus | Wählen Sie TAP Modus, um für TAP oder SPAN Bereitstellungen zu konfigurieren.<br>• **tap**—Überwacht bösartigen Verkehr. |
| Richtlinientyp | Die folgenden Richtlinientypen werden unterstützt:<br>• **mixed**—Wendet sowohl lokale als auch globale Richtlinien an und die lokale Richtlinie hat Vorrang vor der globalen Richtlinie (empfohlen).<br>• **global**—Wendet FireEye-definierte globale Richtlinie auf die festgelegte Schnittstelle an.<br>• **local**—Wendet benutzerdefinierte lokale Richtlinie auf die festgelegte Schnittstelle an.<br>• **none**—Wendet keine Richtlinie an. Es wird keine Richtlinie verwendet. |

Details über das TAP-Deployment finden Sie in der *Bedienungsanleitung* für Ihr Appliance Modell.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um TAP-Modus zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstelle A1 und A2) im TAP-Modus:

   ```
   hostname (config) # policymgr interface A op-mode tap policy-type mixed
   hostname (config) # policymgr interface A re-configure
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

4. Überprüfen Sie Ihre Konfiguration:

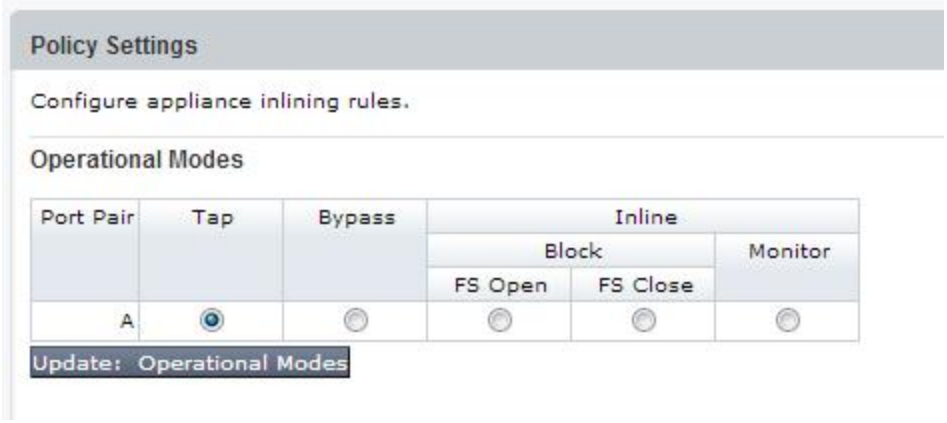
   ```
   hostname (config) # show policymgr interfaces
   Policy enabled: yes
   Interface A
     Active   : yes
     op mode  : tap (tapping)
     fail-safe: open
     policy   : mixed
     tolerance: 1
     Ports    : pether3  pether4
   ```

# SPAN-Modus mit Hilfe der Web-UI konfigurieren

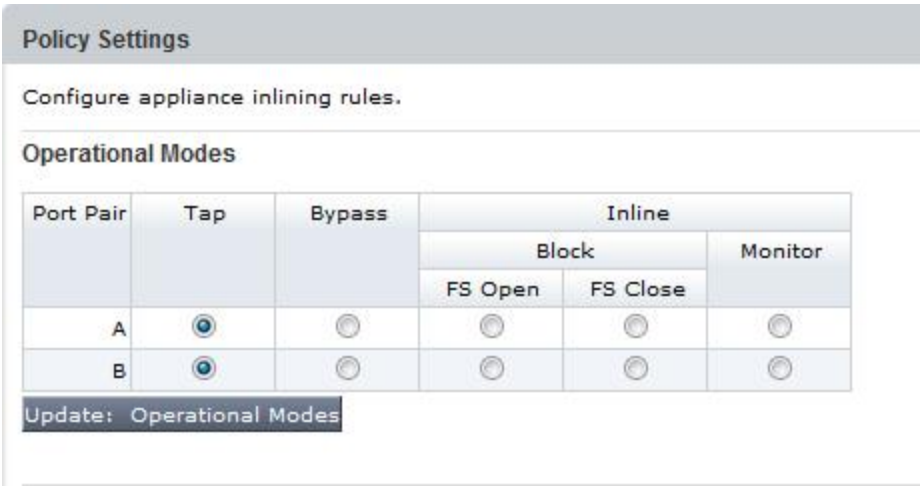
Verwenden Sie die **Policy Settings** Seite, um die Network Security Appliance zu konfigurieren, Netzwerkverkehr von den SPAN Ports eines Gerätes mit Portspiegelungsfähigkeiten zu empfangen.

Im Span-Modus können Sie Appliance mit einem oder zwei Netzwerk-Portpaaren konfigurieren. Das folgende Beispiel zeigt ein Netzwerk-Portpaar.




Das folgende Beispiel zeigt zwei Netzwerk-Portpaare.




# Voraussetzungen

- Operator oder Admin Zugriff

**Um SPAN-Modus zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Inline Operational Modes**.
3. Wählen Sie den **TAP** Betriebsmodus für alle verfügbaren Port Paare.
4. Klicken Sie auf **Update: Operational Modes**.

# SPAN-Modus mit Hilfe der CLI konfigurieren

Verwenden Sie die CLI Befehle in diesem Thema, um die Network Security Appliance zu konfigurieren, Netzwerkverkehr von den SPAN-Ports des Gerätes mit Portspiegelungsfähigkeiten zu empfangen.

| Einstellung | Beschreibung |
|---|---|
| Betriebsmodus | Wählen Sie TAP Modus, um für TAP oder SPAN Bereitstellungen zu konfigurieren.<br>• **tap**—Überwacht bösartigen Verkehr. |
| Richtlinientyp | Die folgenden Richtlinientypen werden unterstützt:<br>• **mixed**—Wendet sowohl lokale als auch globale Richtlinien an und die lokale Richtlinie hat Vorrang vor der globalen Richtlinie (empfohlen).<br>• **global**—Wendet FireEye-definierte globale Richtlinie auf die festgelegte Schnittstelle an.<br>• **local**—Wendet benutzerdefinierte lokale Richtlinie auf die festgelegte Schnittstelle an.<br>• **none**—Wendet keine Richtlinie an. Es wird keine Richtlinie verwendet. |

Details über das SPAN-Deployment finden Sie in der *Bedienungsanleitung* für Ihr Appliance Modell.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um SPAN-Modus zu konfigurieren:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Konfigurieren Sie Paar A (Schnittstellen A1 und A2) im inline Blockiermodus:

   ```
   hostname (config) # policymgr interface A op-mode tap policy-type mixed
   hostname (config) # policymgr interface A re-configure
   ```

3. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

4. Überprüfen Sie Ihre Konfiguration:

```
hostname (config) # show policymgr interfaces

Policy enabled: yes

Interface A
  Active   : yes
  op mode  : tap (tapping)
  fail-safe: open
  policy   : mixed
  tolerance: 1
  Ports    : pether3  pether4
```

# KAPITEL 8: Lizenzschlüssel

Dieses Thema behandelt die folgenden Informationen:



## FireEye Lizenzschlüssel

Lizenzschlüssel sind für den Systembetrieb erforderlich. Die Network Security Appliance benötigt diese Lizenzschlüssel:

| Lizenzschlüssel | Beschreibung |
|---|---|
| **FIREEYE_ APPLIANCE** | Erforderlich, um Ihr System zu registrieren und die Produktfunktionen zu verwenden. |

| Lizenzschlüssel | Beschreibung |
|---|---|
| **CONTENT_ UPDATES** | Ermöglicht Ihrem System den Zugriff auf das Dynamic Threat Intelligence (DTI) - Netzwerk, das die neuesten Informationen zu erweiterten Cyber-Angriffen und Rückrufzielen für Malware bereitstellt.<br><br>Dies ermöglicht FireEye Produkten, proaktiv neue Bedrohungen zu erkennen und Angriffe abzuwehren.<br><br>Die *zweiweg* Freigabelizenz liefert Ihrer Appliance Malware Informationen vom DTI-Netzwerk und teilt Daten über Malware, die von Ihrer Appliance analysiert wurden.<br><br>Die *einweg* Freigabelizenz liefert Ihrer Appliance Malware Informationen, aber es werden keine Informationen an die DTI-Cloud eingegeben.<br><br>• Sie können den `analysis one-way-override enable` Befehl verwenden, um die einweg CONTENT_UPDATES Freigabelizenz auf Ihrer Appliance zu übersteuern und Anfragen an `unity.fireeye.com` zu senden.<br><br>• Standardmäßig ermöglichen lokale Intel-Feeds für FAUDE und Global Cache den Appliances, Erkennung zu verbessern, ohne ihre Einweg-Freigabelizenz für Content Updates zu übersteuern und ohne FAUDE oder den Global Cache direkt aufzurufen. Einzelheiten und Informationen über das Deaktivieren und erneutes Aktivieren der Feeds finden Sie in der *Bedienungsanleitung* für die Appliance.<br><br>**WICHTIG:** Sehen Sie Info über Freigabekombinationen von Support- und Inhaltslizenzen auf Seite 162.<br><br>**HINWEIS:** Wenn Sie eine einweg Lizenz verwenden, wird lokal generierte Intel über alle Appliances hinweg geteilt, die an die Central Management Appliance angehängt sind. |

| Lizenzschlüssel | Beschreibung |
|---|---|
| **FIREEYE_ SUPPORT** | Ermöglicht Ihrem System, Software Image Aktualisierungen und die neuesten Guest Images zu empfangen und je nach Ihrer Freigabeoption Telemetrie und Statistiken auf die DTI-Cloud hochzuladen.<br><br>Die *zweiweg* Freigabelizenz ermöglicht der Appliance, Telemetrie und Statistiken für die Überwachung durch FireEye auf die DTI-Cloud hochzuladen. Die *einweg* Freigabelizenz lädt keine Telemetrie und Statistiken auf die DTI-Cloud hoch.<br><br>**WICHTIG:** Sehen Sie Info über Freigabekombinationen von Support- und Inhaltslizenzen auf Seite 162.<br><br>**HINWEIS:** Klicken Sie hier um Informationen über proaktiven Support für Probleme, die FireEye in hochgeladener Telemetrie und Statistiken beobachtet. |
| **CLOUD_MVX** | Ermöglicht Sensoren, an die FireEye Cloud MVX oder eine Private Cloud MVX einzureichen. |

Die folgenden Lizenzen sind optional.

**HINWEIS:** Die Funktionalität der optionalen Lizenzen ist deaktiviert, wenn die FIREYYE_APPLIANCE Lizenz ungültig ist.

| Lizenzschlüssel | Beschreibung |
|---|---|
| **ATI** | Ermöglicht Ihrer Appliance, Advance Threat Intelligence Funktionen zu verwenden.<br><br>Nicht auf der Network Security SmartVision Produktausgabe unterstützt |
| **MD_ACCESS** | Ermöglicht FireEye Produkten, sich mit der Managed Defense VPN zu verbinden. Ohne diese Lizenz kann Managed Defense den Server nicht verwalten. |
| **AV_ENGINE_SOPHOS** | Ermöglicht Ihrer Appliance, die integrierte Sophos Engine zum Scannen übermittelter Malware Beispiele zu verwenden. |
| **DA_HANCOM** | Ermöglicht Ihrer Appliance, dynamische Analyse von Hancom Office Dateien auszuführen. |

Wenn Lizenzen abgelaufen sind oder innerhalb von 30 Tagen ablaufen, werden Alarme auf der **Appliance License Settings** Seite angezeigt. Details finden Sie unter Lizenzbenachrichtigungen mit Hilfe der Web-UI anzeigen auf Seite 155.

# Die Einweg-Freigabelizenz überschreiben

Eine Einweg-Freigabelizenz auf der Appliances liefert der Network Security Appliance Malware Informationen, aber es werden keine Informationen an die AV-Suite und FAUDE eingereicht. Wenn Sie die Einstellung für die Einweg-Lizenzfreigabe überschreiben, kann die Appliance Informationen, wie z.B. eine MD5 Checksumme an die AV-Suite und FAUDE zur weiteren Malware Analyse senden.

**HINWEIS:** Standardmäßig ermöglichen es die lokalen Intel-Feeds von FAUDE und Global Cache den Appliances, die Erkennung zu verbessern, ohne ihre Einweg CONTENT_UPDATES Freigabelizenz außer Kraft zu setzen und ohne direkt auf FAUDE oder den Global Cache zuzugreifen. Einzelheiten und Informationen über das Deaktivieren und erneutes Aktivieren der Feeds finden Sie in der *Bedienungsanleitung* für die Appliance.

## Voraussetzungen

- Admin oder Operator Zugriff auf die Appliance
- Eine Einweg oder Zweiweg CONTENT_UPDATES Freigabelizenz
- Bestätigen Sie, dass AV-Suite Integration aktiviert ist und AV-Suite Version 6 konfiguriert ist. Verwenden Sie den`show static-analysis config` Befehl.

## Die Einweg-Freigabelizenz mit Hilfe der CLI übersteuern

Folgen Sie diesen Schritten, um die Einstellung der Einweg-Freigabelizenz zu übersteuern und Informationen mit AV-Suite und der FAUDE von der Network Security Appliance zu teilen.

**Um die Einweg-Freigabelizenz zu überschreiben:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Überschreiben Sie die Einweg-Freigabelizenz auf der Appliance.

   ```
   hostname (config) # analysis one-way-override enable
   ```

3. Bestätigen Sie, dass die Einweg-Freigabelizenz überschrieben wurde.

   ```
   hostname # show analysis one-way-override
   one_way license override     :Enabled
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um die Einweg-Freigabelizenz auf ihre Standardeinstellung zurückzusetzen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Setzen Sie die Einweg-Freigabelizenz auf ihre Standardeinstellung zurück.

   ```
   hostname (config) # no analysis one-way-override enable
   ```

3. Bestätigen Sie, dass die Einweg-Freigabelizenz auf ihre Standardeinstellung zurückgesetzt wurde.

   ```
   hostname # show analysis one-way-override
   one_way license override    :Disabled
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Automatische Lizenzaktualisierungen

Die Lizenzaktualisierungsfunktion ermöglicht der Network Security Appliance mit einfacher Netzwerkkonnektivität, automatisch Lizenzen aus dem DTI Netzwerk herunterzuladen und zu installieren. Diese Funktion bietet die folgenden Vorteile:

- Minimale Erstkonfiguration—Die Lizenzaktualisierungsfunktion wird mit dem Konfigurations-Jump-Start Assistenten während der Erstkonfiguration des Systems aktiviert. Dies bedeutet, dass die Funktion voll funktionsfähig ist, nachdem der Jump-Start Assistent abgeschlossen ist.
- Vereinfachte Lizenzverwaltung—Es ist nicht erforderlich, FireEye für Lizenzschlüssel zu kontaktieren, wenn neue Funktionen hinzugefügt oder Lizenzen erneuert werden, weil die neuen Lizenzen automatisch heruntergeladen und installiert werden.
- Skalierbarkeit—Organisationen, wie z.B. solche mit einer großen Anzahl von Appliances, können davon profitieren, dass alle Appliances automatisch aktualisiert werden, anstatt Lizenzschlüssel manuell auf jeder Appliance einzeln einzugeben.

Sie können automatische Lizenzaktualisierungen auf der Network Security Appliance mit Hilfe des Konfigurationsassistenten oder der CLI aktivieren.

## Wie funktioniert es

Die Lizenzaktualisierungsfunktion, wenn aktiviert, lädt die Lizenzen, auf die der Kunde vertraglich anspruchsberechtigt ist, herunter und wendet sie an. Wenn eine aktive Lizenz für eine Funktion bereits installiert ist und der Lizenzierungsdienst eine aktive Lizenz für die Funktion herunterlädt, wird die installierte Lizenz nur dann durch die heruntergeladene Lizenz ersetzt, wenn die heruntergeladene Lizenz neue Funktionalität oder ein späteres Ablaufdatum bietet oder Teil eines neueren Kundenauftrags war. Dieser Prozess ist automatisch; allerdings können Sie Lizenzen auch ausdrücklich aktualisieren.

Die Lizenzaktualisierungsfunktion wird nicht:

- Eine heruntergeladene Lizenz installieren, die verursachen könnte, dass eine Funktion zeitweilig nicht-lizenziert werden könnte.
- Entfernen Sie eine Feature-Lizenz, wenn kein neu bestellter Ersatz dafür vorhanden ist.

Wenn Sie Probleme mit einer von einem automatischem Update abgerufenen Lizenz haben, können Sie den `no fenet license update enable` Befehl verwenden, um den automatischen Updatevorgang zu deaktivieren und den `license install <cr>` Befehl, um Ihre(n) älteren Lizenzschlüssel manuell zu installieren.

Sie können die Systemzeit mit der DTI-Serverzeit synchronisieren, um zu verhindern, dass eine Funktion auf Grund von Zeitunterschieden vorübergehend nicht lizenziert ist. Die ist eine einmalige Synchronisation, aber sie kann wiederholt werden.

Wenn eine Appliance von der Central Management Appliance verwaltet wird, agiert die Central Management Appliance als ein Proxy zwischen der verwalteten Appliance und dem Lizenzierungsdienst. Die Lizenzaktualisierungsfunktion muss trotzdem auf der verwalteten Appliance aktiviert sein. In einer solchen integrierten Umgebung agiert die Central Management Appliance als der DTI-Server für die verwalteten Appliances, so dass der Lizenzierungsdienst die Berechtigungen des Central Management DTI-Netzwerks anstelle der Berechtigungen der Appliance verwendet.

## Automatische Lizenzaktualisierungen aktivieren

In diesem Abschnitt werden zwei Methoden zur Aktivierung automatischer Lizenzaktualisierungen auf der Network Security Appliance beschrieben.

## Konfigurationsassistent Methode

Der Konfigurationsassistent wird normalerweise benutzt, um ein neues System anfänglich zu konfigurieren. Die Schritte des Assistenten, die die folgenden Lizenzaktivierungsschritte einschließen, gestatten einem Benutzer, ein funktionierendes System mit nur minimaler Konfiguration zu haben.

- Enable fenet service?
- Enable fenet license update service?
- Sync appliance time with fenet?
- Update licenses from fenet?

Details über die Schritte des Assistenten finden Sie unter Schritte des Konfigurationsassistenten auf Seite 102.

## CLI Methode

Das folgende Thema beschreibt die Verwendung von CLI Befehlen zum Aktivieren und Arbeiten mit der Lizenzaktualisierungsfunktion.

- Automatische Lizenzaktualisierungen mithilfe der CLI aktivieren unten

# Voraussetzungen

- Eine bestehende Verbindung zwischen der Appliance und dem Internet.
- Operator- oder Adminzugriff, um die Lizenzaktualisierungsfunktion zu aktivieren und Lizenzen herunterzuladen und zu installieren.
- DTI-Netzwerkzugriff, um der Appliance zu ermöglichen, Aktualisierungen direkt vom DTI-Netzwerk zu erhalten.
- (Optional) Adminzugriff zum Synchronisieren der Systemuhr mit der DTI Serveruhr.

## Automatische Lizenzaktualisierungen mithilfe der CLI aktivieren

Wenn die Lizenzaktualisierungsfunktion aktiviert ist, werden Lizenzen automatisch aktualisiert. Sie können Lizenzen auch ausdrücklich aktualisieren.

**Um automatische Lizenzaktualisierungen zu überprüfen und zu aktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus:

```
hostname > enable
hostname # configure terminal
```

2. Überprüfen Sie den Status der Lizenzaktualisierungsfunktion:

```
hostname (config) # show fenet license
fenet License Update Service

Licensing service: Administratively enabled

Last time licensing service was contacted: 2014/08/11 10:50:04
Last time licensing service was contacted successfully: 2014/08/11
10:50:04
Last time keys from licensing service were applied: 2014/08/07 17:50:03
```

3. Wenn der Lizenzaktualisierungsfunktionsdienst deaktiviert ist, aktivieren Sie ihn:

```
hostname (config) # fenet license update enable
```

4. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

**HINWEIS:** Sehen Sie Die Systemuhr mit DTI-Serverzeit mit Hilfe der CLI synchronisieren auf Seite 241 für eine Option, die mögliche Lizenzprobleme verhindert, wenn eine Zeitlücke zwischen den beiden Uhren besteht.

**Um Lizenzen ausdrücklich zu aktualisieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus:

```
hostname > enable
hostname # configure terminal
```

2. Aktualisieren Sie Lizenzen:

```
hostname (config) # fenet license update
```

3. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

**Um automatische Lizenzaktualisierungen zu deaktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus:

```
hostname > enable
hostname # configure terminal
```

2. Deaktivieren Sie die Funktion:

```
hostname (config) # no fenet license update enable
```

3. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

# Manuelle Lizenzinstallation

Wenn die Lizenzaktualisierungsfunktion nicht aktiviert ist, müssen Sie Lizenzschlüssel manuell installieren. Lizenzen müssen installiert werden, wenn eine Beurteilungslizenz

abläuft oder eine Lizenz abläuft oder nicht länger Ihren Anforderungen entspricht. Zusätzlich müssen Ersatzlizenzen nach einer Return Material Authorization (RMA) installiert werden.

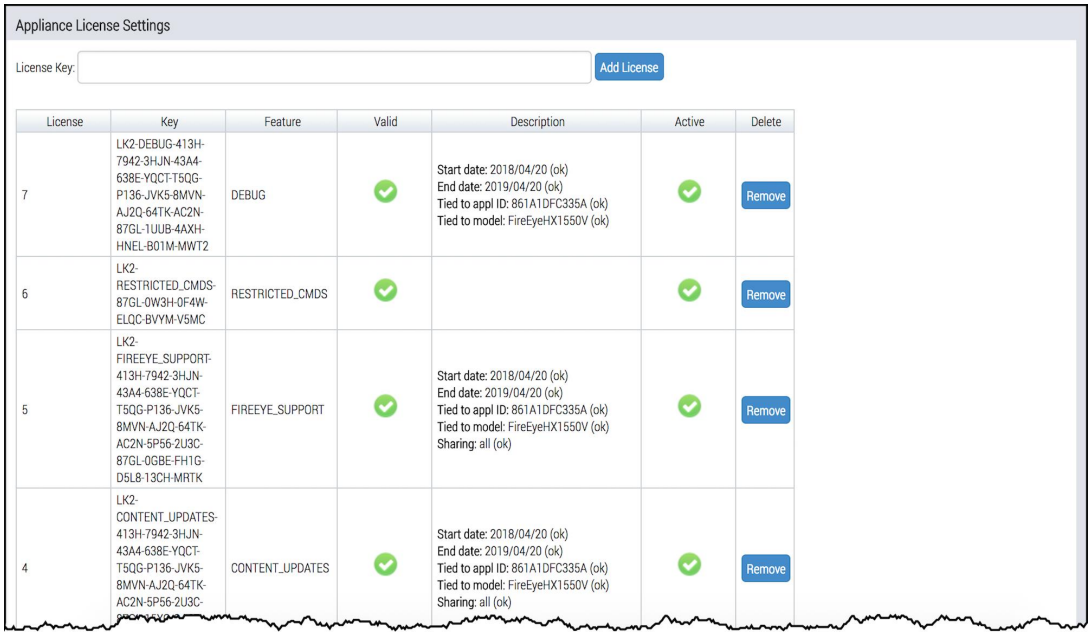
Sie können Ihre Lizenzschlüssel vom Register **Assets** im FireEye Customer Support Portal erhalten, oder indem Sie eine E-Mail an key_request@fireeye.com senden, die die MAC Adresse Ihrer Appliance enthält.

Es gibt zwei Arten, Lizenzen manuell zu installieren, wie in den folgenden Themen beschrieben:

- Lizenzen mit Hilfe der Web-UI installieren unten
- Lizenzen mit Hilfe der CLI installieren auf der nächsten Seite

## Lizenzen mit Hilfe der Web-UI installieren

Verwenden Sie die **Appliance License Settings** Seite, um Lizenzen auf der Network Security Appliance zu installieren.




**HINWEIS:** Das Klicken auf den **Enable VPN** Link in der **Description** Spalte für eine MD_ACCESS Lizenz ermöglicht Ihnen, die Appliance mit Managed Defense (früher FireEye as a Service genannt)über das Internet mit Hilfe einer sicheren SSL VPN Verbindung zu verbinden. Details finden Sie in der *Managed Defense Kurzanleitung*.

## Voraussetzungen

- Admin oder Operator Zugriff.
- Der Lizenzschlüsseltyp, den Sie installieren, ist noch nicht auf der Appliance vorhanden.

**Um Lizenzschlüssel mit Hilfe der Web-UI zu installieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Appliance Licenses**.
3. Fügen Sie den Lizenzschlüssel, den Sie von FireEye erhalten haben, im Feld **License Key** ein..
4. Klicken Sie auf **Add**.

   Die Seite wird aktualisiert, um den Lizenzschlüssel in der Tabelle anzuzeigen. Wenn der Schlüssel gültig ist, wird in der **Valid** Spalte ein Häkchen angezeigt und zusätzliche Informationen werden über die Lizenz angezeigt.

## Lizenzen mit Hilfe der Web-UI entfernen

Verwenden Sie die **Appliance License Settings** Seite, um Network Security Lizenzen zu entfernen.

## Voraussetzungen

- Admin oder Operator Zugriff

**Um Lizenzschlüssel zu entfernen:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Appliance Licenses**.
3. Klicken Sie auf das Symbol in der **Delete** Spalte in der Zeile für die Lizenz, die Sie entfernen wollen.
4. Klicken Sie auf **Yes** in der Bestätigungsnachricht, die angezeigt wird.

## Lizenzen mit Hilfe der CLI installieren

Verwenden Sie die CLI Befehle in diesem Thema, um Lizenzen auf der Network Security Appliance zu installieren.

# Voraussetzungen

- Admin oder Operator Zugriff

**Um Lizenzen zu installieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Installieren Sie jede Lizenz:

   ```
   hostname (config) # license install <key1> <key2> <key3>
   ```

   **HINWEIS:** Sie können die Lizenzschlüssel der Reihe nach, durch Leerzeichen getrennt eingeben, wie oben gezeigt, oder `license install` eingeben und dann Eingabe drücken, um aufgefordert zu werden, die Lizenzschlüssel nacheinander einzugeben.

3. Überprüfen Sie die Lizenzen:

   ```
   hostname (config) # show licenses
   License 1: LK2-FIREEYE_APPLIANCE-0000-0000-0000-0000-0000-0000-0000-
   0000-0000
   Feature:             FIREEYE_APPLIANCE
   Description:         FireEye Appliance
   Valid:               yes
   Start date:          2016/11/21 (ok)
   Tied to Appl ID:     000000000000 (ok)
   Product:             eMPS (ok)
   Type:                PROD (ok)
   Agreement:           EULA (ok)
   Active:              yes
   ...

   License 2: LK2-CONTENT_UPDATES-0000-0000-0000-0000-0000-0000-0000-0000-
   0000
   Feature:             CONTENT_UPDATES
   Description:         Content updates
   Valid:               yes
   Start date:          2016/11/21 (ok)
   End date:            2017/11/21 (ok)
   Tied to Appl ID:     000000000000 (ok)
   Sharing:             all (ok)
   Active:              yes

   License 3: LK2-FIREEYE_SUPPORT-0000-0000-0000-0000-0000-0000-0000-0000-
   0000
   Feature:             FIREEYE_SUPPORT
   Description:         FireEye Support
   Valid:               yes
   Start date:          2016/11/21 (ok)
   End date:            2017/11/21 (ok)
   Tied to Appl ID:     000000000000 (ok)
   Sharing:             all (ok)
   Active:              yes
   ...
   ```

4. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

# Lizenzen mit Hilfe der CLI entfernen

Verwenden Sie die CLI Befehle in diesem Thema, um Lizenzen zu entfernen.

# Voraussetzungen

- Admin oder Operator Zugriff

**Um Lizenzen zu entfernen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus:

```
hostname > enable
hostname # configure terminal
```

2. Führen Sie die installierten Lizenzen auf.

```
hostname (config) # show licenses
License 1: LK2-FIREEYE_APPLIANCE-0000-0000-0000-0000-0000-0000-0000
Feature:              FIREEYE_APPLIANCE
Description:          FireEye Appliance
Valid:                yes
Start date:           2016/11/01 (ok)
Tied to appl ID:      000000000000 (ok)
Product:              MPS (ok)
Type:                 PROD (ok)
Agreement:            EULA (ok)
Op Mode:              inline (ok)
Active:               yes
...

License 2: LK2-CONTENT_UPDATES-0000-0000-0000-0000-0000-0000-0000
Feature:              CONTENT_UPDATES
Description:          Content updates
Valid:                yes
Start date:           2016/11/01 (ok)
End date:             2017/11/01 (ok)
Tied to appl ID:      000000000000 (ok)
Sharing:              all (ok)
Active:               yes

License 3: LK2-FIREEYE_SUPPORT-0000-0000-0000-0000-0000-0000-0000
Feature:              FIREEYE_SUPPORT
Description:          FireEye Support
Valid:                yes
Start date:           2016/11/01 (ok)
End date:             2017/11/01 (ok)
Tied to appl ID:      000000000000 (ok)
Sharing:              all (ok)
Active:               yes
```

3. Bestimmen Sie die Lizenz-ID, um eine individuelle Lizenz zu entfernen. Beispielsweise ist die Lizenz-ID für die Support Lizenz, die im vorherigen Beispiel gezeigt wurde. 3

   ```
   hostname (config) # license delete 3
   ```

4. Speichern Sie Ihre Änderungen:

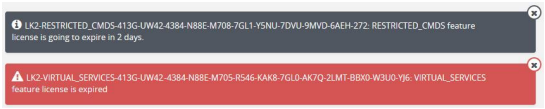
   ```
   hostname (config) # write memory
   ```

**HINWEIS:** Die `show licenses` Befehlsausgabe in diesem Vorgang zeigt die Basislizenzen, die auf einer Network Security Appliance installiert sind. Die Ausgabe ist für Network Security Appliances ähnlich.

# Lizenzbenachrichtigungen mit Hilfe der Web-UI anzeigen

Mit der Lizenz assoziierte Funktionalität endet mit Ablauf einer Lizenz. Wenn beispielsweise die FIREEYE_APPLIANCE Lizenz abläuft, blockiert die Appliance den Zugriff auf alle Seiten, mit Ausnahme der **Appliance License Settings** Seite und CLI Befehle (mit Ausnahme derer, die Lizenzen installieren) werden deaktiviert oder ihre Ausführung schlägt fehl. Zum Beispiel erstellt der `report generate` Befehl keinen Bericht.

Um eine Funktionslücke zu vermeiden, zeigt die **Appliance License Settings** Seite Benachrichtigungen über abgelaufene Lizenzen und Lizenzen an, die innerhalb der nächsten 30 Tage ablaufen. Zum Beispiel:




**HINWEIS:** Informationen über die Aktivierung der Appliance, um Lizenzen automatisch vom DTI Netzwerk herunterzuladen, wenn es Zeit für die Erneuerung ist, finden Sie unter Automatische Lizenzaktualisierungen auf Seite 147.

# KAPITEL 9: Das DTI Netzwerk

Dieses Thema behandelt die folgenden Informationen:



# Das DTI Netzwerk

Das FireEye Dynamic Threat Intelligence (DTI) Netzwerk (Cloud) bietet Teilnehmerplattformen mit den neuesten Informationen über fortgeschrittene Cyberangriffe und Malware Rückrufziele. Dies ermöglicht FireEye Produkten, proaktiv neue Bedrohungen zu erkennen und Angriffe abzuwehren. Die DTI-Cloud wird auch verwendet, um automatische Software-Aktualisierungen zu aktivieren. Letztendlich ist eine Verbindung mit der DTI-Cloud erforderlich, um die Lizenzaktualisierungsfunktion zu verwenden.

# Threat Intelligence

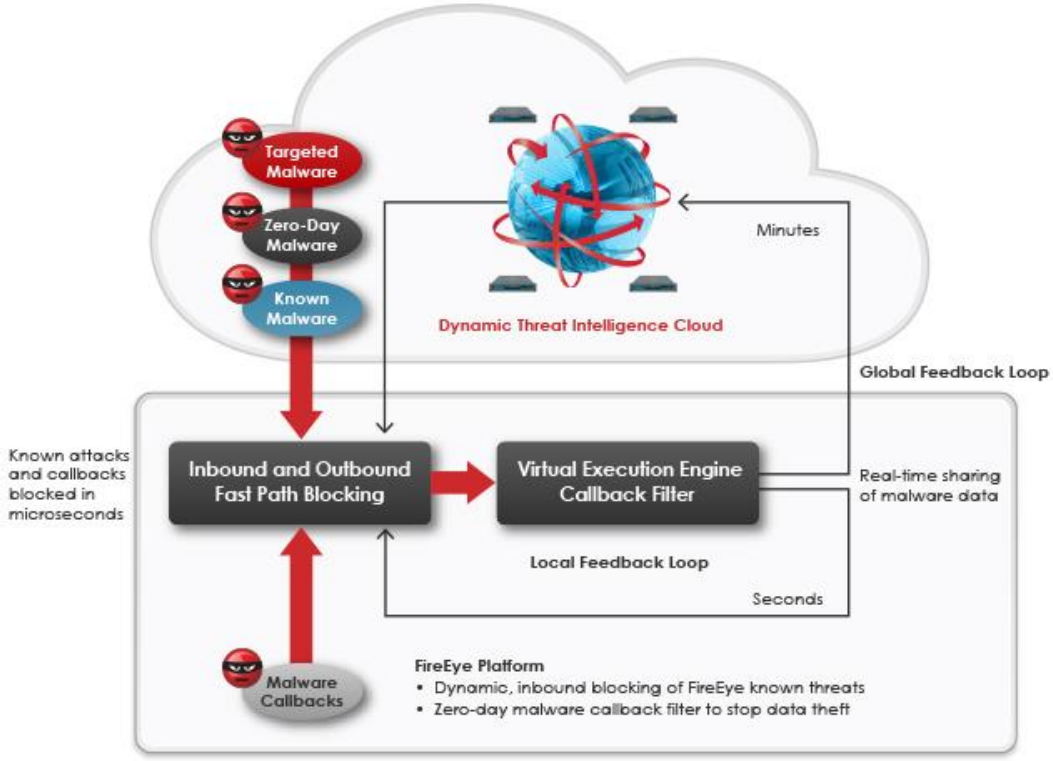
Die FireEye DTI Cloud verbindet FireEye Plattformen, die innerhalb von Kunden Netzwerken, Technologiepartner-Netzwerken und Serviceanbieter-Netzwerken weltweit bereitgestellt werden. Die FireEye Cloud dient als ein globales Verteilerzentrum, um automatisch generierte Threat Intelligence, wie z.B. neue Malware Profile, Schwachstellen Exploits und Verschleierungstaktiken, sowie neue Bedrohungserkenntnisse vom FireEye APT Discovery Center und bestätigte Drittparteien Sicherheits-Feeds effizient gemeinsam zu nutzen. Durch Ausnutzung der FireEye DTI Cloud ist die FireEye Threat Prevention Platform wirksamer bei der Entdeckung unbekannter Zero-Day, hochgradig gezielter Angriffe, die in Cyberkriminalität, Cyberspionage und Cyberaufklärung verwendet werden, sowie bekannter Malware.

**HINWEIS:** Sie benötigen ein Abonnement für den FireEye DTI Cloud Service, bevor Sie die in diesem Abschnitt beschriebenen Funktionen verwenden können.

Wenn die DTI Cloud Threat Intelligence von Kunden und Partnern weltweit empfängt, wird diese Information analysiert und an alle Kunden mit einem DTI Cloud Abonnement verbreitet. Diese Information enthält:

- Neue Malware Profile
- Schwachstellen Exploits
- Verschleierungstaktiken
- Neue Bedrohungserkenntnisse aus den FireEye Labs und bestätigte Drittparteien Sicherheits-Feeds

Jeder Kunde steuert, welche Informationen mit der DTI Cloud geteilt und davon erhalten wird.




## Automatische Lizenzaktualisierung

Die Lizenzaktualisierungsfunktion gestattet Appliances, die gewünschten Lizenzen von der DTI Cloud automatisch herunterzuladen und zu installieren. Diese Funktion bietet die folgenden Vorteile:

- Minimale Erstkonfiguration—Die Lizenzaktualisierungsfunktion wird durch den configuration jump-start Assistenten während der Erstkonfiguration aktiviert. Dies bedeutet, dass die Funktion voll funktionsfähig ist, nachdem der jump-start Assistent abgeschlossen ist.
- Vereinfachte Lizenzverwaltung—FireEye muss keine Lizenzschlüssel bereitstellen, wenn neue Funktionen hinzugefügt oder Lizenzen erneuert werden, weil die neuen Lizenzen automatisch heruntergeladen und installiert werden.
- Skalierbarkeit—Organisationen, wie z.B. solche mit einer großen Anzahl von Appliances, können davon profitieren, dass alle Appliances automatisch aktualisiert werden, anstatt Lizenzschlüssel manuell auf jeder Appliance einzeln einzugeben.

Weitere Informationen über automatische Lizenzaktivierung finden Sie unter Automatische Lizenzaktualisierungen auf Seite 147.

# System-Integritätsüberwachung und Software-Aktualisierungen

Die Network Security Appliance liefert regelmäßige System- und diagnostische Information an die DTI Cloud, wenn sie mit der DTI Cloud verbunden ist. Diese Information wird dann analysiert um sicherzustellen, dass die Appliance wie erwartet funktioniert.

Die System- und Diagnostikprüfungen schließen folgendes ein:

- System Image Version
- Guest Image Profile
- Systemprozesse
- Hardware Status
- Netzwerk Status

Wenn Probleme gefunden werden, wird der Kunde alarmiert. Wenn ein neues System Image oder Guest Image Profil verfügbar ist, können Administratoren wählen, ob sie es herunterladen und dann die Appliance aufrüsten wollen.

**HINWEIS:** Dieser System- und diagnostische Informationsaustausch beinhaltet keine kundenspezifischen geschützten Informationen.

# DTI-Netzwerk Kommunikation

Um mit dem DTI Netzwerk zu kommunizieren, benötigt die Network Security Appliance die folgenden Informationen:

- DTI-Serveradresse
- DTI Netzwerk Benutzername
- DTI Netzwerk Benutzerpasswort

Diese Informationen sind auf neuen physischen Appliances und auf virtuellen Appliances vorkonfiguriert. Für ältere Appliances wurden die Informationen in dem Karton mit Ihrer Appliance geliefert oder auf andere Weise von FireEye bereitgestellt. Die Kommunikation mit dem DTI-Netzwerk wird während der Erstkonfiguration der Appliance aktiviert, wenn Standardwerte angenommen werden, wie unter Überblick über Erstkonfiguration auf Seite 98 beschrieben.

Die Appliance sendet Anfragen an den DTI-Netzwerk für die Services, die in der folgenden Tabelle angezeigt sind.

| DTI-Service | Beschreibung |
|---|---|
| Downloadquelle | Die Quelle für Softwareupdates (System Images, Guest Images und Sicherheitsinhalte). |
| Uploadziel | Das Ziel für Appliance Telemetrie und Statistiken (anonymisierte Daten). |
| MIL | Das Ziel für die alware Intelligence Lab (MIL) Malware Erkennung und Callback-Intelligenz. |
| FAUDE | Das Ziel für Advanced URL Detection Engine (FAUDE) Malware Erkennung und Callback-Intelligenz |
| AV-Suite | Das Ziel zum Speichern von Urteilen sowohl für bösartige (Blackliste) als auch nicht-bösartige (Whiteliste) Objekte im Cloud-basierten Erkennungsservie der AV-Suite. |
| Registrierung | Die Central Management Appliance, die das MVX Cluster verwaltet, an den Sensoren und Hybrid Appliances Beiträge zur Überprüfung und Analyse senden. Dieser Service wird von Appliances benutzt, die an ein MVX Cluster übermitteln oder Teil eines MVX Clusters sind. |
| Helix | Das Ziel für die Integritätsstatistiken von Helix-fähigen Appliances. |

| DTI-Service | Beschreibung |
|---|---|
| Virtuell | Das Ziel für virtuelle Appliance Dienste, z. B. Erneuerungen von Lizenztoken und Informationen zur Systementropie. Dieser Service wird von virtuellen Appliances verwendet. |

# Info über Freigabekombinationen von Support- und Inhaltslizenzen

FireEye bietet Freigabeoptionen für Ihre Support und Content Updates Lizenzen. Die folgende Tabelle zeigt den Inhalt, der auf die DTI-Cloud hochgeladen wurde mit jeder Lizenzfreigabekombination.

Die Support Lizenz Freigabeoption stellt fest, ob Telemetrie und Statistiken hochgeladen wurden. Die Content Update Lizenz-Freigabeoption stellt fest, ob Sicherheitsinhalte und AV-Suite-und FAUDE-Anfragen hochgeladen wurden.

**HINWEIS:** Eine Beschreibung der hochgeladenen Inhaltstypen finden Sie unter DTI-Netzwerk Kommunikation auf der vorherigen Seite. Eine Beschreibung der Lizenzen finden Sie unter FireEye Lizenzschlüssel auf Seite 143.

| Support Lizenz | Content Lizenz | Hochgeladener Inhalt |
|---|---|---|
| Zweiweg | Zweiweg | Telemetrie und Statistiken, Sicherheitsinhalt, FAUDE und AV-Suite Anfragen |
| Zweiweg | Einweg | Telemetrie und Statistiken |
| Zweiweg | Einweg mit Override | Telemetrie und Statistiken, FAUDE und AV-Suite Anfragen |
| Einweg | Einweg | Nichts wird hochgeladen |
| Einweg | Einweg mit Override | FAUDE und AV-Suite Anfragen |
| Einweg | Zweiweg | Telemetrie und Statistiken, Sicherheitsinhalt, FAUDE und AV-Suite Anfragen |

**HINWEIS:** Standardmäßig ermöglichen lokale Intel-Feeds für FAUDE und Global Cache den Appliances, Erkennung zu verbessern, ohne ihre Einweg-Freigabelizenz für Content Updates zu übersteuern und ohne FAUDE oder den Global Cache direkt aufzurufen. Einzelheiten und Informationen über das Deaktivieren und erneutes Aktivieren der Feeds finden Sie in der *Bedienungsanleitung* der Appliance.

# Die aktive Einstellung für einen DTI-Service ändern

Appliances senden Anfragen für DTI-Services an die folgenden Server:

- Dynamic Threat Intelligence (**DTI**)—Der FireEye DTI Server. Die DTI-Serveradressen lauten wie folgt:
  - `staticcloud.fireeye.com` (Downloadquelle und virtueller Service)
  - `up-staticcloud.fireeye.com` (Uploadziel)
  - `mil-staticcloud.fireeye.com` (MIL Service)
  - `unity.fireeye.com` (FAUDE und AV-Suite Services)
  - Helix full URL (Helix Service)
- Content Delivery Network (**CDN**)—Ein Content Delivery Network Server. Die Serveradresse lautet `cloud.fireeye.com` oder `download.fireeye.com`.
- Die Central Management Appliance (**CMS**)—Nur auf verwalteten Appliances verfügbar. Die Adresse ist die Central Management Adresse.
- Ein benutzerdefinierte DTI-Server, falls konfiguriert—Ein benutzerdefinierter DTI-Server, der nur für verwaltete Appliances in einem Network Address Translation (NAT) Deployment verwendet wird, in der die Appliance den nicht-standardmäßigen Dual-Port Adresstyp für die Kommunikation mit der Central Management Appliance benutzt und eine zugängliche Adresse für die Central Management Appliance konfiguriert werden muss. Die Adresse ist die zugängliche Central Management Adresse. Details finden Sie im Eine zugängliche DTI-Serveradresse konfigurieren und aktivieren auf Seite 453.

Jede Appliance hat eine *aktive Einstellung* und *verfügbare Optionen* für jeden DTI-Service. Standardmäßig ist **CMS** die aktive Einstellungen für alle DTI-Services auf verwalteten Appliances. Dies ist die globale Standardeinstellung, dh. alle Appliance, die von der Central Management Appliance verwaltet werden, verwenden diese Einstellung. Sie können die globale Einstellung auf der Central Management Appliance ändern und die globale Einstellung für individuell verwaltete Appliances übersteuern.

Sie können auch die Einstellung für die aktive Downloadquelle für eigenständige Appliance und die Central Management Appliance ändern.

Gründe für die Änderung der aktiven Einstellung für einen DTI-Service enthalten:

- **Effektivere Erkennung und Behebung** . FireEye empfiehlt eine direkte Verbindung mit `unity.fireeye.com` , um Timeouts und Fehler bei den FAUDE und AV-Suite Diensten zu vermeiden.
- **Höhere Download-Geschwindigkeit**. Ein CDN Server befindet sich normalerweise geografisch näher an eigenständigen Appliances als der FireEye DTI Server. Der DTI oder CDN Server könnte näher an verwalteten Appliances als an der Central Management Appliance befinden.
- **Dezentralisierung** —Sie können das Verkehrsaufkommen, das durch die Central Management Appliance fließt, einschränken, wenn Anfragen für einen oder mehrere DTI-Services direkt an das DTI-Netzwerk gesendet werden.
- **Sicherheit**. Ihre Sicherheitsrichtlinien könnten erfordern, dass Sie die Softwareupdates direkt vom FireEye DTI Server herunterladen.
- **HTTP-Proxy**. Sie können ein HTTP-Proxy als Vermittler zwischen einer Appliance und dem DTI-Netzwerk verwenden. In diesem Szenario müssen verwaltete Appliances, die den single-Port Adresstypen benutzen, Verwaltete Appliances, die den dual-Port Adresstypen benutzen, können entweder **CMS** oder **DTI** verwenden. Details finden Sie unter Ein HTTP-Proxys für DTI-Serviceanfragen auf Seite 169.
- **Network Address Translation**. Wenn sich die Central Management Appliance hinter einem NAT-Gateway befindet, könnte eine zugängliche IP-Adresse, die für die verwalteten Appliances erreichbar ist, als eine benutzerdefinierte DTI-Quelle konfiguriert werden müssen. Details finden Sie unter

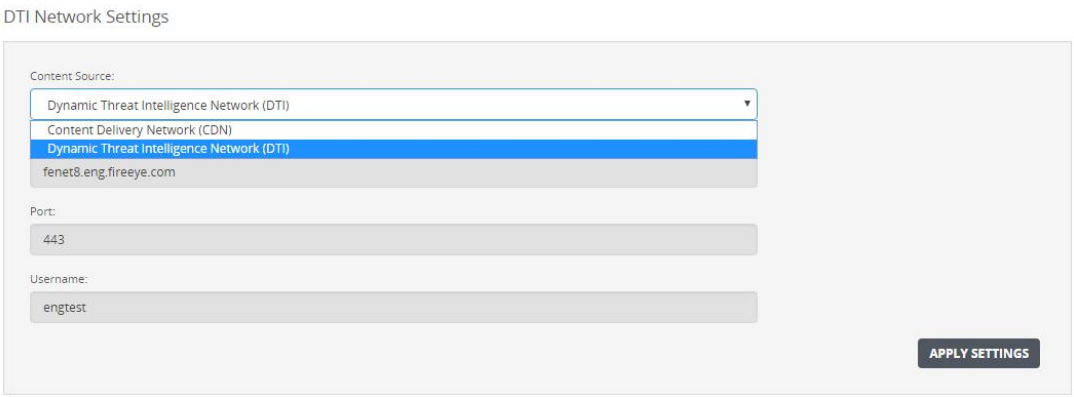
## Voraussetzungen

- Admin Zugriff
- Appliances befinden sich im "online" Modus und mit dem DTI-Netzw.

## Die aktive Quelle für eine eigenständige Appliance mit Hilfe der Web-UI ändern

Verwenden Sie die **DTI Network Settings** Seite, um die Einstellung für die aktive DTI-Quelle für eine eigenständige Appliance zu ändern.




**Um die aktive Quelleneinstellung zu ändern:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **DTI Network**.
3. Wählen Sie die DTI-Quelle, die die Appliance für Softwareupdates verwenden soll, aus der **Content Souce** Liste.
4. Klicken Sie auf **Apply Settings**.

# Die aktive Quelle für eine verwaltete Appliance mit Hilfe der Web-UI ändern

Verwenden Sie die **DTI Network Settings** Seite, um die Einstellung für die aktive DTI-Quelle auf einer verwalteten Appliance zu ändern.


**Um die aktive Quelleneinstellung zu ändern:**

1. Wählen Sie **Settings** > **DTI Network**.
2. Löschen Sie das **Obtain Settings from CM** Kontrollkästchen, wenn es markiert ist.

3. Wählen Sie die neue DTI-Quelle aus der **Content Souce** Liste.
4. Klicken Sie auf **Apply Settings**.

# Aktive Einstellungen für DTI-Services mit Hilfe der CLI ändern

Verwenden Sie die Befehle in diesem Abschnitt, um die aktive Quelleneinstellung auf einer eigenständigen Appliance oder die aktive Einstellung für beliebige DTI-Services auf einer verwalteten Appliance zu ändern.

## Die aktive Quelle auf eigenständigen Appliances ändern

**Um die aktive Quelleneinstellung zu ändern:**

1. Melden Sie sich auf der eigenständigen Appliance an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Zeigen Sie die derzeit aktiven und verfügbaren DTI-Quellen an:

   ```
   hostname (config) # show fenet dti configuration
   ```

4. Ändern Sie die aktive Downloadquelle:

   ```
   hostname (config) # fenet dti source default {CDN | DTI}
   ```

5. Bestätigen Sie Ihre Änderung:

   ```
   hostname (config) # show fenet dti configuration
   ```

6. Speichern Sie Ihre Änderung:

   ```
   hostname (config) # write memory
   ```

## Aktive Einstellungen für DTI-Services auf einer verwalteten Appliance ändern

Wenn die Central Management Appliance die aktive Einstellung für einen DTI Service steuert, müssen Sie die Kontroll auf die verwaltete Appliance verschieben, bevor Sie die Einstellung ändern. Ansonsten behält die Central Management Appliance die Kontrolle und verwendet die Einstellung, die sie für verwaltete Appliances verwendet.

**Um die aktive Einstellung zu ändern:**

1. Melden Sie sich auf der verwalteten Appliance an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Zeigen Sie die derzeit aktiven und verfügbaren DTI-Server an:
   `hostname (config) # show fenet dti configuration`
4. Wenn der `ACTIVE SETTINGS` Wert `Managed by CMS`enthält, verschieben Sie die Einstellung auf die verwaltete Appliance:
   - Um die Kontrolle über die Download `source`einstellung zu verschieben:
     `hostname (config) # no fenet dti source override enable`
   - Um die Kontrolle über die `upload destination` Einstellung zu verschieben:
     `hostname (config) # no fenet dti upload destination override enable`
   - Um die Kontrolle über die `mil`, `faude`, `avsuite`, `helix` oder `virtual` Service Einstellung zu verschieben:
     `hostname (config) # no fenet dti <service> service override enable`
5. Ändern Sie die Einstellung:
   - Um die Download `source` Einstellung zu ändern:
     `hostname (config) # fenet dti source default {CDN | DTI | CMS}`
   - Um die `upload destination` Einstellung zu ändern:
     `hostname (config) # fenet dti upload destination default {DTI | CMS}`
   - Um die `mil`, `faude`, `avsuite`, `helix` oder `virtual` Service Einstellung zu ändern:
     `hostname (config) # fenet dti <service> service default {DTI | CMS}`
6. Bestätigen Sie Ihre Änderungen:
   `hostname (config) # show fenet dti configuration`
7. Speichern Sie Ihre Änderungen:
   `hostname (config) # write memory`

**HINWEIS:** Verwenden Sie die folgenden Befehle, um die Kontrolle über die aktive Einstellung für einen DTI-Service zurück auf die Central Management Appliance zu verschieben:

- `fenet dti source override enable`
- `fenet dti upload destination override enable`
- `fenet dti <service> service override enable`

## Beispiele

In diesem Beispiel wird die aktive Downloadquelle auf einer eigenständigen Appliance von **DTI** auf **CDN** geändert.

`hostname (config) # show fenet dti configuration`

```
DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

     Mode               :  online
     Download source    :  DTI (DTIUser@staticcloud.fireeye.com)
     ...

  AVAILABLE OPTIONS:
  -------------------------------------------------------------
  Download    User                    Address
  -------------------------------------------------------------
  CDN         DTIUser                 cloud.fireeye.com
  DTI         DTIUser                 staticcloud.fireeye.com
  ...
  -------------------------------------------------------------

hostname (config) # fenet dti source default CDN
hostname (config) # show fenet dti configuration

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:
     Mode               :  online
     Download source    :  CDN (DTIUser@cloud.fireeye.com)
     ...
```

In diesem Beispiel wird die aktive Downloadquelle auf einer verwalteten Appliance von `CMS` auf `DTI` geändert.

```
hostname (config) # show fenet dti configuration

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

     Mode               :  online
     Download source    :  CMS (DTIUser@10.2.3.4) - Managed by CMS
     Upload destination :  CMS (DTIUser@10.2.3.4) - Managed by CMS
     ...

hostname (config) # no fenet dti source override enable
hostname (config) # fenet dti source default DTI
hostname (config) # show fenet dti configuration

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : DTI (DTIUser@staticcloud.fireeye.com) - Managed by
Appliance
    Upload destination : CMS (DTIUser@10.2.3.4) - Managed by CMS
    ...
```

# Ein HTTP-Proxys für DTI-Serviceanfragen

Ein HTTP Proxyserver kann als Vermittler zwischen einer Appliance und dem DTI-Netzwerk fungieren. In der folgenden Tabelle wird das Standardverhalten und das Verhalten beschrieben, nachdem ein HTTP-Proxy auf der Appliance konfiguriert und für DTI-Serviceanfragen aktiviert wurde.

| Appliance | Standardverhalten | HTTP-Proxyverhalten |
|---|---|---|
| Eigenständige Appliance | Die Appliance hat eine direkte Verbindung mit dem DTI-Netzwerk. | Die Appliance hat eine Verbindung mit dem DTI-Netzwerk über das HTTP-Proxy. |
| Central Management Appliance | Die Central Management Appliance hat eine direkte Verbindung mit dem DTI-Netzwerk. | Die Central Management Appliance hat eine Verbindung mit dem DTI-Netzwerk über das HTTP-Proxy. |
| Verwaltete Appliance | Die Appliance kommuniziert mit dem DTI-Netzwerk über die Central Management Appliance. | *Single-port* Kommunikation mit der Central Management Appliance (der Standard, in dem sowohl Management als auch DTI-Netzwerk Verkehr SSH Port 22 verwenden)—Die Appliance hat eine Verbindung mit dem DTI-Netzwerk über das HTTP-Proxy.<br>*Dual-Port* Kommunikation mit der Central Management Appliance (der Management Verkehr verwendet SSH Port 22 und DTI-Netzwerk Verkehr verwendet HTTP Port 443)—Die Appliance verbindet entweder direkt mit dem DTI-Netzwerk über das HTTP-Proxy oder über die verwaltende Central Management Appliance mit dem HTTP-Proxy. |

xxx

**WICHTIG:** Wenn ein HTTP-Proxyserver auf einer verwalteten Appliances mit single-Port Kommunikation mit der Central Management Appliance konfiguriert und aktiviert ist, schaltet die verwaltete Appliance automatisch auf den Proxyserver für alle DTI-Services um, wenn die Central Management Appliance nicht mehr verfügbar ist.

Dieser Abschnitt enthält die folgenden Informationen:



# HTTP-Proxyeinstellungen für DTI-Netzwerkservices aktivieren

DTI Netzwerkservices enthalten: `download`, `upload destination`, `mil`, `faude`, `enrollment`, `avsuite`, `helix` und `virtual`. Sie können festlegen, dass eine Appliance Anfragen für einen oder mehrere dieser Services über einen HTTP-Proxyserver sendet. Die Appliance kann entweder durch eine Central Management Appliance verwaltet werden oder eine eigenständige Appliance sein.

**HINWEIS:** Der `helix` DTI-Netzwerkservice wird derzeit nicht genutzt. Informationen darüber, wir Appliances über einen HTTP-Proxyserver mit Helix kommunizieren können, finden Sie im *Helix Integrationshandbuch*.

**HINWEIS:** Der `enrollment` Service bezieht sich nur aus Appliances, die im Sensor oder Hybrid MVX-Modus ausgeführt werden. Der `virtual` Service bezieht sich nur auf virtuelle Appliances.

## Wie es für verwaltete Appliances funktioniert

Standardmäßig sendet eine verwaltete Appliance Anfragen für alle DTI-Netzwerkservices über die Central Management Appliance. Sie können die Appliances stattdessen konfigurieren, die Central Management Appliance zu umgehen und Anfragen für einen oder mehrere DTI-Netzwerkservices durch einen HTTP Proxyserver zu senden.

Die verwaltete Appliance könnte zum Beispiel die Central Management Appliance als die DTI-Quelle für Software-Downloads verwenden, aber für eine effektivere Erkennung und Behebung verwenden Sie den Proxyserver für erkennungsbezogene DTI-Services, wie `faude` und `avsuite`.

Diese Funktion bietet die folgenden Vorteile:

- **Zuverlässigkeit**—Wenn die verwaltete Appliance single-Port Kommunikation verwendet (die Standardmethode) fallen Anfragen für alle DTI-Netzwerkservice

zurück auf den HTTP-Proxyserver, wenn die Central Management Appliance nicht mehr verfügbar ist. Angenommen, die Central Management Appliance ist bei Wartungsarbeiten nicht mehr verfügbar. Die verwaltete Appliance verwendet automatisch den Proxyserver, um das DTI-Netzwerk zu erreichen, bis eine Verbindung mit der Central Management Appliance wiederhergestellt ist. Details finden Sie unter HTTP-Proxyeinstellungen für automatisches Failover mit Hilfe der CLI aktivieren auf der nächsten Seite.

- **Dezentralisierung**—Sie können die Menge des Verkehrs, der durch die Central Management Appliance fließt einschränken, wenn Anfragen für DTI-Services dür einen HTTP-Proxyserver anstelle der Central Management Appliance laufen.
- **Reduzierte Netzwerklatenz**—Sie können Anfragen über einen HTTP-Proxyserver senden, wenn sich die verwaltete Appliance näher am DTI-Netzwerk als der Central Management Appliance befindet.

HTTP-Proxyeinstellungen für einen DTI-Service auf einer verwalteten Appliance werden aktiviert, wenn alle der folgenden Bedingungen erfüllt sind:

- Die Hostadresse des HTTP-Proxyserver ist konfiguriert.
- Der HTTP-Proxyserver ist aktiviert.
- HTTP-Proxyeinstellungen für den DTI-Service sind **nicht** manuell (auch als *administrativ*) deaktiviert.
- Die aktive Einstellung für den DTI-Service ist **nicht** `CMS (<DTIuser>@<address> : singleport) - Managed by CMS`. Diese Einstellung auf der verwalteten Appliance gibt an, das die verwaltende Central Management Appliance die aktive Einstellung steueert und die Appliance single-Port Kommunikation verwendet.

  **HINWEIS:** HTTP-Proxyeinstellungen können aktiviert werden, wenn die aktive Einstellung `CMS (<DTIuser>@<address>) - Managed by CMS` ist. Dies deutet an, dass die verwaltende Central Management Appliance die aktive Einstellung steuert, aber die Appliance dual-Port Kommunikation verwendet.

## Wie es für eigenständige Appliances funktioniert

Standardmäßig senden eigenständige Appliances Anfragen für DTI-Netzwerkservices direkt an das DTI-Netzwerk. Sie können die Appliance stattdessen konfigurieren, Anfragen für einen oder mehrere DTI-Services durch einen HTTP-Proxyserver zu senden.

HTTP-Proxyeinstellungen für einen DTI-Service auf einer eigenständigen Appliance werden aktiviert, wenn alle der folgenden Bedingungen erfüllt sind:

- Die Hostadresse des HTTP-Proxyserver ist konfiguriert.
- Der HTTP-Proxyserver ist aktiviert.

- HTTP-Proxyeinstellungen für den DTI-Service sind **nicht** manuell (auch als *administrativ*) deaktiviert.

### *Voraussetzungen*

- Operator oder Admin Zugriff
- Der HTTP-Proxyserver wird in Ihrem Netzwerk bereitgestellt und auf der Appliance konfiguriert und aktiviert (siehe Einstellung für HTTP-Proxyserver mit Hilfe der CLI konfigurieren auf Seite 264).

## HTTP-Proxyeinstellungen für automatisches Failover mit Hilfe der CLI aktivieren

Sie können eine verwaltete Appliance mit single-Port Kommunikation konfigurieren, die Central Management Appliance DTI-Services zu verwenden, aber auf den HTTP-Proxyserver umschaltet, wenn die Central Management Appliances nicht mehr verfügbar ist. Dies ist das Standardverhalten, wenn ein HTTP-Proxyserver auf der Appliance konfiguriert und aktiviert ist.

**Um automatisches Failover für DTI-Services zu aktivieren:**

1. Melden Sie sich auf der verwalteten Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Konfigurieren und aktivieren Sie den Proxyserver wie unter Einstellung für HTTP-Proxyserver mit Hilfe der CLI konfigurieren auf Seite 264 beschrieben.
4. Bestätigen Sie, dass die Central Management Appliance die aktiven Einstellungen für die DTI-Services steuert, dass der HTTP-Proxyserver aktiviert ist und HTTP-Proxyeinstellungen für DTI-Services deaktiviert sind:

   ```
   hostname (config) # show fenet dti configuration brief
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

### *Beispiel:*

Im folgenden Beispiel werden die Mindesteinstellungen für einen HTTP-Proxyserver konfiguriert und dann aktiviert. Es zeigt dann an, dass die Central Management Appliance derzeit die aktiven Einstellungen für DTI-Services steuert, dass der Proxyserver konfiguriert und auf der Appliance aktiviert ist und dass Proxyeinstellungen derzeit für DTI-Services deaktiviert sind.

Wenn die Central Management Appliance nicht länger verfügbar ist, werden die Werte im `ACTIVE SETTINGS` Abschnitt auf `DTI` verändert und die Werte im `ACTIVE SETTINGS FOR HTTP PROXY` Abschnitt auf `yes`.

```
hostname (config) # fenet proxy host 192.168.2.3
hostname (config) # fenet proxy enable
hostname (config) # show fenet dti configuration brief


DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Upload destination : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Mil service        : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Faude service      : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @192.168.2.3:8080 (User agent:)

    Download source    : no (reason: singleport is in use)
    Upload destination : no (reason: singleport is in use)
    Mil service        : no (reason: singleport is in use)
    Faude service      : no (reason: singleport is in use)
    ...
```

## HTTP-Proxyeinstellungen auf einer single-Port verwalteten Appliance mit Hilfe der CLI aktivieren

Verwenden Sie die Befehle in diesem Thema, um eine verwaltete Appliance zu aktivieren, die single-Port Kommunikation verwendet, um DTI-Serviceanfragen über einen HTTP-Proxyserver zu senden.

**Um HTTP-Proxyeinstellungen für einen DTI-Service zu aktivieren:**

1. Melden Sie sich auf der verwalteten Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Zeigen Sie die aktuelle DTI-Servicekonfiguration an:

   ```
   hostname (config) # show fenet dti configuration brief
   ```

4. Übertragen Sie die Kontrolle über den DTI-Service auf die verwaltete Appliance.
   - Für den `download` Service:

     ```
     hostname (config) # no fenet dti source override enable
     ```
   - Für den `enrollment`, `faude`, `mil` oder `virtual` Service:

     ```
     hostname (config) # no fenet dti <service> service override enable
     ```
   - Für den `upload destination` Service:

     ```
     hostname (config) # no fenet dti upload destination override
     enable
     ```
5. Zeigen Sie die aktuelle DTI-Servicekonfiguration an:

   ```
   hostname (config) # show fenet dti configuration brief
   ```
6. Wenn der Wert für den Service im `ACTIVE SETTINGS FOR HTTP PROXY` Abschnitt `noist`, aktivieren Sie Proxyeinstellungen für den Service.
   - Für den `source` Service:

     ```
     hostname (config) # fenet dti source proxy enable
     ```
   - Für den `enrollment`, `faude` oder `virtual` Service:

     ```
     hostname (config) # fenet dti <service> service proxy enable
     ```
   - Für den `upload destination` Service:

     ```
     hostname (config) # fenet dti upload destination proxy enable
     ```
7. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show fenet dti configuration brief
   ```
8. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## *Beispiele*

Im folgenden Beispiel wird die Kontrolle über den `faude` Service auf die verwaltete Appliance übertragen, wodurch HTTP-Proxyeinstellungen für den Service aktiviert werden.

```
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:
  ACTIVE SETTINGS:

    Mode               : online
    Download source    : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Upload destination : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Mil service        : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Faude service      : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)
```

```
    Download source    : no (reason: singleport is in use)
    Upload destination : no (reason: singleport is in use)
    Mil service        : no (reason: singleport is in use)
    Faude service      : no (reason: singleport is in use)
    ....

hostname (config) # no fenet dti faude service override enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Upload destination : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Mil service        : CMS (User8@10.4.5.6 : singleport) - Managed by CMS
    Faude service      : DTI (User8@unity.fireeye.com) - Managed by Appliance
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)

    Download source    : no (singleport is in use)
    Upload destination : no (singleport is in use)
    Mil service        : no (singleport is in use)
    Faude service      : yes
    ...
```

Im folgenden Beispiel werden HTTP-Proxyeinstellungen für den `source` Service erneut aktiviert.

```
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : DTI (User8@staticcloud.fireeye.com) - Managed by
Appliance
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)
    Download source    : no (reason: administratively disabled)
    ...

hostname (config) # fenet dti source proxy enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : DTI (User8@staticcloud.fireeye.com) - Managed
by Appliance
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:
```

```
Http proxy          : @myproxy.mycompany.com:8080 (user agent:)
Download source     : yes
...
```

## HTTP-Proxyeinstellungen auf einer dual-Port verwalteten Appliance mit Hilfe der CLI aktivieren

Verwenden Sie die Befehle in diesem Thema, um eine verwaltete Appliance zu aktivieren, die dual-Port Kommunikation verwendet, um DTI-Serviceanfragen über einen HTTP-Proxyserver zu senden.

**HINWEIS:** WEnn die Appliance dual-Port Kommunikation verwendet, können Anfragen entweder direkt an das HTTP-Proxy oder über die Central Management Appliance an das HTTP-Proxy (das Standardverhalten) gesendet werden.

**Um HTTP-Proxyeinstellungen für einen DTI-Service zu aktivieren:**

1. Melden Sie sich auf der verwalteten Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Zeigen Sie die aktuelle DTI-Servicekonfiguration an:

   ```
   hostname (config) # show fenet dti configuration brief
   ```

4. *Um DTI-Serviceanfragen direkt an das HTTP-Proxy zu senden (optional)*: Verschieben Sie die Kontrolle über den DTI-Service auf die verwaltete Appliance.

   - Für den `download` Service:

     ```
     hostname (config) # no fenet dti source override enable
     ```

   - Für den `enrollment`, `faude`, `mil` oder `virtual` Service:

     ```
     hostname (config) # no fenet dti <service> service override enable
     ```

   - Für den `upload destination` Service:

     ```
     hostname (config) # no fenet dti upload destination override
     enable
     ```

5. Zeigen Sie die aktuelle DTI-Servicekonfiguration an:

   ```
   hostname (config) # show fenet dti configuration brief
   ```

6. Wenn der Wert für den Service im `ACTIVE SETTINGS FOR HTTP PROXY` Abschnitt `noist`, aktivieren Sie Proxyeinstellungen für den Service.
   - Für den `source` Service:

     ```
     hostname (config) # fenet dti source proxy enable
     ```
   - Für den `enrollment`, `faude` oder `virtual` Service:

     ```
     hostname (config) # fenet dti <service> service proxy enable
     ```
   - Für den `upload destination` Service:

     ```
     hostname (config) # fenet dti upload destination proxy enable
     ```
7. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show fenet dti configuration brief
   ```
8. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## *Beispiele*

Im folgenden Beispiel wird die Kontroll des `source` Service auf die verwaltete Appliance verschoben. Auf diese Weise kann die verwaltete Appliance die Central Management Appliance umgehen und Anfrage für Softwareupdates direkt an den HTTP-Proxyserver senden.

```
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : CMS (User8@10.4.5.6) - Managed by CMS
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)
    Download source    : yes
    ...

hostname (config) # no fenet dti source override enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : DTI (User8@staticcloud.fireeye.com) - Managed
by Appliance
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)
```

```
    Download source    : yes
    ...
```

Im folgenden Beispiel werden HTTP-Proxyeinstellungen für den `faude` Service erneut aktiviert. In diesem Beispiel steuert die Central Management Appliance die DTI-Services, so dass DTI-Anfragen an das HTTP-Proxy über die Central Management Appliance gesendet werden.

```
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : CMS (User8@10.4.5.6) - Managed by CMS
    Upload destination : CMS (User8@10.4.5.6) - Managed by CMS
    Mil service        : CMS (User8@10.4.5.6) - Managed by CMS
    Faude service      : CMS (User8@10.4.5.6) - Managed by CMS
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)

    Download source    : yes
    Upload destination : yes
    Mil service        : yes
    Faude service      : no (reason: administratively disabled)
    ...

hostname (config) # fenet dti faude service proxy enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : CMS (User8@10.4.5.6) - Managed by CMS
    Upload destination : CMS (User8@10.4.5.6) - Managed by CMS
    Mil service        : CMS (User8@10.4.5.6) - Managed by CMS
    Faude service      : CMS (User8@10.4.5.6) - Managed by CMS
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)

    Download source    : yes
    Upload destination : yes
    Mil service        : yes
    Faude service      : yes
    ...
```

## HTTP-Proxyeinstellungen auf einer eigenständigen Appliance mit Hilfe der CLI aktivieren

Verwenden Sie die Befehle in diesem Thema, um auf einer eigenständigen Appliance das Senden von DTI-Serviceanfragen an das DTI-Netzwerk über einen HTTP-Proxyserver zu aktivieren.

**Um HTTP-Proxyeinstellungen für einen DTI-Service zu aktivieren:**

1. Melden Sie sich auf der eigenständigen Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Zeigen Sie die aktuelle DTI-Servicekonfiguration an:

   ```
   hostname (config) # show fenet dti configuration brief
   ```

4. Wenn der Wert für den Service im `ACTIVE SETTINGS FOR HTTP PROXY` Abschnitt `noist`, aktivieren Sie Proxyeinstellungen für den Service.
   - Für den `source` Service:

     ```
     hostname (config) # fenet dti source proxy enable
     ```

   - Für den `enrollment`, `faude` oder `virtual` Service:

     ```
     hostname (config) # fenet dti <service> service proxy enable
     ```

   - Für den `upload destination` Service:

     ```
     hostname (config) # fenet dti upload destination proxy enable
     ```

5. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show fenet dti configuration brief
   ```

6. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

### *Beispiel:*

Im folgenden Beispiel werden HTTP-Proxyeinstellungen für die `faude` und `avsuite` DTI-Services aktiviert.

```
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : DTI (User8@staticcloud.fireeye.com)
    Upload destination : DTI (User8@up-staticcloud.fireeye.com)
    Mil service        : DTI (User8mil-staticcloud.fireeye.com)
    Faude service      : DTI (User8@unity.fireeye.com)
    AVSuite service    : DTI (User8@unity.fireeye.com)
    ...
```

```
  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)

    Download source    : no (reason: administratively disabled)
    Upload destination : no (reason: administratively disabled)
    Mil service        : no (reason: administratively disabled)
    Faude service      : no (reason: administratively disabled)
    AVSuite service    : no (reason: administratively disabled)
    ....

hostname (config) # fenet dti faude service proxy enable
hostname (config) # fenet dti avsuite service proxy enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

    Mode               : online
    Download source    : DTI (User8@staticcloud.fireeye.com)
    Upload destination : DTI (User8@up-staticcloud.fireeye.com)
    Mil service        : DTI (User8@mil-staticcloud.fireeye.com)
    Faude service      : DTI (User8@unity.fireeye.com)
    AVSuite service    : DTI (User8@unity.fireeye.com)
    ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : @myproxy.mycompany.com:8080 (user agent:)

    Download source    : no (reason: administratively disabled)
    Upload destination : no (reason: administratively disabled)
    Mil service        : no (reason: administratively disabled)
    Faude service      : yes
    AVSuite service    : yes
    ...
```

# HTTP-Proxyeinstellungen für DTI-Services deaktivieren

Verwenden Sie die Befehle in diesem Abschnitt, um HTTP-Proxyeinstellungen für einen bestimmten DTI-Service zu deaktivieren.

**Um die HTTP-Proxyeinstellungen für einen DTI-Service zu deaktivieren:**

- Für den Quellservice:

  ```
  hostname (config) # no fenet dti source proxy enable
  ```

- Für den `upload destination` Service:

  ```
  hostname (config) # no fenet dti upload destination proxy enable
  ```

- Für den `mil`, `faude`, `enrollment`, `avsuite` oder `virtual` Service:

  ```
  hostname (config) # no fenet dti <service> service proxy enable
  ```

**HINWEIS:** Wenn die verwaltete Appliance single-Port Kommunikation mit der Central Management Appliance verwendet, können Sie die Steuerung des DTI-Service alternativ auf die Central Management Appliance zurück verschieben. Dadurch wird das HTTP-Proxy für diesen Service automatisch deaktiviert. Verwenden Sie einender folgenden Befehle:

- `fenet dti source override enable`
- `fenet dti upload destination override enable`
- `fenet dti <service> service override enable`

## Beispiele

Im folgenden Beispiel werden die HTTP-Proxyeinstellungen für den `source` Service auf einer verwalteten Appliance, die single-Port Kommunikation verwendet, deaktiviert.

```
hostname (config) # no fenet dti source proxy enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:
    ...
    Download source    : DTI (User8@staticcloud.fireeye.com) - Managed by
Appliance

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : bsmith@192.168.2.3:8080 (user agent:)

    Download source    : no (reason: administratively disabled)
    ...
```

Im folgenden Beispiel wird die Steuerung des `source` Service auf einer verwalteten Aplliance mit single-Port Kommunikation auf die Central Management Appliance verschoben. Durch diese Aktion werden die HTTP-Proxyeinstellungen für den Service deaktiviert.

```
hostname (config) # fenet dti source override enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:

ACTIVE SETTINGS:
    ...
    Download source    : CMS (User8@10.4.5.6 : singleport) - Managed by CMS

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : bsmith@192.168.2.3:8080 (user agent:)

    Download source    : no (reason: singleport is in use)
    ...
```

Im folgenden Beispiel werden die HTTP-Proxyeinstellungen für den `source` Service auf einer verwalteten Appliance mit dual-Port Kommunikation deaktiviert.

```
hostname (config) # no fenet dti source proxy enable
hostname (config) # show fenet dti configuration brief
...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy         : bsmith@192.168.2.3:8080 (user agent:)

    Download source    : no (reason: admnistratively disabled)
    ...
```

Im folgenden Beispiel werden HTTP-Proxyeinstellungen für die `faude` und `avsuite` Services auf einer eigenständigen Appliance deaktiviert.

```
hostname (config) # no fenet dti faude service proxy enable
hostname (config) # no fenet avsuite service proxy enable
hostname (config) # show fenet dti configuration brief

DTI CLIENT CONFIGURATIONS:
  ...

  ACTIVE SETTINGS FOR HTTP PROXY:

    Http proxy          : bsmith@192.168.2.3:8080 (user agent:)

    ...
    Faude service       : no (reason: administratively disabled)
    AVSuite service     : no (reason: administratively disabled)
    ...
```

# DTI Zugriff validieren

Bevor Sie die Funktionen verwenden, die mit dem DTI-Netzwerk assoziiert sind, müssen Sie die Kommunikation zwischen der Appliance und dem DTI-Netzwerk herstellen. Verwenden Sie die folgenden Verfahren, um diese Kommunikation zu überprüfen.

## Voraussetzungen

- Operator oder Admin Zugriff
- Zugriff auf das DTI-Netzwerk

## DTI-Zugriff mit Hilfe der Web-UI überprüfen

Verwenden Sie die **FireEye System Information** Seite, um DTI-Cloud Kommunikation zu überprüfen.

**Um DTI-Zugriff zu überprüfen:**

1. Klicken Sie auf den **About** Tab.
2. Klicken Sie auf **Health Check** oben links auf der Seite.
3. Finden Sie den **Dynamic Threat Intelligence Cloud** Abschnitt.


4. Bestätigen Sie, dass das **DTI Client** Feld **Enabled** (aktiviert) ist.

# DTI-Zugriff mit Hilfe der CLI überprüfen

Verwenden Sie die Befehle in diesem Thema, um DTI-Kommunikation zu überprüfen.

**Um DTI-Zugriff zu überprüfen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Überprüfen Sie den Status des DTI-Service. (Dieses Beispiel stammt von einer verwalteten Appliance.)

```
hostname (config) # show fenet status

Dynamic Threat Intelligence Service:

    Update source  : <online>
    Enabled        : yes
    Download       : DTIUser@10.11.121.13 : singleport
    Upload         : DTIUser@10.11.121.13 : singleport
    Mil            : DTIUser@10.11.121.13 : singleport

HTTP Proxy:

    Address        :
    Username       :
    User-agent     :

Request Session:

    Timeout        : 30
    Retries        : 0
    Speed Time     : 60
    Max Time       : 14400
    Rate Limit     :

    Speed Limit     : 1

Dynamic Threat Intelligence Lockdown:

    Enabled        : no
    Locked         : no
    Lock After     : 5 failed attempts

  UPDATES
                      Enabled   Notify  Scheduled       Last Updated At
                      -------   ------  --------------  ---------------
  Security contents:  yes       no      every           2016/07/20
05:43:00
  Stats contents   :  yes               none            2016/07/20
18:55:00
```

3. Bestätigen Sie die folgenden Informationen:
   - Update-Quelle ist online.
   - DTI-Service ist aktiviert,
   - DTI-Service Benutzername ist der Name, der mit der DTI-Abonnementlizenz bereitgestellt wird.
   - DTI-Serviceadresse ist `cloud.fireeye.com`.

# DTI Berechtigungen konfigurieren

Virtuelle Appliances haben Appliance-spezifische DTI Berechtigungen, die durch den Aktivierungscode der Appliance generiert werden und nicht geändert werden können. Physische Appliances haben werksseitig konfigurierte DTI Berechtigungen, die nicht geändert werden sollten.

Sie sollten die DTI Berechtigungen niemals ändern, es sei denn, wenn Sie eine benutzerdefinierte DTI Quelle in einem Network Address Translation (NAT) Deployment konfigurieren müssen, in denen beide der folgenden Bedingungen wahr sind:

- Die Central Management Appliance befindet sich hinter einem NAT Gateway.
- Die verwaltete Appliance verwendet den nicht-standardmäßigen Dual-Port Adresstyp für die Kommunikation mit der Central Management Appliance.

## Voraussetzungen

- Admin Zugriff

## DTI Berechtigungen mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Thema, um DTI Berechtigungen zu konfigurieren (Benutzername und Passwort).

**Um DTI Berechtigungen zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Bestimmen Sie den Benutzer und das Passwort:

   ```
   hostname (config) # fenet dti source type <name> username <user>
   password <password>
   ```

   Die Variablen haben folgende Werte:

   - <name>—Der Name der benutzerdefinierten DTI-Quelle.
   - <user> und <password>—Die neuen Berechtigungen.

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show fenet dti configuration
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Automatische Überprüfung der Sicherheitsinhalte

Um die Installation von nicht-kompatiblen Sicherheitsinhalten zu verhindern, werden Sicherheitsinhaltspakete automatisch validiert, wenn sie von der FireEye Dynamic Threat Intelligenc(DTI) Cloud oder dem FireEye DTI Offline Update Portal heruntergeladen werden. Diese Funktion wird auf den folgenden Appliances unterstützt:

- Central Management Version 8.1.0 und später.
- Network Security Version 8.0.0 und später.
- Email Security — Server Edition Version 8.1.4 und später.

## Automatische Überprüfung der Sicherheitsinhalte

Wenn ein Paket mit Sicherheitsinhalten heruntergeladen wird, fragt die Appliance das Paket ab, um seine Attribute zu erhalten. Einige der Attribute werden mit Attributen des installierten Sicherheitsinhalts und Werten verglichen, die auf der Ziel Appliance konfiguriert wurden. Die Kriterien, die bestimmen, ob ein heruntergeladenes Paket kompatibel ist, sind in Bedingungen, die auf ein kompatibles Sicherheitsinhaltspaket deuten auf der nächsten Seite aufgeführt.

Wenn die Pakete alle zutreffenden Kompatibilitätsprüfungen besteht, wird der neue Sicherheitsinhalt auf der Ziel Appliance installiert.

Wenn das Paket eine Kompatibilitätsprüfung nicht besteht, tut die Appliance Folgendes:

- Sendet einen Fehlercode in Protokollnachrichten.
- Zeigt eine Fehlernachricht auf der CLI oder der Web-UI an.
- Führt keine weitere Überprüfung des heruntergeladenen Pakets durch.
- Verwirft das heruntergeladene Paket ohne es zu installieren.
- Erfordert, dass das nächste Update des Sicherheitsinhalts ein vollständiges Update-Paket und kein Delta Update-Paket verwendet.

# Bedingungen, die auf ein kompatibles Sicherheitsinhaltspaket deuten

Heruntergeladene Sicherheitsinhaltpakete werden automatisch anhand der folgenden Bedingungen in der aufgeführten Reihenfolge ausgewertet.

1. *Wenn die Appliance mit dem Internet verbunden ist:* Wurde das Paket von dem richtigen Update-Kanal des DTI Download-Servers heruntergeladen?
2. *Wenn die Appliance nicht mit dem Internet verbunden ist:*Wurde das Paket von dem richtigen Inhalts-Kanal des DTI Offline Portal heruntergeladen?
3. Ist die Versionsnummer des  Pakets mit der Ausgabe der Ziel Appliance kompatibel?
4. Entspricht die Akzeptanzebene des Pakets der auf der Ziel Appliance konfigurierten Ebene?
5. *Wenn das heruntergeladene Paket ein Delta-Paket ist:*Ist die Version des Delta Inhaltspakets mit der Version des Sicherheitsinhalts kompatibel, die auf der Ziel Appliance installiert ist?
6. Ist die Version des heruntergeladenen Pakets die gleiche oder eine neuere Version des installierten Inhalts?

# Fehlercodes für nicht-kompatible Sicherheitsinhaltspakete

Die Appliance schreibt eine Protokollnachricht, wenn ein heruntergeladenes Sicherheitsinhaltspaket als nicht kompatibel mit den Einstellungen der Ziel Appliance oder den auf der Appliance installierten Sicherheitsinhalten befunden wird. Die folgenden Abschnitte beschreiben die Fehlercodes für diese Ereignisse:

## 81 — Incompatible DTI download server update channel

Das Paket wurde für einen anderen Update-Kanal als **stable** gebaut (z.B. **bet**), aber die Appliance ist nicht konfiguriert, den gleichen Update-Kanal zu benutzen.

## 82 — Incompatible DTI Offline Portal content channel

Das Paket wurde für einen anderen Inhaltskanal gebaut und davon heruntergeladen als den, der auf der Ziel Appliance konfiguriert wurde. Beispiele für DTI Offline Portal Inhaltskanäle sind **SCNET-5.0**, **SCNET-4.0**, **SCNET-3.0**, **SCNET-2.0** und **SCEP-1.0**.

### 83 — Package version is incompatible with the appliance release

Die auf der Appliance konfigurierte Paketannahme muss mit der Softwareversion der Appliance kompatibel sein. Standardmäßig ist die auf der Appliance konfigurierte Paketannahmestufe **stable**. Andere Paketannahmestufen sind **beta** und **long_beta**.

### 84 — Package acceptance level does not match the target appliance configuration

Die Paketannahmestufe (z.B.**beta** oder **long_beta**) stimmt nicht mit der Annahmestufe überein, die auf der Appliance konfiguriert ist.

### 85 — Delta content package version is incompatible with the installed security content

Das Paket ist ein Delta (inkrementelles) Inhaltspaket und seine Versionsnummer ist mit der auf der Ziel Appliance installierten Sicherheitsinhaltsversion nicht kompatibel.

### 86 — Package version is newer than the installed security content version

Die Paketversion ist neuer als die installierte Sicherheitsinhaltsversion und dies ist kein Inhaltsrollbackvorgang.

# Sicherheitsinhalt aktualisieren

**HINWEIS:** Sie können Sicherheitsinhalt auch manuell mit dem DTI Update Portal aktualisieren. Weitere Informationen finden Sie in der *DTI Offline Update Portal Bedienungsanleitung*.

Wenn Sie DTI Zugriff validieren, überprüft das System nach neuem Sicherheitsinhalt. Wenn neuer Inhalt verfügbar ist, können Sie die neuesten Malware Bedrohungsinformationen von der DTI Cloud auf die Network Security Appliance herunterladen.

Weitere Informationen über die Überprüfung von DTI-Zugriff finden Sie unter DTI Zugriff validieren auf Seite 182.

## Voraussetzungen

- Operator oder Admin Zugriff

# Sicherheitsinhalte mit Hilfe der Web-UI aktualisieren

Verwenden Sie die **Appliance Update** Seite, um Sicherheitsinhalt zu aktualisieren.

# Voraussetzungen

- Admin Zugriff

**Um Sicherheitsinhalte zu aktualisieren:**

1. Klicken Sie auf der **About** Seite auf **Upgrade**.
2. Wählen Sie **DTI**.
3. Klicken Sie auf das **Action** Symbol für Security Content und wählen Sie **Check**.

   Die Appliance prüft nach Aktualisierungen und wenn sie welche findet, aktualisiert den Sicherheitsinhalt.

# Die installierte Version des Sicherheitsinhalts mit Hilfe der CLI überprüfen

Verwenden Sie die Befehle in diesem Thema, um Ihre Version des installierten Sicherheitsinhalts zu überprüfen.

**Um die Version des installierten Sicherheitsinhalts zu überprüfen:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Überprüfen Sie den aktuellen Status des Sicherheitsinhalts mit Hilfe des folgenden Befehls:

   ```
   hostname (config) # show fenet security-content status
   ```

3. Überprüfen Sie den Security Content Updates Abschnitt in der DTI Security Content Status Information Liste, wie im folgenden Beispiel angezeigt:

```
Security Content Updates
Enabled           : yes
Update mode       : online
Last Checked At   : 2020/01/07 00:44:00
Last Applied At   : 2020/01/06 23:45:19
Last Applied Type : full
Timestamp (UTC)   : 2020-01-06 23:15:00
Status            : apply-info: No new security updates available

Security Content Version: 976.292
```

**Um die Security Content Versionen und das Installationsdatum zu überprüfen:**

1. Zeigen Sie Protokolldateien an, die Informationen über den Sicherheitsinhalt enthalten:

```
hostname (config) # show log files all matching "security content
version is"
```

2. Die Ausgabe sieht so ähnlich wie im folgenden Beispiel aus. Sie können durch den frühesten Zeitstempel sehen, wann eine bestimmte Security Content Version verfügbar war. Der spätere Zeitstempel zeigt an, wann sie auf Ihrer Appliance angewendet wurde.

```
Searching log files...
Mar  1 09:38:17 notifyd[18001]: [notifyd.NOTICE]-security content
version is:249.101
Mar  1 14:19:01 notifyd[12385]: [notifyd.NOTICE]-security content
version is:249.101
Mar 14 08:00:00 notifyd[4351]: [notifyd.NOTICE]-security content
version is:252.101
Mar 14 10:15:42 notifyd[10820]: [notifyd.NOTICE]-security content
version is:252.101
```

# Sicherheitsinhalt mit Hilfe der CLI aktualisieren

Verwenden Sie die CLI Befehle in diesem Thema, um Sicherheitsinhalt zu aktualisieren.

**Um Sicherheitsinhalte zu aktualisieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Laden Sie das neueste Sicherheitsinhaltspaket herunter:

```
hostname (config) # fenet security-content download-update
Operation initiated in the background.
  Run 'show fenet security-content status [progress]' for status
```

3. Installieren Sie den Sicherheitsinhalt.

```
hostname (config) # fenet security-content apply-update
Operation initiated in the background.
Run 'show fenet security-content status [progress]' for status
```

4. Überprüfen Sie den Download Status:

```
hostname (config) # show fenet security-content status
```

5. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

# Automatische Sicherheitsupdates konfigurieren

Sie können bestimmen, wie oft der DTI-Netzwerkserver und die Network Security Appliance Sicherheitsinhalte teilen sollen.

## Voraussetzungen

- Admin Zugriff

## Automatische Updates des Sicherheitsinhalts mit Hilfe der Web-UI konfigurieren

Verwenden Sie die **DTI Network Settings** Seite, um automatische Updates des Sicherheitsinhalts zu konfigurieren.

## Voraussetzungen

- Admin Zugriff

**Um automatische Aktualisierungen von Sicherheitsinhalten zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf **DTI Network**. Klicken Sie dann auf das Symbol in der Settings Spalte der **Security Contents** Zeile.
3. Wählen Sie die Update-Häufigkeit von der **Update Frequency** Dropdown-Liste.

- daily (täglich)
- hourly (stündlich)

4. Legen Sie die Startzeit der Aktualisierung in der Dropdown-Liste für die Zeit fest.
   - Wenn Sie eine tägliche Aktualisierung ausgewählt haben, stellen Sie die Zeit für den Start der Aktualisierung, auf einer 24 Stunden Uhr basierend, ein.
   - Wenn Sie eine stündliche Aktualisierung ausgewählt haben, stellen Sie die Minuten nach der Stunde ein, wenn die Aktualisierung starten soll.
5. Klicken Sie auf **Apply Settings**.
6. (Optional) Um E-Mail Benachrichtigungen für jede Aktualisierung von Sicherheitsinhalten zu erhalten, wählen Sie das Kontrollkästchen **Notify**.

**HINWEIS:** Wenn Sie das **Notify** Kontrollkästchen auswählen, stellen Sie sicher, dass Sie Ereignisbenachrichtigungen konfiguriert haben. Lesen Sie die *Network Security Bedienungsanleitung*.

## Automatische Updates des Sicherheitsinhalts mit Hilfe der CLI konfigurieren

Verwenden Sie die CLI Befehle in diesem Thema, um automatische Updates des Sicherheitsinhalts zu konfigurieren.

**Um automatische Aktualisierungen von Sicherheitsinhalten zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie automatische Aktualisierung von Sicherheitsinhalten:

   ```
   hostname (config) # fenet security-content autoupdate action update
   ```

3. Geben Sie das Zeitintervall für die automatische Aktualisierung an:
   - Um täglich zu aktualisieren, geben Sie den folgenden Befehl ein, wobei <hh:mm> die Zeit für den Start des Update festlegt, auf einer 24-Stunden Uhr basierend:

     ```
     fenet security-content autoupdate schedule daily at <hh:mm>
     ```

   - Um stündlich zu aktualisieren, geben Sie den folgenden Befehl ein, wobei <mm> die Anzahl der  Minuten nach der Stunde ist, zu der das Update beginnt.

     ```
     fenet security-content autoupdate schedule hourly at <mm>
     ```

- Um nach einer festgelegten Anzahl von Minuten zu aktualisieren, geben Sie den folgenden Befehl ein, wobei <mm> die Anzahl von Minuten zwischen Updates ist.

  ```
  fenet security-content autoupdate schedule every <mm>
  ```

- Geben Sie den folgenden Befehl ein, um das Standardintervall zu verwenden:

  ```
  fenet security-content autoupdate schedule default
  ```

4. (Optional) Um e-Mail Benachrichtigungen über jedes Update von Sicherheitsinhalten zu erhalten, geben Sie den **fenet security-content autoupdate notification enable** Befehl ein. Benachrichtigungen sind standardmäßig deaktiviert. Nach Aktivierung von automatischen Update Benachrichtigungen können Sie festlegen, welche Art von Benachrichtigungen Sie erhalten wollen.

   - Um eine E-Mail Benachrichtigung zu erhalten, wenn die automatische Aktualisierung von Sicherheitsinhalten fehlschlägt, geben Sie den folgenden Befehl ein: Diese Option ist der Standard.

     ```
     fenet security-content autoupdate notification class fail
     ```

   - Um eine E-Mail Benachrichtigung zu erhalten, wenn die automatische Aktualisierung von Sicherheitsinhalten erfolgreich ist, geben Sie den folgenden Befehl ein:

     ```
     fenet security-content autoupdate notification class info
     ```

5. Überprüfen Sie die Update Konfiguration.

   ```
   hostname (config) # show fenet security-content status
   ```

6. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Warnungen über veraltete Sicherheitsinhalte

Dieses Thema behandelt die folgenden Informationen:

# Information über veraltete Sicherheitsinhalte

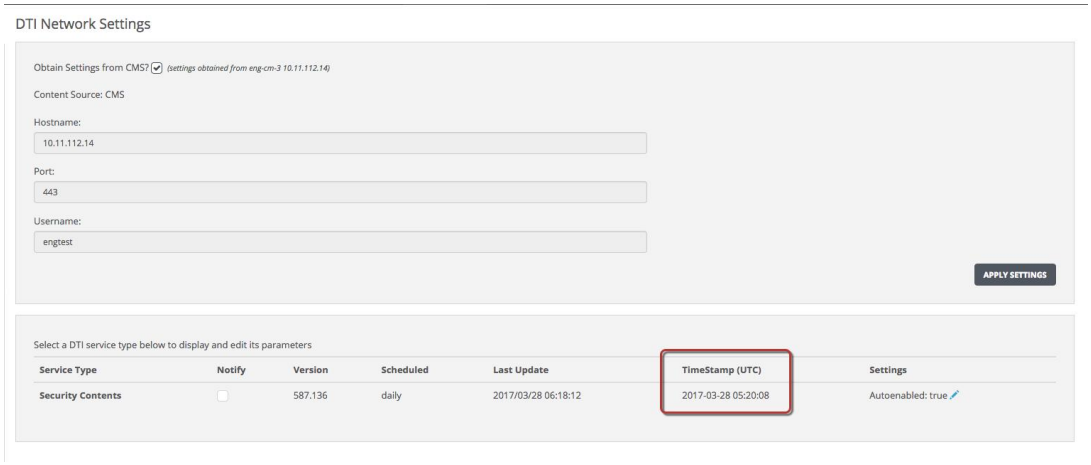
Die Network Security Appliance stellt Alarme aus, wenn der installierte Sicherheitsinhalt veraltet ist. Diese Funktion ermöglicht sicherzustellen, dass FireEye Appliances - insbesondere offline Appliances keine veralteten Sicherheitsinhalte verwenden. Indem Sie regelmäßig die neuesten Sicherheitsinhalte herunterladen und installieren, minimieren Sie falsch negative und falsch positive Ergebnisse.

Diese Funktion wird in Network Security Softwareversion 7.9.2 und später unterstützt.

## Der Security Content Zeitstempel

Das Erstellungsdatum des Sicherheitsinhaltes wird durch einen Zeitstempel angezeigt, der in die Metadaten des Sicherheitsinhaltes eingebettet ist.

In der Appliance Web-UI wird der Zeitstempel des installierten Sicherheitsinhalts in der Content Version Tafel der **About** Seite angezeigt.




In der Appliance CLI wird der Zeitstempel des installierten Sicherheitsinhalts im Timestamp (UTC) Feld der `show fenet security-content status` Befehlsausgabe angezeigt. Dieser Zeitstempel wird auch in der Web-UI und der CLI Befehlsausgabe der verwaltenden Central Management Appliance angezeigt. Lesen Sie das *Central Management Administrationshandbuch*.

## Alarme über veraltete Sicherheitsinhalte

Die Appliance überprüft das Alter des installierten Sicherheitsinhalts regelmäßig, indem sie die Systemzeituhr mit dem Zeitstempel vergleicht, der in den Metadaten des Sicherheitsinhalts eingebettet ist. Wenn der Sicherheitsinhalt für Appliances mit Netzwerkverbindung mehr als 5 Stunden oder für Offline-Geräte mehr als 36 Stunden alt ist, werden Warnungen folgendermaßen verteilt:

- E-Mail wird an Empfänger gesendet, die für den Empfang von Benachrichtigungen für Systemereignisse auf Fehlerebene konfiguriert sind, sofern automatische Aktualisierungen von Sicherheitsinhalt aktiviert sind.
- Die Web-UI zeigt eine Warnmeldung am Anfang des Dashboards an.
- Die Ausgabe eines CLI-Befehls enthält eine Warnmeldung.

# E-Mail Benachrichtigungen für veraltete Sicherheitsinhalte

Die Network Security Appliance kann E-Mail Benachrichtigungen senden, wenn der installierte Sicherheitsinhalt veraltet ist. E-Mail Benachrichtigungen für veraltete Sicherheitsinhalte haben die folgenden Erfordernisse:

- Der E-Mail-Server ist so konfiguriert, dass er Benachrichtigungen für Systemereignisse auf Fehlerebene sendet.
- Automatische Aktualisierungen des Sicherheitsinhalts sind aktiviert.
- E-Mail Empfänger, die Informationen über veraltete Sicherheitsinhalte benötigen, sind konfiguriert, Benachrichtigungen für Systemereignisse auf Fehlerebene zu erhalten.

Sie können die Appliance Web-UI oder CLI verwenden, um E-Mail Benachrichtigungen für veraltete Sicherheitsinhalte zu konfigurieren.

- E-Mail Benachrichtigungen für veralteten Sicherheitsinhalt mit Hilfe der Web-UI konfigurieren unten
- E-Mail Benachrichtigungen über veralteten Sicherheitsinhalt mit Hilfe der CLI konfigurieren auf der nächsten Seite

## E-Mail Benachrichtigungen für veralteten Sicherheitsinhalt mit Hilfe der Web-UI konfigurieren

Auf der Appliance Web-UI können Sie die **Settings > DTI Network** und die **Settings>Email** Seite verwenden, um E-Mail Benachrichtigungen für veraltete Sicherheitsinhalte zu konfigurieren.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um E-Mail Benachrichtigungen für veraltete Sicherheitsinhalte mit Hilfe der Web-UI zu konfigurieren:**

1. Gehen Sie auf die **Settings > DTI Network** Seite.
2. Wählen Sie das **Notify** Kontrollkästchen in der **Security Contents** Zeile.
3. Stellen Sich sicher, dass Ereignisbenachrichtigungen konfiguriert sind, wie in der *Network Security Bedienungsanleitung beschrieben*.
4. Stellen Sie sicher, dass automatische Aktualisierung für Sicherheitsinhalte aktiviert ist. Wenn diese Funktion aktiviert ist, schließt das **Settings** Feld in der **Security Contents** Zeile jetzt die Nachricht "Autoupdate Enabled:true" ein.

   Wenn die Nachricht nicht angezeigt wird, aktivieren Sie die Funktion wie unter Automatische Updates des Sicherheitsinhalts mit Hilfe der Web-UI konfigurieren auf Seite 191 beschrieben.
5. Gehen Sie auf die **Settings > Email** Seite.
6. Stellen Sie sicher, dass die E-Mail Adresse jeder Person, die über veraltete Sicherheitsinhalte gewarnt werden muss, in der **Recipient** Spalte der Tabelle aufgeführt ist.

   Um eine E-Mail Adresse zu der Liste hinzuzufügen, benutzen Sie das **Add Email Recipient** Feld und die **Add Recipient** Schaltfläche, wie unter E-Mail Empfänger mit Hilfe der Web-UI konfigurieren auf Seite 217 beschrieben.
7. Stellen Sie sicher, dass alle Personen, die vor veralteten Sicherheitsinhalten gewarnt werden müssen, so konfiguriert sind, dass Sie E-Mail Benachrichtigungen für Ereignisse auf "failure" Ebene erhalten. Standardmäßig sind Empfänger von E-Mail Benachrichtigungen für den Empfang aller Systemereignisse konfiguriert.

   Um einem Empfänger zu ermöglichen, Benachrichtigungen für Ereignisse auf Fehlerebene zu erhalten, aktivieren Sie das Kontrollkästchen für diesen Empfänger, wie unter beschrieben System-Ereignisbenachrichtigungen mit Hilfe der Web-UI konfigurieren auf Seite 220.

## E-Mail Benachrichtigungen über veralteten Sicherheitsinhalt mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Thema, um E-Mail Benachrichtigungen über verwaltete Sicherheitsinhalte mit Hilfe der Appliance CLI zu konfigurieren.

# Voraussetzungen

- Operator oder Admin Zugriff

**Um E-Mail Benachrichtigungen über veraltete Sicherheitsinhalte mit Hilfe der CLI zu konfigurieren:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie den Status des Sicherheitsinhalts an.

   ```
   hostname (config) # show fenet security-content status
   ```

3. Stellen Sie sicher, dass die Appliance konfiguriert ist, Benachrichtigungen für Systemereignisse auf Fehlerebene zu senden.

   Wenn die Option deaktiviert ist, verwenden Sie den folgenden Befehl, um sie zu aktivieren, wie unter Automatische Updates des Sicherheitsinhalts mit Hilfe der CLI konfigurieren auf Seite 192 beschrieben.

   ```
   hostname (config) # fenet security-content autoupdate notification
   class fail
   ```

4. Stellen Sich sicher, dass Ereignisbenachrichtigungen konfiguriert sind, wie in der *Network Security Bedienungsanleitung beschrieben*.

5. Stellen Sie sicher, dass automatische Aktualisierung für Sicherheitsinhalte aktiviert ist. Wenn diese Funktion aktiviert ist, zeigt das **Enabled** Feld im **Security Content Autoupdate** Abschnitt der Befehlsausgabe "`yes`" an.

   Wenn das Feld "`no`" anzeigt, aktivieren Sie die Funktion, wie unter Automatische Updates des Sicherheitsinhalts mit Hilfe der CLI konfigurieren auf Seite 192 beschrieben.

6. Zeigen Sie die Konfigurationseinstellungen für die Erstellung von E-Mail Alarme für Systemereignisse an.

   ```
   hostname (config) # show email
   ```

   Informationen über die Empfänger der E-Mail Benachrichtigung sind im **Email notification recipients** Abschnitt der Befehlsausgabe aufgeführt. Jeder Eintrag hat das folgende Format:

   ```
   <emailAddress> (<eventLevel>, <detailLevel>)
   ```

   wobei die Konfigurationsparameter wie folgt lauten:

   - `<emailAddress>`—E-Mail Adresse, die System-Ereignisbenachrichtungen empfangen kann.
   - `<eventLevel>`—Die an diesen Empfänger gesendeten Ereignistypen: `all events`, `failure events only` oder `info events only`.
   - `<detailLevel>`—Die an diesen Empfänger gesendeten Informationstypen: `in detail` oder `summarized`.

   Nachfolgend finden Sie ein Beispiel des **Email notification recipients** Abschnitts der `show email` Befehlsausgabe:

   ```
   Email notification recipients:
     alan.brown@yourcompany.com (all events, in detail)
     john.green@yourcompany.com (failure events only, in detail)
     mary.jones@yourcompany.com (info events only, in detail)
     seth.smith@yourcompany.com (all events, summarized)
   ```

   Standardmäßig sind die Empfänger von E-Mail Benachrichtigungen konfiguriert, alle Systemereignisse im Detail zu empfangen, wie im ersten Eintrag des Beispiels angezeigt.

7. Stellen Sie sicher, dass die E-Mail Adresse jeder Person, die über veraltete Sicherheitsinhalte gewarnt werden muss, im **Email notification recipients** Abschnitt der Ausgabe aufgeführt ist.

   Wenn eine E-Mail Adresse von dieser Liste fehlt, fügen Sie den Empfänger, wie unter Empfänger für System-Ereignisbenachrichtigungen hinzufügen und entfernen auf Seite 218 beschrieben, hinzu.

8. Stellen Sie sicher, dass jeder Empfänger, der über veraltete Sicherheitsinhalte gewarnt werden muss, konfiguriert ist, E-Mail Benachrichtigungen für "`failure events only`" oder für "`all events`" zu empfangen.

   **WICHTIG!** Empfänger von Systemereignisbenachrichtigungen. die konfiguriert sind, Benachrichtigungen für "`info events only`" zu empfangen, empfangen keine Benachrichtigungen für veraltete Sicherheitsinhalte.

   Wenn Sie den Ereignistyp ändern müssen, um an den Empfänger einer Ereignisbenachrichtigung zu senden, sehen Sie System-Ereignisbenachrichtigungen für jeden Benutzer konfigurieren auf Seite 221.

9. Bestätigen Sie Ihre Änderungen.

   ```
   hostname (config) # show fenet security-content status
   hostname (config) # show email
   ```

10. Speichern Sie Ihre Änderungen.

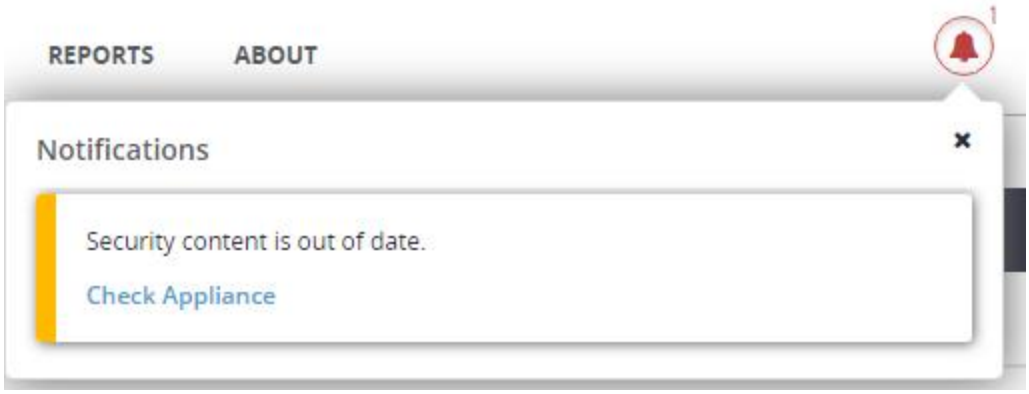
    ```
    hostname (config) # write memory
    ```

## Web-UI Warnung für veraltete Sicherheitsinhalte

In der Benachrichtigungsglocke in der oberen rechten Ecke der Network Security Appliance Web-UI wird die folgende Nachricht angezeigt, wenn Sicherheitsinhalte veraltet sind.

Security content is out of date.

Zum Beispiel:




Um Sicherheitsinhalt zu aktualisieren, klicken Sie auf **Check Appliance**. Die Web-UI zeigt die **About > Upgrade** Seite an, auf der Sie Sicherheitsinhalte aktualisieren können. Details finden Sie unter Sicherheitsinhalte mit Hilfe der Web-UI aktualisieren auf Seite 189.

# CLI-Warnungen für veraltete Sicherheitsinhalte

In der Network Security Appliance CLI können Sie den `show fenet security-content status` Befehl verwenden, um zu überprüfen, ob die Sicherheitsinhalte veraltet sind.



## Information über CLI-Warnungen für veraltete Sicherheitsinhalte

Die Ausgabe des `show fenet security-content status` CLI-Befehl enthält zwei der Parameter, die die Appliance für die Überprüfung nach veralteten Sicherheitsinhalten verwendet. Wenn Sicherheitsinhalte veraltet sind, enthält die Befehlsausgabe auch eine Warnmeldung.

`Warn outdated after`

Das Alter des Sicherheitsinhalts in Stunden, nach dem er als veraltet gilt. Diese Zahl hängt von dem Appliance-Typ ab und ob die Appliance mit dem Internet verbunden ist. Auf Network Security Appliances sind Sicherheitsinhalte veraltet, wenn sie älter als 5 Stunden für eigenständige Appliances und mehr als 36 Stunden für verwaltete Appliances sind.

`Timestamp (UTC)`

Der Datums- und Zeitstempel im UTC-Format, der beim Erstellen des Pakets in die Metadaten des Sicherheitsinhalts geschrieben wurde. Um das Alter des Sicherheitsinhalts zu ermitteln, vergleicht die Appliance diesen Zeitstempel mit der Zeit in der Systemuhr der Appliance.

`WARNING: Security contents are OUTDATED`

Wenn diese Nachricht angezeigt wird, ist der Sicherheitsinhalt auf der Appliance veraltet. In der Appliance Web-UI wird eine ähnliche Warnmeldung am Anfang des Dashboards angezeigt. Wenn E-Mail Benachrichtigungen konfiguriert sind, sendet die Appliance eine E-Mail, um zu warnen, dass der Sicherheitsinhalt veraltet ist.

## Nach CLI-Warnungen für veralteten Sicherheitsinhalt prüfen

Dieser Vorgang zeigt, wie der `show fenet security-content status` Befehl benutzt wird um zu überprüfen, ob der Sicherheitsinhalt veraltet ist.

**Um zu überprüfen, ob der Sicherheitsinhalt veraltet ist:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie den Status des Sicherheitsinhalts an, der auf der Appliance installiert ist.

Wenn der installierte Sicherheitsinhalt veraltet ist, enthält die Befehlsausgabe eine Warnmeldung.

Das folgende Beispiel zeigt den Status des Sicherheitsinhalts für eine eigenständige Network Security Appliance im online Betriebsmodus an:

```
hostname # show fenet security-content status

DTI Security Content Status Information:

  Dynamic Threat Intelligence Service
    Update source        : <online>
    Update channel       : cloud
    Enabled              : yes
    Address              : DTI (cloud.fireeye.com : singleport)
    Username             : DTIUser
    SC acceptance level  : stable
    SC type connected    : yes
    SC channel version   : SCNET-4.0

  Online Analysis Service:
    Service available    : yes
    AV-suite enabled     : yes

  Local Security Content Auto-Generate:
    Enabled              : yes
    Infections enable    : yes
    Callbacks enabled    : yes

  Security Content Autoupdate
    Enabled              : yes
    Action               : update with upload
    Warn outdated after  : 5 hours
    Notify (uploads)     : no
    Notify (downloads)   : no
    Scheduled            : every 15 minutes

  Security Content Uploads
    Enabled              : yes
    Last Uploaded At     : 2017/01/19 16:28:09
    Status               : apply-info: No new security contents

  Security Content Updates
    Enabled              : yes
    Last Checked At      : 2017/01/19 17:50:21
    Last Applied At      : 2017/01/19 12:28:03
    Timestamp (UTC)      : 2017-01-19 11:03:47
    Status               : apply-state: Update in progress ...
    WARNING              : Security contents are OUTDATED.

  Security Content Version: 544.283
```

Der Befehl stellt das Alter des installierten Sicherheitsinhalts fest, indem er den Zeitstempel des Sicherheitsinhalts (`2017-01-19 11:03:47`, im Security Content Updates Abschnitt der Ausgabe angezeigt) mit der Appliance Systemzeit vergleicht.

Die Warnmeldung (`Security contents are OUTDATED`) ist im Security Content Updates Abschnitt enthalten, weil das Alter des Sicherheitsinhalts das Limit überschreitet (`5 hours`, was 2 Wochen entspricht), das im Security Content Autoupdate Abschnitt der Ausgabe angezeigt wird.

# Appliance Telemetrie und Statistiken teilen

Die Network Security Appliance kann anonyme Daten mit der DTI Cloud teilen. Es werden keine kundenspezifischen geschützten Informationen ausgetauscht.

Dieses Thema behandelt die folgenden Informationen:

- Info über die gemeinsame Nutzung von Telemetrie und Statistiken mit der DTI-Cloud unten
- Appliance Telemetrie und Statistiken automatisch mit Hilfe der CLI hochladen auf Seite 204
- Appliance Telemetrie und Statistiken manuell mit Hilfe der CLI hochladen auf Seite 204

## Voraussetzungen

- Admin Zugriff

## Info über die gemeinsame Nutzung von Telemetrie und Statistiken mit der DTI-Cloud

FireEye Appliances pushen anonyme Daten automatisch auf und ziehen Sicherheitsinformationen aus der Dynamic Threat Intelligence (DTI) Cloud.

**HINWEIS:** Alle FireEye Geräte laden Informationen mit Hilfe einer sicheren (HTTPS) Verbindung mit `cloud.fireeye.com` hoch. Standardmäßig kommunizieren verwaltete Appliances mit der DTI Cloud durch die verwaltende Central Management Appliance.

Es werden keine kundenspezifischen oder geschützten Informationen ausgetauscht. Zwei Datentypen werden geteilt: Echtzeit Systemstatistiken und Bedrohungsinformationen.

Informationen über die erforderlichen Lizenzen für die Freigabe dieser Daten finden Sie unter Info über Freigabekombinationen von Support- und Inhaltslizenzen auf Seite 162.

## Echtzeitstatistiken

Die folgenden Echtzeitstatistiken werden anonymisiert und auf die DTI Cloud hochgeladen.

- **Lizenzinformationen**—Status der FireEye Lizenzen auf dem Gerät.
- **Appliance Integrität**—Umgebungsinformationen, die sich auf alle Komponenten beziehen, zum Beispiel Ventilatoren und Festplatten mit System Activity Report Daten.
- **Verkehrsmessungen**—Verkehrsdurchsatzstatistiken und Kapazitätsüberwachung.
- **Statistiken über kritische Subsystemkapazität**—Schnittstellenstatus, Paketanzahl, Anzahl der Flüsse, defekte oder asymmetrische Flüsse, Binärdateien, Paketverlust, protokollbasierte Statistiken, Speichernutzung und Informationen auf Kernel-Ebene.

## Bedrohungsinformationen

Die folgenden Bedrohungsinformationen werden mit der DTI Cloud geteilt:

- **Zeitstempel**—Der Zeitstempel kann als Referenz für andere Ereignisse verwendet werden und zusätzliche Informationen über den Angriff und die verwendeten Methoden liefern.
- **URL**—Liste der bösartigen URLs, die während der Analyse des Datenverkehrs in der Virtual Execution (VX) Engine kontaktiert wurden.
- **MD5**—Ein MD5 Hash wird für Informationen, wie z.B. IP-Adressen oder MAC Adressen generiert. Der MD5 Hash ermöglicht FireEye, die Daten für die Analyse beizubehalten, ohne dass die Daten nachverfolgbar oder in ihrer Ursprungsform erkennbar sind. Die Informationen sind für die Korrelation von mehreren Bedrohungen auf einem gemeinsamen Host wichtig.
- **Dateitypen**—Im Verlauf eines Angriff benutzte Dateitypen. FireEye bestimmt den Eintrittspunkt, die Nutzlast und die verwendeten Methoden.

## Informationen, die nicht auf die DTI Cloud hochgeladen werden

Die folgenden Informationen werden NICHT auf die DTI Cloud hochgeladen:

- Keine kundenspezifischen Informationen
- Keine geschützten Informationen
- Keine Paketerfassungen

## Vorteile der gemeinsamen Nutzung von Daten mit der DTI Cloud

Das Hochladen von Daten in die DTI Cloud bietet folgende Vorteile:

- Teilnehmende FireEye**Appliances** teilen Malware Informationen in Echtzeit.
- Das FireEye **Customer Support** Team kann Ihnen proaktive operative Überwachung und Unterstützung bieten. Diese Überwachung und Unterstützung umfasst die Identifizierung gezielter Angriffe.
- Das FireEye **Research Lags** Team verarbeitet die Sammlung gemeinsam genutzter Daten, um den bösartigen Inhalt zu extrahieren. Aktualisierte Sicherheitsinhalte , von denen einige mit Hilfe anonymer Kundendaten entwickelt wurden, sind in dem Sicherheitsinhalt enthalten, der an die DTI Cloud zur Verteilung an lizenzierte FireEye Appliances und Rechenknoten geliefert werden.
- Die FireEye **DTI Cloud** selbst verwendet Technologie für die Erkennung von Zero-Day Rückrufen.

**HINWEIS:** Sie müssen keine Daten hochladen, um Vorteile der DTI Cloud zu erhalten. Ihre Network Security Appliance kann aktualisierten Sicherheitsinhalt herunterladen und installieren, selbst wenn sie keine Daten hochladen.

# Appliance Telemetrie und Statistiken automatisch mit Hilfe der CLI hochladen

Verwenden Sie die CLI-Befehle in diesem Thema, um Network Security Appliance Telemetrie und Statistiken automatisch alle drei Stunden auf die DTI-Cloud hochzuladen. Es werden keine kundenspezifischen oder geschützten Informationen ausgetauscht.

**Um automatische Aktualisierungen von Systeminformationen zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Stellen Sie den Zeitplan für das Upload von Aggregatsinformationen auf die DTI-Cloud automatisch auf alle drei Stunden ein.

   ```
   fenet stats-content upload auto default
   ```

# Appliance Telemetrie und Statistiken manuell mit Hilfe der CLI hochladen

Verwenden Sie die CLI Befehle in diesem Thema, um aggregierte Systemstatistiken von der Network Security Appliance auf die DTI Cloud zu pushen.

**Um Statistiken manuell auf die DTI Cloud zu pushen.**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Laden Sie die Statistiken hoch.

   ```
   hostname (config) # fenet stats-content upload now
   ```

# KAPITEL 10: Systemsicherheit

In diesem Abschnitt werden Methoden aufgeführt, die Sie für die Sicherung Ihrer FireEye Appliance verwenden können. Detaillierte Informationen über die Implementierung der Methoden findenSie im *FireEye System-Sicherheitshandbuch*.

## AAA

Authentifizierung, Autorisierung und Accounting (AAA) Methoden steuern den Zugriff der User auf Netzwerkressourcen und überwachen Useraktivitäten.

AAA Informationen im *System-Sicherheitshandbuch* beinhalten:

- **Authentifizierung**—Konfigurieren von Authentifizierungsmethoden und -reihenfolge, lokale Authentifizierung (Benutzerkonten, Passwortkomplexität und Passwortrichtlinien), remote Authentifzierung, Common Access Card (CAC) Authentifizierung, Secure Shell (SSH) Authentifizierung und Single Sign-On (SSO) Authentifizierung.
- **Autorisierung**—Definieren der Rollen für lokale Userkonten.
- **Accounting**—Verwalten von Auditprotokollen.
- **FireEye Cloud IAM**—Identity Access Management (IAM), einem Web Service verwenden, der Benutzerauthentifizierung und -autorisierung bietet.

Das Handbuch enthält auch Referenzinformationen über FireEye Appliance-Rollen und Fähigkeiten und FireEye Cloud IAM Berechtigungen.

## Zertifikate

FireEye Appliances verwenden X.509 (TLS/SSL) Zertifikate, um sichere Verbindungen zwischen Appliances und dem Webbrowser zu gestatten, der die Web-UI ausführt sowie remote Server für verschiedene Clientanwendungen zu überprüfen. Sie verwenden die Zertifikate auch, um die E-Mails, die sie an einen Downstream-MTA auf der Email

Security — Server Edition Appliance weiterleiten zu verschlüsseln und die Verbindung mit einem WebDAV Server auf der File Protect Appliance zu sichern.

Zertifikatsinformationen im *System-Sicherheitshandbuch* beinhalten:

- Das System selbst-signierte Serverzertifikat neu generieren
- HTTPS und MTA Serverzertifikate verwalten
- Webserver und SharePoint CA Zertifikatsketten konfigurieren
- Zusätzliche CA Clientzertifikate hinzufügen
- Öffentliche und private Schlüssel importieren und herunterladen und öffentliche Schlüssel exportieren
- Allgemeine Attribute von X.509 Zertifikaten definieren
- Ein CA Zertifkat von einer vertrauenswürdigen Certificate Authority (CA) erhalten
- Die Mindestanforderung der Version für Transport Layer Security (TLS)
- Zertifikatssicherheit verbessern

# KAPITEL 11: System-E-Mail Einstellungen

Die Appliance kann E-Mail Benachrichtigungen über System-Zustandsereignisse senden, zu.B. zu wenig Speicherraum oder ein Stromausfall. Sie kann auch geplante Berichte senden, die Appliance Verkehrsdaten, Malware Analysedaten und von Malware Alarme ausgelöste E-Mail Benachrichtigungen enthalten.

## Systemdiagnose Benachrichtigungen

Der System-E-Mail Server kann Benachrichtigungen über Systemereignisse an konfigurierte Empfänger senden. Sie konfigurieren den E-Mail Server und die Empfänger für diese Ereignisse auf der **Email Settings** Seite der Web-UI oder mit den `email notify` CLI Befehlen. Sie können auch:

- Angeben, ob jeder Empfänger Benachrichtigungen für "fail" Ereignisse, "info" Ereignisse oder sowohl "fail" als auch "info" Ereignisse erhalten soll.
- Angeben, ob jeder Empfänger detaillierte oder zusammenfassende Benachrichtigungen erhalten soll.
- Bestimmte Ereignisse aktivieren oder deaktivieren, Benachrichtigungen auszulösen.

Details finden Sie in:

- Den Mail Server konfigurieren auf der nächsten Seite
- E-Mail Empfänger konfigurieren auf Seite 216
- Systemereignisse konfigurieren auf Seite 219

## Geplante Berichte

Geplante Berichte verwenden den gleichen E-Mail Server und Empfängerliste wie die Systemereignisse. Wenn Sie die CLI verwenden, konfigurieren Sie sie mit Hilfe der `report email` Befehle anstelle der `email notify` Befehle, wie in Den Mail Server für geplante Berichte mit Hilfe der CLI konfigurieren auf Seite 214 beschrieben. Die Berichtsdaten und der Zeitplan werden auf der **Reports** > **Schedule** Seite auf der Web-UI oder mit Hilfe der

`report schedule` Befehle konfiguriert. Lesen Sie den "Berichte" Abschnitt der *Bedienungsanleitung* für Details.

### Malware Warnmeldungen

E-Mail Einstellungen für Malware Warnmeldungen werden auf der **Notification Settings** Seite der Web-UI oder mit Hilfe der `fenotify email` CLI Befehle konfiguriert. Lesen Sie den "Benachrichtigungen" Abschnitt der *Bedienungsanleitung* für Details.

# Den Mail Server konfigurieren

Ereignisbenachrichtigungen für die Systemdiagnose und geplante Berichte können den gleichen Mail Server benutzen. Wenn Sie die CLI für die Konfigurierung des Servers benutzen, müssen Sie zwei getrennte Sätze von CLI Befehlen verwenden. Die Mail Server Einstellungen sind in der folgenden Tabelle beschrieben:

### System Mail Server Einstellungen

| Web-UI Feld | Health Check CLI Parameter | Report CLI Parameter | Beschreibung |
|---|---|---|---|
| Enable email | — | — | Aktiviert die E-Mail Zustellung von Integritätsbenachrichtigungen und geplanten Berichten |
| Mail hub | Mailhub | Server | Der Hostname oder die IP-Adresse des Mail Servers. |
| Port | Mailhub-Port | Port | Der SMTP Port, der zum Sender der E-Mails verwendet wird. Der Standardwert ist 25. |
| Domain | domain | domain | Der Domainname, von dem die E-Mails zu kommen scheint. Der Standardwert ist die aktive Appliance für die Appliance. |

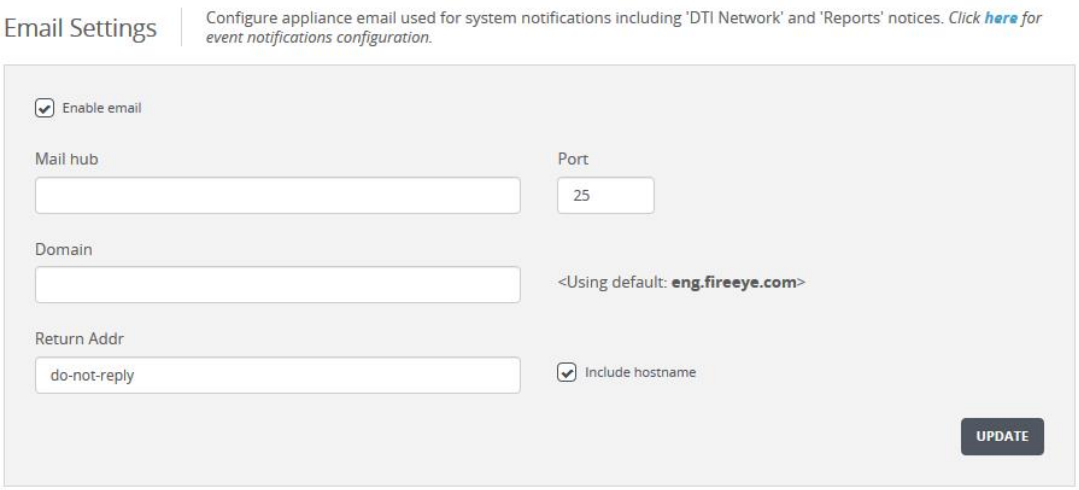
| Web-UI Feld | Health Check CLI Parameter | Report CLI Parameter | Beschreibung |
|---|---|---|---|
| Return Addr | return-addr | return-addr | *Systemdiagnose Parameter*: Der Benutzername oder die voll qualifizierte Absenderadresse, von der E-Mails gesendet werden. Wenn die Zeichenfolge das @ Zeichen enthält, gilt sie als voll qualifiziert. Ansonsten gilt sie als ein Benutzername und nimmt standardmäßig die Form **<username>@<hostname>.<domain>** an. Der Standard Benutzername ist **do-not-reply**.<br>*Report parameter*: Die voll qualifizierte Absenderadresse, von der E-Mails gesendet werden. |
| Incl. hostname | return-host | — | Gibt an, ob der Hostname der Appliance in der Absenderadresse eingeschlossen ist. Wenn es ausgeschlossen ist, nimmt die Absenderadresse das Format **<username>@<domain>** an.<br>Diese Einstellung wird ignoriert, wenn die bereitgestellte Absenderadresse voll qualifiziert ist. |

## Voraussetzungen

- Operator oder Admin Zugriff

## Den Mail Server mit Hilfe der Web-UI konfigurieren

Verwenden Sie die **Email Settings** Seite, um Einstellungen für den Mail Server zu konfigurieren.




**Um den Mail Server zu konfigurieren:**

1. Klicken Sie auf den **Settings** Tab.
2. Klicken Sie auf der Seitenleiste auf **Email**.
3. Bestimmen Sie Einstellungen, wie unter System Mail Server Einstellungen auf Seite 210 beschrieben.
4. Klicken Sie auf **Update**, um Ihre Änderungen zu speichern.

## Den Mail Server für Benachrichtigungen über Systemdiagnosen mit Hilfe der CLI konfigurieren

Verwenden Sie die CLI Befehle in diesem Thema, um den Mail Server zu konfigurieren, der Benachrichtigungen über Systemdiagnosen sendet. Eine Beschreibung für jedes Parameter finden Sie unter System Mail Server Einstellungen auf Seite 210.

**HINWEIS:** Sehen Sie E-Mail Empfänger mit Hilfe der CLI konfigurieren auf Seite 218 für Informationen über die Konfigurierung der Empfänger von Benachrichtigungen. Sehen Sie System Ereignisbenachrichtigungen mit Hilfe der CLI konfigurieren auf Seite 221 für Informationen über die Konfigurierung der Ereignisse, die Benachrichtigungen auslösen.

**Um den E-Mail Server für System-Benachrichtigungen zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Geben Sie den Hostnamen oder die IP-Adresse des Mail Servers an:

```
hostname (config) # email mailhub {<hostname> | <IPv4 or IPv6 address>}
```

3. Geben Sie den SMTP Port an, über den der Mail Server Benachrichtigungen sendet:

   ```
   hostname (config) # email mailhub-port <port>
   ```

4. Geben Sie den Domainnamen an, von dem die E-Mails kommen sollen:

   ```
   hostname (config) # email domain <domainName>
   ```

5. Geben Sie den Benutzernamen oder die voll qualifizierte Absenderadresse an, von der die E-Mails gesendet werden:

   ```
   hostname (config) # email return-addr {<username> | <returnAddress>}
   ```

6. (Optional) Schließen Sie den Hostnamen des Mail Servers in der Absenderadresse ein.

   ```
   hostname (config) # email return-host
   ```

7. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show email
   ```

8. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**HINWEIS:** Um eine Konfiguration zu entfernen oder eine Standard Einstallung wiederherzustellen, hängen Sie `no` an den Befehl an. Um beispielsweise den Hostnamen in der Absenderadresse auszuschließen, verwenden Sie den `no email return-host` Befehl, und um den Standard Domainnamen wiederherzustellen, verwenden Sie den `no email domain` Befehl.

## Beispiele

In diesem Beispiel ist die Absenderadresse nicht vollständig qualifiziert, so dass der Hostname ("hostname") und Domain sie angehängt sind.

```
hostname (config) # email mailhub 10.1.0.0
hostname (config) # email domain mail.acme.com
hostname (config) # email return-addr admin
hostname (config) # show email
Mail hub:          10.1.0.0
Mail hub port:     25
Domain override:   mail.acme.com
Return address:    admin
Include hostname in return address: yes

Current reply address: admin@hostname.mail.acme.com
...
```

In diesem Beispiel ist die Absenderadresse vollständig qualifiziert, so dass der Hostname und Domain nicht eingeschlossen sind.

```
hostname (config) # email mailhub 10.1.0.0
hostname (config) # email domain mail.acme.com
hostname (config) # email return-addr notify@acme.com
hostname (config) # show email
Mail hub:          10.2.0.0
```

```
Mail hub port:     25
Domain override:   mail.acme.com
Return address:    notify@acme.com
Include hostname in return address: yes

Current reply address: notify@acme.com
...
```

In diesem Beispiel werden alle Einstellungen auf Ihre Standardwerte zurückgesetzt.

```
hostname (config) # show email
Mail hub:          10.3.0.0
Mail hub port:     26
Domain override:   mailhost.acme.com
Return address:    admin
Include hostname in return address: no

Current reply address: admin@hostname.mailhost.acme.com
...

hostname (config) # no email mailhub
hostname (config) # no email mailhub-port
hostname (config) # no email return-addr
hostname (config) # email return-host
hostname (config) # show email
Mail hub:
Mail hub port:     25
Domain override:
Return address:    do-not-reply
Include hostname in return address: yes

Current reply address: do-not-reply@hostname.acme.com
...
```

## Den Mail Server für geplante Berichte mit Hilfe der CLI konfigurieren

Verwenden Sie die CLI Befehle in diesem Thema, um den Mail Server zu konfigurieren, der geplante Berichte sendet. Eine Beschreibung für jedes Parameter finden Sie unter System Mail Server Einstellungen auf Seite 210.

**WICHTIG!** Wenn Sie die CLI für die Konfigurierung des E-Mail Servers verwenden, werden die Änderungen nicht auf der **Email Settings** Seite in der Web-UI angezeigt.

**HINWEIS:** Sehen Sie Empfänger für geplante Berichte hinzufügen und entfernen auf Seite 218 für Informationen über die Konfigurierung der Berichtsempfänger mit Hilfe der CLI.

**Um den Mail Server für geplante Berichte zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Geben Sie den Hostnamen oder die IP-Adresse des Mail Servers an:

   ```
   hostname (config) report email smtp server {<hostname> | <ipAddress>}
   ```

3. Geben Sie den SMTP Port an, der vom Mail Server zum Senden von Berichten verwendet wird:

   ```
   hostname (config) # report email smtp port <port>
   ```

4. Geben Sie den Domainnamen an, von dem die E-Mails kommen sollen:

   ```
   hostname (config) # report email smtp domain <domainName>
   ```

5. Geben Sie die voll qualifizierte Absenderadresse an, von der die E-Mails gesendet werden:

   ```
   hostname (config) # report email smtp return-addr <returnAddress>
   ```

6. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show report email
   ```

7. Speichern Sie die Konfiguration:

   ```
   hostname (config) # write memory
   ```

**HINWEIS:** Um eine Konfiguration zu entfernen oder die Standardeinstellung wiederherzustellen, hängen Sie `no` an den Befehl an. Um beispielsweise die Standard Absenderadresse wiederherzustellen, verwenden Sie den `no report email return-addr` Befehl, und um den konfigurierten Domainnamen zu entfernen, verwenden Sie den`the no report email smtp domain` Befehl.

## Beispiele

In diesem Beispiel ist der E-Mail Server konfiguriert, geplante Berichte zu senden.

```
hostname (config) # report email server 10.4.0.0
hostname (config) # report email smtp domain mailer.acme.com
hostname (config) # report email smtp return-addr reports@acme.com
hostname (config) # show report email

Report email configurations:
        SMTP server: 10.4.0.0
        SMTP server port: 25
        SMTP Domain: mailer.acme.com
        SMTP Return addr: reports@acme.com
        ...
```

In diesem Beispiel werden alle Konfigurationseinstellungen auf Ihre Standardwerte zurückgesetzt.

```
hostname (config) # show report email

Report email configurations:
        SMTP server: 10.4.0.0
        SMTP server port: 26
        SMTP Domain: acme.com
        SMTP Return addr: admin@acme.com
        ...
```

```
hostname (config) # no email report smtp server
hostname (config) # no email report smtp port
hostname (config) # no email report smtp domain
hostname (config) # no email report smtp return-addr
hostname (config) # show report email

Report email configurations:
        SMTP server:
        SMTP server port: 25
        SMTP Domain:
        SMTP Return addr: do-not-reply
        ...
```

# E-Mail Empfänger konfigurieren

Die gleichen Benutzer können sowohl System-Ereignisbenachrichtigungen und geplante Berichte empfangen. Wenn Sie die CLI für ihre Konfigurierung benutzen, müssen Sie zwei getrennte Sätze von CLI Befehlen verwenden.

Jeder neue Empfänger erhält detaillierte Benachrichtigungen für alle aktivierten Systemdiagnose Ereignisse. Sie können die Benachrichtigungen für individuelle Benutzer anpassen und konfigurieren, welche spezifischen Ereignisse Benachrichtigungen auslösen. (Sehen Sie Systemereignisse konfigurieren auf Seite 219 für Details.)

**WICHTIG!** Wenn Sie die CLI für die Konfigurierung des Empfängers eines geplanten Berichts verwenden, wird die Änderung nicht in der Web-UI wiedergegeben. Zum Beispiel:

- Sie fügen analyst@acme.com mit Hilfe des `report email recipient analyst@acme.com` CLI Befehls hinzu. Dieser Empfänger wird in der `show report email` Befehlsausgabe aufgeführt, ab wird nicht zur Empfängerliste auf der **Email Setting**s Seite in der Web-UI hinzugefügt.
- Die Empfängerliste auf der **Email Settings** Seite enthält admin@acme.com, aber das **Report** Kontrollkästchen ist nicht markiert. Dann fügen Sie diesen Empfänger mit Hilfe des `report email recipient admin@acme.com` CLI Befehls hinzu. Das **Report** Kontrollkästchen ist auf der **Email Settings** Seite immer noch nicht markiert.

**WICHTIG!** Wenn Sie die Web-UI zum Hinzufügen eines E-Mail Empfängers verwenden, wird der Empfänger aktiviert, sowohl System-Ereignisbenachrichtigungen als auch geplante Berichte zu empfangen. Wenn Sie allerdings den `email notify recipient` CLI Befehl zum Hinzufügen dieses Empfängers verwenden, erhält der Empfänger nur System-Ereignisbenachrichtigungen und keine geplanten Berichte (das **Report** Kontrollkästchen wird auf der **Email Settings** Seite deaktiviert).

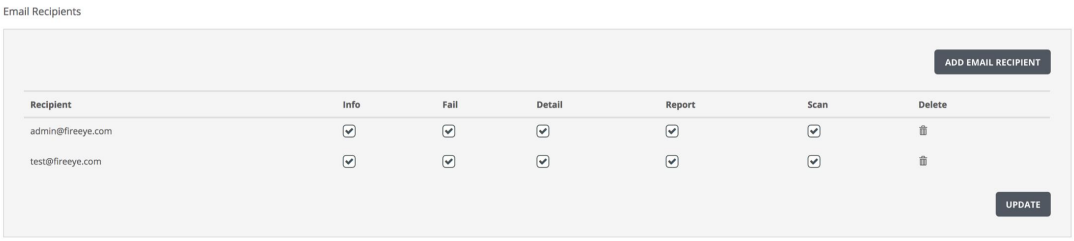
 

## Voraussetzungen

- Operator oder Admin Zugriff

# E-Mail Empfänger mit Hilfe der Web-UI konfigurieren

Verwenden Sie die **Email Settings** Seite, um die E-Mail Empfänger für System-Ereignsbenachrichtigungen und für geplante Berichte hinzuzufügen oder zu entfernen.




1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Email**.
3. Finden Sie den **Email Recipients** Abschnitt.
4. Klicken Sie auf **Add Email Recipient**.
5. Geben Sie die E-Mail Adresse des Benutzers im **Add Email Recipient** Feld ein und klicken Sie dann auf **Add Recipient**.
6. (Optional) Löschen Sie die **Info**, **Fail**, **Detail** und **Scan** Kontrollkästchen nach Bedarf, um die Benachrichtungen anzupassen, die der Benutzer erhält. (Sehen Sie System-Ereignisbenachrichtigungen mit Hilfe der Web-UI konfigurieren auf Seite 220 für Details.)

**Um einen Empfänger für einen geplanten Bericht hinzuzufügen:**

1. Klicken Sie auf **Add Email Recipient**.
2. Geben Sie die E-Mail Adresse des Benutzers im **Add Email Recipient** Feld ein und klicken Sie dann auf **Add Recipient**.
3. Stellen Sie sicher, dass das **Report** Kontrollkästchen markiert bleibt.
4. (Optional) Löschen Sie die **Info**, **Fail**, **Detail** und **Scan** Kontrollkästchen, um zu verhindern, dass der Benutzer System-Ereignisbenachrichtigungen sowie geplante Berichte empfängt.

**Um einen E-Mail Empfänger zu entfernen:**

1. Klicken Sie auf das Symbol in der **Delete** Spalte.
2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**, um die Aktion zu bestätigen.

# E-Mail Empfänger mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Abschnitt, um E-Mail Empfänger für System-Ereignisbenachrichtigungen und geplante Berichte hinzuzufügen oder zu entfernen.

**WICHTIG!** Wenn Sie die CLI zum Hinzufügen oder Entfernen des Empfängers für einen geplanten Bericht verwenden, werden die Änderungen nicht auf der **Email Settings** Seite auf der Web-UI angezeigt.

## Empfänger für System-Ereignisbenachrichtigungen hinzufügen und entfernen

**Um Empfänger für System-Ereignisbenachrichtigungen hinzuzufügen:**

1. Aktivieren Sie den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um einen Empfänger hinzuzufügen:

   ```
   hostname (config) # email notify recipient <emailAddress>
   ```

3. Um einen Empfänger zu entfernen:

   ```
   hostname (config) # no email notify recipient <emailAddress>
   ```

4. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show email
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Empfänger für geplante Berichte hinzufügen und entfernen

**Um Empfänger für geplante Berichte zu konfigurieren;**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um einen Empfänger hinzuzufügen:

   ```
   hostname (config) # report email recipient <emailAddress>
   ```

3. Um einen Empfänger zu entfernen:

   ```
   hostname (config) # no report email recipient <emailAddress>
   ```

4. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show report email
   ```

5. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

## Beispiele

In diesem Beispiel wird analyst@acme.com als Empfänger für eine System-Ereignisbenachrichtung hinzugefügt und user3@acme.com wird entfernt.

```
hostname (config) # show email
...
Email notification recipients:
  admin@acme.com (all events, in detail)
  exec@acme.com (failure events only, in detail)
  user3@acme.com (all events, summarized)
...
hostname (config) # email notify recipient analyst@acme.com
hostname (config) # no email notify recipient user3@acme.com
hostname (config) # show email
...
Email notification recipients:
  admin@acme.com (all events, in detail)
  analyst@acme.com (all events, in detail)
  exec@acme.com (failure events only, in detail)
```

In diesem Beispiel wird analyst@acme.com als Empfänger eines geplanten Berichts hinzugefügt und admin@acme.com wird entfernt.

```
hostname (config) # show report email

Report email configurations:
        ...
        Email recipients:
                admin@acme.com
                exec@acme.com
hostname (config) # report email recipient analyst@acme.com
hostname (config) # no report email recipient admin@acme.com
hostname (config) # show report email

Report email configurations:
        ...
        Email recipients:
                analyst@acme.com
                exec@acme.com
```

# Systemereignisse konfigurieren

Standardmäßig erhalten konfigurierte Benutzer detaillierte Benachrichtigungen über alle aktivierten System-Ereignisse. Informelle Ereignisse werden protokolliert, wenn eine Änderung im System vorliegt. Störungsereignisse werden protokolliert, wenn eine Störung im System vorliegt.

Sie können die CLI verwenden, um zu ändern, welche Ereignisse aktiviert werden. Sie können zum Beispiel festlegen, dass informelle Ereignisse, wie z.B. System-Protokolldateirotationen keine Benachrichtigungen auslösen können.

Sie können für jeden Empfänger festlegen, ob Fehlerbenachrichtigungen, informelle Benachrichtigungen oder beides gesendet werden. Zum Beispiel könnte ein Benutzer wissen wollen, dass ein Datenträger fehlerhaft ist, aber nicht, dass eine übermäßige Temperaturbedingung auf normal zurückgekehrt ist.

Sie können auch festlegen, ob ein Benutzer zusammengefasste oder detaillierte Benachrichtigungen erhält.

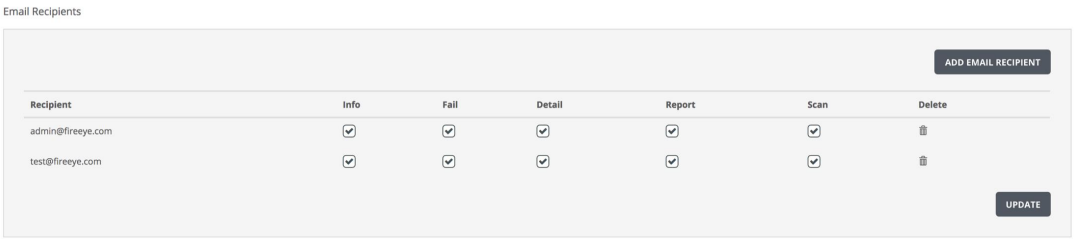
## Voraussetzungen

- Operator oder Admin Zugriff

## System-Ereignisbenachrichtigungen mit Hilfe der Web-UI konfigurieren

Verwenden Sie die **Email Settings** Seite, um den Schweregrad von System-E-Mail Ereignisbenachrichtigungen zu konfigurieren, die an jeden konfigurierten Empfänger gesendet werden sollen.

Um bestimmte Systembenachrichtigungen zu aktivieren oder deaktivieren, müssen Sie die CLI verwenden. Siehe System Ereignisbenachrichtigungen mit Hilfe der CLI konfigurieren auf der nächsten Seite.




**Um den Schweregrad von System-Ereignisbenachrichtigungen zu konfigurieren, die an Empfänger gesendet werden sollen.**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Email**.
3. Finden Sie den **Email Recipients** Abschnitt.
4. Aktivieren oder deaktivieren Sie die **Info** und **Fail** Kontrollkästchen, um den Schweregrad der Ereignisse festzulegen, für den der Benutzer Benachrichtigungen erhält.
5. Aktivieren oder deaktivieren Sie das **Detail** Kontrollkästchen, um festzulegen, welcher Benutzer detaillierte oder zusammengefasste Benachrichtigungen erhalten soll.

6. Wählen oder löschen Sie das **Scan** Kontrollkästchen, um festzulegen, ober der Benutzer eine E-Mail erhält, wenn ein konfigurierter Scan abgeschlossen ist, oder nicht.
7. Klicken Sie auf **Update**, um Ihre Änderungen zu speichern.

# System Ereignisbenachrichtigungen mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Thema, um System-Ereignisbenachrichtigungen für jeden Benutzer anzupassen und zu konfigurieren, welche Ereignisse Benachrichtigungen auslösen.

## System-Ereignisse anzeigen

Sie können alle System-Ereignisse, oder die System-Ereignisse, die derzeit aktiviert sind, Benachrichtigungen auszulösen, nach ihrem Schweregrad sortiert, anzeigen.

**Um alle System-Ereignisse anzuzeigen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie die Ereignisses an:

   ```
   hostname (config) # email notify event ?
   ```

**Um aktivierte System-Ereignisse und deren Schweregrad anzuzeigen:**

- Zeigen Sie die Ereignisse nach Schweregrad an:

  ```
  hostname > show email events
  ```

## System-Ereignisbenachrichtigungen für jeden Benutzer konfigurieren

**Um System-Ereignisbenachrichtigungen für jeden Benutzer zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie die aktuelle Konfiguration an:

   ```
   hostname (config) # show email
   ```

3. Geben Sie den Schweregrad der Ereignisse an, für die jeder Benutzer Benachrichtigungen erhalten sollte.
   - Um "info" Ereignisse zu erhalten:

     ```
     hostname (config) # email notify recipient <emailAddress> class info
     ```

   - Um den Empfang von "info" Ereignissen zu stoppen:

     ```
     hostname (config) # no email notify recipient <emailAddress> class info
     ```

   - Um "failure" Ereignisse zu erhalten:

     ```
     hostname (config) # email notify recipient <emailAddress> class failure
     ```

   - Um den Empfang von "failure" Ereignissen zu stoppen:

     ```
     hostname (config) # no email notify recipient <emailAddress> class failure
     ```

4. Bestimmen Sie das Benachrichtigungsformat.
   - Um detaillierte Benachrichtigungen zu erhalten:

     ```
     hostname (config) # email notify recipient <emailAddress> detail
     ```

   - Um zusammengefasste Benachrichtigungen zu erhalten:

     ```
     hostname (config) # no email notify recipient <emailAddress> detail
     ```

## Konfigurieren, welche Ereignisse Benachrichtigungen auslösen

**Um zu konfigurieren, welche Ereignisse Benachrichtigungen auslösen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie die aktuelle Konfiguration an, wie unter System-Ereignisse anzeigen auf der vorherigen Seite beschrieben.
3. Um ein Ereignis zu aktivieren:

   ```
   hostname (config) # email notify event <event>
   ```

4. Um ein Ereignis zu deaktivieren:

   ```
   hostname (config) # no email notify event <event>
   ```

5. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show email events
   ```

6. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiele

In diesem Beispiel wird admin@acme.com vom Empfang von "Info" Benachrichtigungen gestoppt und das Nachrichtenformat auf eine Zusammenfassung geändert.

```
hostname (config) # show email
...
Email notification recipients:
  admin@acme.com (all events, in detail)
  operator@acme.com (failure events only, in detail)
  user3@acme.com (all events, in detail)
...
hostname (config) # no email notify recipient admin@acme.com info
hostname (config) # no email notify recipient admin@acme.com detail
hostname (config) # show email
...
Email notification recipients:
  admin@acme.com (failure events only, summarized)
  operator@acme.com (failure events only, in detail)
  user3@acme.com (all events, in detail)
```

In diesem Beispiel wird verhindert, dass Protokolldateirotationen Ereignisbenachrichtigungen auslösen:

```
hostname (config) # no email notify event syslog-rotation
```

In diesem Beispiel wird die Auslösung von Ereignisbenachrichtigungen durch DOP-Überladungen (Depth of Processing) deaktiviert:

```
hostname (config) # no email notify event avc-overload
```

Das `avc-overload` Ereignis ist ein "Info" Ebene-Ereignis, das für DOP-Überladungen generiert wurde. DOP-Überladungen treten auf, wenn ein CPU-Konflikt für eine MVX-Engine vorliegt. Wenn eine Überladung häufig auftritt, kann dies die E-Mail und Dateianalyse beeinträchtigen und möglicherweise zu falschen Negativen führen. Wenn eine Appliance konstant weniger als 30% DOP aufweist, ist sie überlastet. Dies ist keine Problem, wenn die Überlastung nur wenige Minuten in der Woche auftritt, aber wenn die Überlastungen mehrere Stunden pro Arbeitstag auftreten, sollte der MVX-Engine mehr CPU-Zeit zugewiesen werden.

# Automatische Unterstützung für System-Ereignisbenachrichtigungen konfigurieren

Sie können die Appliance konfigurieren, E-Mails an `autosupport@fireeye.com` zu senden, wenn bestimmte System-Ereignisse auftreten.

Dies schließt die Konfigurierung von Einstellungen ein um sicherzustellen, dass E-Mail sicher gesendet werden. Sie können einen der folgenden Sicherheitstypen festlegen:

- **none**—Benutzen Sie TLS nicht, um die autosupport E-Mails zu sichern.
- **tls**—Verwenden Sie TLS über dem Standard Server Port, um automatische Unterstützung von E-Mails zu sichern. Senden Sie keine E-Mails, wenn TLS fehlschlägt.
- **tls-none**—Verwenden Sie TLS über dem Standard Server Port, um automatische Unterstützung von E-Mails zu sichern. Die E-Mail wird im Nur-Text gesendet, wenn TLS fehlschlägt.

## Voraussetzungen

- Operator oder Admin Zugriff

## Automatische Unterstützung für System-Ereignisbenachrichtigungen mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Abschnitt, um automatische Unterstützung für System-Ereignisbenachrichtigungen zu konfigurieren. (Sehen Sie System-Ereignisse anzeigen auf Seite 221 für Informationen über die Anzeige einer vollständigen Liste von Ereignissen.)

**Um automatische Unterstützung zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie automatische Unterstützung für E-Mail Benachrichtigungen (standardmäßig deaktiviert):

   ```
   hostname (config) # email autosupport enable
   ```

3. Zeigen Sie die aktuelle Konfiguration für die Generierung von automatischer Unterstützung von E-Mails für Systemereignisse an:

   ```
   hostname (config) # show email
   ```

4. Geben Sie jedes Ereignis an, für das automatische Unterstützung von E-Mail Benachrichtigungen gesendet werden soll:

   ```
   hostname (config) # email autosupport event <event>
   ```

5. Konfigurieren Sie die zusätzlichen Certificate Authority (CA) Zertifikate, die für die Bestätigung der Serverzertifikate verwendet werden.
   - Um nur die integrierte Liste zu benutzen:

     ```
     hostname (config) # email autosupport ssl ca-list none
     ```

   - Um die standardmäßige ergänzende CA Zertifikatsliste zu verwenden:

     ```
     hostname (config) # email autosupport ssl ca-list default-ca-list
     ```

6. Konfigurieren Sie einen Sicherheitstyp, der für die automatische Unterstützung von E-M benutzt werden soll.
   - No TLS:
     ```
     hostname (config) # email autosupport ssl mode none
     ```
   - TLS:
     ```
     hostname (config) # email autosupport ssl mode TLS
     ```
   - TLS none:
     ```
     hostname (config) # email autosupport ssl mode tls-none
     ```

7. Überprüfen Sie die Serverzertifikate:

   ```
   hostname (config) # email autosupport cert-verify
   ```

8. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# KAPITEL 12: Einstellungen von Datum und Uhrzeit

Sie können das Datum und die Uhrzeit der Network Security Appliance manuell einstellen oder einen oder mehrere Network Time Protocol (NTP) Server einstellen, die die Zeit automatisch synchronisieren. Sie können auch eine einmalige Synchronisation der Systemuhr mit der DTI-Serveruhr vornehmen.

Dieses Thema behandelt die folgenden Informationen:



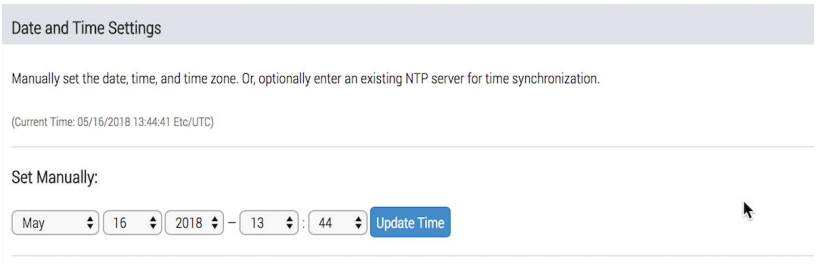
**HINWEIS:** Das Datum und die Uhrzeit werden als Coordinated Universal Time (UTC) in der Datenbank gespeichert. Das Z-Zeichen in der syslog Ausgabe zeigt an, dass die angezeigte Zeit in der UTC Zeitzone liegt; zum Beispiel, 19. Oktober 2016, 16:10:10 Z. Standardmäßig ist die Anzeigezeitzone UTC.

## Manuelle Konfigurierung der Uhrzeit

Sie können das Datum und die Uhrzeit auf Ihrer Network Security Appliance manuell einstellen.

# Das Datum und die Uhrzeit mit Hilfe der Web-UI einstellen

Verwenden Sie die oberen Abschnitt der **Date and Time Settings** Seite, um das Datum und die Uhrzeit für Ihre Network Security Appliance einzustellen.




**WICHTIG!** NTP Synchronisation ist standardmäßig eingestellt und muss deaktiviert werden, bevor Sie das Datum und die Uhrzeit manuell konfigurieren können. Anweisungen über die Deaktivierung von NTP finden Sie unter NTP Server Konfiguration auf Seite 230.

# Voraussetzungen

- Admin Zugriff

**Um das Datum und die Uhrzeit einzustellen:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Date and Time**.
3. Wählen Sie das Datum und die Uhrzeit aus den Dropdown-Listen.
4. Klicken Sie auf **Update Time**.
5. Stellen Sie die Zeitzone wie unter Konfiguration der Zeitzone auf Seite 239 beschrieben ein.

# Das Datum und die Uhrzeit mit Hilfe der CLI einstellen

Verwenden Sie die CLI Befehle in diesem Thema, um die Zeitzone auf Ihrer Network Security Appliance einzustellen.

**WICHTIG!** NTP Synchronisation ist standardmäßig eingestellt und muss deaktiviert werden, bevor Sie das Datum und die Uhrzeit manuell konfigurieren können. Informationen zum Deaktivieren von NTP finden Sie unter NTP Server Konfiguration auf Seite 230.

# Voraussetzungen

- Admin Zugriff

**Um das Datum und die Uhrzeit einzustellen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. (Optional) Verwenden Sie den `clock set <HH>:<MM> <YYYY>/<MM>/<DD>` Befehl, um die Uhrzeit und das Datum festzulegen. Der folgende Befehl legt zum Beispiel die Uhrzeit und das Datum auf 14:00 Uhr am 21. Juli 2014 fest:

   ```
   hostname (config) # clock set 14:00 2014/07/21
   ```

3. Verwenden Sie den `clock timezone <timezone>` Befehl, um die Zeitzone festzulegen. Beispielsweise stellen die folgenden Befehle die Zeitzone auf Pacific Standard Time ein:

   ```
   hostname (config) # clock timezone UTC-offset UTC+8
   hostname (config) # clock timezone America North United_States Pacific
   ```

   **HINWEIS:** Die Zeitzone dient zu Anzeigezwecken und sollte mit Einstellungen für andere Sicherheitsgeräte übereinstimmen.

4. Um die Standard Zeitzone wiederherzustellen:

   ```
   hostname (config) # no clock timezone
   ```

5. Zeigen Sie die konfigurierten Einstellungen für die Uhrzeit und das Datum an:

   ```
   hostname (config) # show clock
   ```

6. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Beispiele

- Uhrzeit und Datum mit Hilfe der nordamerikanischen Central Daylight Zeitzone:

  ```
  hostname > show clock
  Time:        16:39:35
  Date:        2014/06/25
  Time zone:   America North United_States Central
               (US/Central)
  UFC offset: -0500 (UTC minus 5 hours)
  ```

- Uhrzeit- und Datumseinstellungen mit Hilfe der Standard Zeitzone:

  ```
  hostname > show clock
  Time:         21:40:37
  Date:         2014/06/25
  Time zone:    UTC
  ```

```
                (Etc/UTC)
UTC offset:     same as UTC
```

# NTP Server Konfiguration

Anstatt das Systemdatum und -uhrzeit manuell einzustellen, können Sie einen oder mehrere Network Time Protocol (NTP) Server und Peers festlegen, um die Zeit automatisch zu synchronisieren. Standardmäßig wird NTP-Version 4 verwendet, aber Sie können stattdessen Version 3 verwenden. Sie können eine einmalige Aktion ausführen, die die Systemuhr mit einem bestimmten NTP-Server synchronisiert. NTP ist standardmäßig aktiviert. Die Appliance ist mit vier NTP-Servern vorkonfiguriert, die Ihre Appliance verwenden kann, wenn sie sie erreichen kann.

Die Appliance kann authentifizieren, dass die Zeit, die sie von eine m NTP-Server erhält, von einer bekannten und vertrauenswürdigen Quelle ist. Die Systemuhr wird nur aktualisiert, wenn eine Schlüssel-ID in dem eingehenden NTP-Paket mit einer auf der Appliance konfigurierten Schlüssel-ID übereinstimmt und wenn diese Schlüssel-ID auf dem gleichen MD5 oder SHA1 Hashwert sowohl auf dem NTP-Server als auch der Appliance gespeichert ist. Wenn das Schlüssel-ID/Wertpaar auf NTP-Server und Appliance nicht übereinstimmen, wird die Uhr nicht aktualisiert. NTP Authentifizierung ist standardmäßig deaktiviert, aber der NTP-Server muss das Schlüssel-ID/Wertpaar bereits haben und das gleiche Schlüssel-ID/Wertpaar muss auf der Appliance konfiguriert sein und dann dem NTP-Server zugeordnet werden. Insgesamt können 16 Schlüssel auf einer einzigen Appliance konfiguriert werden.

- NTP-Server mit Hilfe der Web-UI konfigurieren auf der nächsten Seite
- NTP-Server mit Hilfe der CLI konfigurieren auf der nächsten Seite
- NTP Authentifizierung mit Hilfe der CLI konfigurieren auf Seite 235

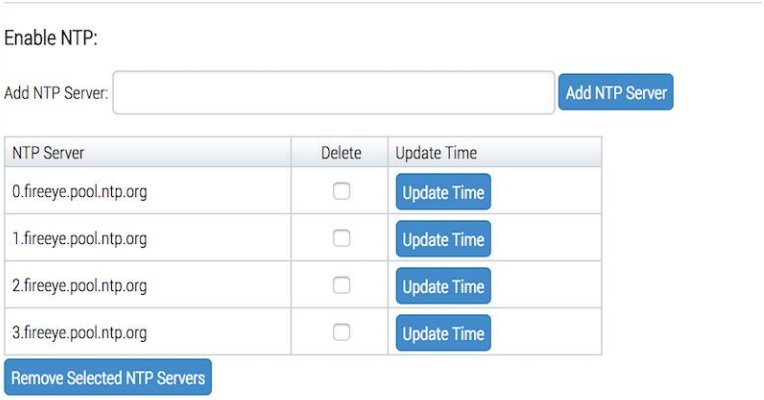
## Voraussetzungen

- Admin Zugriff zum Konfigurieren von NTP
- Monitor, Operator oder Admin Zugriff, um NTP Konfigurations- und Statusinformationen abzurufen
- Verbindung mit mindestens einem NTP Server
- *Für die NTP-Authentifizierung*: Authentifizierung Schlüssel-ID/Wert-Paare auf den NTP-Servern, für die die Authentifizierung konfiguriert wird

# NTP-Server mit Hilfe der Web-UI konfigurieren

Verwenden Sie den **Enable NTP** Abschnitt der **Date and Time Settings** Seite, um NTP-Server zu konfigurieren.




**Um NTP-Server zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Date and Time**.
3. Klicken Sie auf **Add NTP-Server**.
4. Im Feld **Add NTP Server** geben Sie die IP-Adresse oder den Hostnamen des NTP-Servers ein, den Sie verwenden wollen.
5. Klicken Sie auf **Add**.
6. Wiederholen Sie die vorherigen zwei Schritte, um zusätzliche Server hinzuzufügen.
7. Um die Systemzeit einmal mit einem ausgewählten NTP-Server zu synchronisieren, klicken Sie auf **Update** neben dem Servereintrag ein.

   Die Uhrzeit wird aktualisiert und die erforderliche Anpassung wird in einer Nachricht auf der Seite angezeigt.
8. Um einen NTP-Server zu löschen, wählen Sie das Kontrollkästchen neben dem Server und klicken Sie dann auf **Remove NTP Server**.
9. Klicken Sie auf **Yes**, um die Aktion zu bestätigen.

# NTP-Server mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Thema, um NTP-Server zu konfigurieren.

**HINWEIS:** Informationen darüber, dass die Systemuhren nur aktualisiert werden, wenn die Zeit von einer vertrauenswürdigen Quelle stammt, finden Sie unter NTP Authentifizierung mit Hilfe der CLI konfigurieren auf Seite 235.

**Um NTP-Server zu aktivieren und konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie NTP Synchronisierung:

   ```
   hostname (config) # ntp enable
   ```

3. Legen Sie den primären NTP-Server fest:

   ```
   hostname (config) # ntp server <server>
   ```

   wobei `<server>` die IPv4 oder IPv6-Adresse oder der Hostname des NTP Servers ist.

4. Wiederholen Sie den vorherigen Schritt für den sekundären NTP-Server und alle weiteren NTP-Server.

**Um die NTP-Version zu ändern:**

1. Legen Sie die Version fest:

   ```
   hostname (config) # ntp
   ```

2. Um die Version auf einem NTP-Server zu ändern:

   ```
   hostname (config) ntp server <server> version <version>
   ```

   wobei `<server>` die IPv4- oder IPv6-Adresse oder der Hostname des NTP-Servers und `<version>` entweder **3** oder **4** ist.

3. Um die Version auf einem NTP-Peer zu ändern:

   ```
   hostname (config) ntp peer <peer> version <version>
   ```

   wobei `<peer>` die IPv4 oder IPv6-Adresse oder der Hostname des NTP-Peer und `<version>` entweder **3** oder **4** ist.

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um NTP zu deaktivieren:**

1. Deaktivieren Sie NTP-Synchronisierung:

   ```
   hostname (config) # ntp disable
   ```

   *oder*

   ```
   hostname (config) # no ntp enable
   ```

2. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um die Systemzeit mit einem bestimmten NTP-Server einmal zu synchronisieren:**

1. Synchronisieren Sie die Systemzeit:

   ```
   hostname (config) # ntpdate <server>
   ```

   wobei `<server>` die IPv4 oder IPv6-Adresse oder der Hostname des NTP-Servers ist, mit dem synchronisiert werden soll.

2. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um den aktuellen NTP-Laufzeitstatus und Konfiguration anzuzeigen:**

1. Gehen Sie auf den CLI Standardmodus.
2. Zeigen Sie die Information an:

   ```
   hostname > show ntp
   ```

**Um die NTP-Server und ihre Einstellungen anzuzeigen:**

1. Gehen Sie auf den CLI Standardmodus.
2. Zeigen Sie die Information an:

   ```
   hostname > show ntp configured
   ```

## Beispiele

Im folgenden Beispiel werden zwei NTP-Server und ein NTP-Peer konfiguriert.

```
hostname (config) # ntp server 0.acme.pool.ntp.org
hostname (config) # ntp server 1.acme.pool.ntp.org
hostname (config) # ntp peer 5.acme.pool.ntp.org
hostname (config) # show ntp configured
NTP enabled: yes
NTP Authentication enabled: yes
NTP peer 5.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: none
NTP server 0.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: none
NTP server 1.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: none
```

Im folgenden Beispiel wird NTP-Synchronisation auf dem System deaktiviert.

```
hostname (config) # no ntp enable
hostname (config) # show ntp configured
NTP enabled: no
NTP Authentication enabled: yes
No NTP peers configured.
NTP server 0.acme.pool.ntp.org
  Enabled: yes
  ...
```

```
hostname (config) # show ntp
NTP is administratively disabled.
NTP Authentication is administratively enabled.
Clock is unsynchronized.
No NTP associations present.
```

Im folgenden Beispiel wird NTP vorübergehend auf dem "3.acme.pool.ntp.org" Server deaktiviert.

```
hostname (config) # ntp server 3.acme.pool.ntp.org disable
hostname (config) # show ntp configured
NTP enabled: yes
NTP Authentication enabled: yes
No NTP peers configured.
NTP server 0.acme.pool.ntp.org
  Enabled: yes
  ...
NTP server 3.acme.pool.ntp.org
  Enabled: no
  ...
```

Im folgenden Beispiel wird der "2.acme.pool.ntp.org" NTP Server entfernt.

```
hostname (config) # no ntp server 2.acme.pool.ntp.org
```

Im folgenden Beispiel wird die Systemuhr mit dem NTP-Server synchronisiert.

```
hostname (config) # ntpdate 0.acme.pool.ntp.org
 adjust time server 192.168.120.23 offset -0.023716 sec
```

Im folgenden Beispiel wird die NTP Version auf dem "3.acme.pool.ntp.org" Server auf Version 3 geändert.

```
hostname (config) # ntp server 3.acme.pool.ntp.org version 3
hostname (config) # show ntp configured
NTP enabled: yes
NTP Authentication enabled: yes
No NTP peers configured.
...
NTP server 3.acme.pool.ntp.org
  Enabled: yes
  NTP version: 3
  Key: none
```

Das folgende Beispiel zeigt den aktuellen NTP-Laufzeitstatus und Konfiguration an.

```
hostname > show ntp
NTP is administratively enabled.
NTP Authentication is administratively enabled.
Clock is synchronized. Reference: 10.255.34.6  Offset: 1.713 ms.
Active servers and peers:
                                                          Poll    Last
             Conf                      Offset   Ref       Interv  Resp
Address      Type  Status     Stratum (msec)   Clock     (sec)   (sec)
=========================================================================
192.168.1.1  n/a   candidat (+)   2   -0.233   10.2.3.4     64     60
10.2.3.4     n/a   outlyer  (-)   2   12.069   192.168.2.2  64     50
172.16.4.5   n/a   candidat (+)   2   -0.958   10.5.6.7     64     50
10.255.34.6  n/a   sys.peer (*)   2   1.713    172.16.3.4   64     45
```

Das folgende Beispiel zeigt die konfigurierten NTP-Server und ihre Einstellungen an:

```
hostname > show ntp configured
NTP enabled: yes
```

```
NTP Authentication enabled: yes
No NTP peers configured.
NTP server 0.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
NTP server 1.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
NTP server 2.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
NTP server 3.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
```

# NTP Authentifizierung mit Hilfe der CLI konfigurieren

In diesem Thema wird beschrieben, wie die NTP-Authentifizierung mit Hilfe der CLI konfiguriert wird.

## NTP Authentifizierung aktivieren und Schlüssel konfigurieren

Führen Sie die Aufgaben in diesem Abschnitt in der angezeigten Reihenfolge aus, um NTP Authentifizierung zu konfigurieren.

**Besorgen Sie die Authentifizierungsschlüssel vom NTP Server:**

1. Auf dem NTP Server ordnen Sie eine Schlüssel-ID von 1-16 einem MD5 oder SHA1 Hashwert zu.
2. Wiederholen Sie den vorherigen Schritt für zusätzliche Schlüssel-ID/Wertpaare.
3. Kopieren Sie die Schlüssel-ID/Wertpaare und fügen Sie sie ein, so dass sie auf später in diesem Vorgang auf der Appliance konfiguriert werden können.

**Aktivieren Sie NTP und NTP Authentifizierung:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie den aktuellen Status an:

   ```
   hostname (config) # show ntp configured
   ```

3. Wenn `NTP enabled: no` in der Befehlsausgabe erscheint, aktivieren Sie NTP.

   ```
   hostname (config) # ntp enable
   ```

4. Wenn `NTP Authentication enabled: no` in der Befehlsausgabe erscheint, aktivieren Sie NTP Authentifizierung.

   ```
   hostname (config) # ntp authentication enable
   ```

**Definieren Sie die Authentifizierungsschlüssel:**

1. Verwenden Sie den folgenden Befehl, um die Schlüssel-ID und den Hashwert, den Sie vom NTP Server erhalten haben zu konfigurieren:

   ```
   hostname (config) # ntp authentication key <number> hash <type> <value>
   ```

   wobei:

   - <number> ein Integer von **1–16**
   - <type> ist **md5** oder
   - <value> ist der Hashwert

2. Wiederholen Sie den vorherigen Schritt für jeden Schlüssel, den Sie definieren möchten.
3. Zeigen Sie die konfigurierten Schlüssel an.

   ```
   hostname (config) # show ntp authentication configured
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Weisen Sie die Schlüssel den NTP Servern zu:**

1. Um einem NTP Server einen Schlüssel zuzuweisen, verwenden Sie den `ntp server <server> authentication key <number>` Befehl, wobei <server> die IP-Adresse oder der Hostname des NTP Servers und <number> die Ganzzahl ist, die Sie dem Schlüssel in der vorherigen Aufgabe zugewiesen haben.

   Das folgende Beispiel weist Hashschlüssel 1 dem NTP Server 0.acme.pool.ntp.org zu:

   ```
   hostname (config) # ntp server 0.acme.pool.ntp.org authentication key 1
   ```

2. Wiederholen Sie den vorherigen Schritt für jeden Schlüssel, den Sie definieren möchten.
3. Zeigen Sie die zugewiesenen Schlüssel an:

   ```
   hostname (config) # show ntp configured
   ```

4. Überprüfen Sie, ob die Schüssel gültig sind:

   ```
   hostname (config) # show ntp authentication
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## NTP Authentifizierung deaktivieren und Schlüssel entfernen

Sie können einen Authentifizierungsschlüssel nicht vom System löschen, wenn er einem NTP Server zugeordnet ist. Wenn ein Schlüssel einem NTP Server zugeordnet ist, müssen

Sie NTP Authentifizierung auf diesem Server deaktivieren, bevor Sie den Schlüssel löschen können.

**Um NTP Authentifizierung auf dem System zu deaktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie die NTP Authentifizierung:

   ```
   hostname (config) # no ntp authentication
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um NTP Authentifizierung auf einem bestimmten Server zu deaktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um NTP-Authentifizierung mit einem bestimmten NTP Server zu deaktivieren, verwenden Sie den `no ntp server <server> authentication` Befehl, wobei `<server>` der Hostname oder IP-Adresse des NTP-Servers ist.

   Im folgenden Beispiel wird NTP Authentifizierung durch den NTP Server mit dem Hostnamen 1.acme.pool.ntp.org deaktiviert:

   ```
   hostname (config) # no ntp server 1.acme.pool.ntp.org authentication
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um einen NTP Authentifizierungsschlüssel zu löschen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um einen Schlüssel zu löschen, verwenden Sie den `no ntp authentication key <number>` Befehl, wobei `<number>` die Schlüssel-ID ist.

   ```
   hostname (config) # no ntp authentication key 1
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiele

Das folgende Beispiel zeigt die aktuelle Konfiguration.

```
hostname (config) # show ntp configured
NTP enabled: yes
NTP Authentication enabled: yes
```

```
No NTP peers configured.
NTP server 0.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: none
NTP server 1.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: none
NTP server 2.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: none
```

Das folgende Beispiel definiert zwei Authentifizierungsschlüssel und weist jedem einem NTP Server zu.

```
hostname (config) # ntp authentication key 1 hash md5
153ffa51cc765fb257e384e8e6aec8fe

hostname (config) # ntp server 0.acme.pool.ntp.org key 1

hostname (config) # ntp authentication key 2 hash sha1
27a048b642be47d50a9c38427495945429597d91

hostname (config) # ntp server 1.acme.pool.ntp.org key 2

hostname (config) # show ntp configured
NTP enabled: yes
NTP Authentication enabled: yes
No NTP peers configured.
NTP server 0.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: 1
NTP server 1.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: 2
NTP server 2.acme.pool.ntp.org
  Enabled: yes
  NTP version: 4
  Key: none

hostname (config) # show ntp authentication configured
NTP enabled: yes
NTP Authentication enabled: yes
NTP Key Number 1
  Type: md5
  Key: 153ffa51cc765fb257e384e8e6aec8fe
NTP Key Number 2
  Type: sha1
  Key: 27a048b642be47d50a9c38427495945429597d91

hostname (config) # show ntp authentication
NTP is administratively enabled.
NTP authentication is administratively enabled.
Active servers and peers:

Address           auth      keyid
==================================
172.16.2.3        ok         1
10.30.4.3         ok         2
192.168.10.12     none       none
```

Das folgende Beispiel deaktiviert NTP Authentifizierung auf dem 1.acme.pool.ntp.org Server und löscht dann den Schlüssel von dem System, den er benutzt hat.

```
hostname (config) # no ntp server 1.acme.pool.ntp.org authentication
hostname (config) # no ntp authentication key 2
```

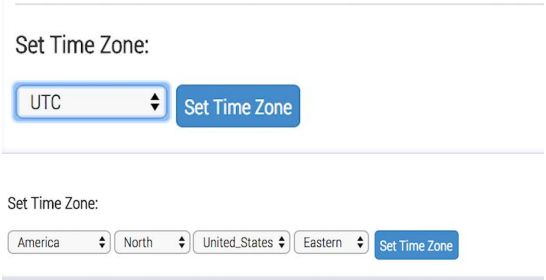
# Konfiguration der Zeitzone

Sie müssen die Zeitzone auf Ihrer Network Security Appliance einstellen, gleichgültig ob Sie das Datum und die Uhrzeit manuell konfigurieren oder mit einem NTP Server synchronisieren.

- Das Datum und die Uhrzeit mit Hilfe der Web-UI einstellen auf Seite 228
- Das Datum und die Uhrzeit mit Hilfe der CLI einstellen auf Seite 228

## Die Zeitzone mit Hilfe der Web-UI einstellen

Verwenden Sie den unteren Abschnitt der **Date and Time Settings** Seite, um die Zeitzone für Ihre Appliance einzustellen.




## Voraussetzungen

- Admin Zugriff

**Um die Zeitzone einzustellen:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Date and Time**.
3. Wählen Sie die Zeitzone von der Dropdown-Liste.
4. Wenn vorhanden, wählen Sie Optionen von anderen Dropdown-Listen.
5. Klicken Sie auf **Set Time Zone**.

# Die Zeitzone mit Hilfe der CLI einstellen

Verwenden Sie die CLI Befehle in diesem Thema, um die Zeitzone auf Ihrer Network Security Appliance einzustellen.

# Voraussetzungen

- Admin Zugriff

**Um die Zeitzone einzustellen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um die Zeitzone festzulegen, verwenden Sie den `clock timezone <timezone>` Befehl.

   Beispielsweise stellen die folgenden Befehle die Zeitzone auf Pacific Standard Time ein:

   ```
   hostname (config) # clock timezone UTC-offset UTC+8
   hostname (config) # clock timezone America North United_States Pacific
   ```

   **HINWEIS:** Die Zeitzone dient zu Anzeigezwecken und sollte mit Einstellungen für andere Sicherheitsgeräte übereinstimmen.

3. Stellen Sie die Standardzeitzone wieder hier:

   ```
   hostname (config) # no clock timezone
   ```

4. Zeigen Sie die konfigurierten Einstellungen für die Uhrzeit und das Datum an:

   ```
   hostname (config) # show clock
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiele

**Uhrzeit und Datum mit Hilfe der North America Central Daylight Timezone einstellen**

```
hostname # show clock
Time:        16:39:35
Date:        2014/06/25
Time zone:   America North United_States Central
             (US/Central)
UFC offset: -0500 (UTC minus 5 hours)
```

**Uhrzeit und Datum mit Hilfe der Standardzeitzone einstellen**

```
hostname # show clock
Time:         21:40:37
Date:         2014/06/25
```

```
Time zone:    UTC
              (Etc/UTC)
UTC offset:   same as UTC
```

# Die Systemuhr mit DTI-Serverzeit mit Hilfe der CLI synchronisieren

Die Systemzeit sollte mit der DTI-Serverzeit so weit wie möglich übereinstimmen. Dies ist für Funktionen wie den Lizenzaktualisierungsservice nötig, in dem Lizenzen vom DTI-Server heruntergeladen und auf der Network Security Appliance installiert werden.

**WICHTIG!** Um Zeitlücken zu vermeiden, die die Gültigkeit Ihrer Lizenz beeinträchtigen könnten, empfiehlt FireEye, dass Sie diese Synchronisierung ausführen, bevor Sie die Funktion aktivieren.

Der `fenet time sync` CLI Befehl ruft die Zeit (in UTC) vom DTI Server ab und synchronisiert dann die Systemuhr damit. Dieser Befehl ist besonders nützlich, wenn Sie keine NTP Server zum Synchronisieren Ihrer Systemuhr verwenden.

**WICHTIG!** Diese Aktion synchronisiert die Systemuhr ein einziges Mal mit dem DTI-Server. Die Systemzeitzone wird nicht geändert.

## Voraussetzungen

- Admin Zugriff

**Um die Systemuhr auf die DTI-Serveruhr zu synchronisieren:**

1. Wechseln Sie auf den CLIKonfigurationsmodus:

   ```
   hostname > enable hostname # configure terminal
   ```

2. Synchronisieren Sie die Uhren:

   ```
   hostname (config) # fenet time sync
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# KAPITEL 13: SSL-Entschlüsselung mit Geräten von Drittanbietern

Standardmäßig verarbeitet die Network Security Appliance Datenverkehr kollektiv, unabhängig von dem Port, der den Verkehr empfangen hat. Wenn die Network Security Appliance die entschlüsselten und verschlüsselten Versionen des gleichen Streams empfängt, werden sie möglicherweise nicht richtig gesammelt.

Sie müssen sicherstellen, dass verschiedene VLAN-Tags auf den ver- und entschlüsselten Streams konfiguriert sind.

Verwenden Sie den `policymgr session interface enable` Befehl auf den NX 300 Modellen, um entschlüsselten SSL-Verkehr auf einer anderen Schnittstelle zu empfangen.

Auf den NX 400 Modellen und höher müssen Sie auch ein VLAN-Tag zu entschlüsseltem Verkehr hinzufügen, der auf einem anderen Portpaar eingeht, damit die Appliance den Datenverkehr analysieren kann.

## Voraussetzungen

- Administratorzugriff auf die Network Security Appliance.

# SSL-Entschlüsselung mit Geräten von Drittanbietern mit Hilfe der CLI konfigurieren

Verwenden Sie die CLI Befehle in diesem Thema, um SSL-Entschlüsselung mit Geräten von Drittanbietern auf den NX 300 oder NX 400 Modellen zu konfigurieren.

**Um SSL-Entschlüsselung mit Geräten von Drittanbietern auf den NX 300 Modellen zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie eine andere Schnittstelle, um entschlüsselten SSL-Verkehr auf der Network Security Appliance zu empfangen.

   ```
   hostname (config) # policymgr session interface enable
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um SSL-Entschlüsselung mit Geräten von Drittanbietern auf den NX 400 Modellen zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Fügen Sie ein VLAN-Tag zu Datenverkehr hinzu, der auf einem anderen Portpaar eingeht.

   ```
   hostname (config) #_debug foxd config custom enable
   hostname (config) # _debug foxd config custom vlan enable
   ```

3. Aktivieren Sie eine andere Schnittstelle, um entschlüsselten SSL-Verkehr auf der Network Security Appliance zu empfangen.

   ```
   hostname (config) # policymgr session interface enable
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

5. Bestätigen Sie den Status der VLAN-Unterstützung.

   ```
   hostname (config) # _debug show foxd config custom
   foxd customized config: yes
     vlan support        : yes
     ........
   ```

6. Starten Sie die Network Content Processing Engine auf der Appliance neu.

   ```
   hostname (config) # pm process foxd restart
   ```

7. Starten Sie den Prozess neu, um Dateien für eine vollständige Analyse an die virtuelle Maschine (VM) zu senden.

   ```
   hostname (config) # pm process silverfish restart
   ```

# TEIL III: Administration

# KAPITEL 14: Netzwerk Administration

Dieses Thema behandelt die folgenden Informationen:



Zusätzliche Informationen über die Konfiguration von Schnittstellen finden Sie in der *CLI Befehlsreferenz*. Informationen über die Verbindung mit, Konfigurierung und Fehlerbehebung von Managed Defense finden Sie in der *Managed Defense Kurzanleitung*.

**WICHTIG:** Sie müssen die gleichen Linkeinstellungen an beiden Enden einer Netzwerkverbindung verwenden. Beispielsweise können Sie die Schnittstellengeschwindigkeit auf einem Ende nicht auf "auto" ändern, wenn auf dem anderen Ende eine manuelle Geschwindigkeit konfiguriert ist.

# Allgemeine Netzwerkkonfiguration

Die folgenden Abschnitte beschreiben allgemeine Einstellungen für Management-Schnittstellen und globale Netzwerkkonfiguration.

## Management-Schnittstelleneinstellungen

Die folgende Liste beschreibt die Konfigurationseinstellungen für die Management-Schnittstelle.

- **IP Version**—Die Appliance unterstützt Dual-Stack für Internet Protocol Version 4 (IPv4) und Version 6 (IPv6) auf der Management-Schnittstelle.
- **DHCP**—Dynamic Host Configuration Protocol (DHCP) verteilt dynamisch Netzwerkkonfigurationsparameter. Wenn DHCP auf der Management-Schnittstelle deaktiviert ist, müssen Sie die IP-Adresse, Subnetzmaske und Standard Gateway oder Next-Hop Gerät manuell konfigurieren.
- **IP Address**—Die IPv4 oder IPv6 Adresse der Management-Schnittstelle. Beide Adressentypen können konfiguriert werden. Die IPv4 Adresse sind standardmäßig aktiviert. Sie müssen die IPv6 Adresse ausdrücklich aktivieren.
- **Subnet Mask**—Die Netzwerkportion der IP-Adresse. Beispielsweise zeigt 255.255.255.0 an, das die ersten 24 Bits einer IPv4 Adresse für die Netzwerkportion einer Adresse verwendet werden.
- **Default Gateway**—Für eine IPv4 Adresse, die IPv4 Adresse des Standardrouters. Für eine IPv6 Adresse, die IPv6 Adresse des Standardrouters oder Next-Hop Gerätes.
- **Autoconf Enabled**—Wenn Stateless Address Autoconfiguration (SLAAC) aktiviert ist, wird der Schnittstelle automatisch eine IPv6 Adresse zugewiesen. Die Adresse basiert auf einem IPv6 Präfix, das von Router-Ankündigungen gelernt wurde, kombiniert mit einer auf der MAC Adresse der Schnittstelle basierenden Schnittstellen-ID.
- **Autoconf Route**—Wenn diese Funkion aktiviert ist, lernt das System eine Standardroute von der automatisch zugeordneten IPv6 Adresse.
- **Autoconf Privacy**—Wenn diese Funktion aktiviert ist, generiert das System zufällige Host IDs (sogenannte  Privacy Extensions), um die IPv6 Adresse zu erstellen. Dies bietet zusätzliche Sicherheit bei der Kommunikation mit Remote-Hosts.

## Globale Netzwerkeinstellungen

Die folgende Liste beschreibt globale Netzwerkkonfigurationseinstellungen.

- **DNS Servers**—Domain Name System (DNS) Server übersetzen Domainnamen in IP-Adressen für das Routing. Mindestens ein DNS-Server ist erforderlich. Optional können Sie einen sekundären DNS-Server konfigurieren, der benutzt wird, wenn der primäre Server nicht erreichbar ist oder einen Domainnamen nicht auflösen kann. Sie können eine Liste von DNS-Servern anzeigen, die für DNS-Auflösung in der Reihenfolge von oben nach unten durchsucht werden sollen. Nur aktive DNS-Server sind aufgeführt. Wenn keiner der DNS-Server den Domainnamen auflösen kann, wird ein Fehler angezeigt.
- **Domain Names**—Die Domainnamen des DNS-Servers lösen auf IP-Adressen auf. Sie können eine Liste von Domainnamen in der Reihenfolge von oben nach unten anzeigen.

- **Hostname**—Der Hostname der Appliance (zum Beispiel dc-01). Sie können die Domain einschließen (z.B. dc-01.acme.com).
- **IPv6**—Sie können IPv6 Routing auf dem System, der Management-Schnittstelle oder beiden aktivieren oder deaktivieren. IPv6 muss auf den Network Security Appliances aktiviert sein, die Mitglieder eines Network Security High Availability (HA) Paares sind. Es ist automatisch von der Central Management Appliance aktiviert, die das HA-Paar verwaltet.
- **VPN**—Sie können virtual private networking (VPN) auf dem System aktivieren oder deaktivieren. Wenn VPN aktiviert ist, kann sich die Appliance mit Managed Defense über das Internet mit Hilfe einer sicheren SSL-VPN Verbindung verbinden. VPN erfordert eine gültige MD_ACCESS Lizenz auf der Appliance. VPN erfordert IPv6 Routing, daher muss IPv6 auf dem System aktiviert sein, bevor Sie VPN aktivieren können. Weitere Informationen finden Sie in der *Managed Defense Kurzanleitung*.

# Voraussetzungen

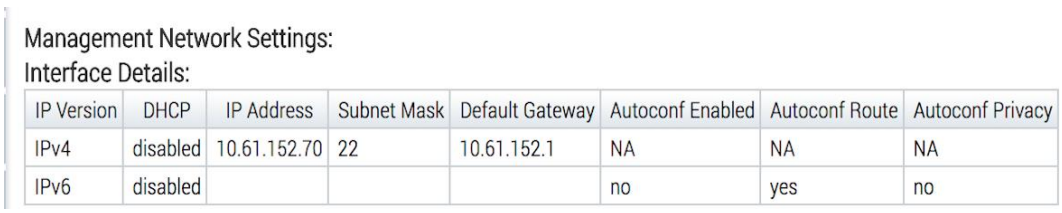
- Operator oder Admin Zugriff

# Allgemeine Netzwerkeinstellungen mit Hilfe der Web-UI konfigurieren

Verwenden Sie die **Network Settings** Seite, um allgemeine Netzwerkeinstellungen für die Network Security Appliance zu konfigurieren. Eine Beschreibung der Informationen und Einstellungen auf dieser Seite finden Sie unter Allgemeine Netzwerkkonfiguration auf Seite 247.

## Einstellungen für Management-Schnittstellendetails anzeigen

Verwenden Sie den **Interface Details** Abschnitt, um die Konfiguration der Management-Schnittstelle anzuzeigen. Dies ist ein schreibgeschützter Abschnitt. Die Management-Schnittstelle wird während der Erstkonfiguration konfiguriert und kann später mit Hilfe der CLI verändert werden. Details finden Sie unter Erstkonfiguration auf Seite 97 oder der *CLI Befehlsreferenz*.



Management Network Settings:
Interface Details:

| IP Version | DHCP | IP Address | Subnet Mask | Default Gateway | Autoconf Enabled | Autoconf Route | Autoconf Privacy |
|---|---|---|---|---|---|---|---|
| IPv4 | disabled | 10.61.152.70 | 22 | 10.61.152.1 | NA | NA | NA |
| IPv6 | disabled | | | | no | yes | no |

**Um die Konfiguration der Management-Schnittstelle anzuzeigen.**

1. Melden Sie sich auf der verwaltenden Central Management Web-UI an.
2. Klicken Sie auf das **Settings** Register.
3. Wählen Sie **Network** auf der Seitenleiste.
4. Finden Sie den **Interface Details** Abschnitt am Anfang der Seite.

## DNS Server konfigurieren

Verwenden Sie den **Configure DNS Server Addresses** Abschnitt, um DNS Serveradressen zu konfigurieren.


**Um DNS Server zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Wählen Sie **Network** auf der Seitenleiste.
3. Im **Configure DNS Server Addresses** Abschnitt geben Sie die IP-Adresse des primären DNS Servers ein.
4. (Optional) Geben Sie die IP-Adresse eines sekundären DNS Servers ein.
5. Klicken Sie auf **Apply**.

Die Reihenfolge, in der die DNS Server durchsucht werden, wird in der **DNS Resolution order** Liste angezeigt. Wenn kein Server aktiv ist, wird eine Fehlernachricht angezeigt.

## Domainnamen konfigurieren

Verwenden Sie den **Configure Domain Names** Abschnitt, um Domainnamen hinzuzufügen oder zu entfernen.

**Um Domainnamen hinzuzufügen:**

1. Klicken Sie auf das **Settings** Register.
2. Wählen Sie **Network** auf der Seitenleiste.
3. Im **Configure Domain Names** Abschnitt klicken Sie auf **Add Domain Name**.
4. Geben Sie einen Domainnamen ein und klicken Sie auf **Add**.


5. Wiederholen Sie die vorangegangenen Schritte, um zusätzliche Domainnamen zu konfigurieren.

Die Reihenfolge, in der die Domainnamen durchsucht werden, wird in der **Domain Names Resolution order** Liste angezeigt.

**Um Domainnamen zu entfernen:**

1. Finden Sie den Domainnamen, den Sie löschen wollen
2. Klicken Sie auf das Löschen (Papierkorb) Symbol in der **Delete** Spalte für jeden Domainnamen, den Sie entfernen wollen.
3. Klicken Sie auf **YES**.

   Der Domainname wird von der Konfiguration gelöscht.
4. Schließen Sie die Nachricht.

## IPv6 aktivieren

Verwenden Sie den **Configure IPv6** Abschnitt, um IPv6 Routing zu aktivieren oder deaktivieren. Sie können diesen Abschnitt auch verwenden, um IPV6 auf der SMTP Schnittstelle zu aktivieren und deaktivieren.

**Um IPv6 Routing zu aktivieren:**

1. Klicken Sie auf den **Settings** Tab.

2. Wählen Sie **Network** auf der Seitenleiste.
3. Aktivieren Sie IPv6:
    - Um IPv6 Routing auf dem System zu aktivieren, wählen Sie das **Global IPv6** Kontrollkästchen und klicken Sie dann auf **Apply**.
    - Um IPv6 auf der Management-Schnittstelle zu aktivieren, wählen Sie das **Management Interface IPv6** Kontrollkästchen und klicken Sie dann auf **Apply**.

**Um IPv6 Routing zu deaktivieren:**

1. Klicken Sie auf den **Settings** Tab.
2. Wählen Sie **Network** auf der Seitenleiste.
3. IPv6 deaktivieren:
    - Um IPv6 Routing auf dem System zu deaktivieren, löschen Sie das **Global IPv6** Kontrollkästchen und klicken Sie dann auf **Apply**.
    - Um IPv6 auf der Management-Schnittstelle zu deaktivieren, löschen Sie das **Management Interface IPv6** Kontrollkästchen und klicken Sie dann auf **Apply**.

## VPN aktivieren

Der **VPN Settings** Abschnitt wird unten auf der Seite angezeigt, wenn eine gültige MC_ ACCESS Lizenz installiert ist. Sie können VPN nur aktivieren, von IPv6 auf dem System aktiviert ist. Details finden Sie in der *Managed Defense Kurzanleitung*.

# Allgemeine Netzwerkeinstellungen mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Thema, um die Netzwerkeinstellungen manuell zu konfigurieren.

**Um allgemeine Netzwerkeinstellungen zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Um DHCP für die Schnittstelle zu deaktivieren:

   ```
   hostname (config) # no interface ether1 dhcp
   ```

   **HINWEIS:** Wenn Sie DHCP verwenden und keine Netzwerkverbindung für die Management-Schnittstelle vorhanden ist, gehen Sie folgendermaßen vor:

   a. Stellen Sie die Netzwerkverbindung wieder her.
   b. Deaktivieren Sie DHCP.
   c. Aktivieren Sie DHCP.

3. Stellen Sie die Schnittstellen IP-Adresse und Netzwerkmaske ein. Zum Beispiel:

   ```
   hostname (config) # interface ether1 ip address 1.1.1.1 255.240.0.0
   ```

4. Bestimmen Sie das Standard Gateway. Zum Beispiel:

   ```
   hostname (config) # ip default-gateway 1.1.1.2 ether1
   ```

5. Bestimmen Sie eine DNS Server. Zum Beispiel:

   ```
   hostname (config) # ip name-server 10.10.20.5
   ```

6. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Layer 3 Weiterleitung mit VRF-Instanzen

Virtuelles Routing und Weiterleitung (VRF) ermöglicht einem Layer 3 Networking-Gerät, mehrere Instanzen einer Routingtabelle gleichzeitig und unabhängig auszuführen. Auf unterstützten Network Security Appliances wird durch Aktivierung von Layer 3 Modus automatisch jedes Portpaar auf einem getrennten Netzwerk-Namespace mit dem Namen **VRF namespace** abgebildet. Die Gesamtzahl der Eingaben, die derzeit ausgeführt werden. Zusammengenommen umfassen ein VRF Namespace und die Routinginformationen, die Sie konfigurieren, eine **VRF Instanz**.

## Beschränkungen

Die folgenden Beschränkungen gelten für Layer 3 Weiterleitung mit VRF Instanzen:

- SSLi ist nicht unterstützt, während Layer 3 Modus aktiviert ist.
- IPv6 Routing ist für Schnittstellen in einer VRF Instanz nicht unterstützt.
- DHCP ist für Schnittstellen in einer VRF Instanz nicht unterstützt.
- Cross-VRF Routing ist nicht unterstützt.
- Cross-Pair Weiterleitung ist nicht unterstützt.
- Inline Weiterleitung ist auf das Portpaar beschränkt.

# Appliances, die VRF und Network Namespaces unterstützen

Layer 3 Weiterleitung mit Hilfe von VRF und Network Namespaces wird auf den folgenden Network Security Appliances unterstützt:

- NX 2500V / NX 2501V
- NX 2550V
- NX 4500V
- NX 6500V

A Network Security virtual appliance is an instance of a Network Security appliance system image and does not have an MVX engine. It functions as a sensor, submitting suspect objects to an MVX cluster for detonation and analysis. Informationen über die Bereitstellung und Arbeit mit virtuellen Appliances finden Sie im *FireEye Geräte- Deploymenthandbuch* auf dem FireEye Dokumentationsportal unter https://docs.fireeye.com/.

Eine Layer 3-fähige virtuelle Appliance auf einem EXSi Host, KVM Server oder Hyper-V Server arbeitet standardmäßig im Layer 2 Modus und Sie müssen einen CLI Befehl verwenden, um Layer 3 Modus ausdrücklich zu aktivieren, um Layer 3 Weiterleitung mit VRF Namespaces zu unterstützen.

Eine Layer 3-fähige virtuelle Appliance in einem Cloud-Deployment, einschließlich auf einer AWS oder Azure Instanz, arbeitet immer im Layer 3 Modus.

# Portpaare auf Netzwerk Namespaces abbilden

Wenn Sie Layer 3 Modus auf einer unterstützten Network Security virtuellen Appliance aktiviert haben, bildet die Appliance die Überwachungs-Portpaare (pether3 bis pether10) statisch auf fixierte Netzwerk Namespaces (vrfA, vrfB, vrfC und vrfD), **VRF Namespaces** genannt ab:

| Network Security Virtuelle Appliance Ports | Network Namespace | |
|---|---|---|
| | Layer 2 Modus | Layer 3 Modus |
| *Management-Ports* | | |
| ether1 | vrf0 | |
| pether2 | vrf0 | |
| *Überwachungsportpaare* | | |
| pether3, pether4 | vrf0 | vrfA |
| pether5, pether6 | vrf0 | vrfB |
| pether7, pether8 | vrf0 | vrfC |
| pether9, pether10 | vrf0 | vrfD |

Innerhalb eines VRF Namespace können Sie ein Standard Gateway und Routentabelle zum Weiterleiten von Paketen auf der Ausgangsschnittstelle konfigurieren. Standardmäßig befinden sich Ausgangsschnittstellen auf pether4, pether6, pether8 und pether 10. Sie können pether3, pether5, pether7 oder pether9 als Ausgangsschnittstelle konfigurieren.

# VRF-Instanzen für Layer 3 Weiterleitung konfigurieren

Dieser Vorgang beschreibt die Konfigurierung von VRF-Instanzen, um Layer 3 Weiterleitung zu unterstützen. In dem Beispiel wurde der Appliance Management Port ether1 bereits mit der Standard Gateway-Adresse 10.14.52.1 und statischen Route 10.14.52.0 /22 konfiguriert.

## Voraussetzungen

- Administrator oder Operator Zugriff auf die unterstützte Network Security Appliance
- Die Appliance arbeitet im Layer 3 Modus.
- Die Appliance ist im inline Modus bereitgestellt.
- Ein oder mehrere Überwachungsportpaare sind mit einem LAN-zugewandten Switch verbunden.

**Um VRF-Instanzen für Layer 3 Weiterleitung zu konfigurieren:**

1. Melden Sie sich auf der Appliance CLI an und gehen Sie auf den Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Wenn sich die Appliance auf einem EXSi-Host, KVM-Server oder Hyper-V-Server befindet, aktivieren Sie den Layer 3 Modus. (Wenn sich die Appliance in einem Cloud-Deployment befindet, ist der Layer 3 Modus immer aktiviert.)

   ```
   hostname (config) # policymgr layer3-mode enable
   hostname (config) # show policymgr layer3-mode status
   ```

   Um den Layer 3 Modus zu deaktivieren, verwenden Sie den `no policymgr layer3-mode enable` Befehl.

3. Bestätigen Sie, dass Überwachungsports auf VRF-Namespaces abgebildet sind. Die folgenden Befehle führen die VF Namespaces auf, was darauf hinweist, dass die Appliance im Layer 3 Modus läuft.

```
hostname (config) # ip default-gateway vrf
vrfA  vrfB  vrfC  vrfD

hostname (config) # ip route vrf
vrfA  vrfB  vrfC  vrfD

hostname (config) # show vrf config
 Netns:
  vrfA
  vrfB
  vrfC
  vrfD
```

Die folgenden Befehle zeigen an, dass pether3 und pether4 auf Netzwerk Namespace vrfA abgebildet sind. In diesem Beispiel wurden statische Routen noch nicht für vrfA konfiguriert.

```
hostname (config) # show interfaces pether3 brief
Interface pether3 status:
   Comment:
   Admin up:           yes
   Link up:            yes
   DHCP running:       no
   IP address:
   Netmask:
   IPv6 enabled:       no
   Speed:              10000Mb/s
   Duplex:             full
   Interface type:     ether
   Interface ifindex:  23
   Interface source:   physical
   Interface namespace:vrfA
   MTU:                1600
   HW address:         00:50:56:01:2F:A1

hostname (config) # show interfaces pether4 brief
Interface pether4 status:
   Comment:
   Admin up:           yes
   Link up:            yes
   DHCP running:       no
   IP address:
   Netmask:
   IPv6 enabled:       no
   Speed:              10000Mb/s
   Duplex:             full
   Interface type:     ether
   Interface ifindex:  24
   Interface source:   physical
   Interface namespace:vrfA
   MTU:                1600
   HW address:         00:50:56:01:2F:A2
```

4. Konfigurieren Sie ein Standard Gateway für jede mit einem LAN-zugewandten Switch verbundene VRF-Instanz. Verwenden Sie den `ip default-gateway vrf <netNamespace> <nextHop> [portName]` Befehl, wobei die Befehlszeilenparameter wie folgt lauten:

   `<netNamespace>`

   Der Netzwerk Namespace für die VRF-Instanz: vrfA, vrfB, vrfC oder vrfD

   `<nextHop>`

   Die IPv4 Adresse der next-Hop Schnittstelle.

   `<portName>`

   Der optionale Überwachungsportname (z.B. pether3).

   Wenn Sie keinen Überwachungsport festlegen, wird die von Ihnen bestimmte Standard Gateway-Adresse auf den der VRF-Instanz zugeordneten Standard Ausgangsport (pether4, pether6, pether8 oder pether10) eingestellt.

   Sie können den `no ip default-gateway vrf <netNamespace>` Befehl verwenden, um das Standard Gateway für eine VRF-Instanz zu löschen.

   In diesem Beispiel werden beide Arten von Befehlen (mit und ohne den optionalen `<portname>`) verwendet, um das Standard Gateway für vrfC und vrfD zu konfigurieren:

   ```
   hostname (config) # ip default-gateway vrf vrfC 192.168.225.3 hostname
   (config) # ip default-gateway vrf vrfD 192.168.227.5 pether9
   ```

   **HINWEIS:** Da der erste Befehl keinen vrfC Überwachungsport festlegt, wird die festgelegte Standard Gateway-Adresse für den Standard Ausgangsport pether8 konfiguriert. Da der zweite Befehl den vrfD Überwachungsport pether9 festlegt, wird pether 9 als die Ausgangs-Schnittstelle verwendet.

5. Erstellen Sie eine Liste der Standard Gateways, indem Sie den `show ip default-gateway [static]` Befehl verwenden.

   Dieses Beispiel zeigt die Standard Gateway-Adressen, die für vrfC und vrfD konfiguriert wurden.

   ```
   hostname (config) # show ip default-gateway static Configured default
   gateway: 10.14.52.1 192.168.225.3 (netns: vrfC) 192.168.227.5 (netns:
   vrfD)
   ```

   Dieses Beispiel zeigt, dass das für vrfD festgelegte Standard Gateway pether9 anstelle dem Standard Ausgangsport (pether10) zugeordnet wurde.

   ```
   hostname (config) # show ip default-gateway Active default gateways:
   192.168.225.3 (interface: pether8, netns: vrfC) 10.14.52.1 (interface:
   ether1) 192.168.227.5 (interface: pether9, netns: vrfD)
   ```

6. Konfigurieren Sie eine Routentabelle für jede mit einem LAN-zugewandten Switch verbundene VRF-Instanz. Um eine statische Route hinzuzufügen, verwenden Sie den `ip route vrf <netNamespace> <nextHop> [portName]` Befehl, wobei die Befehlszeilenparameter wie folgt lauten:

   `<netNamespace>`

   Der Netzwerk Namespace für die VRF-Instanz: vrfA, vrfB, vrfC oder vrfD

   `<nextHop>`

   Die IPv4-Adresse der Next-Hop Schnittstelle, im folgenden Format festgelegt:`<networkPrefix> {<netmask> | /<maskLength>}`

   Beispiel: `192.168.11.20 255.255.255.0`
   Beispiel: `192.168.11.20 /24`

   `<portName>`

   Der optionale Überwachungsportname (z.B. pether3).

   Wenn Sie keinen Überwachungsport festlegen, wird die von Ihnen festgelegte next-Hop Adresse als der der VRF-Instanz zugeordnete Standard Ausgangsport (pether4, pether6, pether8 oder pether10) eingestellt.

   Sie können den `no ip route vrf <netNamespace> <nextHop> [portName]` Befehl verwenden, um die festgelegt Route von einer VRF-Instanz zu entfernen.

   Dieses Beispiel illustriert beide Arten von Befehlen (mit und ohne den optionalen `<portname>`), die zum Hinzufügen von Routen zu vrfC und vrfD verwendet werden.

```
hostname (config) # ip route vrf vrfC 192.168.225.0 /24
hostname (config) # ip route vrf vrfD 10.2.7.20 /24 pether9
hostname (config) # ip route vrf vtfD 104.244.42.0 /24 pether9
hostname (config) # ip route vrf vtfD 192.168.227.0 /24 pether9
```

   **HINWEIS:** Da der erste Befehl keinen vrfC Überwachungsport festlegt, wird die festgelegte Route zum Standard Ausgangsport pether8 hinzugefügt. Da die anderen Befehle den vrfD Überwachungsport pether9 festlegen, wird pether9 als die Ausgangsschnittstelle verwendet.

7. Bestätigen Sie die statischen Routen für die VRF-Instanzen.

   Dieses Beispiel zeigt alle auf der Appliance konfigurierten statischen Routen an.

```
hostname (config) # show ip route static
Destination    Mask             Gateway        Interface  Table
default        0.0.0.0          10.14.52.1                main
Destination    Mask             Gateway        Interface  Table
default        0.0.0.0          192.168.225.3             main
default        0.0.0.0          192.168.227.5             main
10.2.7.20      255.255.255.255  192.168.227.2             main
104.244.42.0   255.255.255.0    192.168.227.2             main
```

   Dieses Beispiel zeigt alle auf der Appliance konfigurierten statischen Routen und Standard Gateways an.

```
hostname (config) # show ip route
Special routes inside name space
Destination    Mask             Gateway        Interface  Source     Netns  Table
default        0.0.0.0          192.168.225.3  pether8    static     vrfC   main
192.168.224.0  255.255.255.0    0.0.0.0        pether7    interface  vrfC   main
192.168.225.0  255.255.255.0    0.0.0.0        pether8    interface  vrfC   main
default        0.0.0.0          10.14.52.1     ether1     static     vrf0   main
10.14.52.0     255.255.252.0    0.0.0.0        ether1     interface  vrf0   main
default        0.0.0.0          192.168.227.5  pether9    static     vrfD   main
10.2.7.20      255.255.255.255  192.168.227.2  pether9    static     vrfD   main
104.244.42.0   255.255.255.0    192.168.227.2  pether9    static     vrfD   main
192.168.226.0  255.255.255.0    0.0.0.0        pether10   interface  vrfD   main
192.168.227.0  255.255.255.0    0.0.0.0        pether9    interface  vrfD   main
192.168.222.0  255.255.255.0    0.0.0.0        pether5    interface  vrfB   main
192.168.223.0  255.255.255.0    0.0.0.0        pether6    interface  vrfB   main
192.168.220.0  255.255.255.0    0.0.0.0        pether3    interface  vrfA   main
192.168.221.0  255.255.255.0    0.0.0.0        pether4    interface  vrfA   main
```

8. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

# IP-Filterung

IP Filterung gestattet Ihnen, Regeln für die Filterung von IP Paketen zu verwalten, die auf der Appliance durch ihre Management-Schnittstellen ein- oder abgehen. IP-Filterung unterstützt IPv4 und IPv6 durch seperate, aber weitgehend identische Sätze von CLI Befehlen. Weitere Informationen finden Sie unter *CLI Befehlsreferenz* .

IP-Filterung ist standardmäßig sowohl für IPv4 als auch IPv6 deaktiviert. Allerdings könnte bei einigen Appliances IP-Filterung durch vorhandene Komponenten auf dem System aktiviert sein, die in der `show ip filter` Befehlausgabe noch immer angezeigt werden.

**HINWEIS:** Die Aktivierung von IPv6 Filterung hat keine Auswirkung, es sei denn, IPv6 ist aktiviert.

# Von IP-Filterungsregeln unterstützte Schnittstellen

Wenn Sie IP-Filterung benutzen, können Schnittstellen in drei Sätze gruppiert werden:

1. **Management-Schnittstellen**: ether*. Für diese Schnittstellen gelten IP-Filterungsregeln. Einige Appliance, z.B. die Network Security Appliance, haben eine Management-Schnittstelle, ether1. Auf der Central Management Plattform und Endpoint Security Appliance gibt es mehrere Management-Schnittstellen mit den Namen ether1, ether2 u.s.w.

   Wenn für eine Regel keine Schnittstelle festgelegt ist, ist der Standard "ether+", was bei der IP-Filterung mit jeder Schnittstelle übereinstimmt, die mit "ether" beginnt.
2. **Datenports**: pether* . Diese Schnittstellen können keine IP-Filterungsregeln haben.
3. **Andere Schnittstellen**: lo, tun0 (wenn ein VPN aktiviert ist). Diese Schnittstellen können automatisch von dem System installierte IP-Filterungsregeln haben. Die Regeln für diese Schnittstellen können nicht konfiguriert werden.

# IP-Filterungsregeln anzeigen

Wenn Sie eine Liste von IP-Filterungsregeln mit Hilfe des `show ip filter` oder `show ipv6 filter` Befehls anzeigen, werden Regeln, die für Management-Schnittstellen wie oben beschrieben hinzugefügt wurden sowie Regeln, die automatisch vom System hinzugefügt wurden, gemeinsam in der Reihenfolge aufgeführt, in der sie angewendet werden.

Wenn Sie auf dem VPN sind, sollten Sie den `show ipv6 filter` Befehl verwenden, der detaillierte Informationen über die Firewall Regeln anzeigt. Der nachfolgend beschriebene `show ipv6 filter configured` Befehl enthält diese Informationen nicht.

Regeln, die manuell konfiguriert sind, werden mit Nummern in der linken Spalte angezeigt, die den Regelnummern entsprechen, die in der `show ip filter configured` und `show ipv6 filter configured` Befehlsausgabe sichtbar sind. Regeln, die automatisch von dem System hinzugefügt werden, haben keine Nummern.

Die Standard Filterkonfiguration für die INPUT und OUTPUT Ketten ist eine ACCEPT Regel mit einer DROP Richtlinie für allen Datenverkehr auf allen Schnittstellen, deren Namen mit "ether" beginnen. Die Standard Konfiguration für FORWARD ist einfach eine DROP Richtlinie ohne Regeln, da Network Security Appliance keine Pakete weiterleiten. Die Aktivierung von IP-Filterung hat keine Auswirkung auf die Funktion Ihres Netzwerks bis Sie neue IP Filterregeln erstellen.

Wenn IP-Filterung aktiviert ist, wird eine zusätzliche Regel automatisch nach allen konfigurierten Regeln vom System hinzugefügt. Diese Regel besteht darin, den gesamten eingehenden und ausgehenden Datenverkehr auf der Loopback "lo" Schnittstelle zu ACCEPT (akzeptieren). Das System benötigt die Loopback Schnittstelle für interne Zwecke.

**HINWEIS:** Wenn Sie Managed Defense aktivieren, werden IP-Filter automatisch aktiviert. Details finden Sie in der *Managed Defense Kurzanleitung*.

**VORSICHT:** Diese Funktion wirkt sich auf die Integration mit Drittanbieterdiensten aus. Verwenden Sie Vorsicht und guten Menschenverstand, wenn Sie IP-Filterungsregeln hinzufügen. Wenn die Regeln nicht ordnungsgemäß eingestellt sind, kann dies zu Problemen führen, wie z.B. Unterbrechung des Datenverkehrs. Zum Beispiel könnte das Hinzufügen von DROP Regeln in der OUTPUT Kette für ether1 oder ether + remote Syslog beeinträchtigen. oder das Hinzufügen von DROP Regeln in der INPUT Kette könnte den externen Zugriff auf Systemdienste wie SNMP stören.

## Voraussetzungen

- Operator oder Admin Zugriff, um IP-Filterung zu konfigurieren
- Monitor, Operator oder Admin Zugriff, um IP-Filterung anzuzeigen

## IP-Filterung mit Hilfe der CLI aktivieren

Verwenden Sie die Befehle in diesem Abschnitt, um IP-Filterung zu aktivieren.

**HINWEISE:**

- Die Standardregeln platzieren keine Einschränkungen auf ein- und ausgehende Pakete auf ether* Schnittstellen. Sie können Regeln mit Hilfe der CLI hinzufügen. Achten Sie darauf. den Zugriff auf benötigte Netzwerkdienste nicht zu blockieren.
- IP-Filterung ist automatisch aktiviert, wenn Sie eine Verbindung mit Managed Defense herstellen, wie in der *Managed Defense Kurzanleitung* beschrieben.

**Um die aktiven Regeln anzuzeigen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:
   ```
   hostname > enable
   ```
2. Zeigen Sie die Regeln an:
   ```
   hostname # show ip filter
   hostname # show ipv6 filter
   ```

**Um IP-Filterung zu aktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.
   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie IP-Filterung:
   ```
   hostname (config) # ip filter enable
   hostname (config) # ipv6 filter enable
   ```
3. Speichern Sie Ihre Änderungen:
   ```
   hostname (config) # write memory
   ```

# Einstellungen für einen HTTP-Proxyserver konfigurieren

Die Konfiguration eines HTTP-Proxyservers auf Ihrer Appliances umfasst die folgenden Aufgaben:

- Konfiguration des Hostnamen oder der IP-Adresse für den Proxyserver.
- Konfiguration des Ports für Client-Kommunikation, wenn Sie den Standardport (Port 8080) nicht annehmen wollen.
- (*Optional*) Aktivieren der Basis Authentifizierung auf dem Proxyserver.
- (*Optional*) Legen Sie eine User-Agentzeichenfolge fest, die in HTTP-Anfragen enthalten ist.
- Aktivieren des Proxyservers.

Sie können dann Ihre Appliance folgendermaßen konfigurieren:

- Anfragen für einen oder mehrere DTI Services über den Proxyserver senden, wie unter Ein HTTP-Proxys für DTI-Serviceanfragen auf Seite 169 beschrieben.
- Senden Sie Anfragen an Helix über den Proxyserver, wie im *Helix Integrationshandbuch* beschrieben.
- Ereignisbenachrichtigungen durch den Proxyserver senden, wie in der *Bedienungsanleitung* oder dem *Administrationshandbuch* für die Appliance beschrieben.

## Voraussetzungen

- Admin Zugriff
- Der HTTP-Proxyserver ist in Ihrem Netzwerk bereitgestellt.

## Einstellung für HTTP-Proxyserver mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Abschnitt, um einen HTTP-Proxyserver auf einer Appliance zu konfigurieren und zu aktivieren.

**Um einen HTTP-Proxyserver zu konfigurieren und zu aktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Konfigurieren Sie den Hostnamen oder die IP-Adresse des Proxyservers und den Port (wenn Sie den Standardport 8080 nicht verwenden möchten):

   ```
   hostname (config) # fenet proxy host <hostname or IP address>[:<port>]
   ```

3. *Optional*:Legen Sie die Berechtigungen für die Basis-Authentifizierung fest:

   - Legen Sie den User fest:

     ```
     hostname (config) # fenet proxy auth basic user <username>
     ```

   - Legen Sie das Passwort fest:

     ```
     hostname (config) # fenet proxy auth basic password <password>
     ```

4. *Optional*: Legen Sie eine User-Agentzeichenfolge fest:

   ```
   hostname (config) # fenet proxy user-agent <string>
   ```

5. Aktivieren Sie den Proxyserver:

   ```
   hostname (config) # fenet proxy enable
   ```

6. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show fenet
   ```

7. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**HINWEIS:** Der `show fenet status` Befehl zeigt auch die HTTP-Proxyeinstellungen an, aber nicht, ob der Proxyserver aktiviert oder deaktiviert ist. Die `show fenet` Befehlsausgabe schließt "`disabled`" ein oder aus, um den Status anzuzeigen.

## Beispiel:

Im folgenden Beispiel wird ein HTTP-Proxyserver mit Basis-Authentifizierungsberechtigungen konfiguriert.

```
hostname (config) # fenet proxy host 192.168.2.3
hostname (config) # fenet proxy auth basic user bsmith
hostname (config) # fenet proxy auth basic password abcd6789
hostname (config) # fenet proxy enable
hostname (config) # show fenet

DTI CLIENT CONFIGURATION:
  ...
  Http proxy       : bsmith@192.168.2.3:8080 (user agent:)
  ...
```

```
hostname (config) # show fenet status
...
HTTP Proxy:

    Address       : 192.168.2.3:8080
    Username      : bsmith
    User-agent    :
    ...
```

# Einstellungen für den HTTP-Proxyserver mit Hilfe der CLI deaktivieren

Verwenden Sie die Befehle in diesem Abschnitt, umeinen HTTP-Proxyserver zu deaktivieren oder seine Konfigurationseinstellungen zu entfernen.

**Um einen HTTP-Proxyserver zu deaktivieren oder seine Konfigurationseinstellungen zu entfernen:**

- Um einen HTTP-Server zu deaktivieren:

  ```
  hostname (config) # no fenet proxy enable
  ```

- Um den HTTP-Proxyserver zu entfernen:

  ```
  hostname (config) # no fenet proxy
  ```

- Um den Basis-Authentifizierungsuser zu entfernen:

  ```
  hostname (config) # no fenet proxy auth basic user
  ```

- Um das Basis Authentifizierungspasswort zu entfernen:

  ```
  hostname (config) # no fenet proxy auth basic password
  ```

- Um die User-Agentzeichenfolge zu entfernen:

  ```
  hostname (config) # no fenet proxy user-agent
  ```

## Beispiel:

Im folgenden Beispiel wird ein HTTP-Proxyserver deaktiviert.

```
hostname (config) # no fenet proxy enable
hostname (config) # show fenet

DTI CLIENT CONFIGURATION:
  ...
  Http proxy          : bsmith@192.168.2.3:8080 (user agent:) Disabled
  ...
```

# Eine andere Management-Schnittstelle definieren

Die Management-Schnittstelle wird für remote Zugriff auf die Web-UI und CLI benutzt, sowie für anderen Managementverkehr (z.B. NTP, SNMP und syslog). Die Standard Management-Schnittstelle ist ether1. Sie können eine andere Schnittstelle (z.B. ether2) für remote Zugriff auf die Web-UI und CLI definieren. Gründe dafür können sein:

- Eine private IP-Adresse wird für ether1 definiert, so dass remote Benutzer sie nicht erreichen können. Sie könnten ether1 für die Verbindung zwischen einer Central Management Appliance und ihrer verwalteten Appliance verwenden und eine zugängliche IP-Adresse für die ether2 Schnittstelle definieren.
- Sie sollten ein Netzwerk für Web-UI und CLI Verkehr und ein anderes Netzwerk für anderen Netzwerkverkehr verwenden.

Beschränkungen für die Listen-Schnittstelle sind standardmäßig auf der Appliance aktiviert. Dies bedeutet, dass nur Schnittstellen, die den folgenden Kriterien entsprechen, HTTP/HTTPS Anfragen (für Web-UI Zugriff) und SSH Verbindungen (für CLI Zugriff) akzeptieren können.

- Die Schnittstelle muss in der Listen Schnittstellenliste enthalten sein. Standardmäßig ist nur ether1 auf dieser Liste.
- Die Schnittstelle muss den unter Voraussetzungen auf der nächsten Seite aufgeführten Zugangsbedingungen entsprechen.

Das System verhindert, dass remote Benutzer aus dem System ausgeschlossen werden, wenn die Kriterien von mindestens einer Schnittstelle nicht erfüllt werden. Wenn keine Schnittstelle die Kriterien erfüllt, werden Beschränkungen für die Listen-Schnittstelle nicht durchgesetzt und all brauchbaren Schnittstellen sind geöffnet und können HTTP/HTTPS Anfragen und SSH Verbindungen akzeptieren.

**Beispiele**

- Die Appliance verwendet die Standard Konfiguration (Beschränkungen der Listen Schnittstelle sind aktiviert und ether1 ist auf der Listen Schnittstellenliste). Sie konfigurieren eine statische IPv4 oder IPv6 Adresse für die ether1 und ether2 Schnittstellen und rufen diese auf. Remote Benutzer haben keinen Zugriff auf das System über ether2, weil es nicht zur Listen Schnittstellenliste hinzugefügt wurde. Sie fahren die ether1 Schnittstelle dann herunter und ether 2 (die einzige funktionsfähige Schnittstelle) wird sofort zugänglich, weil die Beschränkungen der Listen Schnittstelle nicht länger erzwungen werden.
- Sie fügen ether2 zu der Listen Schnittstellenliste hinzu, aber sowohl ether1 als auch ether2 verwenden DHCP, um IPv4 Adressen abzurufen oder DHCPv6 für IPv6 Adressen. Da keine der Schnittstellen den in Voraussetzungen auf der nächsten

Seite aufgeführten IPv4 oder IPv6 statischen Adressanforderungen entspricht, werden die Einschränkungen der Listen-Schnittstelle nicht länger durchgesetzt. Alle funktionstüchtigen Schnittstellen, einschließlich ether1 und ether2, werden zugänglich.

## Voraussetzungen

- Operator oder Admin Zugriff
- Der entsprechende Management-Port ist mit dem  Netzwerk Switch oder Router verbunden.
- Zugangsbedingungen:
  - Die Schnittstelle existiert und läuft.
  - DHCP und zeroconf sind auf der Schnittstelle deaktiviert (für IPv4) oder IPv6 ist sowohl auf der Schnittstelle als auch dem System aktiviert (für IPv6).
  - Die Schnittstelle besitzt eine IPv4 oder IPv6 Adresse:
    - *IPv4*: Mindestens eine statische nonzero IPv4 Adresse ist für die Zuweisung an die Schnittstelle verfügbar.
    - *IPv6*: Eine statische IPv6 Adresse kann der Schnittstelle zugewiesen werden oder die Adresse kann dynamisch durch Stateless Address Autoconfiguration (SLAAC oder DHCPv6 erlangt werden.

## Eine andere Management-Schnittstelle mit Hilfe der CLI definieren

Verwenden Sie die Befehle in diesem Abschnitt auf einer Appliance, die Listen-Schnittstellenbeschränkungen erzwingt, um eine andere Management-Schnittstelle als ether1 zu definieren und sie zur Listen-Schnittstellenliste hinzuzufügen, so dass sie HTTP/HTTPS Anfragen und SSH Verbindungen akzeptieren kann.

**Um eine andere Management-Schnittstelle zu definieren:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Weisen Sie der anderen Schnittstelle eine IP-Adresse zu;

   ```
   hostname (config) # interface <interfaceName> ip address <ipAddress>
   <mask>
   ```

   wobei:

   - `<ipAddress>` die IPv4 oder IPv6Adresse der Schnittstelle ist.
   - `<mask>` die IPv4 Maskenlänge ist, der ein Slash vorangestellt ist (z.B. `/24`) oder eine IPv4 Netzmaske (z.B. `255.255.255.0`) oder die IPv6 Maskenlänge, der ein Slash vorangestellt ist (z.B. `/48`).

3. (*Für IP Routing*) Stellen Sie die statische Route für die Schnittstelle ein:

   ```
   hostname (config) # ip route <networkPrefix> <mask> <gatewayIP>
   <interfaceName>
   ```

   wobei:

   - `<networkPrefix>` das IPv4 oder IPv6 Netzwerk Präfix ist, das das Netzwerk angibt.
   - `<mask>` die IPv4 Maskenlänge ist, der ein Slash vorangestellt ist (z.B. `/24`) oder eine Netzmaske (z.B `255.255.255.0`) oder die IPv6 Maskenlänge, der ein Slash vorangestellt ist (z.B. `/48`).
   - `<gatewayIP>` die IPV4 oder IPv6 Adresse des Gateway oder next-Hop Gerätes ist.
   - `<interfaceName>` der Name der Management-Schnittfläche ist.

4. (*Für Web-UI Zugriff*): Fügen Sie die Schnittstelle zu der Listen-Schnittstellenliste für HTTP/HTTPS Anfragen hinzu:

   ```
   hostname (config) # web server listen interface <interfaceName>
   ```

5. (*Für CLI Zugriff*): Fügen Sie die Schnittstelle zu der Listen-Schnittstellenliste für SSH Verbindungen hinzu:

   ```
   hostname (config) # ssh server listen interface <interfaceName>
   ```

6. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show web
   hostname (config) # show ssh server
   ```

7. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**HINWEIS:** In diesem Vorgang wird der Schnittstelle eine statische IPv4 oder IPv6 Adresse zugewiesen. SLAAC oder DHCPv6 kann stattdessen die IPv6 Adresse zuweisen.

## Beispiel:

Im folgenden Beispiel wird Ether2 als Management-Schnittstelle auf der acme-1-Appliance konfiguriert. Dann wird ether2 zu der Listen-Schnittstellenliste hinzugefügt.

```
            acme-1 (config) # interface ether2 ip address 10.1.2.3 /24
acme-1 (config) # web server listen interface ether2
acme-1 (config) # ssh server listen interface ether2
acme-1 (config) # show web
Web User Interface server:
   Web interface enabled:          yes
   HTTP enabled:                   yes
   HTTP port:                      80
   HTTP redirect to HTTPS:         yes
   HTTPS enabled:                  yes
   HTTPS port:                     443
   HTTPS protocols:                TLSv1
   HTTPS minimum protocol version: TLSv1
   HTTPS cipher list:              compatible
   HTTPS certificate name:         system-self-signed
   HTTPS CA chain name:

   Listen enabled: yes
   Listen Interfaces:
      Interface: ether1
      Interface: ether2
      Interface: lo
   ...

acme-1 (config) # show ssh server
SSH server configuration:
   SSH server enabled:          yes
   Minimum protocol version:    2
   TCP forwarding enabled:      yes
   X11 forwarding enabled:    no
   Audit log file transfers:  yes
   Cipher list:   compatible
   Minimum key length:     1024 bits
   Client Alive Interval:    0
   Client Alive Count Max   3
   SSH server ports:        22

   Interface listen enabled:  yes
   Listen Interfaces:
      Interface: ether1
      Interface: ether2
...
```

**WICHTIG:** Beschränkungen der Listen-Schnittstelle sind auf dem System standardmäßig aktiviert. Wenn allerdings die `Listen enabled` Zeile in der `show web` Befehlsausgabe noist, verwenden Sie den `web server listen enable` Befehl, um Beschränkungen für HTTP/HTTPS Anfragen zu aktivieren. Wenn die `Interface listen enabled` Zeile in der `show ssh server` Befehlsausgabe noist, verwenden Sie den `ssh server listen enable` Befehl, um Beschränkungen für SSH Verbindungen zu aktivieren.

# KAPITEL 15: Die FireEye Software aktualisieren

Die Network Security Appliance sucht automatisch nach neuen System Images und Guest Images Versionen. Aktualisierungen werden fortlaufend vorgenommen und sind leicht herunterzuladen und zu installieren.

Der Network Security Server prüft auch nach neuen Versionen für die Sicherheitsinhalte und lädt diese, sofern konfiguriert, automatisch herunter und installiert sie. Weitere Informationen finden Sie in Sicherheitsinhalt aktualisieren auf Seite 188 und Automatische Sicherheitsupdates konfigurieren auf Seite 191.

Für eine Appliance, die von der Central Management Appliance verwaltet wird, sollten Softwareaktualisierungen vollständig von der Central Management Web-UI ausgeführt werden. Weitere Informationen finden Sie im *Central Management Administrationshandbuch*,

**HINWEISE:**

- Beziehen Sie sich auf das *FireEye DTI Offline Update Portal Handbuch* für Aktualisierungsanleitungen, wenn Ihr Server offline ist und keine Updates vom DTI-Netzwerk herunterladen kann.
- Die Aktualisierungsdauer variieren je nach der Betriebsumgebung auf Ihrer Website und der Größe der Server-Datenbank.
- Starten Sie Ihren Server während eines Upgrades nicht neu, wenn Sie nicht dazu aufgefordert werden.

## Bevor Sie mit der Aufrüstung beginnen

Überprüfen Sie die Elemente in diesem Abschnitt, bevor Sie mit der Aufrüstung beginnen.

- **Userrolle**—Sie müssen Admin Zugriff haben, um die Network Security Appliance zu aktualisieren.

- **Die Appliance sichern**—Sichern Sie Ihre Appliance, bevor Sie die Aufrüstung ausführen. Weitere Informationen finden Sie unter Sicherung und Wiederherstellung einer Datenbank auf Seite 309.
- **Lizenzen**—Bestätigen Sie, dass die folgenden Lizenzen installiert und gültig sind, bevor Sie Aufrüstungen ausführen:
  - CONTENT_UPDATES Lizenz (für die Aktualisierungen für Sicherheitsinhalt erforderlich)
  - FIREEYE_SUPPORT Lizenz (für Softwareaktualisierungen erforderlich)

  **HINWEIS:** Sehen Sie Lizenzschlüssel auf Seite 143 für weitere Informationen. Wenn Sie die Lizenzen erwerben müssen, senden Sie eine E-Mail an key_request@fireeye.com.
- **End-User License Agreement (EULA)**—Die Aufrüstung könnte die Annahme des Endbenutzer-Lizenzvertrags erfordern (EULA) Wenn dies erforderlich ist, funktioniert die Appliance nicht, bis die EULA akzeptiert wird. Um die EULA vor der Aufrüstung zu überprüfen, laden Sie eine Kopie vom FireEye Customer Support Portal unter `http://csportal.fireeye.com` herunter.
- **Mindestversion für die Aufrüstung**—Beziehen Sie sich auf die *Versionshinsweise*, um festzustellen, ob Sie direkt von der aktuellen Version auf die neue Version aufrüsten können.
- **IPMI und BIOS Versionen**—Die neueste IPMI und BIOS Firmware sollte ausgeführt werden. Siehe IPMI und BIOS Firmware Aktualisierungen auf Seite 289.

  **HINWEIS:** Das NX 2550 Modell benötigt IPMI 3.11 und BIOS 1.9.
- **Downloadzeit**—Herunterladen der Betriebssystemsoftware dauert ungefähr 45 Minuten, wenn Sie von der CLI aufrüsten. Herunterladen der Guest Images erfordert normalerweise 2 ½ bis 9 Stunden von der CLI, je nach Verbindungsgeschwindigkeit und ob der vollständige Satz von Guest Images heruntergeladen wird. Ein vollständiger Satz kann 24 Stunden oder mehr erfordern.

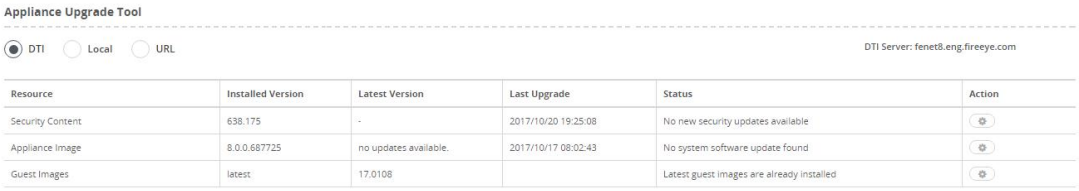
- **Netzwerk-Proxy Konfiguration**—Wenn Sie über eine intelligente Proxy-Appliance verfügen, die für Zugriff auf das Internet erforderlich ist, stellen Sie sicher, dass sie keine Secure Sockets Layser (SSL) Terminierungen mit Zertifikatsaustausch ausführt. Ein Beispiel eines solchen Proxy ist die Blue Coat ProxySG Appliance. Wenn das Proxy SSL Terminierungen ausführt, müssen Sie die Central Management Appliance, den FireEye Dynamic Threat Intelligence (DTI) Netzwerkserver (`staticcloud.fireeye.com`) oder den Content Distribution Network (CDN) Server (`cloud.fireeye.com` oder `download.fireeye.com`) in der Proxy Konfiguration whitelisten.

  Für die Integration mit Drittanbieterprodukten, z.B. ArcSight, Juniper STRM, Blue Coat ProxySG oder Q1 Lab QRadar wenden Sie sich an FireEye Technical Support. Informationen zur Proxykonfiguration finden Sie in der Herstellerdokumentation.

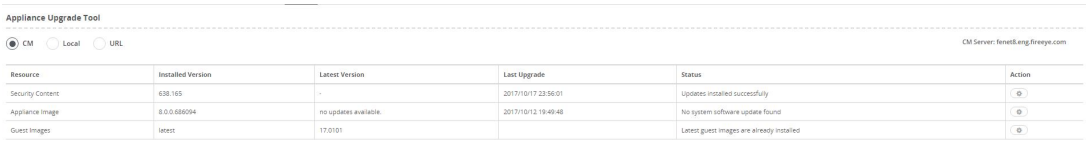
# Die Appliance mit Hilfe der Web-UI aufrüsten

Verwenden Sie die **Upgrade** Seite, um die Network Security Appliance aufzurüsten. Um die **Upgrade** Seite zu öffnen, klicken Sie auf den **About** Tab und klicken Sie dann auf **Upgrade**.

Nachfolgendes Beispiel zeigt die **Upgrade** Seite für eine eigenständige Appliance.




Nachfolgendes Beispiel zeigte die **Upgrade** Seite für eine Appliance, die von der Central Management Appliance verwaltet wird.




## Aufgabenliste für Aktualisierungen

Führen Sie die folgenden Schritte aus (in den nachfolgenden Abschnitten detailliert), um die Network Security Appliance aufzurüsten.

**HINWEIS:** Wenn Ihre Appliance offline ist und keine Updates vom DTI Netzwerk herunterladen kann, führen Sie Eine Aktualisierungsquelle wählen unten aus und lesen Sie die *FireEye DTI Offline Update Portal Bedienungsanleitung* für zusätzliche Anweisungen.

1. Eine Aktualisierungsquelle wählen unten.
2. Nach verfügbarer Aktualisierungssoftware prüfen auf der nächsten Seite.
3. Die Software herunterladen auf der nächsten Seite.
4. Die Softwareaktualisierung installieren auf der nächsten Seite.
5. Die Appliance neu laden oder aktualisieren auf Seite 276.
6. Die Softwareaktualisierungen überprüfen auf Seite 276.

# Eine Aktualisierungsquelle wählen

Die Aktualisierungsquelle ist der Speicherort, von dem die Softwareaktualisierungen heruntergeladen werden.

## Online Optionen

- **DTI**—Die Software wird vom Dynamic Threat Intelligence (DTI) Server oder einem Content Delivery Network (CDN) Server heruntergeladen. Die Serveradresse wird in der oberen rechten Ecke der Seite angezeigt. Sehen Sie Die aktive Einstellung für einen DTI-Service ändern auf Seite 163 für Details über diese Optionen.
- **CM**—Diese Option wird anstelle von **DTI** angezeigt, wenn die Appliance von der Central Management Appliance verwaltet wird. Der Standard Quellserver ist die Central Management Appliance, aber er kann von den drei oben festgelegten DTI-Optionen übersteuert werden.

## Offline Optionen

Die folgenden Optionen können verwendet werden, wenn Ihre Appliance keine Updates von einem DTI-Quellserver herunterladen kann. Details und Aufrüstungsanleitungen finden Sie in der *FireEye DTI Offline Update Portal Bedienungsanleitung*.

- **Local**—Laden Sie eine lokale Datei hoch, die Sie vom FireEye DTI Update Portal für offline Appliances erhalten haben. Klicken Sie auf **Local**, um einen Pfad auf die lokal gespeicherte Aktualisierungssoftware festzulegen und klicken Sie dann auf **Save**.
- **URL**—Laden Sie eine lokale Datei hoch, die Sie von FireEye über das DTI Update Portal für offline Appliances erhalten haben und die auf einer lokalen, durch eine

URL identifizierte Site gehostet wird. Klicken Sie auf **URL**, um eine URL für die Aktualisierungssoftware festzulegen und klicken Sie dann auf **Save**.

**HINWEIS:** Für offline Guest Image sind Aufrüstungen und Downloads effizienter, wenn **Source** auf **URL**und nicht auf **Local** eingestellt ist.

Wenn keine der offline Optionen durchführbar ist, wenden Sie sich an FireEye Technical Support.

## Nach verfügbarer Aktualisierungssoftware prüfen

Klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und klicken Sie dann auf **Check** für eine Ressourcenzeile, um festzustellen, ob Aktualisierungssoftware verfügbar ist.

Der Status wird im erweiterten **Status** Bereich angezeigt.

**HINWEIS:** Wenn die **Check** Option in der **Action** Spalte erscheint, ist die Software bereits für das Download verfügbar oder eine Aktualisierung hat vor Kurzem stattgefunden. Die **Check** Option wird auch während der Software-Downloads nicht angezeigt.

## Die Software herunterladen

Wenn eine Softwareaktualisierung für ein Software Image, Guest Image oder Sicherheitsinhaltsupdate verfügbar ist, wird die **Download** Option in der **Action** Spalte angezeigt.

Klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und klicken Sie dann auf **Download**, um mit dem Softwaredownload zu beginnen.

Der Download Status wird in dem erweiterten **Status** Bereich angezeigt.

## Die Softwareaktualisierung installieren

Der Installationsstatus wird im erweiterten **Status** Bereich angezeigt. Nachdem Sie eine Softwareaktualisierung heruntergeladen haben, klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und klicken Sie dann auf **Install**, um es zu installieren.

Der Installationsstatus wird im erweiterten **Status** Bereich angezeigt. Wenn Sie aufgefordert werden, lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und wenn Sie mit den Bedingungen einverstanden sind, akzeptieren Sie ihn. Wenn Sie ihn nicht akzeptieren, funktioniert die Appliance nicht.

**HINWEIS:** Wenn ein Aktualisierungsvorgang unterbrochen wird oder fehlschlägt, fällt die Appliance Software automatisch auf das aktuell installierte Image zurück.

## Die Appliance neu laden oder aktualisieren

Wenn die Installation von Guest Images oder Sicherheitsinhalten abgeschlossen ist, klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und klicken Sie dann auf **Refresh**. Wenn die Installation des Software Image abgeschlossen ist, klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und klicken Sie dann auf **Reboot**, um den Aktualisierungsvorgang abzuschließen.

**HINWEIS:** Sie müssen über die serielle Schnittstelle auf die Appliance zugreifen, um die Startaktivitäten der Appliance zu überwachen. Sie können CLI Befehle nur über direkte Tastatur- und Monitorverbindung eingeben, bevor der Bootloader mit dem Laden des Kernels beginnt, z.B. um die Ausgabe zu veröffentlichen und nachdem der Bootvorgang abgeschlossen ist.

## Die Softwareaktualisierungen überprüfen

Nachdem Softwareaktualisierungen installiert sind, überprüfen Sie die Installationen:

- Klicken Sie auf das **Settings** Register und klicken Sie dann auf **Guest Images** auf der Seitenleiste, um die installierte Guest Images Version anzuzeigen und zu bestätigen.
- Klicken Sie auf den **About** Tab. Das Versionsinformationen für das aktuelle Software Image, Guest Images, und Sicherheitsinhalt werden auf der **Summary** Seite angezeigt.  Menü.)
- Klicken Sie auf den **Settings** Tab und dann auf **Appliance Licenses** auf der Seitenleiste, um installierte Lizenzen zu überprüfen und anzuzeigen.  Gültige und aktive Lizenzen zeigen das Attribut "True" an. Wenn die Lizenzen nicht gültig und aktiv sind, sind die Updates nicht funktionstüchtig.

# Die Appliance mit Hilfe der CLI aktualisieren

Verwenden Sie die Befehle in den folgenden Abschnitten, um die Network Security Appliance aufzurüsten.

## Aufgabenliste für Aktualisierungen

Führen Sie die folgenden Schritte aus (in den folgenden Abschnitten detailliert), um die Appliance zu aktualisierenn.

1. Das Appliance Software Image herunterladen und installieren unten.
2. Die Appliance neu starten und die EULA annehmen auf der nächsten Seite.
3. Guest Images herunterladen auf Seite 279.
4. Heruntergeladene Guest Image Profile installieren auf Seite 282.
5. Guest Images in einem einzelnen Befehl herunterladen und installieren auf Seite 282.
6. Die Aktualisierung bestätigen auf Seite 283.

**WICHTIG:** Stellen Sie sicher, die Software Image und Guest Image Dateien von dem konfigurierten DTI-Quellserver herunterzuladen, bevor Sie mit den Installationen beginnen.

## Das Appliance Software Image herunterladen und installieren

**Um das Software Image herunterzuladen und zu installieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Suchen Sie nach Downloads:

```
hostname (config) # fenet image check
hostname (config) # show fenet image status
```

3. Laden Sie das Software Image herunter:

```
hostname (config) # fenet image fetch
```

4. Zeigen Sie den Download-Fortschritt an:

```
hostname (config) # show fenet image status

                  Progress of latest action taken:
   action fetch initiated                    Tue Nov 22 13:04:44 2016
   applying fetch for image                  lms
   fetching checksum of the requested image  done
   fetching requested image 7.9.0            initiated
   fetching requested image 7.9.0            done
   action fetch completed                    Tue Nov 22 13:06:03 2016
   fetch-done: OS image downloaded successfully: image-lms_7.9.0.img
```

Wenn Sie die neueste Software bereits heruntergeladen haben, wird möglicherweise ein Fehler angezeigt: "Latest image already downloaded and ready to install (error)." [Das neueste Bild ist bereits heruntergeladen und kann jetzt installiert werden (Fehler)]. Um zu überprüfen, welche Images heruntergeladen wurden, verwenden Sie den folgenden Befehl:

```
hostname (config) # show fenet image list
```

5. Installieren Sie das heruntergeladene Software Image:

```
                    hostname (config) # image install image-lms_
7.9.0.img
hostname (config) # image boot next
```

**HINWEIS:** Wenn ein Aktualisierungsvorgang unterbrochen wird oder fehlschlägt, fällt die Appliance Software automatisch auf das aktuell installierte Image zurück.

6. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

## Die Appliance neu starten und die EULA annehmen

**Um die Appliance neu zu starten und die EULA zu akzeptieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Starten Sie die Appliance neu:

```
hostname (config) # reload
```

3. Nach dem Neustart der Appliance könnte das System die FireEye End User License Agreement (EULA) anzeigen. Lesen Sie die EULA. Klicken Sie auf **Yes** wenn Sie den Bedingungen zustimmen und dann auf **Submit**. Wenn Sie die EULA nicht annehmen wird die Appliance nicht funktionieren.

   Nach Annahme der EULA wird die Anmeldeseite angezeigt. Warten Sie einige Minuten, bevor Sie sich anmelden, da Datenbankeinträge zur Vorbereitung auf das Upgrade aktualisiert werden.

**HINWEIS:** Sie müssen über die serielle Schnittstelle auf die Appliance zugreifen, um die Startaktivitäten der Appliance zu überwachen. Sie können CLI Befehle nur über direkte Tastatur- und Monitorverbindung eingeben, bevor der Bootloader mit dem Laden des Kernels beginnt, z.B. um die Ausgabe zu veröffentlichen und nachdem der Bootvorgang abgeschlossen ist.

# Guest Images herunterladen

Standard Guest Images werden automatisch vom DTI-Quellserver heruntergeladen und installiert. Um ein Guest Image Bündel oder Profil herunterzuladen und zu installieren müssen Sie zunächst den `guest-images configure` Befehl verwenden, um das Guest Image auszuwählen.

In diesem Verfahren wird die Installation von Standard und nicht-Standard Guest Images beschrieben.

**Um Guest Images herunterzuladen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie die für die Appliance konfigurierte Guest Images an:

   ```
   hostname (config) # show guest-images config
   ```

3. Laden Sie die Guest Images herunter, aber installieren Sie sie noch nicht. Das Herunterladen von Guest Images nimmt einige Zeit in Anspruch; gestatten Sie also, dass das Download im Hintergrund läuft.

   ```
   hostname (config) # guest-images download
   ```

   Warten Sie, bis die Appliance die Guest Images vollständig heruntergeladen hat, bevor Sie mit einer Installation beginnen.

   **HINWEIS:** Sie können automatische Downloads der verfügbaren Guest Images ausführen. Details finden Sie in den `fenet guest-images auto download` und `fenet guest-images auto update` Befehlen der *CLI Befehlsreferenz*.

4. Bestätigen Sie, dass die Downloads der Guest Images abgeschlossen ist.

   ```
   hostname (config) # show guest-images download
   ```

   Um ein laufendes Download abzubrechen:

   ```
   hostname (config) # guest-images download cancel
   ```

   Um ein Download wiederaufzunehmen, das auf irgendeinem Grund unterbrochen wurde:

   ```
   hostname (config) # guest-images download resume
   ```

5. Um nicht-standardmäßige Guest Images durch Festlegen des Server-Manifests herunterzuladen:

   Führen Sie diesen Schritt aus, wenn Sie nicht alle verfügbaren Guest Images benötigen.

   a. Laden Sie das Server-Manifest herunter:

      ```
      hostname (config) # guest-images download manifest [version <version-id>
      ```

   b. Zeigen Sie verfügbare Guest Image Bündel an.

      ```
      hostname (config) # show guest-images available bundles
      ```

   c. Notieren Sie die Bündel-ID des Guest Images Bündels, dass Sie aus der angezeigten Liste wollen (nur ein Bündel kann ausgewählt werden).

   d. Wählen Sie das Guest Image Bündel, das installiert werden soll, wobei Sie `bundle_id` aus dem vorherigen Schritt erhalten:

      ```
      hostname (config) # guest-images configure bundle <bundle-id>
      ```

   e. Bestätigen Sie, dass ist Bündel richtig ausgewählt ist.

      ```
      hostname (config) # show guest-images config
      ```

   f. Laden Sie die Guest Images vom FireEye Netzwerk herunter:

      ```
      hostname (config) # guest-images download
      ```

   g. Überwachen Sie den Downloadvorgang:

      ```
      hostname (config) # show guest-images download
      ```

6. Um ein nicht-standardmäßiges Guest Image durch Festlegen der `version` Nummer herunterzuladen:

   Führen Sie diesen Schritt aus, wenn Sie nicht alle verfügbaren Guest Images benötigen.

   Der Versionsdownload wird für Version 17.0101 oder höher unterstützt.

   Sie können nur eine Guest Image Version installieren, die neuer als die derzeit installierte Version ist.

   a. Zeigen Sie unterstützte Guest Images an.

      hostname (config) # **show fenet guest-images status**

   b. Laden Sie die spezifische Guest Image Version vom FireEye Netzwerk herunter:

      ```
      hostname (config) # guest-images download version <version-id>
      ```

   c. Überwachen Sie den Downloadvorgang:

      ```
      hostname (config) # show guest-images download
      ```

7. Um Guest Images mit einem oder mehreren Profilen zu aktualisieren (schließen sich gegenseitig mit Standard- und Bündelsätzen aus):
   a. Laden Sie das Server Manifest herunter:

      `hostname (config) # guest-images download manifest` [**version** <version-id>]

   b. Zeigen Sie verfügbare Guest Image Profile an:
      `hostname (config) # show guest-images available profiles`
   c. Notieren Sie die Profil-ID des benötigten Profils (Profile) aus der angezeigten Liste.
   d. Wählen Sie das Guest Image Profil, das installiert werden soll:
      `hostname (config) # guest-images configure profile <profileID>`

      wobei`<profileID>` das Profil ist, das Sie im vorherigen Schritt notiert haben.
   e. Wiederholen Sie den vorherigen Schritt für jedes zusätzliche, erforderliche Profil.
   f. Bestätigen Sie, dass alle erforderlichen Profile konfiguriert sind.:
      `hostname (config) # show guest-images configuration`
   g. Laden Sie die Guest Images herunter:
      `hostname (config) # guest-images download`
   h. Überwachen Sie den Download-Fortschritt:
      `hostname (config) # show guest-images download`

      **HINWEIS:** Wenn Sie ein Problem mit dem Download erfahren, beschreibt die Ausgabe des `show guest-images download` Befehls das Problem, einschließlich der Benachrichtigung über die spezifische Datei, die den Fehler ausgelöst hat. Probleme mit der Netzwerkverbindung rufen Download-Ausfälle hervor. Wiederholen Sie das Download mit Hilfe des `guest images download` Befehls. Das System startet das Download erneut an dem Punkt, an dem er unterbrochen wurde oder fehlgeschlagen ist. Wenn das Problem anhält, wenden Sie sich an FireEye Technical Support.

8. Speichern Sie Ihre Änderungen:

   `hostname (config) # write memory`

## Heruntergeladene Guest Image Profile installieren

**Um Standard Guest Images herunterzuladen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Nachdem der Download abgeschlossen ist, installieren Sie die Guest Images:

   ```
   hostname (config) # guest-images install
   ```

3. Bestätigen Sie, dass Guest Images ordnungsgemäß installiert sind:

   ```
   hostname (config) # show guest-images
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Guest Images in einem einzelnen Befehl herunterladen und installieren

**Um Standard Guest Images herunterzuladen und zu installieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Guest Images herunterladen und installieren:

   ```
   hostname (config) # guest-images download-and-install
   ```

**HINWEIS:** Wenn die Appliance von einer Central Management Appliance verwaltet wird, ist der Downloadvorgang für Guest Images automatisiert. Die verwaltete Appliance prüft täglich nach Aktualisieren für die Guest Images und veranlasst dann die Central Management Appliance, das angeforderte Guest Image Update zu Hosting herunterzuladen. Die verwaltete Appliance lädt die Aktualisierungen automatisch herunter und installiert diese, nachdem die Central Management Appliance den Download abgeschlossen hat.

3. Zeigen Sie den Downloadstatus der Guest Images an:

   ```
   hostname (config) # show guest-images download
   ```

   Um ein laufendes Download abzubrechen:

   ```
   hostname (config) # guest-images download cancel
   ```

   Um ein Download wiederaufzunehmen, das auf irgendeinem Grund unterbrochen wurde:

   ```
   hostname (config) # guest-images download-and-install resume
   ```

4. Bestätigen Sie, dass die Guest Images ordnungsgemäß installiert sind:

   ```
   hostname (config) # show guest-images
   ```

## Die Aktualisierung bestätigen

**Um die Aktualisierung zu bestätigen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie die Informationen über die Version für das aktuelle System Image an:

   ```
   hostname (config) # show version
   ```

3. Zeigen Sie alle Guest Images an:

   ```
   hostname (config) # show guest-images
   ```

# Automounting auf einem USB Gerät konfigurieren

Sie können Automounting auf einem USB Gerät konfigurieren, das an die Network Security Appliance angehängt ist. Es kann immer nur ein USB-Gerät installiert werden. Sie können HTTP Zugriff konfigurieren, um System Images, Guest Images, oder Sicherheitsinhalt von dem USB Gerät auf der Appliance zu installieren.

**HINWEIS:** Sie können Automounting auf einem USB Gerät nur mit Hilfe der CLI konfigurieren.

## Voraussetzungen

- Admin Zugriff

# Automounting auf einem USB Gerät mit Hilfe der CLI aktivieren oder deaktivieren

Verwenden Sie die Befehle in diesem Thema, um Automounting auf einem an die Network Security Appliance angeschlossenes USB Gerät zu aktivieren oder deaktivieren. Sie müssen Automounting aktivieren, wenn das USB Gerät angeschlossen ist. Automounting ist standardmäßig deaktiviert. Automounting mountet das USB nicht, wenn es bereits an die Appliance angeschlossen ist.

## Voraussetzungen

- Admin Zugriff

**Um Automounting auf einem USB Gerät zu aktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie Automounting auf einem an die Appliance angeschlossenen USB Gerät:

   ```
   hostname (config) # media usb auto-mount enable
   ```

3. Stöpseln Sie das USB Gerät sofort in die Appliance ein.
4. Überprüfen Sie die Automounting Konfiguration des USB Geräts.

   ```
   hostname (config) # show media usb
   USB auto-mount configuration:
   Enabled:             yes
   Local web access:    yes
   Top-level directory: fireeye
   ```

**Um Automounting auf dem USB Gerät zu deaktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie Automounting auf dem USB Gerät:

   ```
   hostname (config) # no media usb auto-mount enable
   ```

3. Überprüfen Sie die Automounting Konfiguration des USB Geräts.

   ```
   hostname (config) # show media usb
   USB auto-mount configuration:
   Enabled:             no
   ```

```
Local web access:    yes
Top-level directory: fireeye
```

# HTTP Zugriff für die Installation von Softwareaktualisierungen mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Thema, um HTTP Zugriff für die Installation von Softwareupdates von einem USB Gerät auf die Appliance zu konfigurieren. Standardmäßig haben Sie nur lokalen Zugriff auf die Inhalte in dem `fireeye` Verzeichnis für die erste Partition von einer festgelegten URL.

## Voraussetzungen

- Admin Zugriff
- Aktivieren Sie Automounting auf dem USB Gerät mit der angeschlossenen Appliance. Details über die Aktivierung von Automounting finden Sie unter Automounting auf einem USB Gerät mit Hilfe der CLI aktivieren oder deaktivieren auf der vorherigen Seite.

**Um HTTP Zugriff für die Installation von Softwareupdates von einem USB Gerät zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie HTTP Zugriff auf der Loopback-Schnittstelle auf der Appliance.

   ```
   hostname (config) # media usb web-access enable local
   ```

   Lokaler Webzugriff ist standardmäßig aktiviert.

3. Bestimmen Sie das oberste Verzeichnis als den Speicherort, aus dem Softwareaktualisierungen auf einem USB Gerät extrahiert werden soll.

   ```
   hostname (config) # media usb web-access top-dir fireeye
   ```

   Dieses Verzeichnis wird als die URL verwendet, um die Software auf dem USB Gerät zu extrahieren. Wenn Sie zum Beispiel das Installationsverzeichnis als `fireeye/gi-13.0701` bestimmt haben, ist die URL für die Installation `http://localhost/media/usb1/fireeye/gi-13.0701`.

4. Bestätigen Sie, dass das USB Gerät installiert ist.

   ```
   hostname (config) # show media usb
   USB auto-mount configuration:
     Enabled:            yes
     Local web access:   yes
   ```

```
  Top-level directory: fireeye
USB auto-mount status:
  Device mounted:      yes
  Access URL:          N/A
```

5. Laden Sie Softwareupdates herunter und verwenden die festgelegten URL als den Speicherort für die Installation der Aktualisierungen. Einen vergleichbaren Vorgang finden Sie unter Guest Images von einem USB Gerät mit Hilfe der CLI installieren unten.

## Guest Images von einem USB Gerät mit Hilfe der CLI installieren

Verwenden Sie die Befehle in diesem Thema, um Guest Images von einem USB Gerät auf der Appliance zu installieren. Standardmäßig haben Sie nur lokalen Zugriff auf die Inhalte in dem `fireeye` Verzeichnis für die erste Partition von einer festgelegten URL.

## Voraussetzungen

- Admin Zugriff
- Aktivieren Sie Automounting auf dem USB Gerät mit der angeschlossenen Appliance. Details über die Aktivierung von Automounting finden Sie unter Automounting auf einem USB Gerät mit Hilfe der CLI aktivieren oder deaktivieren auf Seite 284.
- Konfigurieren Sie HTTP Zugriff. Details finden Sie unter HTTP Zugriff für die Installation von Softwareaktualisierungen mit Hilfe der CLI konfigurieren auf der vorherigen Seite.
- Führen Sie die Schritte in der folgenden Reihenfolge aus, um die Dateien ordnungsgemäß einzurichten, um Guest Images von einem USB Gerät zu installieren:
    1. Laden Sie die Guest Images tar Datei vom FireEye Netzwerk herunter.
    2. Extrahieren Sie die Inhalte auf das USB Gerät.
    3. Entfernen Sie die Versionsnummern. Kopieren Sie die folgenden Dateinamen:
        - `server-manifest.VERSION` bis `server-manifest`
        - `server-manifest.VERSION.md5` bis `server-manifest.md5`
        - `server-manifest.VERSION.v2` bis `server-manifest.v2`
        - `server-manifest.VERSION.v2.md5` bis `server-manifest.v2.md5`

**Um Guest Images von einem USB Gerät herunterzuladen:**

1. Laden Sie Guest Images mit Hilfe der angegebenen URL als den Speicherort für die Guest Images herunter.

   ```
   hostname (config) # guest-images download url <URL>
   ```

   wobei `URL` der Speicherort ist, den Sie als das Verzeichnis der obersten Ebene für die Installation bestimmt haben.

   Warten Sie, bis die Appliance die Guest Images vollständig heruntergeladen hat, bevor Sie mit einer Installation beginnen.

2. Überprüfen Sie den Download-Fortschritt:

   ```
   hostname (config) # show guest-images download
   ```

3. Nachdem der Download abgeschlossen ist, installieren Sie die Guest Images:

   ```
   hostname (config) # guest-images install
   ```

4. Bestätigen Sie, dass Guest Images ordnungsgemäß installiert sind:

   ```
   hostname (config) # show guest-images
   ```

# Ein USB Gerät mit Hilfe der CLI mounten oder unmounten

Verwenden Sie die Befehle in diesem Thema, um ein USB Gerät manuell auf die angeschlossene Appliance zu mounten oder unmounten. FireEye empfiehlt, dass Sie das USB Gerät physisch von dem Port entfernen. Verwenden Sie den `media usb mount` Befehl, bevor Sie das Laufwerk anbringen und den `media usb eject` Befehl, nachdem Sie es trennen.

**HINWEIS:** Der `media usb eject` Befehl hat keine Wirkung, wenn das USB Gerät nicht gemountet ist.

# Voraussetzungen

- Admin Zugriff

**Um ein USB Gerät zu mounten:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Mounten Sie das USB Gerät auf die angeschlossene Appliance:

   ```
   hostname (config) # media usb mount
   ```

**Um ein USB Gerät zu unmounten:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Unmounten Sie das USB Gerät von der angeschlossenen Appliance:

   ```
   hostname (config) # media usb eject
   ```

# KAPITEL 16: IPMI und BIOS Firmware Aktualisierungen

Neue Intelligent Platform Management Interface (IPMI) Firmware und BIOS Firmware sind im Lieferumfang des Appliance Software Image enthalten, werden aber nicht automatisch installiert, wenn Sie auf eine neue Appliance Version aktualisieren. Es ist wichtig, die Firmware zu aktualisieren, um sicherzustellen, dass die neueste, sicherste Version verwendet wird. BIOS Firmware Aktualisierungen sind mit IPMI Aktualisierungen verbunden und sollten beide aktualisiert werden. Die IPMI Firmware muss zuerst aktualisiert werden.

Standardmäßig werden Sie über die Verfügbarkeit einer neueren Version benachrichtigt, wenn die IPMI Schnittstelle mit einer IP-Adresse konfiguriert wurde. Die Nachricht wird angezeigt, wenn Sie sich auf der CLI anmelden und die **IPMI** Karte auf der **About > Summary** Seite in der Web-UI anzeigen. Wenn Sie möchten, können Sie die Benachrichtigung deaktivieren, damit sie nicht mehr angezeigt wird. Details finden Sie unter IPMI Firmware Benachrichtigungen mit Hilfe der CLI aktivieren und deaktivieren auf Seite 292.

Sie können den `show ipmi version include-firmware-update-notice` Befehl verwenden, um die Nachricht anzuzeigen, selbst wenn Ihre IPMI Firmware aktuell ist.

Beachten Sie Folgendes:

- Die IPMI Web-UI ist während der IPMI Firmware Aktualisierung nicht verfügbar.
- Der IPMI Firmware Typ ist für das Appliance Modell spezifisch, es ist also möglich, dass nicht alle Modelle eine IPMI Firmware Aktualisierung in der gleichen Network Security Softwareausgabe erhalten.
- IPMI und BIOS Firmware beziehen sich auf Hardware, also sind nur Updates für physische Appliances erforderlich. Die in diesem Abschnitt beschriebenen Befehle sind nicht in der CLI einer virtuellen Appliance verfügbar.
- IPMI und BIOS Firmware Updates werden nicht auf allen Appliances Modellen unterstützt.

**WICHTIG!** Durch Aktualisierung der IPMI Firmware werden alle Einstellungen auf die Werkseinstellungen zurückgesetzt, einschließlich des IPMI Benutzernamen und Passworts, Netzwerkkonfiguration und Ereignisprotokolle. Bevor Sie mit der Aktualisierung beginnen, sammeln Sie alle Informationen, die Sie für die Neukonfiguration der IPMI benötigen.

## Voraussetzungen

- Admin Zugriff

# IPMI und BIOS Firmware aktualisieren

Dieser Vorgang beschreibt die Verwendung von CLI Befehlen für das Update der IPMI und BIOS Firmware auf der Network Security Appliance.

**HINWEIS:** Das NX 2550 Modell benötigt eine Aktualisierung auf IPMI 3.11 und BIOS 1.9. Sie müssen die IPMI vor BIOS aktualisieren.

## IPMI Firmware aktualisieren

**Um die IPMI Firmware zu aktualisieren:**

**VORSICHT:** IPMI Netzwerk- und Passwort-Einstellungen werden nach diesem Upgrade auf die Werkseinstellungen zurückgesetzt und IPMI Protokolle werden gelöscht. Notieren Sie sich Ihre Einstellungen und sichern Sie Ihre IPMI Protokolle.

**WARNUNG:** Fahren Sie die Appliance während der Aktualisierung nicht herunter oder trennen Sie die Stromzufuhr.

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname> enable
   hostname# configure terminal
   ```

2. Überprüfen Sie die auf der Appliance installierte Version:

   ```
   hostname (config) # show ipmi
   ```

3. Beginnen Sie mit der Aktualisierung:

   ```
   hostname (config)# ipmi firmware update latest
   ```

4. Bestätigen Sie die Aktualisierung:

   ```
   hostname (config)# show ipmi
   ```

Wenn die Aktualisierung fehlschlägt, versuchen Sie die Schritte erneut.

Wenn IPMI-Funktionen nicht vollständig wiederhergestellt wurden, führen Sie einen kompletten Energiezyklus (ungeplante Abschaltung) auf der Appliance aus:

1. Stoppen Sie den Neuladevorgang:

   ```
   hostname (config)# reload halt
   ```

2. Trennen Sie alle Netzkabel für zwei Minuten.
3. Schließen Sie nach zwei Minuten die Netzkabel wieder an und starten Sie die Appliance neu.

# BIOS Firmware aktualisieren

**WICHTIG:** Stellen Sie sicher, dass die IPMI Firmware aktualisiert ist, bevor Sie diesen Vorgang ausführen.

**Um die BIOS Firmware zu aktualisieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname> enable
   hostname# configure terminal
   ```

2. Überprüfen Sie die installierte Version:

   ```
   hostname (config) # show system bios
   ```

3. Beginnen Sie mit der Aktualisierung:

   ```
   hostname (config)# system bios firmware update latest
   ```

   **WARNUNG:** Während der Aktualisierung schalten Sie die Appliance nicht ab oder unterbrechen die Stromzufuhr.

4. Bestätigen Sie die Aktualisierung:

   ```
   hostname (config)# show system bios
   ```

5. Stoppen Sie den Neuladevorgang:

   ```
   hostname (config)# reload halt
   ```

6. Trennen Sie alle Netzkabel für zwei Minuten.
7. Schließen Sie nach zwei Minuten die Netzkabel wieder an und starten Sie die Appliance neu.

# IPMI Firmware Benachrichtigungen mit Hilfe der CLI aktivieren und deaktivieren

In diesem Vorgang wird die Verwendung der CLI Befehle für die Deaktivierung und erneute Aktivierung von Benachrichtigung über veraltete IPMI Firmware auf der Network Security Appliance beschrieben. Diese Benachrichtigung ist standardmäßig aktiviert.

**Um Benachrichtigungen über veraltete Firmware zu deaktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie Benachrichtigungen:

   ```
   hostname (config) # no ipmi firmware update notice enable
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um Benachrichtigungen über veraltete Firmware erneut zu aktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie Benachrichtigungen:

   ```
   hostname (config) # ipmi firmware update notice enable
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# KAPITEL 17: Protokollverwaltung

Dieses Thema behandelt die folgenden Informationen:

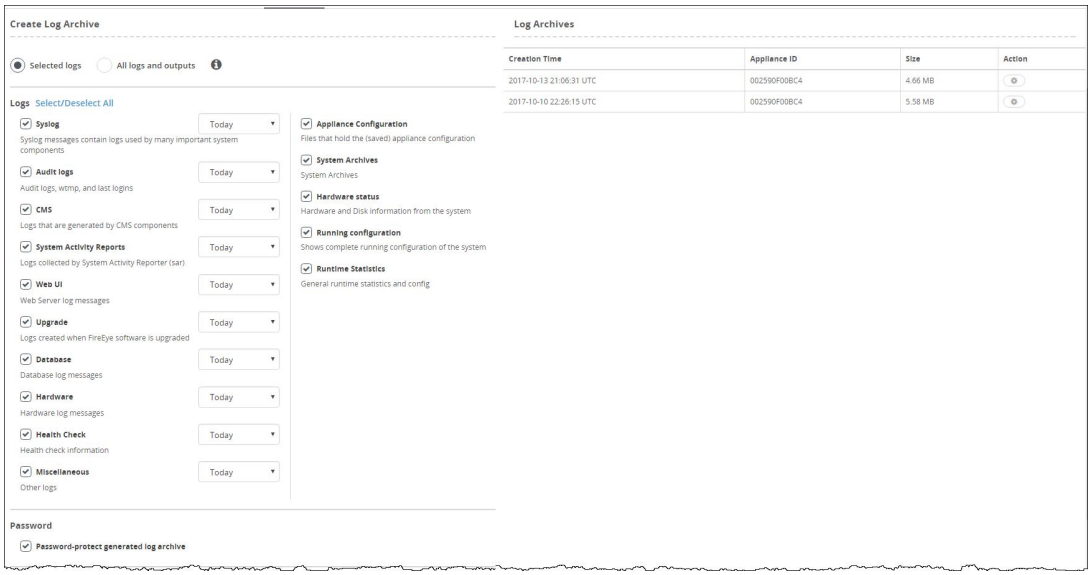


Eine vollständige Liste und Details über Befehlsnutzung und Parameter finden Sie in der *CLI Befehlsreferenz*.

**HINWEIS:** Möglicherweise müssen Sie Protokolle herunterladen und sie demFireEye Technical Support zur Fehlersuche zur Verfügung stellen.

# Protokolle mit Hilfe der Web-UI verwalten

Verwenden Sie die **About** > **Log Manager** Seite, um Appliance Protokolle zu verwalten. Die Seite ermöglicht Ihnen, die Erstellung von Protokollen für unterschiedliche Zeiträume anzupassen.




**HINWEIS:** Möglicherweise müssen Sie Protokolle herunterladen und diese FireEye Technical Support für die Fehlersuche zur Verfügung stellen. Möglicherweise werden Sie aufgefordert, die Protokolle auf FireEye hochzuladen.

**Um Protokolle zu verwalten:**

1. Klicken Sie auf den **About** Tab.
2. Klicken Sie auf **Log Manager**.
3. Wählen Sie, welche Protokollkategorien einbezogen werden sollen, indem Sie auf **Selected Logs** oder **All logs and outputs** klicken.
4. Aktivieren oder deaktivieren Sie Kontrollkästchen, um die Kategorien festzulegen, die Sie in den Protokollen einbeziehen wollen.
5. Wenn eine Dropdown-Liste vorhanden ist, wählen Sie den Zeitraum, den das Protokoll erfassen soll. Der Standard ist **today** (heute). Die anderen Optionen sind **past week**, **past 2 weeks** und **past month** (letzte Woche, letze 2 Wochen und letzter Monat).
6. Wenn Sie die heruntergeladenen Protokolldateien anzeigen wollen, deaktivieren Sie das **Password-protect generated log archive** Kontrollkästchen im **Password** Bereich.

   **WICHTIG:** Wenn dieses Kontrollkästchen aktiviert ist, können Sie die Dateien nicht öffnen.

7. Klicken Sie auf **Create**. Das Protokoll wird zum **Log Archives** Bereich hinzugefügt.

8. Um ein Protokoll herunterzuladen, klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und dann auf **Download**.

   Das Protokollarchiv wird auf Ihr lokales Dateisystem heruntergeladen. Der Archivname beginnt mit dem Hostnamen der Appliance.

9. Um ein Archiv zu löschen, klicken Sie auf das Aktionssysmbol ( ) in der **Action** Spalte und dann auf **Delete**.

10. Wenn FireEye Sie auffordert, ein Archiv hochzuladen, klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und dann auf **Upload**. Die Datei wird automatisch auf FireEye hochgeladen.

# Die aktuelle Protokollkonfiguration anzeigen

Dieses Thema beschreibt die Verwendung von CLI Befehlen, um die aktuelle Protokollkonfiguration auf der Network Security Appliance anzuzeigen. Eine vollständige Liste der Protokollierungsbefehle und die Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um die aktuelle Protokollkonfiguration anzuzeigen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie die aktuelle Protokollierungskonfiguration an:

   ```
   hostname # show logging
   Local logging level:                  notice
      Override for class mgmt-back:      notice
      Override for class mgmt-front:     notice

   Remote syslog default level:          notice
   No remote syslog servers configured.

   Receive remote messages via UDP:      no

   Receive remote messages via TCP:      no

   Receive remote messages via TLS:      no

   Log file rotation:
      Log rotation size threshold:       256 megabytes
      Archived log files to keep:        40

   Log format:
      Timestamp format:                  rfc-3164
      Subsecond timestamp field:         disabled

   Secure channel logs:                  yes
   ```

# Einen Syslog Server mit Hilfe der CLI konfigurieren

Dieses Thema beschreibt die Benutzung von CLI Befehlen, um einen syslog Server für Protokollnachrichten auf der Network Security Appliance festzulegen. Eine vollständige Liste der Protokollierungsbefehle und die Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um einen syslog Server festzulegen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um einen syslog Server festzulegen, an den Protokollierungsnachrichten gesendet werden sollen, benutzen Sie den `logging <serverAddress>` Befehl, wobei `<serverAddress>` die Server IP-Adresse ist. Zum Beispiel:

   ```
   hostname (config) # logging 10.10.20.62
   ```

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show logging
   Local logging level:                    notice
      Override for class mgmt-back:        notice
      Override for class mgmt-front:       notice

   Remote syslog default level:            notice
   Remote syslog servers:
      10.10.20.62                          notice
         protocol:                         udp
         port:                             514
   [ . . . ]
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Den Mindestschweregrad von Nachrichten, die an Syslog Server gesendet wurden, mit Hilfe der CLI konfigurieren

In diesem Thema wird beschrieben, wie mit Hilfe von CLI Befehlen der Mindestschweregrad von Protokollnachrichten, die an den Syslog-Server gesendet werden, festgelegt wird. Eine vollständige Liste der Protokollierungsbefehle und deren Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um den Mindestschweregrad von Protokollnachrichten zu konfigurieren, die an Syslog Server gesendet werden:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Um den Mindestschweregrad von Nachrichten festzulegen, die an Syslog-Server gesendet werden, verwenden Sie den `logging trap <severity>` Befehl, wobei`<severity>` eins der Folgenden ist:
   - **none**—Deaktiviert Protokollierung.
   - **emerg**—Systemfehler.
   - **alert**—Sofortige Aktion erforderlich.
   - **crit**—Kritischer Zustand.
   - **err**—Fehlerzustand
   - **warning**—Warnungszustand.
   - **notice**—Normaler, aber bedeutender Zustand.
   - **info**—Informelle Nachricht.
   - **debug**—Debug-Ebene Nachricht.

   Im folgenden Beispiel wird festgelegt, dass alle Protokollmeldungen mit der error Fehlerstufe oder höher an den Syslog-Server gesendet werden:

   ```
   hostname (config) # logging trap err
   ```

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show logging
   Local logging level:                    notice
      Override for class mgmt-back:        notice
      Override for class mgmt-front:       notice

   Remote syslog default level:            err
   Remote syslog servers:
      10.10.20.62err
         protocol:                         udp
         port:                             514
   [ . . . ]
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Den Mindestschweregrad für Nachrichten, die auf dem lokalen Laufwerk gespeichert sind, mit Hilfe der CLI konfigurieren

In diesem Thema wird die Verwendung von CLI Befehlen für die Festlegung des Mindestschweregrads für Protokollnachrichten, die auf dem lokalen Laufwerk gespeichert sind, beschrieben. Eine vollständige Liste der Protokollierungsbefehle und deren Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um den Mindestschweregrad von Protokollnachrichten, die auf dem lokalen Laufwerk gespeichert sind, zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Um den Mindestschweregrad von Nachrichten festzulegen, die auf dem lokalen Laufwerk gespeichert sind, verwenden Sie den `logging local <severity>` Befehl, wobei `<severity>` eins der Folgenden ist.
   - **none**—Deaktiviert Protokollierung.
   - **emerg**—Systemfehler.
   - **alert**—Sofortige Aktion erforderlich.
   - **crit**—Kritischer Zustand.
   - **err**—Fehlerzustand.
   - **warning**—Warnungszustand.
   - **notice**—Normaler, aber bedeutender Zustand.
   - **info**—Informelle Nachricht.
   - **debug**—Debug-Ebene Nachricht.
   - **override**—Übersteuerung einer Protokollebene.

   Das folgende Beispiel legt fest, dass alle Protokollnachrichten mit einem Schweregrad von "error" oder höher in den Protokolldateien auf dem lokalen Laufwerk gespeichert werden.

   ```
   hostname (config) # logging local err
   ```

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show logging
      Local logging level:                  err
      Override for class mgmt-back:       notice
      Override for class mgmt-front:      notice
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Systeminterne Audit-Nachrichten von der Audit-Protokolldatei mit Hilfe der CLI ausschließen

In diesem Thema wird beschrieben, wie systeminterne Audit-Nachrichten von der Audit-Protokolldatei auf der Network Security Appliance herausgefiltert werden. Eine vollständige Liste der Protokollierungsbefehle und deren Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um das Herausfiltern von internen Audit-Nachrichten zu aktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enablehostname # configure terminal
   ```

2. Aktivieren Sie die Filterfunktion:

   ```
   hostname (config) # logging files audit filter exclude-system-internal
   enable
   ```

# Die Protokollrotation für bestimmte Protokolldateien konfigurieren

In diesem Thema wird die Aktivierung und Konfigurierung von dateibasierten Protokollrotationen für Auditprotokolle und Anmeldeverlaufprotokolle auf der Network Security Appliance beschrieben. Sie können diese Protokolldateien zu einem festgelegten Zeitpunkt, wenn Sie eine festgelegte Datengröße erreichen oder wenn sie einen festgelegten Prozentsatz des Festplattenspeichers einnehmen, rotieren. Wenn Sie die Kriterien für einzelne Dateitypen konfigurieren, wird die globale Konfiguration überschrieben. Eine vollständige Liste der Protokollierungsbefehle und deren Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um dateibasierte Protokollrotation zu aktivieren und konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enablehostname # configure terminal
   ```

2. Aktivieren Sie die Rotationsfunktion für den festgelegten Dateityp:

   ```
   hostname (config) # logging files rotation file-type {audit | login-
   history} criteria enable
   ```

3. Legen Sie entweder die Häufigkeit oder Dateigröße fest, mit der ein neues Protokoll erstellt werden soll.

   ```
   hostname (config) # logging files rotation file-type {audit | login-
   history} criteria {frequency {daily | monthly | weekly | yearly} | size
   <megabytes> | size-pct <percentage>}
   ```

# Das Zeitstempelformat mit Hilfe der CLI konfigurieren

Dieses Thema beschreibt die Benutzung von CLI Befehlen, um das syslog Zeitstempelformat festzulegen. Eine vollständige Liste der Protokollierungsbefehle und deren Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um das in Protokollnachrichten verwendete Zeitstempelformat zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Geben Sie den `logging fields timestamp format <format>` Befehl ein, wobei `<format>` eins der Folgenden ist:

   - **rfc-3164**—Verwenden Sie das in RFC-3164 festgelegte Zeitstempfelformat (zum Beispiel, May 13 15:12:01).
   - **rfc-3339**—Verwenden Sie das in RFC-3339 festgelegte Zeitstempelformat (zum Beispiel, 2017-05-15T15:22:33).

   Das folgende Beispiel bestimmt, dass alle Protokollnachrichten das RFC-3339 Format verwenden:

   ```
   hostname (config) # logging fields timestamp format rfc-3339
   ```

3. Bestätigen Sie Ihre Änderungen:

```
hostname (config) # show logging
   Local logging level:                err

   Remote syslog default level:        notice
   No remote syslog servers configured.

Receive remote messages via UDP:       no

Receive remote messages via TCP:       no

Receive remote messages via TLS:       no

Log file rotation:
   Log rotation size threshold:        256 megabytes
   Archived log files to keep:         40

Log format:
   Timestamp format:                   rfc-3339

   Subsecond timestamp field:          disabled

Secure channel logs:                   no
```

4. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

# Die aktive Protokolldatei auf einen Netzwerkspeicherort mit Hilfe der CLI hochladen

Dieses Thema beschreibt die Verwendung von CLI Befehlen zum Hochladen der aktiven Protokolldatei auf einen Netzwerkspeicherort. Eine vollständige Liste der Protokollierungsbefehle und deren Verwendung und Parameter finden Sie in der *CLI Befehlsreferenz*.

## Voraussetzungen

- Admin Zugriff

**Um die aktive Protokolldatei auf einen Netzwerkspeicherort hochzuladen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um die aktive Protokolldatei auf einen bestimmten Netzwerkspeicherort mit Hilfe von file transfer protocol (FTP), trivial file transfer protocol (TFTP), secure copy (SCP) oder SSH file transfer protocol (SFTP) hochzuladen, verwenden Sie den folgenden Befehl:

   ```
   hostname (config) # logging files upload current <uploadURL>
   ```

   Das `<uploadURL>` Parameter bestimmt den Protokoll- und Dateispeicherort.

   - `ftp://<domain>/<path>/<fileName>`
   - `tftp://<domain>/path>/<fileName>`
   - `scp://<username>[:<password>]@<hostname>/<path>/<fileName>`
   - `sftp://<domain>/<path>/<fileName>`

   **HINWEIS:** Für das SCP Protokoll müssen Sie außerdem die Berechtigungen festlegen. Sie können das Passwort auf der Befehlszeile eingeben oder es eingeben, wenn Sie auf der CLI dazu aufgefordert werden.

   Das folgende Beispiel verwenden SCP, um die aktive Protokolldatei auf `logs/FE_log.gz` hochzuladen:

   ```
   hostname (config) # logging files upload current
   scp://it123@example.com/logs/FireEye_log.gz
   Password (if required): ************
   ```

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show log files
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# KAPITEL 18: Sicherung und Wiederherstellung einer Datenbank

In diesem Abschnitt wird beschrieben, wie Sie die Appliance Datenbank sichern und wiederherstellen und Sicherungsdateien auf der Appliance verwalten. Er enthält die folgenden Themen:



## Einführung in Sicherung und Wiederherstellung einer Datenbank

Sie können die Appliance Konfiguration und Daten sichern, wiederherstellen, hochladen, herunterladen und löschen. Sie können eine Datenbank von einer älteren Sicherung wiederherstellen. Sicherungsdateien können gelöscht werden, um Speicherraum für neue Sicherungen zu schaffen.

Sie können steuern, welche Daten gesichert werden, indem Sie eins der folgenden Profile verwenden.

- **config**—Sichert die Konfigurationsdatenbank, die Appliance Konfigurationseinstellungen speichert.
- **config+fedb**—Sichert die Konfigurationsdatenbank, FireEye Appliance Datenbank und Appliance-spezifische Daten.
- **fedb**—Sichert die FireEye Appliance Datenbank.
- **full**—Sichert die Konfigurationsdatenbank, FireEye Appliance Datenbank, Appliance-spezifische Daten und erkannte Daten (Malware, Warnungen, Berichte, Videos und so weiter). Alle erkannten Daten (mit Ausnahme von firmeneigenen FireEye Daten) werden mit diesem Profil gesichert.

**HINWEIS:** Lizenzschlüssel und Guest Images sind nicht in der Sicherung enthalten. Sie müssen die Lizenzschlüssel und Guest Images getrennt erneut installieren. Netzwerkeinstellungen können wiederhergestellt werden.

# Aufgabenliste für Sicherung und Wiederherstellung einer Datenbank

Führen Sie die Schritte zum Sichern und Wiederherstellen der Datenbank in der folgenden Reihenfolge aus:

1. Melden Sie sich auf der Web-UI oder CLI an.
2. Überprüfen Sie den Status des letzten Sicherungs- und Wiederherstellungsvorgangs. Details über die Anzeige des letzten Sicherungs- und Wiederherstellungsvorgangs finden Sie unter Die Ergebnisse der letzten Sicherung und Wiederherstellung anzeigen auf der nächsten Seite.
3. Schätzen Sie den Speicherraum, der für die Sicherungsdatei eines bestimmten Profils benötigt wird. Details über die Schätzung des benötigten Speicherraums finden Sie unter Den für die Sicherung benötigten Speicherraum schätzen auf Seite 312.
4. Bestimmen Sie ein Sicherungsprofil und einen Speicherort für die Sicherungsdatei. Entscheiden Sie, ob die Verschlüsselung mit öffentlichen und privaten Schlüsseln eingeschlossen werden soll. Starten Sie die Sicherung. Details über die Festlegung eines Sicherungsprofils, einschließlich von Verschlüsselung und Start oder Abbruch der Sicherung finden Sie unter Die Datenbank sichern auf Seite 314

   Um zu planen, wie oft Sie den Sicherungsauftrag automatisch ausführen wollen, sehen Sie Automatische Sicherungen planen auf Seite 321.

5. Um die Datenbank wiederherzustellen, wählen Sie die Sicherungsdatei. Details über die Wiederherstellung der Datenbank finden Sie unter Die Datenbank von einer Sicherungsdatei wiederherstellen auf Seite 327.
6. Überwachen Sie den Status des Sicherungs- oder Wiederherstellungsvorgangs.

# Die Ergebnisse der letzten Sicherung und Wiederherstellung anzeigen

Sie können die Details für die letzten Sicherungen und Wiederherstellungen anzeigen. Details der letzten Sicherung und Wiederherstellung schließen Folgendes ein:

- Status der Sicherung oder Wiederherstellung (z.B. "running")
- Typ des Sicherungsprofils oder Wiederherstellungsprofils
- Ziel der Sicherungsdatei oder Quelle der Wiederherstellungsdatei
- Startzeit der Sicherung oder Wiederherstellung
- Endzeit der Sicherung oder Wiederherstellung
- Ergebnis der Sicherung oder Wiederherstellung (z.B. "success")

Nach einer Sicherung oder Wiederherstellung markiert die Appliance das Ergebnis als "success" (Erfolg) oder "failure" (Scheitern). Wenn eine Sicherung oder Wiederherstellung ausgeführt wird, zeigt die Appliance den Status als "running" (in Betrieb) an.

## Voraussetzungen

- Admin Zugriff

## Die Ergebnisse der letzten Sicherung und Wiederherstellung mit Hilfe der Web-UI anzeigen

Die **Backup and Restore** Seite zeigt die Statusdetails über die letzte Sicherung und Wiederherstellung an. Beispiel Statusdetails werden in der folgenden Abbildung angezeigt.

## Den Status der letzten Sicherung und Wiederherstellung mit Hilfe der CLI anzeigen

Verwenden Sie die Befehle in diesem Abschnitt, um den Status für die letzten Sicherungs- und Wiederherstellungsvorgänge zu sehen.

**Um die Details der letzten Sicherung anzuzeigen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie die Details der letzten Sicherung an. Zum Beispiel:

   ```
   hostname # show backup status
   Backup status:                  not-running
   Last backup profile:            full
   Last backup destination:        local
   Last backup start time:         2016/12/08 18:32:58.112
   Last backup end time:           2016/12/08 18:34:26.301
   Last Backup result:             success
   ```

**Um die Details der letzten Wiederherstellung anzuzeigen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie die Details der letzten Wiederherstellung an. Zum Beispiel:

   ```
   hostname # show restore status
   Restore status:                 not-running
   Last restore profile:           fedb
   Last restore source:            usb
   Last restore start time:        2016/12/08 21:13:53.151
   Last restore end time:          2016/12/08 21:13:53.151
   Last restore result:            success
   ```

# Den für die Sicherung benötigten Speicherraum schätzen

Die Appliance schätzt die Größe der Sicherungsdatei und berechnet den benötigten Speicherraum. Der verfügbare Speicherraum muss größer als der geschätzte Speicherraum sein, der für die Ausführung des Sicherungsvorgangs erforderlich ist. Die Größe hängt von dem Profil ab, das Sie auswählen (in Einführung in Sicherung und Wiederherstellung einer Datenbank auf Seite 309 beschrieben).

Details über die Schätzungen von Sicherungen für jedes Profils schließen Folgendes ein:

- Größenschätzung der Datenbankdatei, auf dem Sicherungsprofil basierend
- Verfügbarer Speicherraum, auf dem Sicherungsprofil basierend
- Kann die Sicherung ausgeführt werden

## Voraussetzungen

- Admin Zugriff, um die Schätzung auszuführen
- Monitor, Operator oder Admin Zugriff, um die Sicherungsschätzung mit Hilfe der CLI anzuzeigen (In der Web-UI können diese Rollen nur vorhandene Sicherungsdateien anzeigen, und nicht die Sicherungsschätzung.)

## Den für die Sicherungsdatei benötigten Speicherraum mit Hilfe der Web-UI schätzen

Verwenden Sie die **Backup and Restore** Seite, um den für die Sicherungsdatei benötigten Speicherraum zu schätzen.

**Um den für die Sicherungsdatei benötigen Speicherraum zu schätzen:**

1. Klicken Sie auf den **Settings** Tab.
2. Klicken Sie auf **Appliance Backup & Restore** auf der Seitenleiste.
3. Wählen Sie die Profil, die Sie schätzen wollen. (Sehen Sie Einführung in Sicherung und Wiederherstellung einer Datenbank auf Seite 309 für Beschreibungen.)
4. Klicken Sie in der **Estimate Backup** Spalte auf **Estimate**.

   Details über die Sicherungsschätzungen für das ausgewählte Profil werden angezeigt.

## Den für die Sicherungsdatei benötigten Speicherraum mit Hilfe der CLI schätzen

Verwenden Sie die Befehle in diesem Abschnitt, um den Speicherraum zu schätzen, der für die Sicherungsdatei benötigt wird.

**Um den für die Sicherungsdatei benötigen Speicherraum zu schätzen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie die Schätzung für den Typ des Sicherungsprofils an:
    - Um die Schätzung für die Konfigurationsdatenbank anzuzeigen, geben Sie ein:

      ```
      hostname # show backup estimate profile config
      ```
    - Um die Schätzung für die FireEye Appliance Datenbank anzuzeigen, geben Sie ein:

      ```
      hostname # show backup estimate profile fedb
      ```
    - Um die Schätzung sowohl für die Konfigurationsdatenbank als auch die FireEye Appliance Datenbank anzuzeigen, geben Sie ein:

      ```
      hostname # show backup estimate profile config+fedb
      ```
    - Um die Schätzung für die Konfigurationsdatenbank, FireEye Appliance Datenbank und erkannten Daten (Malware, Warnungen, Berichte u.s.w.) anzuzeigen, geben Sie ein:

      ```
      hostname # show backup estimate profile full
      ```

### Beispiel:

Das folgende Beispiel zeigt die Schätzungen an, die für einen vollständigen Sicherungsvorgang verfügbar sind.

```
hostname # show backup estimate profile full
-----------------------------------------------
         # Estimates for full backup
-----------------------------------------------
  Local space available                : 950462 MB
  Space reserved for other purposes    : 502295 MB
  Space available for backups          : 448167 MB
  Estimated space required for backup  : 1736 MB
  Can perform local or remote backup   : yes
  USB space available                  : 1764 MB
  Can perform USB backup               : yes
```

# Die Datenbank sichern

Sie können die Sicherungsdatei auf drei Arten speichern:

- Auf ein lokales Ziel auf der Appliance
- Auf einen remote Server (dies erstellt zuerst eine lokale Sicherung und überträgt sie dann auf den remote Server)
- Auf ein USB Gerät, das mit Ihrem lokalen Gerät verbunden ist

Verwenden Sie den `media usb mount` Befehl, um das USB Gerät an die angeschlossene Appliance zu hängen. Wenn das USB Gerät angehängt ist, verwenden Sie den `media usb eject` Befehl, um das USB Gerät abzuhängen. Informationen über das An- oder Abhängen eines USB Gerätes finden Sie unter Ein USB Gerät mit Hilfe der CLI mounten oder unmounten auf Seite 287.

Die Appliance muss über ausreichenden Speicherplatz verfügen, um eine Sicherung zu speichern. Sie können mit einer Sicherung nicht fortfahren, wenn auf dem angeforderten Sicherungsziel nicht genügend Speicherraum vorhanden ist. Informationen über die Schätzung des Speicherraums finden Sie unter Den für die Sicherung benötigten Speicherraum schätzen auf Seite 312.

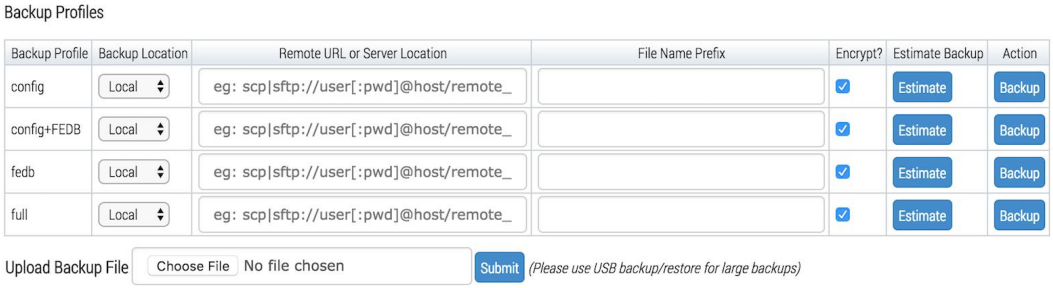
**HINWEIS:** Die Appliance ist vollständig funktionstüchtig, während der Sicherungsvorgang läuft.

## Voraussetzungen

- Admin Zugriff

## Die Datenbank mit Hilfe der Web-UI sichern

Verwenden Sie die **Backup and Restore** Seite, um die Datenbank zu sichern.




**Um die Datenbank zu sichern:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf **Appliance Backup & Restore** auf der Seitenleiste.

3. Finden Sie das Sicherungsprofil und wählen Sie dann den Speicherort für die Sicherung von der Dropdown Liste.
    - **Local**—Speichert die Sicherungsdatei auf ein lokales Ziel auf der Appliance.

      **WICHTIG:** Wenn die Anzahl der Sicherungsdateien auf Ihrer Appliance den festgelegten Grenzwert für Ihre Appliance erreicht, müssen Sie alte Sicherungen löschen, um weiterhin lokale Sicherungen durchführen zu können.

    - **USB**—Speichert die Sicherungsdatei auf ein USB Gerät, das mit Ihrem lokalen Gerät verbunden ist.
    - **Remote**—Speichert die Sicherungsdatei auf einen remote Server. Dies erstellt zunächst eine lokale Sicherung und überträgt sie dann auf den remote Server.

    **HINWEIS:** Eine Beschreibung jedes Sicherungsprofils finden Sie unter Einführung in Sicherung und Wiederherstellung einer Datenbank auf Seite 309.

4. Wenn Sie **RemoteServer** ausgewählt haben, geben Sie den Speicherort der remote Sicherungsdatei in der **Remote URL or Server Location** Spalte ein:

    `scp://<username>:<password>@<hostname>/<directory>`

    wobei `<username>` und `<password>` remot Server Adminberechtigungen sind, `<hostname>` ist der remote Server und `<directory>` ist das Verzeichnis, in dem die Sicherungsdatei gespeichert werden soll.

5. Geben Sie ein benutzerdefiniertes Präfix für den Namen der Sicherungsdatei in der **File Name Prefix** Spalte ein.

    Sie können das Präfix verwenden, um die Liste der Sicherungsdateien zu sortieren.

6. (Optional) Deaktivieren Sie das **Encrypt** Kontrollkästchen, um die Verschlüsselung öffentlicher und privater Schlüssel für Sicherungsvorgänge zu deaktivieren. Jede Sicherungsdatei ist standardmäßig mit Hilfe der öffentlichen und privaten Schlüsselpaare signiert. Standardmäßig ist Verschlüsselung immer in der Sicherung eingeschlossen.

    **HINWEIS:** Verschlüsselung verzögert den Sicherungsvorgang. Sicherungen werden nur mit Hilfe von statischen Schlüsseln verschlüsselt.

7. Klicken Sie auf **Backup** in der **Action** Spalte.

    Eine Fortschrittsleiste zeigt den Status des Sicherungsvorgangs an.

    **HINWEIS:** Um eine laufende Datenbanksicherung abzubrechen, klicken Sie auf das rote **X** in der Fortschrittsleiste.

# Die Datenbank mit Hilfe der CLI sichern

Verwenden Sie die Befehle in diesem Abschnitt, um die datenbank zu sichern.

**Um die Datenbank zu sichern:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Um ein Profil auf einen bestimmten Speicherort zu sichern:

   ```
   hostname (config) # backup profile <profile> to <backup location>
   [prefix <prefix>]
   ```

   **Parameter**

   *profile*

   Bestimmen Sie den **Profil**typ für die Sicherung.

   - **config**: Um das Profil für die Konfigurationsdatenbank einzustellen:
   - **fedb**: Um das Profil für die Network Security Appliance Datenbank einzustellen:
   - **config+fedb**: Um das Profil sowohl für die Konfigurationsdatenbank als auch die Network Security Appliance Datenbank einzustellen:
   - **full**: Um das Profil für die Konfigurationsdatenbank, Network Security Appliance Datenbank und erkannten Daten (Malware, Alarme, Berichte u.s.w.) einzustellen:

   *Speicherort für die Sicherung*

   Bestimmen Sie den **Speicherort** für die Sicherungsdatei.

   - **local**: Um die Sicherungsdatei auf ein lokales Ziel auf der Appliance zu speichern:

     **WICHTIG:** Wenn die Anzahl der Sicherungsdateien auf Ihrer Appliance den festgelegten Grenzwert für Ihre Appliance erreicht, müssen Sie alte Sicherungen löschen, um weiterhin lokale Sicherungen durchführen zu können.

     Der folgende Befehl löscht automatisch die älteste lokale Sicherungsdatei (wenn das Limit für Sicherungsdateien überschritten wird) und sichert dann die Appliance: `backup profile <profile> to local auto-delete-old`. Details finden Sie in der CLI Befehlsreferenz.

     Details über die Festlegung eines Grenzwertes für die Anzahl von Sicherungsdateien finden Sie unter Die Anzahl der Sicherungsdateien auf Ihrer Appliance begrenzen auf Seite 320.

   - **usb**: Um die Sicherungsdatei auf ein USB-Laufwerk auf Ihrem lokalen Gerät zu speichern:

- **url**: Um die Sicherungsdatei auf einem remote Server zu speichern:

  wobei `<url>` remote Server-Administratorberechtigungen (`<username>` und `<password>`), den remote Server ( `<hostname>`)) und das Verzeichnis, in dem die Sicherungsdatei gespeichert werden soll (`<directory>` ) im folgenden Format festlegt:

  ```
  scp://<username>[:<password>]@<hostname>/<directory>
  ```

  **HINWEIS:** Wenn Sie das Administrator-Passwort für den remote Host nicht im `backup profile` Befehl festlegen (wobei das Passwort als Klartext sichtbar sein würde), fordert die CLI Eingabe des Passworts und verschleiert die Tastatureingabe, während Sie tippen.

  Eine remote Sicherung erstellt zuerst eine lokale Sicherung und überträgt Sie dann auf den remote Server.

*Präfix*

Bestimmt ein benutzerdefiniertes Präfix für den Namen der Sicherungsdatei:

3. (Optional) Überwachen Sie den Fortschritt des Sicherungsvorgangs.
   - Um die Fortschrittsverfolgung für den Sicherungsvorgang zu deaktivieren:

     ```
     hostname (config) # backup profile <profile> to <backup location> progress no-track
     ```

   - Um die Fortschrittsverfolgung für den Sicherungsvorgang zu aktivieren:

     ```
     hostname (config) # backup profile <profile> to <backup location> progress track
     ```

   Standardmäßig ist Fortschrittsverfolgung aktiviert.

4. (Optional) Deaktivieren Sie öffentliche und private Schlüsselverschlüsselung für den Sicherungsvorgang:

   ```
   hostname (config) # backup profile <profile> to <backup location> no-encryption
   ```

   Im folgenden Beispiel wird die Appliance Datenbank auf ein lokales Ziel auf der Appliance ohne Verschlüsselung gesichert.

   ```
   hostname (config) # backup profile fedb to local no-encryption
   ```

   **HINWEIS:** Verschlüsselung ist standardmäßig aktiviert. Verschlüsselung verzögert den Sicherungsvorgang. Sicherungen werden nur mit Hilfe von statischen Schlüsseln verschlüsselt.

**HINWEIS:** Um eine laufende Sicherung abzubrechen, geben Sie den `backup cancel` Befehl ein. Wenn Sie den laufenden Sicherungsvorgang abbrechen, beendet das System den aktuellen Schritt, bevor der gesamte Vorgang abgebrochen wird.

## Beispiele

**HINWEIS:** Die folgenden Beispiele stammen von einer Virtual Execution Appliance, aber sie treffen auch auf Network Security Appliances zu.

Im folgenden Beispiel werden die Konfigurationsdatenbank, erkannte Daten sowie Artefakte auf ein lokales Ziel auf der Appliance gesichert.

```
hostname (config) # backup profile full to local
Step 1 of 5: Performing Sanity checks
100.0%  [##########################################################################]
Step 2 of 5: Backing up config db
100.0%  [##########################################################################]
Step 3 of 5: Backing up fedb
100.0%  [##########################################################################]
Step 4 of 5: Backing up Artifacts
100.0%  [##########################################################################]
Step 5 of 5: Generating Backup package
100.0%  [##########################################################################]
```

Im folgenden Beispiel werden die Konfigurationsdatenbank, erkannte Daten sowie Artefakte auf ein remote Ziel gesichert.

```
hostname (config) # backup profile full to scp://remoteAdmin3@vx-2/vx-2-bkp
Password (if required): ********
Step 1 of 4:  Performing Sanity checks
100.0%  [##########################################################################]
Step 2 of 4:  Backing up config db
100.0%  [##########################################################################]
Step 3 of 4:  Generating backup package
100.0%  [##########################################################################]
Step 4 of 4:  Transferring backup to remote loc
100.0%  [##########################################################################]
```

# Die Anzahl der Sicherungsdateien auf Ihrer Appliance begrenzen

Für **Local Backups** können Sie einen Grenzwert für die Anzahl der Sicherungsdateien festlegen, die auf Ihrer Appliance gespeichert werden können. Wenn die Anzahl der Sicherungsdateien auf Ihrer Appliance den festgelegten Grenzwert erreicht, müssen Sie alte Sicherungen löschen, um weiterhin lokale Sicherungen durchführen zu können.

**HINWEIS:** Standardmäßig ist die Höchstzahl von Sicherungsdateien, die auf Ihrer Appliance gespeichert werden können, **25**.

**Um die Höchstzahl von Sicherungsdateien festzulegen, die auf Ihrer Appliance gespeichert werden können:**

1. Gehen Sie auf den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. (Optional) Um die Details für lokale Sicherungsdateien anzuzeigen, wie z.B. Zähler und Dateinamen:

   ```
   hostname (config) # show backup available local list
   ```

3. Legen Sie die Höchstzahl von Sicherungsdateien fest, die auf Ihrer Appliance gespeichert werden können.

   ```
   hostname (config) # backup limit <max-number-of-backups-allowed>
   ```

   Nachdem der Backupzähler auf der Appliance die Höchstzahl erreicht, müssen Sie die alten Sicherungen löschen, um Platz für neue zu schaffen. Informationen über die Löschung von Sicherungsdateien finden Sie unter Ältere Sicherungsdateien mit Hilfe der CLI löschen auf Seite 332.

4. (Optional) Um das benutzerdefinierte Höchstzahl für Sicherungen auf den Standardwert zurückzusetzen:

   ```
   hostname (config) # backup reset maxcount
   ```

# Automatische Sicherungen planen

Sie können automatische Sicherungsaufträge konfigurieren und aktivieren. Sie können festlegen, wie oft der Sicherungsauftrag automatisch ausgeführt werden soll.

**HINWEIS:** Sie können automatische Sicherungsaufträge nur mit Hilfe der CLI planen.

## Voraussetzungen

- Admin Zugriff
- Ausreichender Speicherraum für automatische Sicherungen

  **WICHTIG!** Zusätzlicher Speicherraum ist erforderlich, wenn Sie planen, automatische Sicherungen regelmäßig auszuführen. Sie müssen die generierten Sicherungen überwachen und unnötige Sicherungen löschen.

## Automatische Sicherungen mit Hilfe der CLI planen

Verwenden Sie die Befehle in diesem Abschnitt, um automatische Sicherungen für die Datenbank zu planen.

**Um den geplanten Sicherungsauftrag zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Erstellen Sie den Auftrag, indem Sie die Job ID festlegen:.

   ```
   hostname (config) # job <jobID>
   ```

3. Bestimmen Sie die Sequenznummer für den geplanten Sicherungsauftrag.

   ```
   hostname (config) # job <jobID> command <sequenceNumber>
   ```

4. Verwenden Sie den `backup profile` Befehl, um den Profiltyp festzulegen.

   ```
   hostname (config) # job <jobID> command <sequenceNumber> "backup
   profile <profile>"
   ```

   - Um den Sicherungsauftrag für die Konfigurationsdatenbank zu planen:

     ```
     hostname (config) # job <jobID> command <sequenceNumber> "backup
     profile config"
     ```

   - Um den Sicherungsauftrag für die FireEye Appliance zu planen:

     ```
     hostname (config) # job <jobID> command <sequenceNumber> "backup
     profile fedb"
     ```

   - Um den Sicherungsauftrag für die Konfigurationsdatenbank sowie die FireEye Appliance zu planen:

     ```
     hostname (config) # job <jobID> command <sequenceNumber> "backup
     profile config+fedb"
     ```

   - Um die Sicherungsaufgabe für die Konfigurationsdatenbank, FireEye Appliance Datenbank und erkannte Daten (Maolware, Warnungen, Berichte u.s.w.) zu planen:

     ```
     hostname (config) # job <jobID> command <sequenceNumber> "backup
     profile full"
     ```

5. Verwenden Sie den `backup profile` Befehl, um den Speicherort für die Sicherungsdatei festzulegen.

   ```
   hostname (config) # job <jobID> command <sequenceNumber> "backup
   profile <profile> to <backupLocation>"
   ```

   - Um den Sicherungsauftrag auf ein lokales Ziel auf der Appliance zu planen:

     ```
     hostname (config) # job <jobID> command <sequenceNumber> "backup
     profile <profile> to local"
     ```

   - Um den Sicherungsauftrag auf einem Remoteserver zu planen:

     ```
     hostname (config) # job <jobID> command <sequenceNumber> "backup
     profile <profile> to <url>"
     ```

     wobei `<url>` der festgelegte remote Speicherort mit Hilfe des folgenden Formats ist:

     ```
     scp://<username>:<password>@<hostname>/<remotePath>
     ```

   - Um den Sicherungsauftrag auf ein USB Laufwerk auf Ihrem lokalen Gerät zu planen:

     ```
     hostname (config) # job <jobID> command <sequenceNumber> "backup
     profile <profile> to usb"
     ```

6. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um automatische Sicherungen für die Datenbank zu planen:**

1. Legen Sie fest, wie oft die Sicherungsaufgabe automatisch ausgeführt werden soll.

   - Um täglich zu planen, geben Sie das Enddatum, Startdatum oder Uhrzeit ein:

     ```
     hostname (config) # job <jobID> schedule daily end date
     <yyyy/mm/dd>
     ```

     ```
     hostname (config) # job <jobID> schedule daily start date
     <yyyy/mm/dd>
     ```

     ```
     hostname (config) # job <jobID> schedule daily time <hh:mm:ss>
     ```

     Die Parameterwerte sind wie folgt:

     - `<yyyy/mm/dd>` legt das End- oder Startdatum für die Sicherungsaufgabe fest.
     - `<hh:mm:ss>` legt die Startzeit für die Sicherungsaufgabe im 24-Stunden Format fest.

   - Um monatlich zu planen, geben Sie ein:

     ```
     hostname (config) # job <jobID> schedule monthly day-of-month
     <day>
     ```

     wobei `<day>` der Tag des Monats ist, an dem die Sicherung stattfinden soll.

- Um einmal zu planen, geben Sie ein:

  ```
  hostname (config) # job <jobID> schedule once time <hh:mm:ss> date <yyyy/mm/dd>
  ```

  Die Parameterwerte sind wie folgt:

  - <hh:mm:ss> legt die Startzeit für die Sicherungsaufgabe im 24-Stunden Format fest.
  - <yyyy/mm/dd> Legt das Startdatum für die Sicherungsaufgabe fest.

- Um eine Sicherung zu planen, die regelmäßig nach einem von Ihnen definierten Zeitplan ausgeführt werden soll, geben Sie das End- und Startdatum oder den Zeitintervall ein.

  ```
  hostname (config) # job <jobID> schedule periodic end
  date <yyyy/mm/dd> time  <hh:mm:ss>
  ```

  ```
  hostname (config) # job <jobID> schedule periodic start
  date <yyyy/mm/dd> time  <hh:mm:ss>
  ```

  ```
  hostname (config) # job <jobID> schedule periodic interval
  <timeInterval>
  ```

  Die Parameterwerte sind wie folgt:

  - <yyyy/mm/dd> legt das End- oder Startdatum für die Sicherungsaufgabe fest.
  - <hh:mm:ss> legt die End- oder Startzeit für die Sicherungsaufgabe im 24-Stunden Format fest.
  - <timeInterval> ist im Format von "2h3m4s."

- Um wöchentlich zu planen:

  ```
  hostname (config) # job <jobID> schedule <frequency> weekly day-of-week <day>
  ```

  Das <day> Parameter ist der Wochentag, an dem der Sicherungsauftrag stattfinden soll. Gültige Werte sind `sun` (Sonntag), `mon` (Montag), `tue` (Dienstag), `wed` (Mittwoch), `thu` (Donnerstag), `fri` (Freitag) und `sat` (Samstag).

- Um einen Zeitplantyp festzulegen, geben Sie ein:

  ```
  hostname (config) # job <jobID> schedule <type>
  ```

  wobei <type> der Zeitplantyp für die Sicherungsaufgabe ist. Gültige Werte sind:

| Wert | Beschreibung |
|---|---|
| once | Die Sicherung wird nur einmal ausgeführt |
| daily | Die Sicherung wird täglich ausgeführt |
| weekly | Die Sicherung wird wöchentlich ausgeführt |
| monthly | Die Sicherung wird monatlich ausgeführt |
| periodic | Die Sicherung wird automatisch nach einem von Ihnen definierten Zeitplan ausgeführt |

2. Aktivieren Sie die Konfiguration für den geplanten Sicherungsauftrag.

   ```
   hostname (config) # job <jobID> enable
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

4. Überprüfen Sie den Status für den geplanten Sicherungsauftrag. Zum Beispiel:

   ```
   hostname (config) # show job

   Job 333:
      Status:              pending
      Enabled:             yes
      Continue on failure: no

      Schedule type:       daily
      Time and date:       2016/08/16 00:00:00 +0000

      Last exec time:      N/A
      Next exec time:      Sun 2016/08/17 00:00:00 +0000
      Commands:
         Command 1: backup profile config to local
   ```

# Sicherungsdateien herunterladen

Sie können Sicherungsdateien von der Appliance auf Ihr lokales Gerät herunterladen.

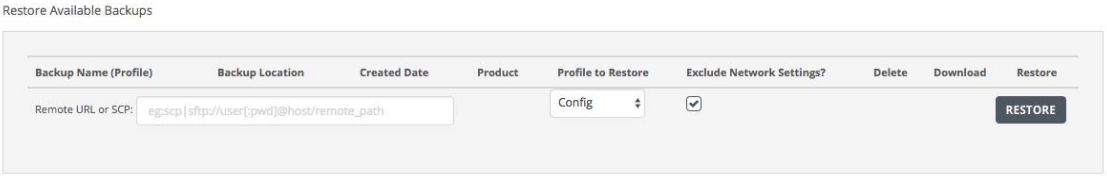
**HINWEIS:** Eine Sicherungsdatei wird nur mit Hilfe der Web-UI heruntergeladen.

## Voraussetzungen

- Admin Zugriff

## Sicherungsdateien mit Hilfe der Web-UI herunterladen

Verwenden Sie die **Backup and Restore** Seite, um eine Sicherungsdatei von der Appliance auf Ihre lokale Maschine herunterzuladen.




**HINWEIS:** Diese Abbildung stammt von einer Email Security — Server Edition Appliance, trifft aber auch auf Network Security Appliances zu.

**Um eine Datenbank-Sicherungsdatei herunterzuladen:**

1. Klicken Sie auf den **Settings** Tab.
2. Klicken Sie auf **Appliance Backup & Restore** auf der Seitenleiste.
3. Im **Restore Available Backups** Abschnitt finden Sie die Sicherungs-FEBKP Datei in der **Backup name (Profile)** Spalte.
4. Klicken Sie auf den grünen Pfeil in der **Download** Spalte, um die Sicherung herunterzuladen.

# Sicherungsdateien hochladen

Sie können Sicherungsdateien von Ihrem lokalen Gerät auf die Appliance hochladen Eine Sicherungsdatei wird verwendet, um die Datenbank für mehrere Appliances wiederherzustellen. Die hochgeladenen Sicherungsdateien werden am selben Speicherort gespeichert, auf dem Sie die lokalen Sicherungsdateien gespeichert haben.

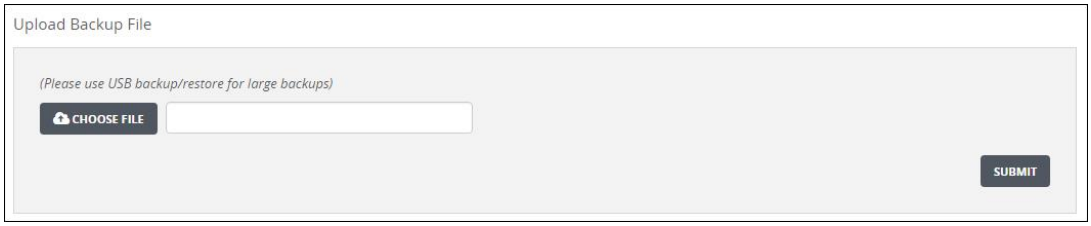
**HINWEIS:** Sie können die Web-UI zu Hochladen einer Sicherungsdatei verwenden oder die Sicherungsdatei direkt über SCP auf das /data/fe-backups Verzeichnis auf der Appliance kopieren.

## Voraussetzungen

- Admin Zugriff

## Sicherungsdateien mit Hilfe der Web-UI hochladen

Verwenden Sie die **Backup and Restore** Seite, um eine Sicherungsdatei von Ihrer lokalen Maschine auf die Appliance hochzuladen.




**Um eine Sicherungsdatei von Ihrer lokalen Maschine hochzuladen.**

1. Klicken Sie auf den **Settings** Tab.
2. Klicken Sie auf **Appliance Backup & Restore** auf der Seitenleiste.
3. Im **Upload Backup File** Bereich klicken Sie auf **Choose File** und navigieren Sie dann auf die Sicherungsdatei, die Sie hochladen wollen.
4. Klicken Sie auf **Submit**, um die Sicherungsdatei von Ihrer lokalen Maschine hochzuladen.

   Ein Fehler tritt auf, wenn eine ungültige Sicherungsdatei hochgeladen wird.

# Die Datenbank von einer Sicherungsdatei wiederherstellen

Sie können die Sicherheit von drei Standorten wiederherstellen:

- Von Ihrer lokalen Appliance
- Von einem remote Server. Stellen Sie die aktuellen Netzwerkeinstellungen nicht wieder her, während die Appliance einen Wiederherstellungsvorgang von einem remote Server ausführt.
- Von einem mit Ihrer lokalen Maschine verbundenen Gerät.

## Nutzungsrichtlinien

Folgen Sie diesen Nutzungsrichtlinien wenn Sie die Datenbank von einer Sicherungsdatei wiederherstellen:

- Die Anwendung ist während der Wiederherstellung nicht vollständig funktionsfähig. Beispielsweise wird der Erkennungsvorgang für Alarme während der Wiederherstellung gestoppt.

- Die Wiederherstellung kann nicht während der Ausführung abgebrochen werden.
- Wenn die Wiederherstellung fehlschlägt, können Sie die Appliance auf die werkseitig installierten Standards zurücksetzen. Wenn Sie nur die Konfigurationsdatenbank wiederherstellen, wird die Appliance automatisch auf die ursprüngliche Konfiguration zurückgesetzt.
- Nur die config, config+fedb und fedb Sicherungsprofile können von einer Softwareaktualisierung wiederhergestellt werden. Die Sicherung kann nicht von einer Softwarezurückstufung wiederhergestellt werden.
- Eine Sicherung kann nicht aus einer anderen Produktfamilie wiederhergestellt werden.
- Eine Sicherung kann nicht von einer Version vor Network Security 7.5.0 wiederhergestellt werden.

## Voraussetzungen

- Admin Zugriff
- Bestätigen Sie, dass Sie eine FEBKP Datei der aktuellen Datenbank haben, bevor Sie mit der Wiederherstellung beginnen.
- Finden Sie die vorherige Sicherung, die Sie wiederherstellen wollen.
- Bestätigen Sie die Details für die Appliance, Sicherungsprofil, Version, Hostname und Datenstempel. Diese Details werden überprüft, während die Wiederherstellung ausgeführt wird.

## Die Datenbank von einer Sicherungsdatei mit Hilfe der Web-UI wiederherstellen

Verwenden Sie die **Backup and Restore** Seite, um die Datenbank von einer Sicherungsdatei wiederherzustellen.


**HINWEIS:** Diese Abbildung stammt von einer Email Security — Server Edition Appliance, trifft aber auch auf Network Security Appliances zu.

**Um die Datenbank von einer Sicherungsdatei wiederherzustellen:**

1. Klicken Sie auf den **Settings** Tab.
2. Klicken Sie auf **Appliance Backup & Restore** auf der Seitenleiste.

3. Finden Sie die Sicherungs FEBKP Datei, die Sie wiederherstellen wollen, in der **Backup Name (Profile)** Spalte.

   Sie können alles mit Hilfe eines vollständigen Profils wiederherstellen oder Teile mit Hilfe eines der anderen Profile.

4. Wenn Sie Remote Server ausgewählt haben, scrollen Sie nach unten, um den Speicherort der remote Sicherungsdatei im **Remote URL oder SCP** Feld einzugeben:

   ```
   {scp|sftp}://<username>:<password>@<hostname>/<filePath>
   ```

   wobei `<username>` und `<password>` remote Server Administratorberechtigungen, `<hostname>` der remote Host und `<filepath>` der vollständige Pfad der Sicherungsdatei ist.

   Wählen Sie dann das Profil aus, das Sie von der Dropdown-Liste wiederherstellen wollen.

5. (Optional) Löschen Sie das **Exclude Network Settings** Kontrollkästchen, um die Netzwerkeinstellungen aus der Sicherungsdatei einzuschließen. Standardmäßig sind die Netzwerkeinstellungen nicht im Wiederherstellungsvorgang enthalten.

   **ACHTUNG!** Stellen Sie die aktuellen Netzwerkeinstellungen nicht wieder her, während die Appliance einen Wiederherstellungsvorgang von einem remote Server ausführt.

6. Klicken Sie auf **Restore**, um die Sicherung wiederherzustellen.
7. Klicken Sie im Bestätigungsdialogfeld auf **Yes**.

   **HINWEIS:** Die Appliance ist während der Wiederherstellung nicht vollständig funktionsfähig. Die Wiederherstellung kann nicht während der Ausführung abgebrochen werden.

   Das Guest Image und Lizenzschlüssel müssen getrennt eingegeben werden.

# Die Datenbank von einer Sicherungsdatei mit Hilfe der CLI wiederherstellen

Verwenden Sie die Befehle in diesem Abschnitt, um die Datenbank von einer Sicherungsdatei wiederherzustellen.

**Um die Datenbank von einer Sicherungsdatei wiederherzustellen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Finden Sie die Sicherungs- FEBKP Datei, die Sie wiederherstellen wollen.

- Um eine Liste der Sicherungsdateien auf dem USB Laufwerk anzuzeigen:

  ```
  hostname (config) # show backup available on-usb
  ```

- Um eine Liste der Sicherungsdateien anzuzeigen:

  ```
  hostname (config) # show backup available local
  ```

3. Legen Sie ein Sicherungsprofil fest.

   - Um das Profil für die Konfigurationsdatenbank einzustellen:

     ```
     hostname (config) # restore profile config
     ```

   - Um das Profil für die Appliance Datenbank einzustellen:

     ```
     hostname (config) # restore profile fedb
     ```

   - Um das Profil für die Konfigurationsdatenbank sowie der Appliance Datenbank einzustellen:

     ```
     hostname (config) # restore profile config+fedb
     ```

   - Um das Profil für die Konfigurationsdatenbenk, Appliance Datenbank und erkannten Daten (Malware, Alarme, Berichte u.s.w.) einzustellen:

     ```
     hostname (config) # restore profile full
     ```

4. Bestimmen Sie den Speicherort der Sicherungsdatei.

   - Um die Sicherung von dem lokalen Ziel auf der Network Security Appliance wiederherzustellen:

     ```
     hostname (config) # restore profile <profile> from local
     ```

   - Um die Sicherung von einem remote Server wiederherzustellen:

     ```
     hostname (config) # restore profile <profile> from <url>
     ```

     wobei `<url>` remote Server Administratorberechtigungen festlegt (`<username>` und `<password>`), den remote Server (`<hostname>`)und den vollständigen Pfad der Sicherungsdatei (`<filepath>`) im folgenden Format:

     ```
     {scp|sftp}://<username>[:<password>]@<hostname>/<filepath>
     ```

     **HINWEIS:** Wenn Sie das remote Host Administratorpassword nicht im `restore profile` Befehl festlegen (wobei das Passwort als Klartext sichtbar sein würde), fordert CLI das Passwort an und verschleiert die Tastataureingabe während Sie tippen.

   - Um die Sicherung von einem USB Laufwerk auf Ihrem lokalen Gerät wiederherzustellen:

     ```
     hostname (config) # restore profile <profile> from usb
     ```

5. Geben Sie den Namen der Sicherungsdatei ein:

   ```
   hostname (config) # restore profile <profile> from <backupLocation>
   backup <name>
   ```

6. (Optional) Stellen Sie die Netzwerkeinstellungen von der relevanten Sicherung wieder her:

   ```
   hostname (config) # restore profile <profile> from <backupLocation>
   backup <name> include-network-config
   ```

   **VORSICHT!** Stellen Sie die aktuellen Netzwerkeinstellungen nicht wieder her während die Network Security Appliance einen Wiederherstellungsvorgang von einem remote Server ausführt.

7. (Optional) Überwachen Sie den Fortschritt der Wiederherstellungsvorgangs. Fortschrittsverfolgung ist standardmäßig aktiviert.

   - Um Fortschrittsverfolgung für den Wiederherstellungsvorgang zu deaktivieren:

     ```
     hostname (config) # restore profile <profile>
     from <backupLocation> backup <name> progress no-track
     ```

   - Um Fortschrittsverfolgung für den Wiederherstellungsvorgang zu aktivieren:

     ```
     hostname (config) # restore profile <profile>
     from <backupLocation> backup <name> progress track
     ```

     Sie können die Fortschrittsverfolgung mit Hilfe von **Strg+C** abbrechen. Der Wiederherstellungsvorgang wird im Hintergrund fortgeführt. Verwenden Sie den `show restore status` Befehl, um den Status des Wiederherstellungsvorgangs zu finden.

## Beispiel:

Das folgende Beispiel zeigt die Wiederherstellung der Sicherung einer Konfigurationsdatenbank von einer lokalen Appliance.

```
hostname (config) # restore profile config from local backup vx-Config-7.9.0-
vx-2-20160802-239500.febkp
Password (if required): ********
Step 1 of 4:  Performing Sanity checks
 100.0%  [#########################################################################]
Step 2 of 4:  Extracting backup package
 100.0%  [#########################################################################]
Step 3 of 4:  Restoring config db
 100.0%  [#########################################################################]
Step 4 of 4:  Restart system services
 100.0%  [#########################################################################]
```

**HINWEIS:** Dieses Beispiel stammt von einer Virtual Execution Appliance, aber es trifft auch auf Network Security Appliances zu.

# Ältere Sicherungsdateien löschen

Sie können ältere Sicherungsdateien löschen, um Platz für neue Sicherungsdateien zu schaffen.

## Voraussetzungen

- Admin Zugriff

## Ältere Sicherungsdateien mit Hilfe der Web-UI löschen

Verwenden Sie die **Backup and Restore** Sseite, um eine Sicherungsdatei zu löschen.


**HINWEIS:** Diese Abbildung stammt von einer Email Security — Server Edition Appliance, trifft aber auch auf Network Security Appliances zu.

**Um eine Sicherung zu löschen:**

1. Klicken Sie auf den **Settings** Tab.
2. Klicken Sie auf **Appliance Backup & Restore** auf der Seitenleiste.
3. Im **Restore Available Backups** Bereich finden Sie die Sicherungs-FEBKP Datei, die Sie löschen wollen, in der **Backup Name (Profile)** Spalte.
4. Klicken Sie auf das Symbol in der **Delete** Spalte.
5. Klicken Sie auf **Yes**, um die Aktion zu bestätigen.

## Ältere Sicherungsdateien mit Hilfe der CLI löschen

Verwenden Sie die Kommentare in diesem Abschnitt, um ältere Sicherungsdateien zu löschen

**WICHTIG!** Wenn Sie eine Sicherungsdatei von einem USB-Laufwerk mit Hilfe des `backup delete from usb` Befehls löschen, könnte die Löschung einige Minuten dauern.

**Um eine Sicherungsdatei zu löschen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Bestimmen Sie den Speicherort der Sicherungsdatei.

   - Um eine Datei von der Appliance zu löschen, geben Sie ein:

     ```
     hostname (config) # backup delete from local
     ```

   - Um eine Datei von einem USB-Laufwerk auf Ihrem lokalen Gerät zu entfernen, geben Sie ein:

     ```
     hostname (config) # backup delete from usb
     ```

     **HINWEIS:** Um eine remote Sicherungsdatei zu löschen, müssen Sie sich auf dem Remoteserver anmelden und die Datei manuell löschen.

3. Bestimmen Sie den Namen der Sicherungsdatei, um sie vom Speicherort der Sicherung zu löschen.

   ```
   hostname (config) # backup delete from <backupLocation> name
   <backupName>
   ```

   wobei `<backupName>` die Sicherungs-FEBKP Datei ist, die Sie löschen wollen.

## Beispiel:

Das folgende Beispiel zeigt, wie Sie eine Datenbank-Sicherung löschen, die sich lokal auf einer Appliance befindet.

```
hostname (config) # backup delete from local name wMPS-Config-7.9.0-IE-NX900-
20160807-220207.febkp
```

# KAPITEL 19: Systemintegrität und Leistung

Die Network Security Appliances bietet Informationen über ihre Integrität und Status.

- Ergebnisse von Systemintegrität- und Leistungsüberprüfung anzeigen auf Seite 339
- Deploymentprüfung auf Seite 343
- Auslastungs- und Leistungsprüfungen auf Seite 356

Informationen zum Überprüfen des Status eines MVX Clusters finden Sie unter *FireEyeNetwork Security Deploymenthandbuch für MVX Smart Grid*

## Voraussetzungen

- Monitor, Operator, Analyst oder Admin Zugriff

# Systemintegrität Erzwingung

FireEye ermöglicht Ihnen, die Höchstzahl von VMs je nach Bedarf dynamisch anzupassen und VM Ressourcen dynamisch zwischen URL- und Datei- Managementanforderungen zuzuordnen.

## VM-Drosselung

Integrierte Appliances, die die integrierte Analyseengine vewenden, können die Höchstzahl von VMs je nach der aktuellen Systembelastung anpassen. Der Systemzustand wird überwacht und die Belastung wird dynamisch angepasst, um den besten Durchsatz und die beste Erkennungsstabilität für eine größere Bandbreite von Verkehrsprofilen und -mustern zu erzielen. (Folglich ist VM-Drosselung eine Form der QoS-Erzwingung.) Die Appliance bleibt maximal geladen, aber nicht überlastet.

Die CLI ist

```
[no] analysis vm-throttling [auto | disable
```

wobei **auto** die Verwendung der Systemeinstellungen auf der Appliance (für Typ, Modell, Image und Version spezifisch) und **disable** die Deaktivierung der Drosselung, unabhängig von den Einstellungen bedeutet.

Diese Funktion ist standardmäßig aktiviert.

## Voraussetzungen

- Dynamische Analyse
- Admin Zugriff
- "auto" Systemeinstellungen (wenn vorher deaktiviert; führen Sie **no analysis vm-throttling disable** aus, um erneut zu aktivieren.)

**Um doie**

1. Wechseln Sie in den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie VM-Drosselung:

   ```
   hostname (config) # analysis vm-throttling disable
   ```

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show analysis config
   Non-malicious duplicate file timeout : 24
   Malicious duplicate file timeout : 4

   Non-malicious duplicate URL timeout : 4
   Malicious duplicate URL timeout : 2

   Analysis reset duplicate URL timeout : 2017/08/13 01:51:34

   Blacklist retroactive hunting : Enabled
   Blacklist retroactive hunting time : 0 hours

   VM throttling : Disabled

   Riskware detection : Disabled
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um die VM-Drosselung nach manueller Deaktierung erneut zu aktivieren:**

1. Wechseln Sie in den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Aktivieren Sie VM-Drosselung:

   ```
   hostname (config) # analysis vm-throttling auto
   ```

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show analysis config
   Non-malicious duplicate file timeout : 24
   Malicious duplicate file timeout : 4

   Non-malicious duplicate URL timeout : 4
   Malicious duplicate URL timeout : 2

   Analysis reset duplicate URL timeout : 2017/08/13 01:51:34

   Blacklist retroactive hunting : Enabled
   Blacklist retroactive hunting time : 0 hours

   VM throttling : AUTO
   NX dynamic split : AUTO

   Riskware detection : Disabled
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## VM Dynamic Split (nur integrierte Network Security Appliances)

Integrierte NX Appliances können Ihre VM-Zuordnung zwischen URL und Dateianalyse dynamisch anpassen. In früheren Ausgaben hatte das System 75% der VMs statisch der URL-Übermittlung und 25% der Dateianalyse zugewiesen. Das System kann den Schwellenwert ändern. Je mehr VMs der Dateianalyse zugewiesen sind, desto schnelle wird eine Dateiwarteschlange verarbeitet.

Diese Funktion erfordert VM-Drosselung für die Aktivierung. (Siehe VM-Drosselung auf Seite 335

Die CLI ist

```
[no] analysis nx-dynamic-split [auto | disable
```

wobei **auto** die Verwendung der Systemeinstellungen auf der Appliance (für Typ, Modell, Image und Version spezifisch) und **disable** die Deaktivierung von Dynamic Split, unabhängig von den Einstellungen bedeutet.

Diese Funktion ist standardmäßig aktiviert.

## Voraussetzungen

- Integriertes NX
- VM-Drosselung aktiviert
- Admin Zugriff
- "auto" Systemeinstellungen (wenn vorher deaktiviert; führen Sie **no analysis nx-dynamic-split disable** aus, um erneut zu aktivieren.)

**Um die Deaktivierung der VM dynamischen Teilung zu erzwingen:**

1. Gehen Sie auf CLI Konfigurierung:
   ```
   hostname > enable
   hostname # configure terminal
   ```
2. Deaktivieren Sie dynamische Teilung:
   ```
   hostname (config) # analysis nx-dynamic-split disable
   ```
3. Bestätigen Sie Ihre Änderungen:
   ```
   hostname (config) # show analysis config
   Non-malicious duplicate file timeout : 24
   Malicious duplicate file timeout : 4

   Non-malicious duplicate URL timeout : 4
   Malicious duplicate URL timeout : 2

   Analysis reset duplicate URL timeout : 2017/08/13 01:51:34

   Blacklist retroactive hunting : Enabled
   Blacklist retroactive hunting time : 0 hours

   VM throttling : AUTO
   NX dynamic split : Disabled

   Riskware detection : Disabled
   ```
4. Speichern Sie Ihre Änderungen:
   ```
   hostname (config) # write memory
   ```

**Um die VM dynamische Teilung nach manueller Deaktivierung erneut zu aktivieren:**

1. Gehen Sie auf CLI Konfigurierung:
   ```
   hostname > enable
   hostname # configure terminal
   ```
2. Aktivieren Sie dynamische Teilung:
   ```
   hostname (config) # analysis nx-dynamic-split auto
   ```
3. Bestätigen Sie Ihre Änderungen:
   ```
   hostname (config) # show analysis config
   Non-malicious duplicate file timeout : 24
   Malicious duplicate file timeout : 4

   Non-malicious duplicate URL timeout : 4
   Malicious duplicate URL timeout : 2

   Analysis reset duplicate URL timeout : 2017/08/13 01:51:34

   Blacklist retroactive hunting : Enabled
   Blacklist retroactive hunting time : 0 hours

   VM throttling : AUTO
   NX dynamic split : AUTO

   Riskware detection : Disabled
   ```
4. Speichern Sie Ihre Änderungen:
   ```
   hostname (config) # write memory
   ```

# Ergebnisse von Systemintegrität- und Leistungsüberprüfung anzeigen

Sie könnten allgemeine Statusinformationen über die Ergebnisse von Systemintegritäts- und Appliance Leistungsüberprüfung anzeigen.

## Voraussetzungen

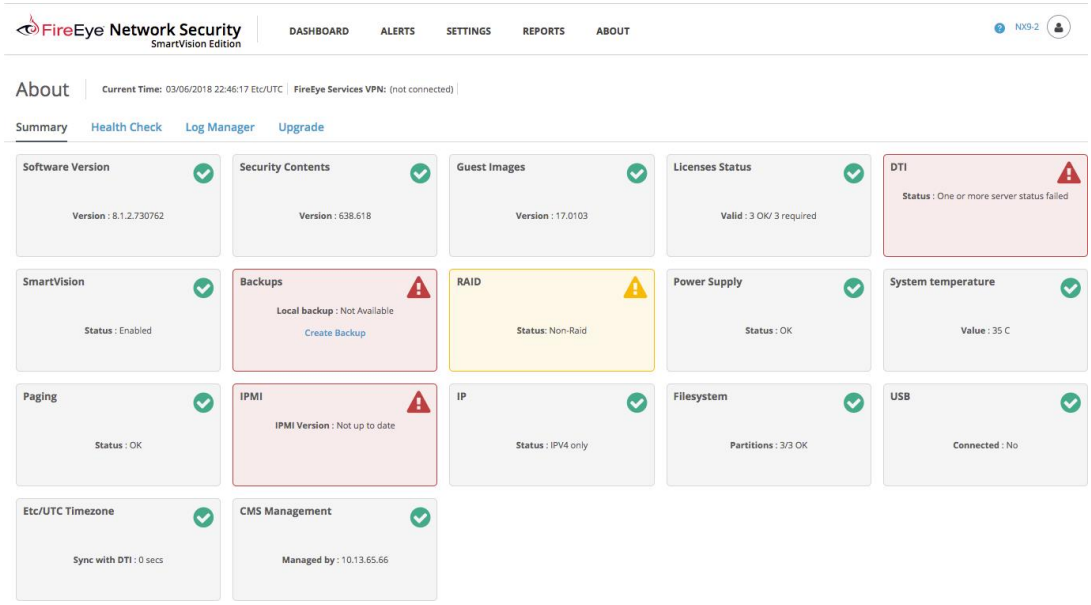
- Admin, Operator, Monitor oder Analyst Zugriff

# Ergebnisse von Systemintegrität- und Leistungsüberprüfung mit Hilfe der Web-UI anzeigen

Verwenden Sie die **About** > **Summary** Seite, um allgemeine Statusinformationen über die Appliance Komponenten anzuzeigen. Die Tafeln der **Summary** Seiten zeigen eine Zusammenfassung von Appliance Integrität, Leistung und Status an.

Dieses Beispiel stammt von einem SmartVision Edition Sensor (bei dem es sich um eine Network Security Appliance mit einer SmartVision Edition FIREEYE_APPLIANCE Lizenz handelt), gilt jedoch auch für Network Security Appliances.

Dieses Beispiel stammt von einem SmartVision Edition-Sensor; dies ist entweder eine Network Security Hardware oder eine virtuelle Appliance mit einer SmartVision Edition FIREEYE_APPLIANCE Lizenz.




Die Farbe einer Displaytafel deutet den Status jeder Appliance Komponente an:

| Farbe | Beschreibung |
|---|---|
| Grau | Eine graue Tafel bedeutet, dass die Appliance Komponente in gutem Zustand ist. |
| Gelb | Eine gelbe Tafel bedeutet, dass sich die Appliance Komponente in einem Warnzustand befindet. |
| Rot | Eine rote Tafel bedeutet, dass sich die Appliance Komponente im kritischen Zustand befindet. |

Die folgende Tabelle beschreibt jede Displaytafel auf der **Summary** Seite.

| Tafel | Beschreibung |
|---|---|
| Software Version | Vergleicht die Softwareversion, die auf dem System ausgeführt wird, mit der verfügbaren Software auf dem DTI-Netzwerk. Eine rote Tafel bedeutet, dass auf Ihrer Appliance nicht die aktuelle Softwareversion ausgeführt wird. Um das Software Image zu aktualisieren, klicken Sie auf **Upgrade**. Die Web-UI zeigt die **About** > **Upgrade** Seite, auf der Sie das neueste Software-Image aktualisieren können. |
| Security Contents | Vergleicht die Sicherheitsinhaltsversion auf der Appliance mit der verfügbaren Version auf dem DTI-Netzwerk und zeigt den Status und die Version an, die derzeit installiert ist. Eine rote Tafel deutet an, dass Sicherheitsinhalt überholt ist. Um Sicherheitsinhalte zu aktualisieren, klicken Sie auf **Upgrade**. Die Web-UI zeigt die **About** > **Upgrade** Seite an, auf der Sie den Sicherheitsinhalt aktualisieren können. |
| Sensor Enrollment | Zeigt den Registrierstatus für einen Sensor an, der mit einem MVX Cluster registriert ist. |
| Guest Images | Vergleicht die Guest Images Version auf der Appliance mit der verfügbaren Version auf dem DTI-Netzwerk. Eine rote Tafel bedeutet, dass eine neuere Version vorhanden ist. |
| Lizenzen | Zeigt die Anzahl der installierten Lizenzen an, die gültig und aktiv sind. Eine rote Tafel bedeutet, dass Lizenzen abgelaufen sind. Eine gelbe Tafel bedeutet, dass Lizenzen innerhalb der nächsten 30 Tage ablaufen. |
| DTI | Zeigt an, ob die Appliance Aktualisierungen des Sicherheitsinhalts vom DTI-Netzwerk empfangen und Analysestatistiken an das DTI-Netzwerk hochladen kann. Eine rote Tafel bedeutet, dass Dienste nicht erreichbar sind. |
| SmartVison | Zeigt an, ob SmartVision auf der Appliance aktiv ist. SmartVision kann die laterale Bewegung von Malware erkennen. Eine SmartVision Appliance ist eine der folgenden:<br>• SmartVision Edition Sensor<br>• SmartVision-fähiger Classic Edition Network Security Sensor<br>• SmartVision-fähiger Classic Edition Network Security integrierte Appliance |

| Tafel | Beschreibung |
|---|---|
| Backups | Zeigt den Status des letzten Sicherungsvorgangs an. Eine rote Tafel bedeutet, dass der letzte Sicherungsvorgang fehlgeschlagen ist oder die Daten auf der Appliance noch nie gesichert wurden. Um die Datenbank zu sichern, klicken Sie auf **Create Backup**. Die Web-UI zeigt die **Settings** > **Appliance Backup & Restore** Seite an, auf der Sie die Datenbank sichern können. |
| Global Cache | Zeigt an, ob der globale Cache auf dem System aktiviert ist. |
| RAID | Zeigt den Gesamtstatus von RAID an. Wenn ein RAID Fehler aufgetreten ist, wird eine Fehlernachricht angezeigt. Eine gelbe Tafel bedeutet, dass eine Nicht-RAID Festplatte erkannt wurde. |
| Power Supply | Zeigt den Gesamtstatus der Stromversorgung an. Eine rote Tafel bedeutet, dass die Stromversorgung in kritischem Zustand ist. |
| System Temperature | Zeigt die aktuelle Temperatur und Maßeinheiten auf dem System an. Eine rote Tafel bedeutet, dass die Temperatur einen System-definierten Schwellenwert unter- oder übersteigt. |
| Paging | Zeigt an, ob das System den Auslagerungsvorgang begonnen hat. Eine gelbe Tafel bedeutet, dass der Auslagerungsvorgang ausgeführt wird. |
| IPMI | Vergleicht die IPMI Firmwareversion, die auf dem System ausgeführt wird, mit der verfügbaren Version auf dem DTI-Netzwerk. Eine rote Tafel bedeutet, dass eine neuere Version vorhanden ist. |
| IP | Zeigt IPv4, IPv6 oder beides an. |
| Network Deployment | Zeigt den Status von Netzwerkinformationen an, die auf Probleme mit Appliance Deployment hinweisen könnten. Eine rote Tafel bedeutet, dass ein Problem mit einem Netzwerk Deployment gefunden wurde. |
| Filesystem | Zeigt den Status der Anzahl der Partitionen mit freiem Speicherplatz an. Eine gelbe Tafel bedeutet, dass der freie Speicherplatz in einer der Partitionen unter 10 Prozent gesunken ist. |
| USB | Zeigt an, ob ein USB Gerät mit der Appliance verbunden ist. |
| Timezone | Zeigt die Zeitzone für Ihre Appliance an. Die **Timezone** Tafel zeigt auch die Anzahl der Sekunden an, seit die Appliance mit dem DTI-Server synchronisiert wurde. |
| CMS Management | Zeigt den Status an, ob eine Appliance von der Central Management Appliance verwaltet wird. |

**Um die Ergebnisse von Systemintegriatäts- und Leistungsüberprüfung anzuzeigen:**

1. Klicken Sie auf das Register **About**.
2. Klicken Sie auf **Summary**.

# Deploymentprüfung

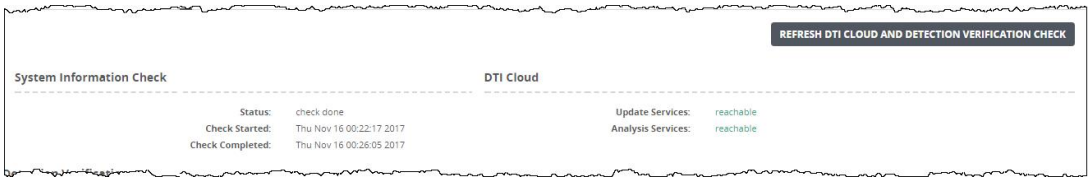
Die **About** > **Deployment Check** Seite besteht aus drei Abschnitten:

- **Dynamic Threat Intelligence Cloud**—Überprüft, ob die Appliance Aktualisierungen von Sicherheitsinhalten vom DTI Netzwerk empfangen und Analysestatistiken auf das DTI Netzwerk hochladen kann. Siehe DTI-Services mit Hilfe der Web-UI überprüfen unten.
- **Detection Verification**—Überprüft, ob die Appliance die Callback, Callback block, Web analysis, Binary analysis, Domain match, archive analysis und IPS alerts Warnungstypen erkennen kann. Siehe Alarmerkennung überprüfen auf der nächsten Seite.
- **Network Deployment Check**—Erfasst allen TCP-Verkehr für eine festgelegte Dauer und prüft nach Netzwerkproblemen, einschließlich Duplikatpakete, asymmetrischen TCP-Verkehr, Paketverlust und Pakete außerhalb der Reihenfolge. Siehe Netzwerk Deployment überprüfen auf Seite 345.

## DTI-Services mit Hilfe der Web-UI überprüfen

Der **DTI Cloud** Abschnitt der **About** > **Deployment Check** Seite zeigt an, ob die Appliance Aktualisierungen von Sicherheitsinhalten vom DTI-Netzwerk empfangen kann und Analysestatistiken darauf hochzuladen. Sehen Sie DTI Zugriff validieren auf Seite 182, wenn die Services in diesem Abschnitt nicht erreichbar sind.

Die anderen beiden Abschnitte auf der **About** > **Deployment Check** Seite sind nicht davon abhängig, dass DTI-Cloudservices erreichbar sind.




## Voraussetzungen

- Monitor, Analyst, Operator oder Admin access

**Um die DTI Cloud Statusinformation zu aktualisieren:**

1. Klicken Sie auf das Register **About**.
2. Klicken Sie auf **Deployment Check**.
3. Klicken Sie auf **Refresh DTI Cloud and Detection Verification Check**.

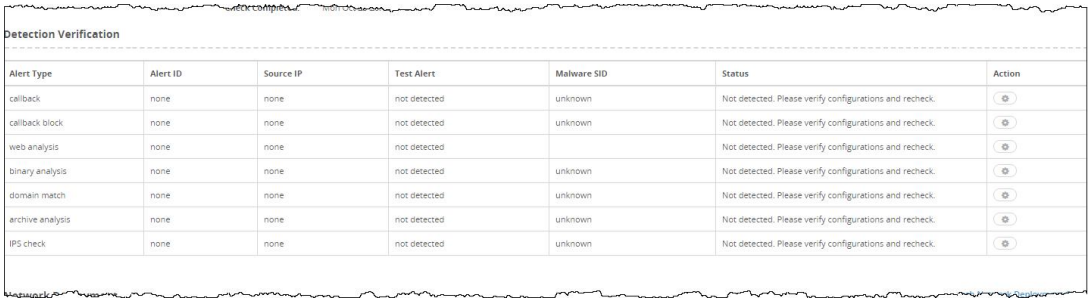
# Alarmerkennung überprüfen

Warnungserkennungstest ermöglichen Ihnen zu überprüfen, ob die Appliance Rückruf, Rückrufblock, Webanalyse, Binäranalyse. Domainabgleich, Archivanalyse und IPS-Warnungen erkennen kann.

**WICHTIG!** Der Laptop oder das Gerät, von dem aus Sie den Test durchführen, muss sich in dem Netzwerk befinden, in dem die Network Security Appliance inline bereitgestellt ist.

## Warnungserkennung mit Hilfe der Web-UI überprüfen

Verwenden Sie die **About** > **Deployment Check** Seite im **Detection Verification** Abschnitt, um die Network Security Appliance Warnungserkennung zu überprüfen.


Detection Verification

| Alert Type | Alert ID | Source IP | Test Alert | Malware SID | Status | Action |
|---|---|---|---|---|---|---|
| callback | none | none | not detected | unknown | Not detected. Please verify configurations and recheck. | |
| callback block | none | none | not detected | unknown | Not detected. Please verify configurations and recheck. | |
| web analysis | none | none | not detected | | Not detected. Please verify configurations and recheck. | |
| binary analysis | none | none | not detected | unknown | Not detected. Please verify configurations and recheck. | |
| domain match | none | none | not detected | unknown | Not detected. Please verify configurations and recheck. | |
| archive analysis | none | none | not detected | unknown | Not detected. Please verify configurations and recheck. | |
| IPS check | none | none | not detected | unknown | Not detected. Please verify configurations and recheck. | |

# Voraussetzungen

- Monitor-, Analyst-, Operator- oder Administratorzugriff.
- Network Security Appliance wird inline bereitgestellt.
- Laptop oder Gerät, von dem Sie testen, befindet sich in dem Netzwerk, in dem die Network Security Appliance bereitgestellt ist.
- Alarme und Benachrichtigungen werden konfiguriert.

**Um Warnungserkennung zu überprüfen:**

1. Klicken Sie auf das Register **About**.
2. Klicken Sie auf **Deployment Check**.

3. Auf der **Detection Verification** Tabelle klicken Sie auf das Aktionssymbol ( ) in der **Action** Spalte und dann auch **Check**, um zu testen, ob die Appliance die folgenden Alarmtypen erkennen kann.
    - Callback
    - Callback block
    - Web analysis
    - Binary analysis
    - Domain match
    - Archive analysis
    - IPS check (wenn IPS verfügbar ist)
4. Klicken Sie auf **Refresh DTI Cloud and Detection Verification Check**, um die Prüfergebnisse in der **Detection Verification** Tabelle anzuzeigen.

Wenn eine der Prüfungen fehlschlägt, überprüfen Sie, dass die Hardware richtig für Ihre Bereitstellung installiert ist (sehen Sie das *Hardware Administration Handbuch* für Ihre Network Security Appliance für Installations- und Bereitstellungsanleitungen). Wenn die Hardware richtig installiert ist, wenden Sie sich an FireEye Technical Support.

## Netzwerk Deployment überprüfen

Die Network Security Software überprüft automatisch nach Netzwerk Statusinformationen, die auf Probleme mit der Bereitstellung der Appliance hinweisen könnten. Das System führt den Vorgang zur Deploymentprüfung automatisch um Mitternacht aus. Sie können eine Deploymentprüfung ausdrücklich von der Appliance Web-UI oder CLI aus starten, vorausgesetzt dass noch kein Deploymentprüfungs-Vorgang läuft.

Eine Netzwerk Deploymentprüfung erfasst allen TCP Verkehr, der in den Überwachungsports während einer bestimmten Zeitdauer ein- und austritt und analysiert dann den erfassten Verkehr für Duplikatpakete, Pakete außer der Reihenfolge, Paketverlust und asymmetrische Verkehrsflüsse. Je nach Anzahl der Pakete erzeugt die Netzwerk Deploymentprüfung eine Gesamtwertung von Erfolg oder Misserfolg. Wenn die Netzwerk Deploymentprüfung fehlschlägt, identifiziert der Web-UI und CLI Output die bestimmten Paketzahlen, die Probleme mit der Netzwerk Deploymentprüfung andeuten.

Um Probleme beim Netzwerk-Deployment der Appliance zu untersuchen, können Sie die neuesten Paketerfassungsdateien hochladen, um erfasste Verkehrsdaten (wie Quelle, Ziel, Paketnummer und Beschreibung) zu analysieren. Weitere Informationen finden Sie unter Paketerfassungsdateien zur Analyse hochladen auf Seite 352.

Die folgenden Ereignisse lösen Benachrichtigungen über Netzwerk Deploymentprüfung aus:

- Die Ergebnisse der Deploymentprüfung wechseln von Erfolg zu Misserfolg.
- Das System startet erneut und die letzte Deploymentprüfung schlägt fehl.
- Jeder verwaltete Vorgangsneustart und die letzte Deploymentprüfung resultiert in Scheitern.

Wenn die Benachrichtigungen über *Scheitern der Deploymentprüfung* und *Wiederherstellung von Deploymentprüfung* auf Ihrer Appliance konfiguriert und aktiviert sind, werden Benachrichtigungen über Deploymentprüfung per E-Mail und SNMP Traps gesendet. Anleitungen finden Sie unter Traps senden auf Seite 375.

Dieser Abschnitt enthält die folgenden Themen:



## Ergebnisse der Netzwerk-Deploymentprüfung anzeigen

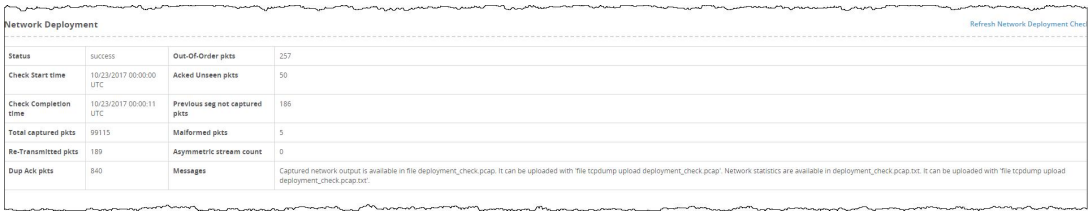
Sie können die Prüfergebnisse des Netzwerk-Deployments anzeigen. Das System führt die Netzwerk-Deploymentprüfung automatisch jeden Tag um Mitternacht aus.

# Voraussetzungen

- Monitor-, Analyst-, Operator- oder Adminzugriff

### *Ergebnisse der Netzwerk-Deploymentprüfung mit Hilfe der Web-UI anzeigen*

Verwenden Sie die **About** > **Deployment Check** Seite im **Network Deployment** Abschnitt, um die Ergebnisse der Netzwerk-Deploymentprüfung anzuzeigen.




In der folgenden Tabelle werden die Felder für die Ergebnisse der Netzwerk Deploymentprüfung beschrieben.

| Feld | Beschreibung |
|---|---|
| Status | Gesamtstatus des Netzwerk-Deployments:<br>**success**—Es wurden keine Netzwerk Deploymentfehler entdeckt.<br>**failed**—Es wurden Netzwerk-Deploymentprüfungsfehler gefunden. |
| Check start time | Datum und Uhrzeit, zu der die Paketerfassung begonnen wurde. |
| Check completion time | Datum und Uhrzeit, zu der die Analyse beendet wurde. |
| Total captured pkts | Größe (in Paketen) der analysierten Paketerfassung.<br>Wenn diese Zahl unter einen durch das System definierten Schwellenwert fällt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |
| Re-Transmitted pkts | Anzahl der erneut übermittelten Pakete.<br>Wenn diese Anzahl einen durch das System definierten Schwellenwert übersteigt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |
| Dup Ack pkts | Anzahl der TCP DUP ACK Datensätze in der Erfassung.<br>Wenn diese Anzahl einen durch das System definierten Schwellenwert übersteigt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |
| Out-of-Order pkts | Anzahl der umsortierten Pakete in der Erfassung.<br>Wenn diese Anzahl einen durch das System definierten Schwellenwert übersteigt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |
| Acked unseen pkts | Anzahl der TCP ACKed unseen Segmente in der Erfassung.<br>Wenn diese Anzahl einen durch das System definierten Schwellenwert übersteigt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |
| Previous seg not captured pkts | Anzahl der Pakete, die mit einer Sequenznummer größer als die nächste erwartete Sequenznummer in dieser Verbindung angekommen sind.<br>Wenn diese Anzahl einen durch das System definierten Schwellenwert übersteigt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |

| Feld | Beschreibung |
|---|---|
| Malformed pkts | Anzahl der fehlerhaften Pakete in der Erfassung. Ein Absender könnte ein fehlerhaftes Paket übermitteln oder ein Paket kann während der Übermittlung beschädigt werden.<br>Wenn diese Anzahl einen durch das System definierten Schwellenwert übersteigt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |
| Asymmetric stream count | Anzahl der asymmetrischen Streams in der Erfassung.<br>Wenn diese Anzahl einen durch das System definierten Schwellenwert übersteigt, zeigt ein Sternchen (*) an, dass ein Netzwerk-Deploymentproblem vorliegen könnte. |
| Messages | **Latest deployment check is still running. (Die letzte Deploymentprüfung wird noch ausgeführt.) Following is status for previous check: (Nachfolgend sehen Sie den Status für die letzte Prüfung.)**<br>Wenn Sie diesen Befehl ausführen, während eine Netzwerk-Deploymentprüfung noch ausgeführt wird, wird diese Nachricht angezeigt: Die Ergebnisse der letzten Netzwerk Deploymentprüfung werden angezeigt.<br>**Captured network output is available in file deployment_check.pcap. (Die erfasste Netzwerkausgabe ist in der Datei deployment_check.pcap verfügbar.) It can be uploaded with 'file tcpdump upload deployment_ check.pcap'. (Sie kann mit 'file tcpdump upload deployment_check.pcap' hochgeladen werden.) Network statistics are available in deployment_ check.pcap.txt. (Netzwerkstatistiken sind in deployment_check.pcap.txt verfügbar.) It can be uploaded with 'file tcpdump upload deployment _ check.pcap.txt'. (Es kann mit 'file tcpdump upload deployment _ check.pcap.txt' hochgeladen werden.)**<br>Unabhängig davon, ob das Gesamtergebnis der Netzwerk-Deploymentprüfung **success** oder **failed**, können Sie den erfassten und analysierten Netzwerkverkehr auf einen remote Host hochladen, wie unter Paketerfassungsdateien zur Analyse hochladen auf Seite 352 beschrieben. |

**Um Ergebnisse der Netzwerk Deploymentprüfung anzuzeigen:**

1. Klicken Sie auf das Register **About**.
2. Klicken Sie auf **Deployment Check**.

   Überprüfen Sie die Ergebnisse im **Network Deployment** Abschnitt.

## *Ergebnisse der Netzwerk-Deploymentprüfung mit Hilfe der CLI anzeigen*

Verwenden Sie die CLI Befehle in diesem Thema, um die Ergebnisse anzuzeigen.

In der folgenden Tabelle werden die Felder für die Ergebnisse der Netzwerk-Deploymentprüfung beschrieben.

| Feld | Beschreibung |
|---|---|
| Status | Gesamtergebnisse der Paketerfassungsanalyse:<br>**success**—Es wurden keine Netzwerk-Deploymentfehler entdeckt.<br>**failed**—Es wurden Netzwerk-Deploymentprüfungsfehler entdeckt. |
| Start time | Datum und Uhrzeit, zu der die Paketerfassung begonnen wurde. |
| End time | Datum und Uhrzeit, zu der die Analyse beendet wurde. |
| Captured data size (bytes) | Größe (in Bytes) der analysierten Paketerfassung. |
| Captured packet count | Größe (in Paketen) der analysierten Paketerfassung.<br>Wenn diese Zahl unter eine durch das System definierte Schwelle fällt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk-Deploymentproblem andeuten könnte. |
| Re-transmit packet count | Anzahl der erneut übermittelten Pakete.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |
| Dup ACK packet count | Anzahl der TCP DUP ACK Datensätze in der Erfassung.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |
| Out-Of-Order packet count | Anzahl der umsortierten Pakete in der Erfassung.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |
| Acked unseen packet count | Anzahl der TCP ACKed unseen Segmente in der Erfassung.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |

| Feld | Beschreibung |
|---|---|
| Previous seg not captured packet count | Anzahl der Pakete, die mit einer Sequenznummer größer als die nächste erwartete Sequenznummer in dieser Verbindung angekommen sind.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |
| Malformed packet count | Anzahl der fehlerhaften Pakete in der Erfassung. Ein Absender könnte ein fehlerhaftes Paket übermitteln oder ein Paket kann während der Übermittlung beschädigt werden.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |
| Stream count | Anzahl der aktiven Streams in der Erfassung.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |
| Asymmetric stream count | Anzahl der asymmetrischen Streams in der Erfassung.<br>Wenn diese Anzahl eine durch das System definierte Schwelle übersteigt, zeigt ein Sternchen (*) an, dass der Wert ein Netzwerk Deploymentproblem andeuten könnte. |
| Messages | `Latest deployment check is still running. Following is status for previous check:`<br>Wenn Sie diesen Befehl ausführen, während eine frühere Netzwerk-Deploymentprüfung noch läuft, wird diese Nachricht angezeigt. Die Ergebnisse der letzten Netzwerk-Deploymentprüfung werden angezeigt.<br>`Captured network output is available in file deployment_check.pcap. It can be uploaded with 'file tcpdump upload deployment_check.pcap'. Network statistics are available in deployment_check.pcap.txt. It can be uploaded with 'file tcpdump upload deployment_check.pcap.txt'.`<br>Unabhängig davon, ob das Gesamtergebnis der Netzwerk-Deploymentprüfung `success` oder `failed` ist, können Sie den erfassten und analysierten Netzwerkverkehr auf einen remote Host hochladen, wie unter Paketerfassungsdateien zur Analyse hochladen auf Seite 352 beschrieben.<br>`Please run 'deployment check network start'`<br>Wenn Sie die Ergebnisse der letzten Netzwerk-Deploymentprüfung gelöscht haben, wird diese Meldung anstelle der Statuszeilen angezeigt. |

**Um Ergebnisse der Netzwerk-Deploymentprüfung anzuzeigen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie die vollständigen Ergebnisse an:

   ```
   hostname # show deployment check network

   Network deployment check configuration:
     Packet Capture Duration:                    120

   Network deployment check status:
     Status:                                     success
     Start time:                                 2017/07/21 00:00:00
     End time:                                   2017/07/21 00:00:19
     Captured data size (bytes):                 10712908
     Message: Captured network output is available in file deloyment_
   check.pcap. It can      be downloaded with 'file tcpdump upload
   deployment_check.pcap'. Network statistics are available in deployment_
   check.pcap.txt. It can be uploaded with 'file tcpdump upload deployment
   _check.pcap.txt'.
   ```

3. Zeigen Sie nur Konfigurationsinformationen an:

   ```
   hostname # show deployment check network config

   Network deployment check configuration:

     Packet Capture Duration:                    120
   ```

4. Zeigen Sie nur Statusinformationen an:

   ```
   hostname # show deployment check network status

   Network deployment check status:

     Status:                                     success

     Start time:                                 2017/07/21 01:19:55

     End time:                                   2017/07/21 01:20:56

     Captured data size (bytes):                 10277941

     Message:  Captured network output is available in file deployment_
   check.pcap.  It can be uploaded with 'file tcpdump upload deployment_
   check.pcap'. Network statistics are available in deployment_
   check.pcap.txt. It can be uploaded with 'file tcpdump upload deployment
   _check.pcap.txt'.
   ```

5. Zeigen Sie nur Details an:

```
hostname # show deployment check network status detail

Latest deployment check is still running. Following is status for
previous check

Network deployment check status:
  Status:                                    failed
  Start time:                                2017/07/24 08:44:38
  End time:                                  2017/07/24 08:44:48
  Captured data size (bytes):                10691225
  Captured packet count:                     97239
  Re-transmit packet count:                  12079
  Dup ACK packet count:                      870
  Out-Of-Order packet count:                 21303 *
  Acked unseen packet count:                 162
  Previous seg not captured packet count:    4180
  Malformed packet count:                    0
  Stream count:                              1260
  Asymmetric stream count:                   94
  Message: Captured network output is available in file deployment_
check.pcap. It can be downloaded with 'file tcpdump upload deployment_
check.pcap'. Network statistics are available in deployment_
check.pcap.txt. It can be uploaded with 'file tcpdump upload deployment
_check.pcap.txt'.
  * Indicates error
```

## Paketerfassungsdateien zur Analyse hochladen

Um Probleme beim Netzwerk-Deployment der Appliance zu untersuchen, können Sie die neuesten Dateien mit erfassten Verkehrsdaten auf einen remote Host hochladen.

- **deployment_check.pcap**—Nachdem Sie diese Datei hochgeladen haben, verwenden Sie einen Paketbrowser, um den erfassten Verkehr zu analysieren.
- **deployment_check.pcap.txt**—Nachdem Sie diese Datei hochgeladen haben (die von der **deployment_check.pcap** Datei abgeleitet wurde), öffnen Sie sie in einem Texteditor, um den erfassten Verkehr zu analysieren.

Sie können die Dateien über File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Secure File Transfer Protocol (SFTP) oder Secure Copy (SCP) hochladen.

# Voraussetzungen

- Admin Zugriff

### *Paketerfassungsdaten zur Analyse mit Hilfe der CLI hochladen*

Verwenden Sie die Befehle in diesem Abschnitt, um Paketerfassungsdateien auf einen Remotespeicherort hochzuladen.

**Um Paketerfassungdateien hochzuladen:**

1. Gehen Sie auf den CLI Konfigurationsmodus:

   `hostname > enable hostname # configure terminal`

2. Um die `.pcap` Datei hochzuladen:

   `hostname (config) # tcpdump upload deployment_check.pcap <URL>`

3. Um die `.txt` Datei hochzuladen:

   `hostname (config) # tcpdump upload deployment_check.pcap.txt <URL>`

Das `<URL>` Parameter muss der vollständige Pfad zum Uploadziel sein. Zum Beispiel:

- `ftp://<domain>/<path>/<fileName>`
- `tftp://<domain>/<path/<fileName>`
- `scp://<username>:[<password>]@hostname>/<path>/<fileName>`

### *Beispiel:*

Das folgende Beispiel lädt die **deployment_check.pcap** Datei auf das `debug` Verzeichnis bei acme.com hoch.

```
nx-12 (config) # file tcpdump upload deployment_check.pcap
scp://it123:it123pass@acme.com/debug/deployment_check.pcap
```

## Eine Netzwerk-Deploymentprüfung starten

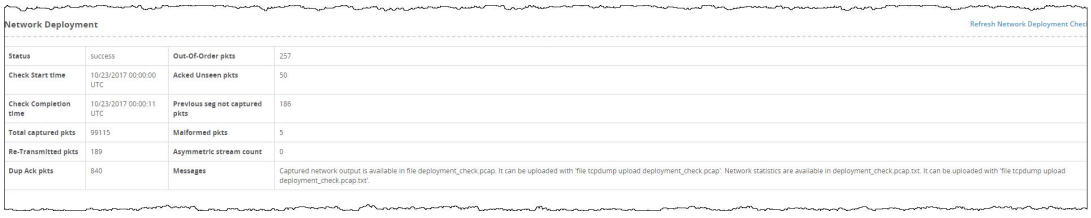
Sie können eine Netzwerk-Deploymentprüfung ausdrücklich von der Network Security Web-UI oder CLI starten.

# Voraussetzungen

- Monitor-, Analyst-, Operator- oder Administratorzugriff.
- Überwachungsschnittstellen sind "up".

### *Eine Netzwerk-Deploymentprüfung mit Hilfe der Web-UI starten*

Sie können eine Netzwerk-Deploymentprüfung manuell von der Network Security Web-UI starten, solange keine andere Prüfung ausgeführt wird.



**Um eine Netzwerk-Deploymentprüfung zu starten:**

1. Klicken Sie auf das Register **About**.
2. Klicken Sie auf **Deployment Check**.
3. Klicken Sie auf **Refresh Network Deployment Check**.

   Informationen über die Anzeige der Ergebnisse finden Sie unter Ergebnisse der Netzwerk-Deploymentprüfung anzeigen auf Seite 346.

### *Eine Netzwerk-Deploymentprüfung mit Hilfe der CLI starten*

Sie können eine Netzwerk-Deploymentprüfung manuell von der CLI starten, solange keine andere Prüfung ausgeführt wird.

**Um eine Netzwerk-Deploymentprüfung zu starten:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Starten Sie die Prüfung:

   ```
   hostname # deployment check network start
   Network deployment check has been started. Please run 'show deployment
   check network status' for status update
   ```

Informationen über die Anzeige der Ergebnisse finden Sie unter Ergebnisse der Netzwerk-Deploymentprüfung anzeigen auf Seite 346.

Befehlsdetails finden Sie in der *CLI Befehlsreferenz*.

## Die maximale Dauer der Paketerfassung konfigurieren

Sie können die Standard maximale Dauer der Paketerfassung, die von der Netzwerk Bereitstellungsprüfungsfunktion verwendet wird, überschreiben, Der Standardwert ist 120 Sekunden. Die maximale Erfassungszahl ist 100000 Pakete, unabhängig von der Dauer der Paketerfassung.

# Voraussetzungen

- Operator oder Admin Zugriff

**Um die maximale Dauer der Paketerfassung zu konfigurieren:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. (Optional) Zeigen Sie die aktuelle Dauer an:

   ```
   hostname # show deployment check network
   ```

3. Legen Sie die neue Dauer fest:

   ```
   hostname # deployment check network duration <seconds>
   ```

Das folgende Beispiel stellt die obere Grenze für die Dauer von Paketerfassung auf 60 Sekunden ein.

```
hostname # deployment check network duration 60
```

Befehlsdetails finden Sie in der *CLI Befehlsreferenz*.

## Ergebnisse der Netzwerk Bereitstellungsprüfung löschen

Sie können die Ergebnisse der letzten Netzwerk Deploymentprüfung löschen. Dieser Vorgang lässt die Paketerfassung selbst in Takt. Die Paketerfassungsdaten werden in den `deployment_check.pcap` und `deployment_check.pcap.txt` Dateien gespeichert, die Sie auf einen remote Host hochladen können (siehePaketerfassungsdateien zur Analyse hochladen auf Seite 352). Die nächste Netzwerk Deploymentprüfung, gleichgültig ob automatisch um 00:00 Uhr (Mitternacht) oder ausdrücklich mit Hilfe der CLI oder Web-UI gestartet, generiert einen neuen Satz von Ergebnissen.

**HINWEIS:** Wenn eine Netzwerk-Deploymentprüfung zu einem Failed Status führt, werden Benachrichtigungen für Netzwerk-Deploymentprüfungen ausgelöst, um die fehlgeschlagenen Ereignisse zu melden. Wenn Sie die Ergebnisse nicht löschen, werden nachfolgende Systemneustarts und verwaltete Verfahren Neustarts neue Benachrichtigungen für die gleichen Ereignisse auslösen.

# Voraussetzungen

- Monitor-, Analyst-, Operator- oder Adminzugriff

**Um die neuesten Ergebnisse der Netzwerk Bereitstellungsprüfung zu löschen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Löschen Sie die Ergebnisse:

   ```
   hostname # deployment check network clear
   ```

### *Beispiel:*

Das folgende Beispiel zeigt den Status der Netzwerk Deploymentprüfung nachdem die Ergebnisse gelöscht wurden.

```
hostname # show deployment check network status detail
Network deployment check status:
  Message:    Please run 'deployment check network start'
  * Indicates error
```

Befehlsdetails finden Sie in der *CLI Befehlsreferenz*.

# Auslastungs- und Leistungsprüfungen

Die Network Security Appliance sammelt und meldet fortlaufend relevante Daten über ihre Auslastung. Es gibt empfohlene Auslastungsgrade, die als*rated limits* (Nenngrenzen) bekannt sind und für jedes Appliance Modell spezifisch sind. Die Überschreitung dieser Grenzwerte kann die Erkennungswirksamkeit von Malware, Paketverlust und Warteschlangenfehler verursachen.

Sie können die Auslastungsdaten als ein Tools für zukünftige Kapazitätsplanung verwenden. Wenn Ihre Appliance fortlaufend oder kritisch die angegebenen Grenzwerte überschreitet, erhalten Sie wichtige Nachrichten und Ereignisbenachrichtigungen, die Sie anweisen, sich an FireEye für Anweisungen zu wenden.

Auslastungsdaten und die zugehörigen Nenngrenzen werden im **Appliance Utilization** Abschnitt auf dem Dashboard in der Web-UI und der **show sizing stats** CLI Befehlsausgabe gemeldet. Auf dem Dashboard können Sie Statistiken für den aktuellen Tag, die letzte Woche oder den letzten Monat anzeigen.

Der **Appliance Utilization** Abschnitt des Network Security Dashboards enthält ein Urteil, das die Auslastungszone angibt, in der Ihre Appliance arbeitet (auf dem letzten Stundendurchschnitt basierend) und die empfohlenen Maßnahmen, die durchgeführt werden sollten.

Der Dashboard Abschnitt enthält auch die folgenden Diagramme:

- **Utilization Summary** zeigt die Gesamt-Auslastungsebene der Appliance an.
- **MVX Web Analysis** zeigt die Webseiten an, die darauf warten, bon der Network Security MVX Engine analysiert zu werden, als Prozenzsatz der Kapazität.
- **Total Bandwidth (Mbps**) zeigt den Gesamtverkehr in Mbps an, der durch die Überwachungsports laufen. Die Schwellenwerte basieren auf der Nennbandbreite für die Appliance.

Im folgenden Beispiel arbeitet die Appliance in der guten Zone. Obwohl sie im Berichtszeitraum die Nenngrenze für die Gesamtbandbreite überschritten hat, war sie zu dem Zeitpunkt, als das Diagramm erstellt wurde, wieder im guten Bereich.


# Voraussetzungen

- Monitor-, Operator- oder Admin-Zugriff

# Auslastungsstatistiken mit Hilfe der Web-UI anzeigen

Verwenden Sie den **Appliance Utilization** Abschnitt des Network Security Dashboards, um Auslastungsstatistiken für den aktuellen Tag, die letzte Woche oder den letzten Monat anzuzeigen.

**Um den Auslastungsstatus anzuzeigen:**

1. Klicken Sie auf die **Dashboard** Schaltfläche am Anfang der Network Security Web-UI, um das Dashboard zu öffnen.
2. Wenn sich Ihre Appliance in der Warn- oder kritischen Zone befindet, wird der **Appliance Utilization** Abschnitt am Anfang des Dashboards angezeigt. Wenn sie sich in der guten Zone befindet, scrollen Sie ans Ende des Dashboards, um diesen Abschnitt anzuzeigen.

3. Um den Berichtszeitraum festzulegen, klicken Sie auf die **Day**, **Week** oder **Month** Schaltfläche am Ende dieses Abschnitts.

4. Um die Daten zu aktualisieren, klicken Sie auf das Symbol.

**TIPP:**Um alle anderen Dashboard Abschnitte auszublenden, klicken Sie auf das Symbol. Klicken Sie erneut auf das Symbol, um die anderen Abschnitte anzuzeigen.

# Nutzungsstatistiken mit Hilfe der CLI anzeigen

Verwenden Sie den `show sizing stats` Befehl, um Nutzungsstatistiken anzuzeigen.

**Um Auslastungsstatistiken anzuzeigen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie die Statistiken an:

   ```
   hostname # show sizing stats
   ```

## Beispiel:

Wie im folgenden Beispiel demonstriert, zeigt dieser Befehl den aktuellen Status und Wert für jede Messung, sowie die Benchmarks an, anhand derer die Messungen vorgenommen wurden.

```
hostname # show sizing stats

Stat                            Status    Value    Warning      Critical
                                                   Level        Level
Utilization summary:            Warning   1        1            2
Web analysis MVX utilization(%): ok       9        75           95
Total bandwidth (Mbps):         Warning   888      750          950
```

# Systemintegrität und -status prüfen

Sie können die Web-UI oder CLI verwenden, um Integritäts- und Statusinformationen anzuzeigen.

## Voraussetzungen

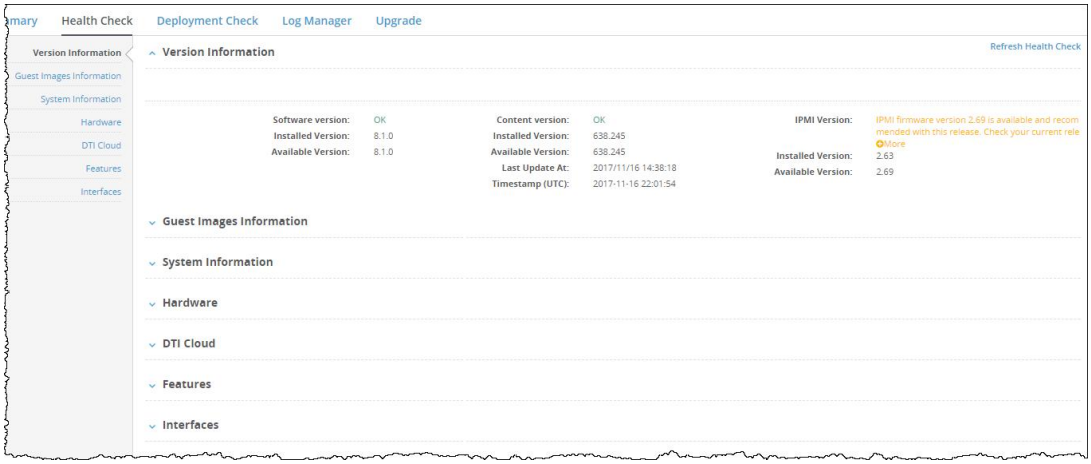
- Monitor, Operator, Analyst oder Admin Zugriff

## Systemintegrität mit Hilfe der Web-UI überprüfen

Verwenden Sie die **Health Check** Seite, um Appliance Integrität und Status zu überprüfen.

Diese Abbildung zeigt eine Network Security Appliance, aber repräsentiert auch Network Security Appliances.

Details über die Informationen, die angezeigt werden, wenn Sie Deploymentprüfung auf Seite 343Deployment Check **am Anfang dieser Seite anklicken, finden Sie unter** .




**Um Integrität und Status anzuzeigen:**

1. Klicken Sie auf den **About** Tab.
2. Klicken Sie auf **Health Check**.

   Die Ergebnisse der letzten Integritätsprüfung werden angezeigt.
3. Überprüfen Sie die Systeminformationen.
4. Um die Ergebnisse zu aktualisieren, klicken Sie auf **Refresh Health Check**.

Die folgenden Abschnitte enthalten Beschreibungen der Informationen in jedem Bereich auf der Seite.

## Versionsinformation

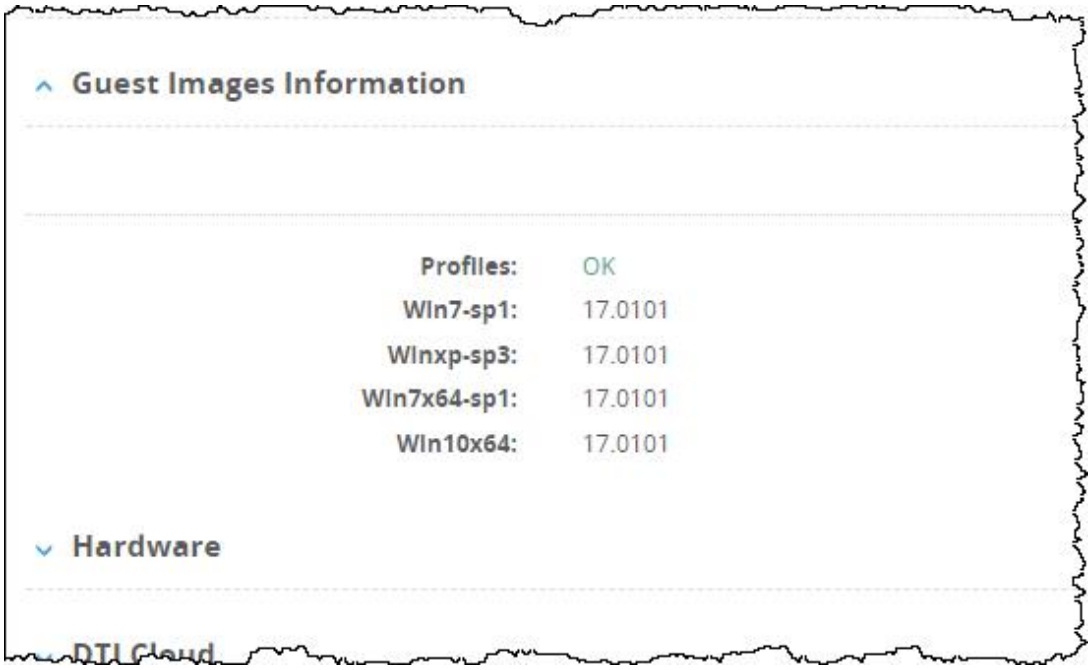
Der **About > Health Check > Version Information** Abschnitt bietet einen aktuellen Blick auf die Software, die auf Ihrer Appliance ausgeführt wird und vergleicht diese mit der verfügbaren Software auf dem FireEye DTI Netzwerk.

**HINWEIS:** Informationen über die IPMI-Version werden nicht für einen Benutzer angezeigt, dem eine Analysten Rolle zugewiesen ist.


| Information | Beschreibung |
|---|---|
| Software Version | Vergleicht die Softwareversion, die auf dem System ausgeführt wird, mit der verfügbaren Software auf dem DTI-Netzwerk. Wenn eine neuere Version vorhanden ist, werden Administratoren aufgefordert, die Software zu aktualisieren. |
| Installed Version | Zeigt die aktuelle Softwareversion an, die auf dem System ausgeführt wird. |
| Available Version | Zeigt die aktuelle Softwareversion an, die im DTI Netzwerk verfügbar ist. |
| Content Version | Vergleicht die Sicherheitsinhaltsversion auf der Appliance mit der verfügbaren Version auf dem DTI-Netzwerk und zeigt den Status und die Version an, die derzeit installiert ist. Wenn eine neuere Version vorhanden ist, oder wenn eine Fehlerbedingung vorliegt, werden Administratoren aufgefordert, entsprechende Maßnahmen zu ergreifen. |
| Last Updated At | Zeigt an, wann der Sicherheitsinhalt zuletzt aktualisiert wurde. |
| IPMI Version | Vergleicht die IPMI Firmwareversion, die auf dem System ausgeführt wird, mit der verfügbaren Version auf dem DTI Netzwerk. Wenn eine neuere Version vorhanden ist, werden Administratoren aufgefordert, die Firmware zu aktualisieren. |
| Installed Version | Zeigt die aktuelle IPMI Firmwareversion an. |
| Available Version | Zeigt die neueste verfügbare IPMI Firmwareversion an. |

## Guest Images Information

Der **About > Health Check > Guest Images Information** Abschnitt bietet einen aktuellen Blick auf die auf Ihrer Appliance installieren Guest Images.




| Information | Beschreibung |
|---|---|
| Profiles | Vergleicht die Profilversionen innerhalb Ihres installierten Guest Image und vergleicht diese Profile mit den neuesten verfügbaren Profilen auf dem DTI Netzwerk. Wenn neuere Profile verfügbar sind, werden Administratoren aufgefordert, ihre Guest Images zu aktualisieren. |
| *Profile Versions* | Für jedes im aktuellen Guest Image gefundene Profil wird die Profilnummer angezeigt. |

## System Information

Der **About > Health Check > System Information** Statusbereich bietet einen aktuellen Status Ihrer Appliance-Hardware und warnt Administratoren, wenn Probleme auftreten.

| Information | Beschreibung |
|---|---|
| Product Info | Status gibt an, ob die Appliance normal funktioniert. Wenn ein Problem mit der Leistung der System-Hardware vorliegt, wird der Administrator benachrichtigt. |
| Model | Das Hardwaremodell. |
| Name | Der Produktname. |
| Type | Der Produkttyp. |
| License | Zeigt an, ob die Softwarelizenz erfolgreich installiert wurde. |
| Processing Load | Bietet eine Analyse der Gesamtlast, die das System ausführt. Wenn die Kapazität fast erreicht ist, wird der Administrator benachrichtigt. |
| Average Load | Die durchschnittliche Verarbeitungslast, die vom System verarbeitet wird. |
| Elapsed | Die aktuelle Betriebszeit des Systems in Tagen, Stunden, Minuten und Sekunden. |
| Detection Engine | Zeigt den Status der Erkennungsengine an. Wenn die Erkennungs-Engine nicht läuft, wird der Administrator benachrichtigt. |
| VM Analyzing | Die Anzahl virtueller Maschinen, die derzeit verdächtige Inhalte analysieren. |
| VM Allowed | Die maximale Anzahl von VMs, die gleichzeitig verdächtige Inhalte analysieren können. |

## Hardware

Der **About > Health Check > Hardware** Abschnitt liefert den Status auf den Hardwarekomponenten der Appliance.

Informationen über die Festplatte, RAID und Chassis werden nicht für einen Benutzer angezeigt, dem die Analyst-Rolle zugewiesen ist.


| Information | Beschreibung |
|---|---|
| Disk | Zeigt an, ob die Festplatte online ist. Wenn ein Problem aufgedeckt wird, wird der Administrator benachrichtigt. |

| Information | Beschreibung |
|---|---|
| Device State | Zeigt den aktuellen Status der Festplatte an. |
| Device Support | Zeigt den auf dem System verfügbaren Gerätetyp an. |
| Self Assessment | Zeigt an, ob das Laufwerk seine internen Selbsttests bestanden hat. |
| User Capacity | Zeigt die Datenträgerkapazität auf dem Laufwerk an. |
| Chassis | Zeigt den Status des Hardwarechassis an. Wenn ein Problem aufgedeckt wird, wird der Administrator benachrichtigt. |
| Lock | Liefert den Status des Chassisschlosses. |
| Boot Up State | Liefert den Startstatus. |
| Power Supply State | Liefert den Status der Stromversorgung. |
| RAID | Liefert den Status von RAID. |

## Dynamic Threat Intelligence DTI Cloud

Der **About > Health Check > DTI Cloud** Abschnitt zeigt den Status der Verbindung zwischen der Appliance und dem DTI Netzwerk an.

Dieses Beispiel stammt von einer Network Security Appliance, aber repräsentiert auch andere FireEye Appliances.


| Information | Beschreibung |
|---|---|
| DTI Client | Zeigt, ob der DTI Client auf dem System ausgeführt wird. |
| Username | Zeigt den aktuellen Benutzer des Systems an. |
| Support Updates | Zeigt den Status der Supportlizenz an. |
| Security Content | Zeigt an, ob die Freigabe von Sicherheitsinhalten auf dem System aktiviert ist. |
| Sharing | Zeigt den Typ der erworbenen Content Update Lizenz an. |
| Content Updates | Zeigt den Status der Content Update Lizenz an. |

| Information | Beschreibung |
|---|---|
| Download | Vergleicht die Quelle für Software Updates (System Images, Guest Images und Sicherheitsinhalte) mit der verfügbaren Downloadquelle auf dem DTI Netzwerk und zeigt den Status an. |
| Upload | Vergleicht das Ziel, das für Software Uploads benutzt wird mit dem verfügbaren Uploadziel auf dem DTI Netzwerk und zeigt den Status an. |
| Last Communication Time | Zeigt an, wann Software Updates zuletzt herunter- und hochgeladen wurden. |

## Features

Der **About > Health Check > Features** Abschnitt zeigt den Status der Funktionen auf der Network Security Appliance an.

Dieses Beispiel stammt von einer Network Security Appliance aber repräsentiert auch Network Security Appliances.


| Information | Beschreibung |
|---|---|
| IPS | Zeigt an, ob Integrated Intrusion Prevention System (IPS) Funktionen auf der Network Security Appliance aktiviert sind. |
| ATI | Zeigt an, ob die Advanced Threat Intelligence (ATI) Funktion aktiviert ist. Wenn Sie die ATI Funktion aktivieren, werden Informationen über MVX verifizierte Ereignisse auf den Network Security Appliances geliefert. |
| Riskware | Zeigt an, ob die Riskware-Erkennungsfunktion aktiviert ist. Wenn Sie die Riskware-Erkennungsfunktion aktivieren, können Sie zwischen bösartigen Dateien und Riskware auf der Network Security Appliance unterscheiden. |

| Information | Beschreibung |
|---|---|
| TapSender | Zeigt an, ob das Evidence Collector Modul aktiviert ist. Wenn Sie das Evidence Collector Modul aktivieren, sendet die Appliance die Netzwerk Ereignisprotokolle an FireEye Threat Analytics Platform (TAP) auf dem AWS Endpunkt, den Sie zur weiteren Analyse bestimmt haben. |
| SmartVison | Zeigt an, ob SmartVision auf der Appliance aktiv ist. SmartVision kann die laterale Bewegung von Malware erkennen. Eine SmartVision Appliance ist eine der folgenden:<br>• SmartVision Edition Sensor<br>• SmartVision-fähiger Network Security Sensor<br>• SmartVision-fähige Network Security integrierte Appliance |
| Custom IOC | Zeigt an, ob eine Central Management Appliance aktiviert ist, Indicators of Compromise [Gefährdungsindikatoren] (IOCs) von einem Drittparteien Feed zu empfangen und sie an alle verwalteten Network Security Appliances oder eine bestimmte verwaltete Network Security Appliance zu verteilen. |

## Interfaces

Der **About > Health Check > Interfaces** Abschnitt zeigt Informationen über jeden verfügbaren Ethernet Port auf der Network Security Appliance an.

Der **About > Health Check > Interfaces** Abschnitt wird nicht für einen Besucher angezeigt, dem eine Analyst Rolle zugewiesen ist.


Interfaces

| | Auto Negotiation | Duplex | Link Detected | Link Transceiver | Link Speed | MAC Address | RX Packet | TX Packet |
|---|---|---|---|---|---|---|---|---|
| **Ether1:** Up | off | Full | yes | internal | 10Gb/s | 00:50:56:01:6A:04 | 1772525 | 1468215 |

| Information | Beschreibung |
|---|---|
| Interface | Gibt an, ob der Ethernet Port ein- oder ausgeschaltet ist. |
| Auto Negotiation | Gibt an, ob Auto Negotiation aktiviert ist. |
| Duplex | Der Typ der Duplex Kommunikation, der von dem Ethernet Port verwendet wird. |
| Link Detected | Gibt an, ob der Ethernet Port derzeit mit einem anderen Port verbunden ist. |

| Information | Beschreibung |
|---|---|
| Link Transceiver | Der Standort des Link Transceivers, der für die Generierung von Ethernetverkehr benutzt wird. |
| Link Speed | Die höchste, auf dem Ethernet Port verfügbare Datengeschwindigkeit. |
| MAC Address | Die Mac Adresse des Ethernet Ports. |
| RX Packet | Die Anzahl der Pakete, die der Ethernet Port während dieser Verbindung empfangen hat. |
| TX Packet | Die Anzahl der Pakete, die der Ethernet Port während dieser Verbindung übermittelt hat. |
| TX Packets Dropped | Die Anzahl der Pakete, die durch Ethernet-Verkehr abgelegt wurden. |

## Systemintegrität mit Hilfe der CLI überprüfen

Verwenden Sie die CLI Befehle in diesem Thema, um Integritäts- und Statusinformationen über Network Security Appliance Komponenten anzuzeigen. Dieses Thema beschreibt ausgewählte Befehle, die Informationen über System, Hardware Status, DTI Netzwerk und Schnittstellen zurückgeben. Eine vollständige Liste von Befehlen und Details über Ihre Benutzung und Parameter finden Sie in der *CLI Befehlsreferenz*.

- Monitor-, Operator- oder Admin-Zugriff
- Admin Zugriff für den `show ipmi` Befehl

**HINWEIS:** Die Beispiele in diesem Abschnitt stammen von einer Network Security Appliance, aber sie sind auch für Network Security Appliances repräsentativ.

**Um die Integrität der Appliance zu überprüfen:**

1. Gehen Sie auf den CLI Aktivierungsmodus:

   ```
   hostname > enable
   ```

2. Zeigen Sie detaillierte Informationen über das System und die darauf ausführende Software an.

```
hostname # show version
Product name:      Web MPS [licensed]
Product model:     FireEyeNX9450
Product edition:   Classic
Bandwidth:         2000 Mb
Product release:   wMPS (wMPS) 7.7.0.433916
Build ID:          #433916
Build date:        2015-12-29 17:21:57
Build arch:        x86_64
Built by:          root@vta114
Version summary:   wmps wMPS (wMPS) 7.7.0.433916
#433916 2015-12-29 17:21:57 x86_64 build@vta108:FireEye (xxx)
Content Version:   385.314
Appliance ID:      XXXXXXXXXXX

Product model:     FireEyeNX9450
Host ID:           XXXXXXXXXX
System serial num: XXXXXXXXX
System UUID:       XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXX

Uptime:            3d 6h 34m 34.205s
CPU load averages: 0.36 / 0.40 / .38
Number of CPUs:    32
System memory:     9210 MB used / 119984 MB free / 129194 MB total
Swap:              0 MB used / 65536 MB free / 65536 MB total
```

3. Zeigen Sie die IPMI Konfiguration an:

```
hostname # show ipmi
IPMI LAN Settings
----------------------------------------
Admin Shut Down         : no
Shut Down               : no
IP Address Source       : Static Address
IP Address              : 192.168.42.27
Subnet Mask             : 0
Default Gateway IP      : 0

IPMI Firmware Installed
------------------------------
Firmware Version:         2.67
Device:                   1
IPMI Version:             2.0

IPMI Firmware Available For Update
----------------------------------
New Firmware Version:     2.67
New Firmware Filename:    FireEye_V267.bin
Firmware Update Notice:   Firmware is up to date for this release

IPMI Firmware Availability Notice is enabled
```

4. Zeigen Sie den allgemeinen Systemstatus an.

```
hostname * show system health
Overall system feature status: Good
```

5. Zeigen Sie den aktuellen Status von System und verfügbaren Services an:

```
hostname # show show health all
Health Status:

Last Updated at: : 2019-11-06T20:31:00
Service: : System CPU/Memory/Disk IO Health
Health Status: : Healthy
Details: : Healthy

Service: : Global Cache
Health Status: : Healthy
Details: : Healthy
.
.
.
```

6. Zeigen Sie Informationen über das Dynamic Threat Intelligence (DTI) Netzwerk an:

```
hostname # show fenet status
Dynamic Threat Intelligence Service:

    Update source   : <online>
    Enabled         : yes
    Download        : DTIUser@cloud.fireeye.com
    Upload          : DTIUser@up-cloud.fireeye.com
    Mil             : DTIUser@mil-cloud.fireeye.com

HTTP Proxy:

     Address        :
     Username       :
     User-agent     :

Request Session:

     Timeout        : 30
     Retries        : 3
     Speed Time     : 60
     Max Time       : 14400
     Rate Limit     :

     Speed Limit    : 1

Dynamic Threat Intelligence Lockdown:

Enabled             : no
Locked              : no
Lock After          : 5 failed attempts

 UPDATES
                    Enabled   Notify  Scheduled   Last Updated At
                    -------   ------  ---------   -------------------
 Security contents: yes       no      every       2016/07/18 19:28:00
 Stats contents:    yes               none        2016/07/18 15:55:00
```

7. Zeigen Sie Status- und Datenverkehrsstatistiken für alle Schnittstellen an:

```
hostname # show interfaces

Interface ether1 status:
   Comment:
   Admin up:           yes
   Link up:            yes
   DHCP running:       no
   IP address:         172.00.00.00
   Netmask:            255.000.0.0
   IPV6 enabled:       no
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  12
   Interface source:   physical
   MTU:                1500
   HW address:         00:25:90:D0:A3:76

   RX bytes:        3114981133   TX bytes:       227921679
   RX packets:       31934013     TX packets:     367951
   RX mcast packets: 31564        TX discards:    0
   RX discards:      296          TX errors:      0
   RX errors:        1            TX overruns:    0
   RX overruns:      0            TX carrier:     0
   RX frame:         0            TX collisions:  0
                                  TX queue len:   1000

Interface ether2 status:
   Comment:
   Admin up:           yes
   Link up:            no
   DHCP running:       no
   IP address:
   Netmask:
   IPV6 enabled:       no
   Speed:              UNKNOWN
   Duplex:             UNKNOWN
   Interface type:     ethernet
   MTU:                1500
   HW address:         00:25:90:D0:A3:77

   RX bytes:           0              TX bytes:       0
   RX packets:         0              TX packets:     0
   RX mcast packets:   0              TX discards:    0
   RX discards:        0              TX errors:      0
   RX errors:          0              TX overruns:    0
   RX overruns:        0              TX carrier:     0
   RX frame:           0              TX collisions:  0
                                      TX queue len:   0

Interface pether2 status:
   Comment:
   Admin up:           yes
   Link up:            no
   DHCP running:       no
   IP address:
   Netmask:
   IPV6 enabled:       no
   Speed:              UNKNOWN
   Duplex:             UNKNOWN
   Interface type:     ethernet
   Interface ifindex:  9
```

```
   Interface source:   physical
   Bridge group:       ether2
   MTU:                1500
   HW address:         00:25:90:D0:A3:77

   RX bytes:           0            TX bytes:       0
   RX packets:         0            TX packets:     0
   RX mcast packets:   0            TX discards:    0
   RX discards:        0            TX errors:      0
   RX errors:          0            TX overruns:    0
   RX overruns:        0            TX carrier:     0
   RX frame:           0            TX collisions:  0
                                    TX queue len:   1000

Interface pether3 status:
   Comment:
   Admin up:           yes
   Link up:            yes
   DHCP running:       no
   IP address:         127.0.0.10
   Netmask:            255.255.255.0
   IPV6 enabled:       no
   Speed:              1000 MB/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  6
   Interface source:   physical
   MTU:                1500
   HW address:         00:25:90:D0:A3:67

   RX bytes:           31628620500   TX bytes:       0
   RX packets:         46795         TX packets:     0
   RX mcast packets:   367056        TX discards:    0
   RX discards:        212322        TX errors:      0
   RX errors:          0             TX overruns:    0
   RX overruns:        0             TX carrier:     0
   RX frame:           0             TX collisions:  0
                                     TX queue len:   1000
```

# KAPITEL 20: SNMP-Daten

FireEye Appliances senden Simple Network Management Protocol (SNMP) Daten, um anormale Bedingungen an administrative Computer zu übermitteln, die sie überwachen und steuern. Die administrativen Computer werden *SNMP Manager* genannt.

SNMP-Daten schließen folgendes ein:

- Information, die durch den SNMP-Manager abgerufen wird (pulled). Diese Information wird als Antwort auf Anfragen gesendet, die der SNMP Manager an die Appliance sendet. Siehe SNMP-Daten abrufen unten.
- Ereignisse (bekannt als *Traps*), die von der Appliance an den SNMP-Manager gesendet (pushed) werden. Traps melden normalerweise Bedingungen, wie beispielsweise Laufwerkausfall oder überhöhte Temperatur. Sie sind nicht angefordert; dies bedeutet, dass sie nicht als Antwort auf Anfragen vom SNMP-Manager gesendet wurden. Siehe Traps senden auf Seite 375.

# SNMP-Daten abrufen

Dieser Abschnitt beschreibt den Abruf von SNMP-Informationen von der Network Security Appliance.

Eine Management Information Base (MIB) ist eine in einem bestimmten Format geschriebene Textdatei, in der alle verwaltbaren Funktionen eines Gerätes in einem Baum angeordnet sind. Jeder Zweig dieses Baums enthält eine Nummer und einen Namen und der vollständige Pfad vom der Spitze des Baumes bis zum Interessenpunkt formt den Object Identifier oder OID. Der OID ist eine Zeichenfolge von Werten, durch Punkte getrennt, wie zum Beispiel **.1.3.6.1.2.1.1.3.0.**

Sie können Datenanfragen über ein Objekt mit Hilfe des OID senden, aber es könnte einfacher sein, stattdessen den symbolischen Namen des Objekts zu verwenden. Ein MIB gestattet SNMP-Tools, die symbolischen Namen in OIDs zu übersetzen, bevor die Anfragen an das verwaltete Gerät gesendet werden. Symbolische Namen für Objekte in der FireEye MIB schließen **feSerialNumber.0**, **feHardwareModel.0**, **feProductLicenseActive0**, **feFanIsHealthy.1**, und so weiter ein.

Die FireEye MIB mit dem Namen FE-FIREEYE-MIB muss von der Network Security Appliance auf den SNMP-Manager heruntergeladen werden, so dass sie auf einen SNMP-Browser oder anderes Tool geladen werden kann. Ein typischer SNMP-Browser kann die Werte abrufen, die die Appliance unterstützt und sie dann in einer Hierarchie anzeigen, so dass Sie auf den Wert navigierten können, den Sie in der Anfrage einschließen müssen.

Dieser Abschnitt enthält die folgenden Themen:



# Zugriff auf SNMP-Daten liefern

Um Zugriff auf SNMP v3 Daten zu gewähren, konfigurieren Sie einen Benutzernamen und ein Passwort.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um Zugriff auf SNMP-Daten zu aktivieren:**

1. Wechseln Sie auf den CLIKonfigurationsmodus:

   ```
   hostname > enable hostname # configure terminal
   ```

2. Bestätigen Sie, dass SNMP aktiviert ist.

   ```
   hostname (config) # show snmp
   ```

   Wenn die Ausgabe `SNMP enabled: no` anzeigt, geben Sie den `snmp-server enable` Befehl ein.

3. *SNMP v3*: Überprüfen Sie den SNMP-Benutzer und Passwort:

   ```
   hostname (config) # snmp-server user <username> v3 enable hostname
   (config) # snmp-server user <username> v3 auth sha <password>
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Die MIB herunterladen

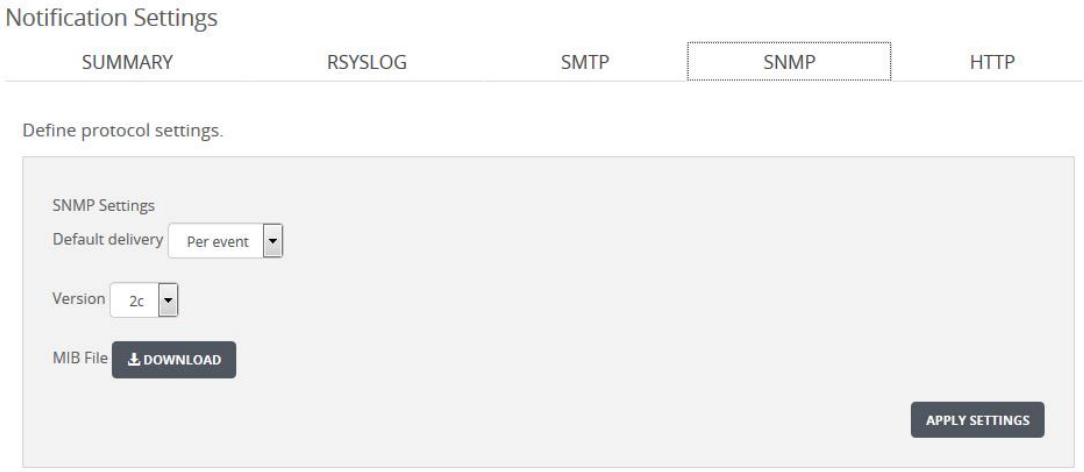
Sie können die MIB (Management Information Base) von der Web-UI oder der Eingabeaufforderung herunterladen.

# Voraussetzungen

- Analyst, Operator oder Admin Zugriff

## Die MIB mit Hilfe der Web-UI herunterladen

Verwenden Sie die **Notification Settings** Seite, um die MIB herunterzuladen.




**Um die MIB herunterzuladen:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Notifications.**
3. Klicken Sie auf den **SNMP** Tab.
4. Im **Define protocol settings** Abschnitt klicken Sie auf **Download**

## Die MIB mit Hilfe der Eingabeaufforderung herunterladen

Dieser Abschnitt beschreibt das Herunterladen der FE-FIREEYE-MIB auf SNMP Managern, die auf Microsoft Windows, Linux und Apple Geräten ausgeführt werden. Die MIB-Datei wird mit Hilfe eines Programms abgerufen, das durch Port 22 verbindet, der normalerweise für Protokolle wie SSH, SCP und PSCP verwendet wird. Da Zugriff auf Dateiebene durch Richtlinien verweigert wird, muss der direkte Pfad auf die MIB Datei festgelegt werden.

**Um die FireEye MIB auf Windows Geräte herunterzuladen:**

1. Laden Sie das pscp.exe Tool herunter (auf der PuTTY Download Seite verfügbar).
2. Navigieren Sie auf ein Eingabeaufforderungsfenster.
3. Ändern Sie das Verzeichnis, auf das Sie das pscp.exe Tool heruntergeladen haben:

   ```
   cd Downloads
   ```

4. Kopieren Sie die MIB-Dateien von der Appliance.

   ```
   pscp.exe -r -scp
   admin@<appliance><applianceIPAddress>:/usr/share/snmp/mibs \Temp\mibs\
   ```

5. Wenn Eingabe des Kennworts gefordert wird, geben Sie **admin** ein.

   Die Dateien werden auf das `\Temp\mibs` Verzeichnis auf dem Windows Gerät kopiert.

6. Wechseln Sie auf das `mibs` Verzeichnis:

   ```
   cd C:\Temp\mib
   ```

7. Laden Sie die MIB in einen SNMP-Browser oder Tool, oder öffnen Sie die MIB-Datei:

   ```
   vi FE-FIREEYE-MIB.txt
   ```

**Um die FireEye MIB auf Linux Geräte herunterzuladen:**

1. Kopieren Sie die MIB-Datei von der Appliance mit Hilfe des OpenSSH Client:

   ```
   scp -r admin@<appliance><applianceIPAddress>:/usr/share/snmp/mibs
   /usr/<userDirectoryName>
   ```

2. Wenn Eingabe des Kennworts gefordert wird, geben Sie **admin** ein.

   Die Dateien werden auf das `mibs` Verzeichnis kopiert, das sich im `/usr/<userDirectoryName>` Verzeichnis befindet.

3. Wechseln Sie auf das `mibs` Verzeichnis:

   ```
   cd mibs
   ```

4. Laden Sie die MIB in einen SNMP Browser oder Tool, oder öffnen Sie die MIB Datei:

   ```
   vi FE-FIREEYE-MIB.txt
   ```

**Um die FireEye MIB auf Apple Geräte herunterzuladen:**

1. Navigieren Sie auf den Terminal Emulator.
2. Kopieren Sie die MIB-Dateien von der Appliance.

   ```
   scp -r admin@<applianceIPAddress>:/usr/share/snmp/mibs ~/
   ```

3. Wenn Eingabe des Kennworts gefordert wird, geben Sie **admin** ein.

   Die Dateien werden auf das `mibs` Verzeichnis kopiert, das sich im Benutzerverzeichnis befindet.

4. Laden Sie die MIB in einen SNMP-Browser oder Tool, oder öffnen Sie die MIB-Datei:

   ```
   vi FE-FIREEYE-MIB.txt
   ```

## Anfragen für SNMP-Informationen senden

Dieses Thema beschreibt zwei Methoden, SNMP-Informationen abzurufen.

- Der `snmpget` Befehl ruft den Wert eines bestimmten Objekts ab.
- Der `snmpwalk` Befehl durchläuft die Objekthierarchie und ruft automatisch die Werte von Objekten für den von Ihnen festgelegten Teilbaum oder Knoten ab.

Beispiele allgemeiner Befehle folgen, die SNMP-Daten abrufen. Die Befehle werden von der SNMP-Manager Anwendung eingegeben. Die IP-Adresse in den Befehlen ist die IP-Adresse der Appliance.

**SNMP v3 Befehle:**

```
snmpmgr # snmpget  -m +FE-FIREEYE-MIB -v 3 -u myname -a MD5 -A mypassword -l
authNoPriv 172.0.0.0 feTemperatureValue.0
```

```
snmpmgr # snmpwalk  -m +FE-FIREEYE-MIB -v 3 -u myname -a MD5 -A mypassword -l
authNoPriv 172.0.0.0 enterprises.25597
```

**SNMP v2c Befehle:**

```
snmpmgr # snmpget  -m +FE-FIREEYE-MIB -v 2c -c public 172.0.0.0
feSupportLicenseActive.0
```

```
snmpmgr # snmpwalk -m +FE-FIREEYE-MIB -v 2c -c public 172.0.0.0 fireeye
```

```
snmpmgr # snmpwalk -v 2c -c public 172.0.0.0 enterprises.25597
```

Um die in der Tabelle formatierten Lizenzablaufdaten abzurufen, verwenden Sie einen Befehl, der dem folgenden ähnelt (für verschiedene SNMP-Manager-Anwendungen sind verschiedene Befehle erforderlich):

```
snmpmgr # snmptable -c public -Of -v 2c localhost feLicenseFeatureTable
```

Überprüfen Sie die Anzahl der Tage in der rechten Spalten. Wenn der Wert kleiner als 30 ist, wenden Sie sich an Ihren Systemadministrator.

# Traps senden

Dieser Abschnitt beschreibt die Konfiguration von allgemeinem SNMP Support auf der Network Security Appliance, Aktivieren und Konfigurieren von Traps und Einstellen von Trap Protokollierung. Detaillierte Informationen über SNMP Befehle und Optionen für fortgeschrittenere Konfigurationen finden Sie in der *CLI Befehlsreferenz*.

## Traps aktivieren und deaktivieren

Unterschiedliche Ereignisse können die Appliance veranlassen, Traps an den SNMP-Manager zu senden. Die meisten Ereignisse sind standardmäßig aktiviert. Dieses Thema beschreibt die Aktivierung der Appliance, um Traps zu senden, die IP-Adresse des SNMP-Managers zu konfigurieren, der die Traps erhalten soll und individuelle Ereignisse zu aktivieren und deaktivieren.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um Traps und Ereignisse zu aktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus:

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. SNMP ist standardmäßig aktiviert. Bestätigen Sie, dass es aktiviert ist:

   ```
   hostname (config) # show snmp
   ```

   Wenn die Ausgabe `SNMP enabled: no`anzeigt, geben Sie den **`snmp-server enable`** Befehl ein.

3. Aktivieren Sie die Appliance, um Benachrichtigungen an den SNMP-Manager zu senden:

   ```
   hostname (config) # snmp-server enable notify
   ```

4. Legen Sie die IPv4 oder IPv6-Adresse des SNMP-Managers fest.

   ```
   hostname (config) # snmp-server host <IPv4 or IPv6 address> traps
   public
   ```

5. Speichern Sie Ihre Änderungen

   ```
   hostname (config) # write memory
   ```

**Um die Ereignisse anzuzeigen, die aktiviert werden können oder derzeit aktiviert sind:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie eine Liste aller Ereignisse an, die aktiviert werden können:

   ```
   hostname (config) # snmp-server notify event ?
   ```

3. Zeigen Sie die Ereignisse an, die derzeit aktiviert sind:

   ```
   hostname (config) # show snmp events
   ```

**Um bestimmte Ereignisse zu aktivieren oder deaktivieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Deaktivieren Sie ein Ereignis:

   ```
   hostname (config) # no snmp-server notify event <event>
   ```

   Zum Beispiel verhindert der folgende Befehl, dass ein Trap gesendet wird, wenn die Temperatur der Appliance normal ist:

   ```
   hostname (config) # no snmp-server notify event normal-temperature
   ```

3. Aktivieren Sie ein Ereignis:

   ```
   hostname (config) # snmp-server notify event <event>
   ```

   Zum Beispiel ermöglicht der folgende Befehle, dass die Appliance ein Trap sendet, wenn ein Schnittstellenlink geändert wird:

   ```
   hostname (config) # snmp-server notify event if-link-change
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Trap-Nachrichten protokollieren

Der snmptrapd Dienst empfängt und protokolliert Trap-Benachrichtigungen.

**Um Trap-Protokollierung einzustellen:**

1. Melden Sie sich in der SNMP- Manager Anwendung an.
2. Aktivieren Sie den snmptrapd Service:

   ```
   snmptrapd
   ```

3. Legen Sie den Protokollspeicherort fest:

   ```
   /var/log/snmptrapd.log
   ```

# KAPITEL 21: Anmeldebanner und Nachrichten

Dieses Thema behandelt die folgenden Informationen:

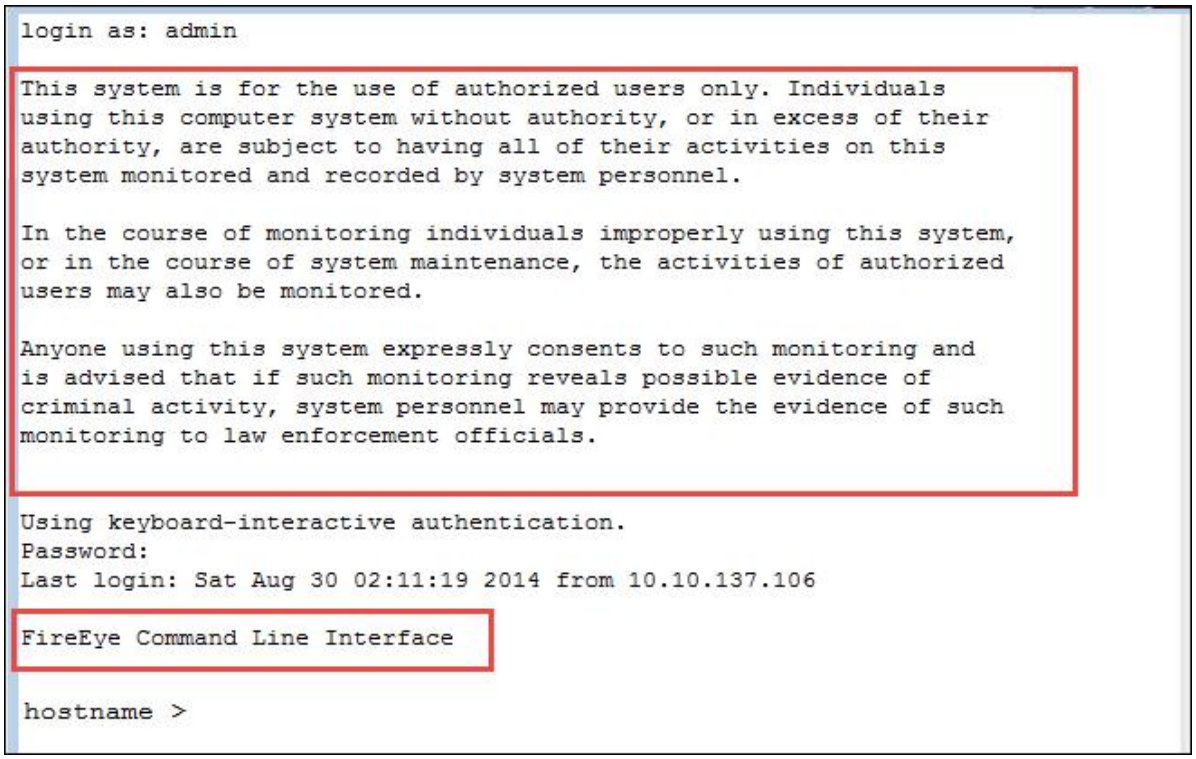


## Login Banner und Nachrichten

Sie können die Nachricht, die angezeigt wird, wenn sich Benutzer auf der Network Security Appliance anmelden, anpassen oder entfernen. Sie können die folgenden Nachrichten konfigurieren:

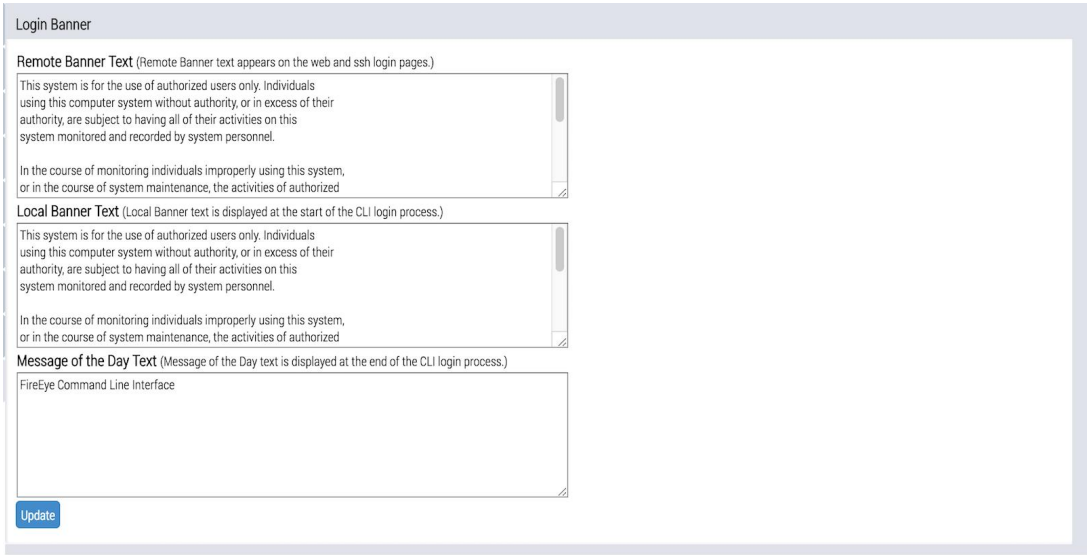
- **Remote Banner**—Wird auf der Web-UI Anmeldeseite und der SSH Anmeldeseite angezeigt.
- **Local Banner**—Wird angezeigt, nachdem der Benutzername in der CLI Sitzung eingegeben wurde.
- **Message of the Day**—Wird angezeigt, nachdem der Benutzer authentifiziert und auf der Appliance CLI angemeldet ist.

Das Standard Local Banner und die Message of the Day werden in den folgenden Illustrationen angezeigt.




# Anmeldebanner und Nachrichten mit Hilfe der Web-UI anpassen

Verwenden Sie die **Login Banner** Seite, um die Nachrichten zu konfigurieren, die Benutzer sehen, wenn sie sich auf der Network Security Appliance anmelden.



## Voraussetzungen

- Operator oder Admin Zugriff

**Um Anmeldenachrichten zu konfigurieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **Login Banner**.
3. Im **Remote Banner Text** Feld löschen Sie den vorhandenen Text und geben Sie dann die Nachricht ein, die auf den Web-UI und SSH Anmeldeseiten angezeigt werden soll. Sie können bis zu 2000 Zeichen eingeben.

   **WICHTIG!** Wenn Sie den Bannertext später mit Hilfe des `banner login` CLI Befehls ändern, wird der neue Text auf der Web-UI Anmeldeseite und der SSH Anmeldeseite angezeigt und überschreibt den Text, den Sie hierfür festgelegt haben.

4. Im **Local Banner Text** Feld löschen Sie allen vorhandenen Text und geben Sie dann die Nachricht ein, die in der CLI nach Eingabe des Benutzernamens angezeigt werden soll. Sie können bis zu 2000 Zeichen eingeben.
5. Im **Message of the Day Text** Feld löschen Sie allen vorhandenen Text und geben Sie die Nachricht ein, die in der CLI nach der Authentifizierung des Benutzers angezeigt werden soll. Sie können bis zu 2000 Zeichen eingeben.
6. Klicken Sie auf **Update**.

   Die Nachricht wird angezeigt, wenn sich der Benutzer das nächste Mal anmeldet.

# Anmeldebanner und Nachrichten mit Hilfe der CLI anpassen

Verwenden Sie die CLI Befehle in diesem Thema, um die Nachrichten zu konfigurieren, die User sehen, wenn sie sich auf der Appliance anmelden.

- Die *login* Nachricht wird angezeigt, nachdem der Benutzername eingegeben wurde.
- Die *local login message* wird in der CLI Anmeldung angezeigt, nachdem der Username eingegeben wurde.
- Die *remote Anmeldenachricht* wird auf der SSH Anmeldeseite angezeigt.
- Die *message of the day* (Nachricht des Tages) wird angezeigt, nachdem das Kennwort eingegeben und der Benutzer authentifiziert wurde.

**HINWEIS:**Nachrichten können länger als eine Zeile sein. Um eine neue Zeile hinzuzufügen, tippen Sie >. Jede Nachricht kann bis zu 2000 Zeichen enthalten.

## Voraussetzungen

- Operator oder Admin Zugriff

**Um die Nachrichten anzupassen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie den aktuellen Bannertext an:

   ```
   hostname (config) # show banner
   ```

3. Führen Sie die folgenden Aufgaben nach Bedarf aus.

   - Um die gleiche Nachricht für die *lokale Anmeldenachricht* zu konfigurieren (die in der CLI Anmeldung angezeigt wird) sowie die *remote Anmeldenachricht* (die auf der Web-UI Anmeldeseite und der SSH Anmeldeseite angezeigt wird), verwenden Sie den folgenden Befehl:

     ```
     hostname (config) # banner login "<text>"
     ```

     **IMPORTANT!** Die *Anmeldenachricht*, die Sie mit Hilfe des **banner login "<text>"** Befehls konfigurieren, überschreibt auch die *remote Nachricht*, die auf der Web-UI Anmeldeseite und der SSH Anmeldeseite angezeigt wird. Verwenden Sie die Anmeldebanner und Nachrichten mit Hilfe der Web-UI anpassen auf Seite 380, um eine eindeutige Web-UI und SSH Anmeldenachricht festzulegen.

   - Um nur die lokale Anmeldenachricht zu ändern, verwenden Sie den folgenden Befehl:

     ```
     hostname (config) # banner login-local "<text>"
     ```

   - Um nur die remote Anmeldenachricht zu ändern, verwenden Sie den folgenden Befehl:

     ```
     hostname (config) # banner login-remote "<text>"
     ```

   - Um die Nachricht des Tages (Message of the Day) zu ändern, verwenden Sie den folgenden Befehl:

     ```
     hostname (config) # banner motd "<text>"
     ```

   - Um die lokale Anmeldenachricht, die remote Anmeldenachricht oder beide zu löschen:

     ```
     hostname (config) # banner login ""
     hostname (config) # banner login-local ""
     hostname (config) # banner login-remote ""
     ```

   - Um die Nachricht des Tages zu löschen:

     ```
     hostname (config) # banner motd ""
     ```

   - Um die Standard Nachrichten wiederherzustellen:

     ```
     hostname (config) # no banner login
     hostname (config) # no banner motd
     ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiele

Das folgende Beispiel ändert die Nachricht des Tages.

```
hostname (config) # banner motd “There are no maintenance activities
scheduled for this week.”
```

Das folgende Beispiel ändert die lokale und remote Anmeldenachricht:

```
hostname (config) # banner login "This FireEye appliance is the property of
Acme, Inc.
>
>Unauthorized access is prohibited and is punishable by law."
```

Das folgende Beispiel zeigt die aktuellen Nachrichten.

```
hostname # show banner
Banner:
     Message of the Day (MOTD): Für diese Woche sind keine
Wartungsaktivitäten geplant.

     Login: This FireEye appliance is the property of Acme, Inc.
Unauthorized access is prohibited and is punishable by law.
```

Das folgende Beispiel zeigt die Standard Nachrichten an:

```
hostname # show banner

Banner:
    Message of the Day (MOTD): FireEye Befehlszeilenschnittstelle

    Local login: This system is for the use of authorized users only.
>
>Individuals using this computer system without authority, or in excess of
their authority, are subject to having all of their activities on this system
monitored and recorded by system personnel.

    Network login: This system is for the use of authorized users only.
>
>Individuals using this computer system without authority, or in excess of
their authority, are subject to having all of their activities on this system
monitored and recorded by system personnel.
```

# KAPITEL 22: Unterstützte Funktionen

Auf der Web-UI Features Seite werden Kacheln für die für diese Appliance verfügbaren Funktionen angezeigt. Kacheln für aktivierte Funktionen sind mit einem Häkchen markiert und grün umrandet. Funktionen, die in der gerade angezeigten Ausgabe von Central Management eingeführt wurden, sind als **New** gekennzeichnet.

## Voraussetzungen

- Admin, Operator, Monitor oder Analyst Zugriff

# Unterstützte Funktionen mit Hilfe der Web-UI anzeigen

Verwenden Sie die **Supported Features** Seite, um die für eine Appliance verfügbaren Funktionen anzuzeigen.

**Um die unterstützen Funktionen anzuzeigen:**

1. Klicken Sie auf den **Features** tab or click **About > Supported Features**.
2. Um nach Kategorie zu filtern, wählen Sie eine der folgenden Optionen in dem Auswahlfeld oben links auf der Seite.
    - Detection
    - Integration
    - Management
3. Klicken Sie auf **Enabled** oder **Disabled**, um nach aktivierten oder deaktivierten Funktionen zu filtern.
4. Klicken Sie auf **New Features Only**, um nur neue Funktionen anzuzeigen.

5. Klicken Sie auf **i** in einer Kachel, um Informationen über die Funktion anzuzeigen, einschließlich der Version, in der sie veröffentlicht wurde, die gebotene Sicherheitskategorie und alle zusätzlichen Anforderungen.

# KAPITEL 23: Speicherplatzverwaltung

Für einige Appliance Prozesse ist eine bestimmte Menge an Speicherplatz erforderlich. Wenn kein Speicherplatz verfügbar ist, werden die Prozesse nicht gestartet. Eine Fehlermeldung beschreibt das Problem.

So müssen Sie zum Beispiel möglicherweise Dateien und Artefakte löschen, um Speicherplatz freizugeben, wenn nicht genügend Speicherplatz für eine Datenbanksicherung, zum Abrufen von SNMP Daten oder zum Senden von System-Benachrichtigungen vorhanden ist. Es kann auch erforderlich sein, vor der Aktualisierung der Appliance Speicherplatz freizugeben.

System-Tools helfen Ihnen, den Speicherplatz automatisch und bei Bedarf zu verwalten. Details finden Sie unter Dateien automatisch löschen unten. Siehe Bereinigung nach Bedarf mit Hilfe von Profilen auf Seite 391.

## Dateien automatisch löschen

Die Appliance überwacht und gibt in regelmäßigen Intervallen Speicherplatz frei. Dateien, E-Mails und Aufzeichnungen von virtuellen Maschinen werden je nach Größe und Altersbeschränkungen automatisch gelöscht. Dateien werden von der ältesten angefangen gelöscht, so dass alle Artefakttypen innerhalb ihrer festgelegten Speicherplatzbeschränkungen bleiben. Sie können die Grenzwerte ändern, um die Bereinigung zu optimieren.

Die Standardgrenzwerte lauten wie folgt:

| Artefakttyp und Maße | Standardgrenzwerte |
|---|---|
| Größe bösartiger Dateien | 20 GB |
| Tage für bösartige Dateien | 30 Tage |
| Größe nicht-bösartiger Dateien | 20 GB |

| Artefakttyp und Maße | Standardgrenzwerte |
|---|---|
| Tage für nicht bösartige Dateien | 15 Tage |
| Größe der Erfassung bösartiger virtueller Maschinen | 20 GB |
| Tage für die Erfassung bösartiger virtueller Maschinen | 30 Tage |
| Größe der Erfassung nicht-bösartiger virtueller Maschinen | 20 GB |
| Tage für die Erfassung nicht-bösartiger virtueller Maschinen | 15 Tage |
| Größe bösartiger E-Mails | 20 GB |
| Tage für bösartige E-Mails | 30 Tage |

Informationen über die Verwaltung der Bereinigungsgrenzwerte für Artefakte finden Sie in den folgenden Abschnitten:

- Grenzwerte für automatische Bereinigung von Artefakten mit Hilfe der CLI ändern unten
- Die Standardgrenzwerte für automatische Bereinigung von Artefakten mit Hilfe der CLI wiederherstellen auf Seite 391

## Grenzwerte für automatische Bereinigung von Artefakten mit Hilfe der CLI ändern

Sie können die Grenzwerte für die Bereinigung von Artefakten ändern, um den Speicherplatz automatisch zu löschen, je nach dem von Ihrer Appliance normalerweise verarbeiteten Artefaktvolumen und dem verfügbaren Speicherplatz. Sie können diese nur mit Hilfe von CLI-Befehlen ändern.

**Um die Bereinigungsgrenzwerte für Artefakte zu ändern:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Zeigen Sie die aktuellen Grenzwerte an:

```
hostname (config) # show analysis artifacts-cleanup

Malicious Files:
       Keep Size (GB) : 20
       Keep Days      : 30

Malicious VM Captures:
       Keep Size (GB) : 20
       Keep Days      : 30

Malicious Emails:
       Keep Size (GB) : 20
       Keep Days      : 30

Non Malicious Files:
       Keep Size (GB) : 20
       Keep Days      : 15

Non Malicious VM captures:
       Keep Size (GB) : 20
       Keep Days      : 15
```

3. Legen Sie neue Grenzwerte für alle Einstellungen fest, die Sie ändern wollen:
   - Um den Grenzwert für bösartige Dateien nach Tag zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup malicious files keep days 30
     ```

   - Um den Grenzwert für nicht-bösartige Dateien nach Tag zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup non-malicious files keep days 10
     ```

   - Um den Grenzwert für bösartige E-Mails nach Tag zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup malicious emails keep days 30
     ```

   - Um den Grenzwert für die Erfassung bösartiger virtueller Maschinen nach Tag zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup malicious vm-captures keep days 30
     ```

   - Um den Grenzwert für die Erfassung nicht-bösartiger virtueller Maschinen nach Tag zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup non-malicious vm-captures keep days 10
     ```

   - Um den Grenzwert für bösartige Artefaktdateien nach Größe zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup malicious files keep size 40
     ```

   - Um den Grenzwert für nicht-bösartige Artefaktdateien nach Größe zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup non-malicious files keep size 20
     ```

   - Um den Grenzwert für bösartige E-Mails nach Größe zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup malicious emails keep size 40
     ```

   - Um den Grenzwert für die Erfassung bösartiger virtueller Maschinen nach Größe zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup malicious vm-captures keep size 40
     ```

   - Um den Grenzwert für die Erfassung nicht-bösartiger virtueller Maschinen nach Größe zu ändern:

     ```
     hostname (config) # analysis artifacts-cleanup malicious vm-captures keep size 20
     ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Die Standardgrenzwerte für automatische Bereinigung von Artefakten mit Hilfe der CLI wiederherstellen

Sie können alle Bereinigungsgrenzwerte für Artefakte auf Ihre Standards durch einen einzelnen CLI Befehl wiederherstellen.

**Um Standardwerte für die Bereinigungsgrenzwerte für Artefakte auf die Standards zurückzusetzen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Um Bereinigungsgrenzwerte für Artefakte auf die Standards zurückzusetzen:

   ```
   hostname (config) # analysis artifacts-cleanup set-default
   ```

3. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Bereinigung nach Bedarf mit Hilfe von Profilen

Sie können den von Systemdateien, wie z. B. Sicherungen, Speicherauszügen, Berichten, Protokolldateien und einige Arten von Artefakten verwendeten Speicherplatz analysieren. Datenträgerverwaltungsprofile werden für Gruppen von Systemdateitypen definiert. Mithilfe dieser Profile können Sie Daten löschen, um Speicherplatz freizugeben.

Einige Daten, wie z.B. Konfigurationsdaten, können nicht gelöscht werden.

Nachfolgend sehen Sie die Profile, die Sie für die Datenträgerverwaltung verwenden können:

| Profil | Beschreibung |
|---|---|
| backups | Während der benutzerinitiierten Sicherungs- und Wiederherstellungsvorgänge erstellte Sicherungsdateien. |
| fedb-backups | Während der System-Image Updates erstellte Datenbannk |
| logs | Protokolldateien |
| malicious-artifacts | Auf der Appliance generierte bösartige Artefaktdateien |

| Profil | Beschreibung |
|---|---|
| nonmalicious-artifacts | Auf der Appliance generierte nicht-bösartige Artefaktdateien |
| reports | Berichtsdateien |
| smartvision | SmartVision Kontextdateien |
| snapshots | System-Snapshots |
| sysdumps | System-Dumps |
| tcpdumps | TCP-Erfassungsdateien |
| temp-files | Temporäre Dateien |

Weitere Informationen finden Sie unter:

- Eine Zusammenfassung der Speicherplatznutzung mit Hilfe der CLI anzeigen unten
- Speicherplatznutzung nach Profil mit Hilfe der CLI anzeigen auf der nächsten Seite
- Daten mit Hilfe der CLI löschen, um Speicherplatz freizugeben auf Seite 394

# Eine Zusammenfassung der Speicherplatznutzung mit Hilfe der CLI anzeigen

Sie können eine Zusammenfassung der Speicherplatznutzung für die `/config`, `/var` und `/data` Dateisysteme und zugehörigen Profile anzeigen. Sie sollten diesen Befehl ausführen, um Speicherplatznutzung zu analysieren.

**HINWEIS:** Dateien vom `/config` Dateisystem können nicht gelöscht werden. Speicherplatzinformationen für dieses Dateisystem dienen nur zu Informationszwecken.

**Um eine Zusammenfassung der Speicherplatznutzung anzuzeigen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

2. Zeigen Sie die Zusammenfassung der aktuellen Speicherplatznutzung an:

```
hostname (config) # show system cleanup summary
```

```
Statistics for /config filesystem:
Space Total          182 MB
Space Used             7 MB
Space Free           175 MB
Space Available      166 MB
Space Percent Free   96%
Inodes Percent Free  99%

Statistics for /var filesystem:
```

```
Space Total          20031 MB
Space Used            2682 MB
Space Free           17348 MB
Space Available      16324 MB
Space Percent Free   86%
Inodes Percent Free  99%

Statistics for /data filesystem:
Space Total          1068532 MB
Space Used           126189 MB
Space Free           942343 MB
Space Available      888058 MB
Space Percent Free   88%
Inodes Percent Free  99%

Statistics for /data/db filesystem:
Space Total          125863 MB
Space Used           958 MB
Space Free           124905 MB
Space Available      118489 MB
Space Percent Free   99%
Inodes Percent Free  99%

Profile Name           | Description                     | Occupied Space | Cleanable Space | Filesystems
====================== | ================================|================================================
backups                | Unified Backups                 |           0 MB |             0 MB | /data
fedb-backups           | FEDB Backups                    |        6446 MB |          6446 MB | /data
logs                   | Application log files           |         427 MB |           411 MB | /var
malicious-artifacts    | Malicious Malware Artifacts     |           0 MB |             0 MB | /data
nonmalicious-artifacts | Non-malicious Malware Artifacts |           0 MB |             0 MB | /data
reports                | Reports                         |           1 MB |             1 MB | /data
snapshots              | System snapshots                |           8 MB |             5 MB | /data
sysdumps               | System dumps                    |           0 MB |             0 MB | /data
tcpdumps               | TCP capture files               |           0 MB |             0 MB | /var
temp-files             | Temporary files                 |           0 MB |             0 MB | /var
```

# Speicherplatznutzung nach Profil mit Hilfe der CLI anzeigen

Speicherplatznutzung kann nach Profil angezeigt werden. Sie sollten diesen Befehl ausführen, um die besten Daten zur Löschung für ein bestimmtes Profil zu ermitteln.

**Um eine Zusammenfassung der Speicherplatznutzung nach Profil anzuzeigen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie die aktuelle Speicherplatznutzung für ein Profil an:

   ```
   hostname (config) # show system cleanup profile [backups | fedb-backups
   | logs | malicious-artifacts | nonmalicious-artifacts | reports |
   smartvision | snapshots | sysdumps | tcpdumps]
   ```

   Profilbeschreibungen finden Sie unterBereinigung nach Bedarf mit Hilfe von Profilen auf Seite 391.

   Nachfolgend wird als Beispiel die Speicherplatznutzung für das `logs` Profil angezeigt:

   ```
    hostname (config) # show system cleanup profile logs
   Older than  | Size
   ============|=============
    365 days   |           0 MB
    180 days   |          25 MB
     90 days   |         212 MB
     30 days   |         342 MB
      7 days   |         382 MB
      1 day    |         405 MB
       All     |         411 MB
   ```

## Daten mit Hilfe der CLI löschen, um Speicherplatz freizugeben

Nachdem Sie die Speicherplatznutzung analysiert haben, können Sie Daten löschen, um den erforderlichen Speicherplatz freizugeben.

**Um Daten für die Freigabe von Speicherplatz zu löschen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Löschen Sie Daten:

```
hostname (config) # system cleanup profile {backups | fedb-backups |
logs | malicious-artifacts | nonmalicious-artifacts | reports |
smartvision | snapshots | sysdumps | tcpdumps | temp-files} {all |
older-than <no. of days>} [force]
```

wobei:

- **all** alle Daten löscht, die für dieses Profil gelöscht werden können
- **older-than <no. of days>** löscht Daten, die älter als die festgelegte Anzahl von Tagen sind
- **force** löscht die gewünschten Daten, ohne eine Bestätigung zu verlangen

Wenn Sie die `force` Option nicht verwenden, erfordert der Befehls eine Bestätigung.

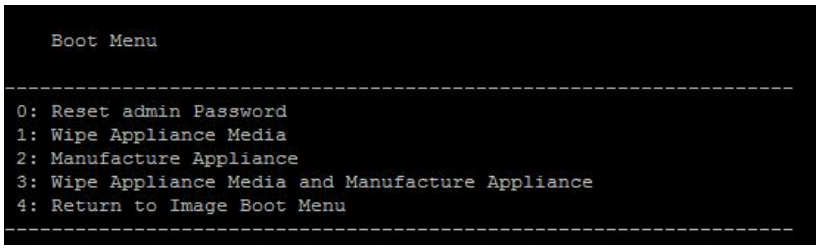
Das folgende Beispiel löscht zum Beispiel Daten, die mit dem `logs` Profil übereinstimmen. Es werden nur Daten gelöscht, die älter als 180 Tage sind.

```
hostname (config) # system cleanup profile logs older-than 180
This will remove cleanable files older than 180 days for the profile
'logs'. Do you want to continue? [y/n]: y
25 MB of disk space freed.
```

# KAPITEL 24: Start-Manager Dienstprogramme

Das Tools Menü bietet Zugriff auf die Start-Manager Dienstprogramme.

In der Konsole wird das Tools Menü manchmal *Boot Menu* genannt.




**Reset admin Password**

Setzt das "Admin" Passwort der Werkseinstellung zurück. Dieses Passwort, normalerweise "admin", ist das Passwort, das für die Anmeldung auf der physischen oder seriellen Konsole benutzt wird. Aus Sicherheitsgründen kann der Admin Benutzer dieses Passwort nicht für die remote Anmeldung auf der Web-UI oder CLI der Appliance verwenden. Also muss das Passwort während der Erstkonfiguration der Appliance in der Konsole geändert werden. Diese Option ist geeignet, wenn das konfigurierte Admin Passwort für remote Zugriff verloren gegangen ist oder vergessen wurde. Der "Admin" Benutzer kann sich mit dem Standard Passwort in die physische oder serielle Konsole einloggen und es dann ändern, damit das Passwort auch für den Remote Zugriff verwendet werden kann.

**Wipe Appliance Media**

Setzt die Appliance Medien zurück. Die Appliance ist danach nicht mehr betriebsfähig. Diese Option ist geeignet, wenn Sie vorhaben, ein RMA zu verwenden, um die Appliance zu ersetzen und Kundendaten bereits mit Hilfe der Datenbank-Sicherungsfunktion gespeichert haben. Weitere Informationen finden Sie unter Persistente Medien löschen auf Seite 406.

**Manufacture Appliance**

Stellt die Appliance auf Werkseinstellungen zurück, einschließlich ihrer ursprünglichen Herstellungsparameter (z.B. Hostname und DTI Berechtigungen). Diese Option ist geeignet, wenn Sie eine vollständigere Zurücksetzung auf die Werkseinstellungen vornehmen müsseln, als mit dem `reset factory` CLI Befehlen möglich ist. Wenn Sie mit Hilfe dieses Dienstprogramms herstellen, bleiben nur die ursprüngliche System Image Version und Herstellungszeitstempel im Systemprotokoll erhalten.

**Wipe Appliance Media and Manufacture Appliance**

Setzt die Appliance Medien zurück und stellt die Appliance auf Werkseinstellungen ein. Diese Option ist geeignet, wenn Sie die Appliance am Ende einer Beurteilung an FireEye zurücksenden, so dass sie für eine weitere Beurteilung verwendet werden kann. Weitere Informationen finden Sie unter Persistente Medien löschen auf Seite 406.

**Return to Image Boot Menu**

Kehrt auf das Image Boot Menü zurück, wo Sie eine installierte Abbildung von einem bestimmten Boot-Speicherort starten können. Diese Option ist geeignet, wenn Sie eine neue System Image Version installieren aber stattdessen eine frühere Version benutzen wollen oder wenn Sie aus Versehen vom falschen Boot Speicherort gebootet haben.

**WICHTIG:** Nachdem Sie diese Option ausgewählt haben, sollten Sie genau auf die Konsole achten, so dass Sie keine Reihe von fünf Punkten (`.`) verpassen,die in einer Sekunde Abstand angezeigt werden. Bevor die Konsole über den fünften Punkt hinaus bewegt, drücken Sie eine beliebige Taste zweimal, um zum Startmenü zurückzukehren.

# Mit dem Tools Menü arbeiten

In den folgenden Themen werden der Zugriff und die Benutzung des Tools Menüs beschrieben.



## Systemanforderungen

Stellen Sie sicher, dass die folgenden Erfordernisse erfüllt sind:

- Modellnummern und Systemimage Versionen:
  - **Malware Analysis** Version 8.0.0 oder später wird auf einem der folgenden Appliance Modelle ausgeführt: AX 5500, AX 5550.
  - **Central Management** Version 8.1.0 oder höher wird auf einem der folgenden Appliance Modelle ausgeführt: CM 4500, CM 7500, CM 9500.
  - **Email Security — Server Edition** Version 8.0.0 oder höher wird auf einem der folgenden Appliance Modelle ausgeführt:: EX 3500, EX 5500, EX 8500.
  - **File Protect** Version 8.0.0 oder höher wird auf dem FX 6500 Modell ausgeführt.
  - **Endpoint Security** Version 4.0.0 oder höher wird auf einem der folgenden Appliance-Modelle ausgeführt: HX 4000, HX 4400, HX 4402.
  - **Network Security** Version 8.0.0 oder höher wird auf einem der folgenden Appliance Modelle ausgeführt: NX 1500, NX 2500, NX 2550, NX 3500, NX 4500, NX 5500, NX 7500, NX 10450, NX 10550.
  - **Virtual Execution** Version 8.0.0 oder höher wird auf einem der folgenden Appliance Modelle ausgeführt:: VX 5500, VX 12500.
- Sie haben jetzt Zugriff auf die physische oder serielle Konsole (siehe Zugriff auf die physische oder serielle Konsole auf Seite 93).
- Die oben angegebenen Mindestversion des Systemimage ist auf beiden Boot-Partitionen auf der Appliance installiert. Wenn die Appliance ursprünglich nicht mit dieser Systemimageversion hergestellt wurde, müssen Sie die Aufrüstungsschritte unten ausführen, um diese
- Sie haben das Appliance-spezifische Passwort für das Tools Menü von FireEye Technical Support erhalten oder ein anderes Passwort konfiguriert, wir in Das Passwort für das Tools Menü einstellen auf der nächsten Seite beschrieben.

## Beschränkungen

- Die **Manufacture Appliance** und **Wipe Appliance Media and Manufacture Appliance** Optionen erfordern, dass die Appliance ursprünglich mit einem Systemimage hergestellt wurde, dass das Tools Menü unterstützt.
- Alle Protokollierungen gehen an die serielle Konsole. Wenn Sie die physische Konsole für den Zugriff auf das Tools Menü benutzen, können Sie den Fortschritt nicht auf dem VGA Monitor überwachen.

## Aufrüstungsschritte

Die Mindestversion des Systemimage muss auf beiden Startpartitionen installiert sein, bevor Sie Zugriff auf das Tools Menü erhalten. Führen Sie die Schritte in diesem Abschnitt

aus, wenn Sie ein Upgrade von einer früheren Version durchführen.

**HINWEIS:** Diese Schritte sind nicht erforderlich, wenn Ihre Appliance ursprünglich mit der Mindestversion des Systemimage ausgestattet wurde. Die Mindestversionen sind in Systemanforderungen auf Seite 398 aufgeführt.

**Um das Tools Menü bei einem Upgrade von einer früheren Version zu aktivieren:**

1. Rufen Sie ein unterstütztes Systemimage ab und installieren sie es:

   ```
   hostname (config) # fenet image check hostname (config) # show fenet image status hostname (config) # fenet image fetch hostname (config) # show fenet image status hostname (config) # image install <image>
   ```

   Dies installiert das Systemimage in einer der Startpartitionen.

2. Bestätigen Sie die Startpartition für das neue Systemimage

   ```
   hostname (config) # show images
   ```

   Zum Beispiel auf einer Network Security Appliance:

   ```
   hostname (config) # show images Installed images: Partition 1: wmps wMPS (wMPS) 8.0.0 ... Partition 2: wmps wMPS (wMPS) 7.9.4 ... Last boot partition: 2 Next boot partition: 2
   ```

3. Wenn erforderlich, ändern Sie `Next boot partition` , so dass die Appliance von der Partition mit dem neuen Systemimage startet, wenn Sie neu geladen wird:

   ```
   hostname (config) # image boot next hostname (config) # write memory
   ```

4. Laden Sie die Appliance erneut:

   ```
   hostname (config) # reload
   ```

5. Installieren Sie das neue System Image erneut, um es auf die andere Boot-Partition zu stellen:

   ```
   hostname (config) # image install <image>
   ```

6. Ändern Sie die nächste Boot-Partition:

   ```
   hostname (config) # image boot next hostname (config) # write memory
   ```

7. Laden Sie die Appliance erneut:

   ```
   hostname (config) # reload
   ```

Wenn Sie das Standardpasswort für das Tools Menü nicht verwenden wollen, können Sie jetzt ein neues konfigurieren, wie in Das Passwort für das Tools Menü einstellen unten beschrieben. Benutzer, die das Passwort kennen, können auf das Tools Menü bei jedem nachfolgenden Appliance Neuladen zugreifen, wie in Zugriff auf das Tools Menü auf Seite 402 beschrieben.

## Das Passwort für das Tools Menü einstellen

Das Tools Menü erfordert ein Passwort. Es gibt zwei Optionen:

- **Standard Passwort**. Ein einzigartiges Passwort, das von der Appliance ID abgeleitet wurde, ist auf der Appliance vorgegeben und Sie können es von FireEye Technical Support erhalten.
- **Konfiguriertes Passwort**. Sie können stattdessen ein anderes Passwort in Klartext oder als eine Hash-Zeichenfolge einstellen. Ein Passwort in Klartext wird gehasht, bevor es gespeichert wird.

# Voraussetzungen

- Admin Zugriff

## Das Passwort für das Tools Menü in Klartext mit Hilfe der CLI einstellen

Verwenden Sie die Befehle in diesem Abschnitt, um dass Passwort für das Tools Menü in Klartext einzustellen.

**Um ein Passwort in Klartext einzustellen:**

1. Melden Sie sich auf der Appliance CLI an.
2. Gehen Sie auf den CLI Konfigurationsmodus:

   ```
   hostname > enable hostame # configure terminal
   ```

3. Stellen Sie das Passwort ein:

   ```
   hostname (config) # boot bootmgr tools password <password>
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**HINWEIS:** Alternativ können Sie den `boot bootmgr tools password 0 <password>` Befehl verwenden, um das Passwort in Klartext einzustellen oder den `boot bootmgr tools password` Befehl, um das Passwort in Klartext bei der Aufforderung einzugeben.

### *Beispiel:*

Im folgenden Beispiel wird "fyd4k8q2" als das Passwort für das Tools Menü eingestellt.

```
hostname (config) # boot bootmgr tools password fyd4k8q2
```

## Das Passwort mit Verschlüsselung für das Tools Menü mit Hilfe der CLI einstellen

Verwenden Sie die Befehle in diesem Abschnitt, um das Passwort für das Tools Menü mit einer Hash-Zeichenfolge einzustellen.

**Um ein verschlüsseltes Passwort einzustellen:**

1. Melden Sie sich auf der Appliance CLI an.
2. Gehen Sie auf den CLI Konfigurationsmodus:

   ```
   hostname > enable hostame # configure terminal
   ```

3. Stellen Sie das Passwort ein:

   ```
   hostname (config) # boot bootmgr tools password 7 <password>
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

### *Beispiel:*

Im folgenden Beispiel wird ein verschlüsseltes Passwort für das Tools Menü eingestellt.

```
hostname (config) # boot bootmgr tools password 7
$6$xuQN2G3r$ufK5k8dUDdpp0hPETrtjBIDZ3f3PhCxGYagp2k0gvgv/YrD88GNIkUsaKRVDMsPAy
QlcGuzhRXaBpCCVPeQd1
```

## Das Standardpasswort für das Tools Menü mit Hilfe der CLI wiederherstellen

Verwenden Sie die Befehle in diesem Abschnitt, um das Standardpasswort für das Tools Menü wiederherzustellen. Sie müssen dieses Passwort von FireEye Technical Support erhalten.

**Um das Standardpasswort für das Tools Menü wiederherzustellen:**

1. Melden Sie sich auf der Appliance CLI an.
2. Gehen Sie auf den CLI Konfigurationsmodus:

   ```
   hostname > enable hostname # configure terminal
   ```

3. Stellen Sie das Passwort wieder her:

   ```
   hostname (config) # no boot bootmgr tools password
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Zugriff auf das Tools Menü

Verwenden Sie das Verfahren in diesem Abschnitt, um auf das Tools Menü zuzugreifen.

**Um auf das Tools Menü zuzugreifen:**

1. Stellen Sie eine Verbindung mit der physischen oder seriellen Konsole her, wie in Zugriff auf die physische oder serielle Konsole auf Seite 93 beschrieben.

**HINWEIS:** Wenn Sie die physische Konsole für den Zugriff auf das Tools Menü benutzen, können Sie den Fortschritt nicht auf dem VGA Monitor überwachen.

2. Melden Sie sich auf der Konsole mit Hilfe der Admin Berechtigungen an.
3. Gehen Sie auf den CLI Konfigurationsmodus:

   ```
   hostname > enable hostname # configure terminal
   ```

4. Laden Sie die Appliance erneut:

   ```
   hostname (config) # reload
   ```

5. Achten Sie beim erneuten Laden genau auf die Konsole, damit Sie die `boot:` Aufforderung nicht verpassen.
6. Wenn Sie die `boot:` Aufforderung sehen, drücken Sie die Eingabetaste.
7. Achten Sie genau auf die Konsole, so dass Sie eine Reihe von 5 Punkten nicht verpassen (`.`).die in einer Sekunde Abstand angezeigt werden.
8. Bevor die Konsole den fünften Punkt passiert, drücken Sie zweimal eine beliebige Taste. Ein Image Startmenü, wie das folgende auf einer Network Security Appliance, wird angezeigt.

   ```
    Boot Menu ----------------------------------------------------------
   --- 0: wmps wMPS (wMPS) 8.0.0... 1: wmps wMPS (wMPS) 8.0.0... 2: Tools
   Menu ----------------------------------------------------------
   ```

9. Drücken Sie den Abwärtspfeil auf Ihrer Tastatur, um die **2. Tools** Menüoption auszuwählen.
10. Drücken Sie Eingabe.
11. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für das Tools Menü ein, das Sie von Ihrem Administrator erhalten haben.
12. Das Tools Menü (als "Boot Menu" beschriftet) wird angezeigt.

    ```
     Boot Menu ----------------------------------------------------------
    --- 0: Reset admin Password 1: Wipe Appliance Media 2: Manufacture
    Appliance 3: Wipe Appliance Media and Manufacture Appliance 4: Return
    to Image Boot Menu ----------------------------------------------------
    -----------
    ```

13. Wählen Sie eine Option (in Start-Manager Dienstprogramme auf Seite 397 beschrieben).

**HINWEIS:** Wenn Sie Option 4 auswählen, achten Sie auf die Konsole, so dass Sie eine Reihe von fünf Punkten nicht verpassen, die im Abstand von einer Sekunde angezeigt werden und drücken Sie dann zweimal auf eine beliebige Taste, um Zugriff auf das Image Startmenü zu erhalten.

## Beispiel:

Das folgende Beispiel von einer Network Security Appliance greift auf das Tools Menü zu.

```
nx-03 (config) # reload
Configuration changed: save changes?
Configuration changes saved.
Rebooting...
...
boot:
Booting from local disk...
PXE-MOF: Exiting Intel Boot Agent.

Booting default image in 3 seconds.

...

This terminal is not active or input for output while booting.

Booting default image in 1 seconds.

    Boot Menu
----------------------------------------------------------------
0: wmps wMPS (wMPS) 8.0.0...
1: wmps wMPS (wMPS) 8.0.0...
2: Tools Menu
----------------------------------------------------------------

    Verwenden Sie ^ und v Tasten, um auszuwählen, welcher Eintrag markiert
ist.
    Drücken Sie die Eingabetaste, um das ausgewählte Image zu booten, oder
drücken Sie "p", um ein
    Passwort zum Entsperren der nächsten Reihe von Funktionen einzugeben.

  Highlighted entry is 2:

Booting: 'Tools Menu'

Password: ********
.......

    Boot Menu
----------------------------------------------------------------
0: Reset admin Password
1: Wipe Appliance Media
2: Manufacture Appliance
3: Wipe Appliance Media and Manufacture Appliance
4: Return to Image Boot Menu
----------------------------------------------------------------

    Verwenden Sie ^ und v Tasten, um auszuwählen, welcher Eintrag markiert
ist.
    Drücken Sie die Eingabetaste, um das ausgewählte Image zu booten, oder
drücken Sie "p", um ein
    Passwort zum Entsperren der nächsten Reihe von Funktionen einzugeben.

  Highlighted entry is 0:
```

**HINWEIS:** Die in der Konsolenanleitung angegebene `'p'` Option ist nicht verfügbar.

# Das Tools Menü deaktivieren

Um zu verhindern, dass Benutzer auf das Tools Menü zugreifen, deaktivieren Sie das Tools Menü Passwort.

# Voraussetzungen

- Admin Zugriff

## Das Tools Menü mit Hilfe der CLI deaktivieren

Verwenden Sie die Befehle in diesem Abschnitt, um das Passwort für das Tools Menü zu deaktivieren, wodurch verhindert wird, dass Benutzer auf das Tools Menü zugreifen können.

**Um das Tools Menü zu deaktivieren:**

1. Melden Sie sich auf der Appliance CLI an.
2. Gehen Sie auf den CLI Konfigurationsmodus:

   ```
   hostname > enable hostname # configure terminal
   ```
3. Deaktivieren Sie das Passwort:

   ```
   hostname (config) # boot bootmgr tools disable password
   ```
4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Verfügbarkeit des Tools Menüs anzeigen

Sie können anzeigen, ob das Tools Menü auf der Appliance verfügbar ist.

# Voraussetzungen

- Monitor-, Operator- oder Admin-Zugriff

## Verfügbarkeit des Tools Menüs mit Hilfe der CLI anzeigen

Verwenden Sie einen der folgenden Befehle um anzuzeigen, ob Benutzer Zugriff auf das Tools Menü haben.

- `show bootvar`
- `show images`

Wenn ein Passwort für das Tools Menü festgelegt ist (entweder das Standard Passwort oder ein konfiguriertes Passwort) haben Benutzer Zugriff auf das Tools Menü. Wenn das Passwort für das Tools Menü deaktiviert ist, haben Benutzer keinen Zugriff auf das Tools Menü.

### *Beispiele*

Das folgende Beispiel von einer Network Security Appliance zeigt, dass das Passwort für das Tools Menü festgelegt wurde und User Zugriff auf das Tools Menü haben.

```
nx-05 > show bootvar
Installed images:

  Partition 1:
  wmps wMPS (wMPS) 7.4.0 xxx

  Partition 2:
  wmps wMPS (wMPS) 8.0.0 xxx

Last boot partition: 1
Next boot partition: 1

Boot manager admin password:      undisclosed password set
Boot manager tools menu password: undisclosed password set
...
```

Das folgende Beispiel zeigt, dass das Passwort für das Tools Menü deaktiviert ist, so dass Benutzer keinen Zugriff auf das Tools Menü haben.

```
nx-01 > show images
Installed images:

Partition 1:
  wmps wMPS (wMPS) 7.4.0 ...

  Partition 2:
  wmps wMPS (wMPS) 8.0.0 ...

No image files are available to be installed.

No image install currently in progress.

Boot manager admin password:          undisclosed password set
Boot manager tools menu password:     password disabled
```

# Persistente Medien löschen

Sie können proprietäre und vertrauliche Daten sicher von den persistenten Medien auf einer Appliance löschen (*zurücksetzen*) bevor Sie sie am Ende einer Bewertung an FireEye zurücksenden oder wenn Sie eine Return of Materials Authorization (RMA) benutzen müssen, um eine Appliance zu ersetzen. Der sichere Löschvorgang überschreibt jedes adressierbare Byte des Mediengerätes mindestens einmal und überprüft dann, dass der Vorgang erfolgreich war.

Sie verwenden das Tools Menü (auch als *Boot* bekannt) im Bootmanager, um diese Aktionen auszuführen. Der Bootmanager erfordert seriellen oder physischen Konsolenzugriff und ein Passwort. Sie können entweder nur die Appliance Medien löschen oder die Appliance Medien löschen und die Appliance fertigen. Diese Optionen werden in Start-Manager Dienstprogramme auf Seite 397 beschrieben.

Der Zurücksetzungsvorgang können je nach Datenträgergröße sechs bis zehn Stunden dauern. Der Status des aktuellen Vorgangs wird in der Konsole angezeigt, so dass Sie den Fortschritt, der regelmäßig aktualisiert wird, überwachen können.

# Voraussetzungen

- Stellen Sie sicher, dass die Anforderungen für das Tools Menü erfüllt sind. Siehe Systemanforderungen auf Seite 398.

# Persistente Medien mit Hilfe des Tools Menüs löschen

Verwenden Sie den Vorgang in diesem Abschnitt, um persistente Medien von der Appliance zu löschen.

**Um persistente Medien zu löschen:**

1. Gehen Sie auf das Tools Menü (als *Boot* Menü angezeigt), wie unter Zugriff auf das Tools Menü auf Seite 402 beschrieben.

```
 Boot Menu ----------------------------------------------------------
--- 0: Reset admin Password 1: Wipe Appliance Media 2: Manufacture
Appliance 3: Wipe Appliance Media and Manufacture Appliance 4: Return
to Image Boot Menu -------------------------------------------------
-----------
```

2. Um nur die Median zu löschen, verwenden Sie die ^ und v Tasten und wählen Sie **1: Wipe Appliance Media**.

   **VORSICHT**: Diese Option macht das Gerät unbrauchbar.

3. Um sowohl die Medien zu löschen, als auch die Appliance zu fertigen, wählen Sie **3: Wipe Appliance Media and Manufacture Appliance**.
4. Drücken Sie Eingabe.

## Beispiel:

Im folgenden Beispiel von einer Network Security Appliance greift auf das Tools Menü zu und löscht dann die Appliance Medien und stellt die Appliance her. Der Kürze halber wird auf einige Konsolenausgaben verzichtet.

```
nx-03 (config) # reload
Configuration changed: save changes?
```

```
Configuration changes saved.
Rebooting...
...
boot:
Booting from local disk...
PXE-MOF: Exiting Intel Boot Agent.

Booting default image in 3 seconds.

...

This terminal is not active for input or output while booting.

Booting default image in 1 seconds.

    Boot Menu
----------------------------------------------------------------
0: wmps wMPS (wMPS) 8.0.0...
1: wmps wMPS (wMPS) 7.9.4...
2: Tools Menu
----------------------------------------------------------------

    Verwenden Sie ^ und v Tasten, um auszuwählen, welcher Eintrag markiert
ist.
    Drücken Sie die Eingabetaste, um das ausgewählte Image zu booten, oder
drücken Sie "p", um ein
    Passwort zum Entsperren der nächsten Reihe von Funktionen einzugeben.

  Highlighted entry is 2:

Booting: 'Tools Menu'

Password: ********
.......

    Boot Menu
----------------------------------------------------------------
0: Reset admin Password
1: Wipe Appliance Media
2: Manufacture Appliance
3: Wipe Appliance Media and Manufacture Appliance
4: Return to Image Boot Menu
----------------------------------------------------------------

    Verwenden Sie ^ und v Tasten, um auszuwählen, welcher Eintrag markiert
ist.
    Drücken Sie die Eingabetaste, um das ausgewählte Image zu booten, oder
drücken Sie "p", um ein
    Passwort zum Entsperren der nächsten Reihe von Funktionen einzugeben.

  Highlighted entry is 3:


Booting: 'Wipe Appliance Media and Manufacture Appliance'
...

Running /etc/init.d/rcS.d/S33diskwipe
- Preparing to run diskwipe...
*** WARNING: DO NOT POWER OFF! ***

== Detecting disks to wipe
== Wiping system disks
scrub: using NNSA NAP-14.1-C patterns
```

```
scrub: please verify that device size below is correct!
scrub: scrubbing /dev/sda 1919313510400 bytes (~1787GB)
scrub: random  |.......|
..................
```

**HINWEIS:** Die in der Konsolenanleitung angegebene `'p'` Option ist nicht verfügbar.

# TEIL IV: CM Integration

# KAPITEL 25: Management durch eine Central Management Appliance beantragen

Dieses Thema behandelt die folgenden Informationen:



Sie können eine Anfrage senden, zu der Central Management Appliance zur Verwaltung hinzugefügt zu werden. Ein Rendezvous-Vorgang ermöglicht Appliances, die Anfrage zu versuchen und gestattet dem Central Management Administrator, die Liste der ausstehenden Anfragen zu sehen.

Um eine Managementanfrage zu senden, müssen Sie folgendes aktivieren:

- Rendezvous-Vorgang auf der Central Management Appliance (standardmäßig aktiviert)
- Automatische Rendezvous-Versuche auf der anfragenden Appliance
- Automatische Verbindungsfunktion auf der anfordernden Appliance, sodass automatisch versucht wird, eine Verbindung mit der Central Management Appliance nach dem Rendezvous-Versuch erfolgreich (standardmäßig aktiviert)

Anleitungen für die Überprüfung und Aktivierung dieser Einstellungen sind in dem in Eine Appliance vorbereiten, eine Managementanfrage zu senden auf der nächsten Seite beschriebenen Verfahren eingeschlossen.

**VORSICHT!** Der Rendezvous-Vorgang hat eine Kennung (bekannt als *Servicename*), die standardmäßig auf "cmc" eingestellt ist. Die Central Management Appliance und die anfragende Appliance müssen den gleichen Servicenamen haben; wenn Sie den Servicenamen auf einer ändern, müssen Sie ihn auch auf der anderen ändern. Der `cmc rendezvous service-name <hostname>` Befehl ändert den Servicenamen; der `no cmc rendezvous service-name` Befehl stellt den Standardwert wieder her. Details finden Sie im *CLI Befehlsreferenz*.

**HINWEIS:** Siehe Eine Managementanfrage in einem NAT-Deployment senden auf Seite 459 für Verfahren, die in einem Network Address Translation (NAT) Deployment ausgeführt werden müssen.

# Eine Appliance vorbereiten, eine Managementanfrage zu senden

Verwenden Sie die Befehle in diesem Abschnitt, um eine Appliance vorzubereiten, eine Managementanfrage an die Central Management Appliance zu senden.

**Um das Senden einer Anfrage vorzubereiten:**

1. Melden Sie sich auf der anfragenden Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

3. Aktivieren Sie automatische Rendezvous-Versuche:

   ```
   appl-hostname (config) # cmc rendezvous client auto
   ```

4. Bestätigen Sie, dass die automatische Verbindungsfunktion aktiviert ist:
   a. Zeigen Sie Appliance (Client) Informationen an:

      ```
      appl-hostname (config) # show cmc client
      ```

   b. Wenn `Autoconnect: no` angezeigt wird, aktivieren Sie automatische Verbindung:

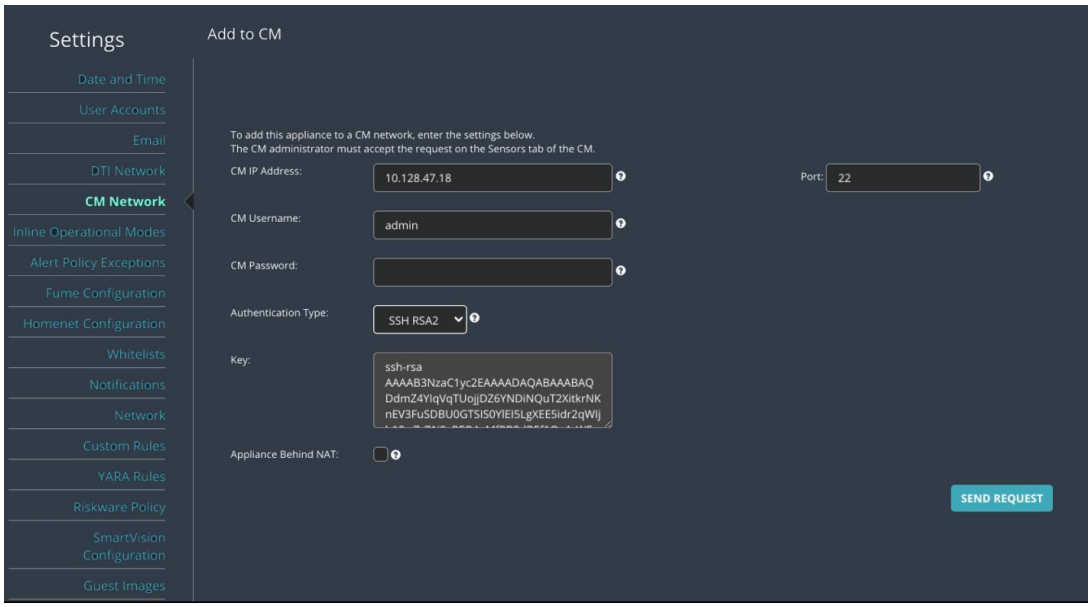
      ```
      appl-hostname (config) # cmc client connection auto
      ```

5. Speichern Sie Ihre Änderungen:

   ```
   appl-hostname (config) # write memory
   ```

# Eine Managementanfrage mit Hilfe der Web-UI senden

Verwenden Sie die **Add to CM** Seite in der Network Security Web-UI, um eine Anfrage zu starten, zur Central Management Appliance hinzugefügt zu werden.



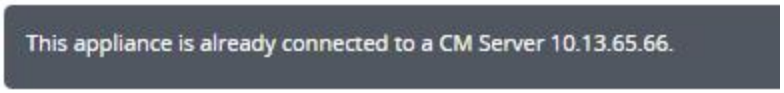

**Um eine Managementanfrage zu initiieren:**

1. Klicken Sie auf das **Settings** Register.
2. Klicken Sie auf der Seitenleiste auf **CM Network**.
3. In den **CM IP-Address** und **Port** Feldern geben Sie die Central Management IP-Adresse und den remote Management-Port ein, der standardmäßig 22 ist.
4. In der **Authentication Type** Dropdown-Liste wählen Sie **SSH RSA1** oder **SSH RSA2**. Der Schlüssel wird im **Key** Feld generiert.
5. In den **CM Username** und **CM Password** Felden geben Sie die Berechtigungen der Central Management Benutzer ein, die die Appliance zum Anmelden auf der Central Management Appliance verwenden soll, um sich anzukündigen.
6. Wenn sich die Appliance hinter einem NAT-Gateway befindet, wählen Sie das **Appliance Behind NAT** Kontrollkästchen.

   **HINWEIS:** Siehe Network Address Translation (NAT) konfigurieren auf Seite 443 für detaillierte NAT-Deploymentinformationen.

7. Klicken Sie auf **Send Request**.

   In einer Nachricht werden Sie darüber informiert, ob die Anfrage erfolgreich war oder nicht oder dass die Appliance bereits von der Central Management Appliance verwaltet wird. Wenn die Anfrage erfolgreich ist, kann ein Central Management Administrator die Anfrage annehmen oder ablehnen. Beispielnachrichten folgen.



# Eine Managementanfrage mit Hilfe der CLI senden

Verwenden Sie die Befehle in diesem Abschnitt auf einer Appliance, um eine Anfrage zu starten, zur Central Management Appliance hinzugefügt zu werden.

**Um eine Managementanfrage zu initiieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Bestimmen Sie den Hostnamen oder die IP-Adresse der Central Management Appliance:

   ```
   hostname (config) # cmc client server address <hostname, IPv4 or IPv6 address>
   ```

3. Legen Sie den Authentifizierungstyp und die Berechtigungen des Central Management Benutzers fest, den die Appliance für die Anmeldung auf der Central Management Appliance verwenden soll, um sich anzukündigen.

   ```
   hostname (config) # cmc client server auth authtype <authType>
   ```

   ```
   hostname (config) # cmc client server auth <authType> username <username>
   ```

   ```
   hostname (config) # cmc client server auth <authType> {password <password>} | {identity <identityName>}
   ```

   wobei:

   - <authType> kann **password**, **ssh-dsa2** oder **ssh-rsa2** sein.
   - **password** <password> wird mit der Passwort-Authentifizierung verwendet.
   - **identity** <identityName> wird mit SSH-DSA2 und SSH-RSA2 Authentifizierung verwendet.

4. Aktivieren Sie automatische Rendezvous-Versuche:

   ```
   hostname (config) # cmc rendezvous client auto
   ```

5. Bestätigen Sie, dass die automatische Verbindungsfunktion aktiviert ist:

   a. Zeigen Sie Appliance (Client) Informationen an:

      ```
      hostname (config) # show cmc client
      ```

   b. Wenn `Autoconnect: no` angezeigt wird, aktivieren Sie die automatische Verbindung:

      ```
      hostname (config) # cmc client connection auto
      ```

6. Starten Sie den Konfigurationsassistenten.

   ```
   hostname (config) # configuration jump start
   ```

7. Beantworten Sie die Fragen des Konfigurations-Assistenten und geben Sie bei Frage 14 **yes** ein, um eine Anfrage zur Verwaltung durch die Central Management Appliance zu senden

```
...

Schritt 14: Send a request to be managed by CMS (Die häufigste Methode
ist die Einrichtung der Verwaltung über das CMS) [yes/no]? yes

Schritt 15: CMS Address? [10.128.32.104]

Schritt 16: CMS Server username? [admin]

Schritt 17: CMS Server admin password (Eingeben oder unverändert lassen)?

Schritt 18: CMS Port? [22]

Schritt 19: Appliance Reachable to CMS? [yes]

Schritt 20: Authetication type (0->password,1->ssh-rsa2,2->ssh-dsa2)?
[ssh-rsa2] 1

Auth is already set to ssh-rsa2

Connection to CMS is in process...

Schritt 19: Appliance Reachable to CMS? [yes]

Connection announcement succeeded;

... waiting for server acceptance

You have entered the following information:

...

Um eine Antwort zu ändern, geben Sie die entsprechende Schrittnummer
ein.

Ansonsten drücken Sie Eingabe, um die Änderungen zu speichern und zu
schließen.
```

8. Drücken Sie **Eingabe**, um Ihre Änderungen zu speichern.

# Eine Management-Anfrage mit Hilfe der CLI für eine Verbindung senden, die das Verschieben von Appliance IP-Adressen unterstützt

Befolgen Sie diese Schritte, um eine Management-Verbindung zu beantragen, die Änderungen an der Appliance IP-Adresse und automatische Wiederverbindung mit der Central Management Appliance unterstützt.

Diese Funktion verwendet CMC Rendezvous-Funktionalität, um den Client-Datensatz in der CMC einzustellen. Die Central Management Console (CMC) bietet generelle Management- und Steuerungsfähigkeiten für den Rendezvous-Server (Central Management Appliance) und seine Clients (verwaltete Appliances).

**HINWEIS:** Der Rendezvousvorgang erfordert Konfiguration sowohl auf der Central Management Appliance als auch der anfragenden Appliance. Sie verwenden die `cmc rendezvous server` Befehle auf der Central Management Appliance und die `cmc rendezvous client` Befehle auf der verwalteten Appliance.

## Voraussetzungen

- Die Central Management Appliance wurde aktiviert, um diese Funktion zu unterstützen. Sehen Sie "Die Annahme von Anfragen nach Management-Verbindungen vorbereiten, die das Verschieben von Appliance IP-Adressen mit Hilfe der CLI unterstützen" im *Central Management Administrationshandbuch*.

**Um eine Management-Verbindung zu beantragen, die das Verschieben von Appliance IP-Adressen unterstützt:**

1. Melden Sie sich bei der Network Security Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Legen Sie die IP-Adresse der Central Management Appliance fest, mit der Sie sich verbinden wollen.

   ```
   hostname (config) # cmc rendezvous client server-addr 10.13.65.66
   ```

4. Legen Sie Client-initiierte Rendezvousversuche mit der Central Management Appliance fest:

   ```
   hostname (config) # cmc rendezvous client enable-client-init
   ```

5. Aktivieren Sie automatische Rendezvousversuche mit der Central Management Appliance:

```
hostname (config) # cmc rendezvous client auto
```

**HINWEIS:** Nachdem automatisches Rendezvous aktiviert ist, wird die lokale IP-Adresse der Appliance anstelle der zugeordneten Adresse in der Anfrage eingeschlossen, wenn sich die anfragende verwaltete Appliance hinter einem NAT-Gateway befindet.

6. (Optional) Wenn sich die verwaltete Network Security Appliance hinter einem NAT-Gateway befindet, verhindern Sie, dass die Appliance ihre private IP-Adresse mit der Central Management Appliance kommuniziert.

```
hostname (config) # no cmc rendezvous client send-client-address
```

**HINWEIS:** Um das Standard Verhalten wieder herzustellen, so dass die Appliance ihre lokale IP-Adresse in Rendezvousversuchen mit der Central Management Appliance enthält, verwenden Sie den `cmc rendezvous client send-client-address` Befehl.

7. Zeigen Sie die CMC Rendezvous-Konfiguration und -Status an.

```
hostname (config) # show cmc rendezvous
CMC rendezvous service name: cmc

CMC client:
   Server address: 10.13.65.66
   Automatic rendezvous: yes
   Initial retry delay (after boot or disconnect): 30 seconds
   Short retry interval (after unsuccessful announcement): 300 seconds
   Long retry interval (after successful announcement): 86400 seconds

   Include client address in rendezvous: yes
   Use client initiated connection's config for rendezvous: yes
   Under CMC management: yes

   How to authenticate to server for rendezvous:
   Authentication type: password
   Password for password auth: ********
```

8. Legen Sie die IP-Adresse der Central Management Appliance fest, die die Appliance verwalten soll:

```
hostname (config) # cmc client server address 10.13.65.66
```

9. Legen Sie die Passwort-basierte Authentifizierung mit der Central Management Appliance fest:

```
hostname (config) # cmc client server auth authtype password
hostname (config) # cmc client server auth password username my_CMname
hostname (config) # cmc client server auth password password ########
```

10. Zeigen Sie die CMC Client-Konfiguration und -Status an.

```
hostname (config) # show cmc client
```

11. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

# KAPITEL 26: Den Adresstyp für DTI-Network Serviceanfragen ändern

Dieses Thema behandelt die folgenden Informationen:



## Informationen über die Änderung des Adresstyps für DTI-Network Serviceanfragen

Standardmäßig verwenden Network Security Appliances einen Single-Port Adresstyp für die folgenden Arten der Kommunikation mit der Central Management Appliance:

- Remote Management—Initiiert die Verbindung und konfiguriert die Appliance.
- DTI Network Service— Fordert Software-Update (z.B. System-Images, Guest-Images, und Sicherheitsinhalte) vom DTI-Netzwerk.

Die Single-Port Konfiguration verwendet standardmäßig nur SSH Port 22. Dadurch wird die Komplexität der Firewall-Regeln reduziert und eine zusätzliche Ebene für Sicherheit und Privatsphäre zwischen der Central Management Appliance und der Appliance, die sie verwaltet, bereitgestellt.

Sie können stattdessen die verwaltete Appliance konfigurieren, den Dual-Port Adresstypen zu verwenden. Bei dem Dual-Port Adresstyp verwendet der Managementverkehr den SSH Port (Port 22) und der DTI-Network Service Verkehr verwendet den HTTPS-Port (Port 443).

In Umgebungen, in denen sich die Central Management Appliance hinter einem Network Address Translation (NAT) Gateway befindet, entfällt durch die Verwendung eines einzelnen Ports auch die Notwendigkeit, einen zusätzlichen HTTPS-Port (443) für die verwaltete Appliance öffnen zu müssen, um Softwareupdates von der Central Management Appliance anzufordern. (Details über NAT-Deployment finden Sie unter Network Address Translation (NAT) konfigurieren auf Seite 443 und Auf Single-Port oder Dual-Port Kommunikation in einem NAT-Deployment wechseln auf Seite 457.)

**HINWEIS:** Wenn Sie den Adresstypen auf einer Appliance ändern, die bereits zu der Central Management Appliance mit Hilfe einer Client-inittierten Verbindung hinzugefügt wurde, wird die Verbindung dieser Appliance kurzfristig unterbrochen und dann mit Hilfe der neuen Konfiguration erneut verbunden.

## Voraussetzungen

- Admin Zugriff auf die verwaltete Appliance

# Single-Port Kommunikation mit Hilfe der CLI wiederherstellen

Single-Port Kommunikation ist das Standardverhalten auf der Network Security Appliance und erfordert keine Konfiguration. Verwenden Sie die Befehle in diesem Thema, um Single-Port Kommunikation wiederherzustellen, wenn Dual-Port Kommunikation aktiviert wurde.

**WICHTIG!** Bevor Sie Single-Port Kommunikation wiederherstellen, stellen Sie sicher, dass **CMS** die konfigurierte DTI-Quelle ist (siehe Die aktive Einstellung für einen DTI-Service ändern auf Seite 163 für Details).

**Um Single-Port Kommunikation wiederherzustellen:**

1. Melden Sie sich bei der Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

```
hostname > enable
hostname # configure terminal
```

3. Wenn Ihre Appliance bereits zu der Central Management Appliance hinzugefügt wurde, tippen Sie **yes**, um zu bestätigen, dass Sie den Konfigurationsmodus starten wollen.

```
******************
*** CMS notice ***
******************
    This system is under management of a CMS. Please note that
    the CMS may update this system's configuration, which could
    overwrite changes that you have made locally.

    Enter 'YES' to enter configuration mode anyway: yes
```

4. Aktivieren Sie Single-Port Kommunikation:

```
hostname (config) # fenet dti source type CMS address-type cms-
singleport
```

**HINWEIS:** Sie können auch den `no fenet dti source type CMS address-type` Befehl verwenden, um Single-Port Kommunikation zu aktivieren.

5. Bestätigen Sie die Konfiguration:

```
hostname (config) # show fenet dti configuration
```

Die Einträge in der Active Settings Liste enden mit folgendem Text:

```
: singleport) - Managed by CMS
```

6. Speichern Sie Ihre Änderungen:

```
hostname (config) # write memory
```

## Beispiel:

Dieses Beispiel aktiviert Single-Port Kommunikation.

```
hostname (config) # fenet dti source type CMS address-type cms-singleport
hostname (config) # show fenet dti configuration

DTI CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

   Mode               : online
   Download source    : CMS (DTIUser@10.2.0.0 : singleport) - Managed by CMS
   Upload destination : CMS (DTIUser@10.2.0.0 : singleport) - Managed by CMS
   Mil service        : CMS (DTIUser@10.2.0.0 : singleport) - Managed by CMS
   AVSuite service    : CMS (DTIUser@10.2.0.0 : singleport) - Managed by CMS

  AVAILABLE OPTIONS:

  ------------------------------------------------
  Download   User                 Address
  ------------------------------------------------
  CDN        DTIUser              cloud.fireeye.com
  CMS        DTIUser              10.2.0.0
```

```
DTI        DTIUser              staticcloud.fireeye.com
...
```

# Dual-Port Kommunikation mit Hilfe der CLI konfigurieren

Single-Port Kommunikation ist das Standardverhalten und erfordert keine Konfiguration. Verwenden Sie die Befehle in diesem Thema, um stattdessen Dual-Port Kommunikation zu aktivieren.

**Um Dual-Port Kommunikation zu aktivieren:**

1. Melden Sie sich bei der Appliance CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Wenn Ihre Appliance bereits zu der Central Management Appliance hinzugefügt wurde, tippen Sie **yes**, um zu bestätigen, dass Sie den Konfigurationsmodus starten wollen.

   ```
   ******************
   *** CMS notice ***
   ******************
       This system is under management of a CMS. Please note that
       the CMS may update this system's configuration, which could
       overwrite changes that you have made locally.

       Enter 'YES' to enter configuration mode anyway: yes
   ```

4. Aktivieren Sie Dual-Port Kommunikation:

   ```
   hostname (config) # fenet dti source type CMS address-type cms-auto
   ```

   **HINWEIS:** Sie können auch den **no fenet dti source type CMS address-type** Befehl verwenden, um Dual-Port Kommunikation wiederherzustellen.

5. Bestätigen Sie die Konfiguration:

   ```
   hostname (config) # show fenet dti configuration
   ```

   Das Wort "Singleport" sollte in den Einträgen der Active Settings Liste nicht auftreten.

6. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiel:

Das folgende Beispiel aktiviert Dual-Port Kommunikation.

```
hostname (config) # fenet dti source type CMS address-type cms-auto
hostname (config) # show fenet dti configuration

 CLIENT CONFIGURATIONS:

  ACTIVE SETTINGS:

   Mode               : online
   Download source    : CMS (DTIUser@10.2.0.0) - Managed by CMS
   Upload destination : CMS (DTIUser@10.2.0.0) - Managed by CMS
   Mil service        : CMS (DTIUser@10.2.0.0) - Managed by CMS
   AVSuite service    : CMS (DTIUser@10.2.0.0) - Managed by CMS

  AVAILABLE OPTIONS:
  ------------------------------------------------
  Download   User                 Address
  ------------------------------------------------
  CDN        DTIUser              cloud.fireeye.com
  CMS        DTIUser              10.2.0.0
  DTI        DTIUser              staticcloud.fireeye.com
  ...
```

# TEIL V: Anhänge

# ANHANG A: Secure Shell (SSH) Authentifizierung konfigurieren

Dieses Thema behandelt die folgenden Informationen:



## Info über SSH-Authentifizierung

Das Secure Shell (SSH) Protokoll wird für sichere Kommunikation zwischen der Central Management Appliance und den Appliances, die sie verwaltet, benutzt. Wenn die Central Management Appliance die Verbindung initiiert, meldet sie sich als ein remote "admin" Benutzer auf der verwalteten Appliance an. Wenn die verwaltete Appliance die Verbindung initiiert, meldet sie sich als ein remote "admin" Benutzer auf der Central Management Appliance an. SSH-*Benutzerauthentifizierung* überprüft die Identität des entfernten Benutzers, der die Verbindung versucht.

SSH *Hostauthentifizierung* überprüft die Identität der Central Management Appliance auf der verwalteten Appliance und überprüft die Identität der verwalteten Appliance auf der Central Management Appliance.

**HINWEIS:** Die Themen in diesem Abschnitt beschreiben die Konfigurierung der SSH Authentifizierung für eine Client-inittierte Verbindung (wobei der Administrator einer verwalteten Appliance eine Managementanfrage an die Central Management Appliance sendet und ein Central Management Administrator die Anfrage annimmt oder ablehnt). Informationen über eine Server-initiierte Verbindung (wo der Central Management Administrator eine Appliance direkt aus der Central Management Web-UI oder CLI hinzufügt, finden Sie im *Central Management Administrationshandbuch*.

# Benutzerauthentifizierung

Der Remote-Benutzer kann sich mit einem Passwort oder einem Public Key (öffentlichen Schlüssel) authentifizieren. Nachdem die Verbindung erstellt ist, wird sie durch das konfigurierte Passwort oder den öffentlichen Schlüssel gesteuert.

## Passwortauthentifizierung

Bei der Passwortauthentifizierung wird ein Passwort für den remote Benutzer konfiguriert. Dies ist der anfängliche Authentifizierungstyp für eine Appliance, die zu der Central Management Appliance mit Hilfe der Web-UI hinzugefügt wird.

## Public Key Authentifizierung

Public Key Authentifizierung verwendet ein Schlüsselpaar - einen öffentlichen und einen privaten Schlüssel. Bei der Public Key Authentifizierung wird eine SSH-DSA2 oder SSH-RSA2 Identität für den remote Benutzer konfiguriert und wird auf die Central Management Appliance gepusht.

Vorteile der Public Key Authentifizierung:

- Der private Schlüssel verbleibt auf der Network Security Appliance und kann nicht vom öffentlichen Schlüssel berechnet werden. Dies ist ein Vorteil gegenüber der Passwortauthentifizierung, bei der das Passwort geknackt werden könnte.
- Wenn Sie Passwortauthentifizierung verwenden, können Richtlinien zur Passwortänderung die Verbindung zwischen der Central Management Plattform und der verwalteten Appliance abbrechen.

  Angenommen, Benutzer auf der Central Management Appliance müssen Ihre Passwörter alle 90 Tage ändern. Als Administrator der Network Security Appliance könnten Ihnen diese Richtlinie nicht bekannt sein. Nachdem das Passwort für den remote-Benutzer geändert wurde, wird die Verbindung mit der Central Management Appliance unterbrochen, bis Sie das Passwort auf der Network Security Appliance ändern.

  **Best Practice:** Die Richtlininien zur Passwortänderung nur auf Passwortauthentifizierung zutreffen, empfiehlt FireEye, public Key Authentifizierung für diese Verbindung zu verwenden.

Details finden Sie in den folgenden Themen:

- Einen public Key (öffentlichen Schlüssel) mit Hilfe der CLI erstellen auf der nächsten Seite
- Benutzerauthentifizierung mit Hilfe der CLI konfigurieren auf Seite 434

# Einen public Key (öffentlichen Schlüssel) mit Hilfe der CLI erstellen

Verwenden Sie die Befehle in diesem Abschnitt, um einen neuen öffentlichen Schlüssel für SSH-Benutzerauthentifizierung zu erstellen. Sie können diesen Schlüssel anstelle des Passwortes verwenden, um den remote Benutzer zu authentifizieren.

**Um einen öffentlichen Schlüssel zu erstellen:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Erstellen Sie den public Key:

   ```
   hostname (config) # cmc auth <keyType> identity <identityName> generate
   ```

   wobei `<keyType>` **ssh-dsa2** oder **ssh-rsa2** sein kann und `<identityName>` ein benutzerfreundlicher Name ist.

3. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show cmc auth identities
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um einen public Key zu entfernen:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Entfernen Sie den public Key:

   ```
   hostname (config) # no cmc auth <keyType> identity <identityName>
   ```

3. Bestätigen Sie Ihre Änderung:

   ```
   hostname (config) # show cmc auth identities
   ```

4. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiel:

Im folgenden Beispiel wird auf der NX 04 Appliance eine SSH-DSA2 Identität mit dem Namen "admin4" erstellt.

```
NX-04 (config) # cmc auth ssh-dsa2 identity admin4
NX-04 (config) # show cmc auth identities
DSA2 identity admin4:
   Public Key:
ssh-dss AAA3NzaC1kc3MAAACBAJl3PisWNnz/gYLvL4JC7xFMoq3HE89rai7trnJmpxjylArYhf
MzaGndFA4qGRZMFzhiz9Jhi/+W1ufIrXLGzakC0lAAAAFQCuMCsMwMGN9zT5w2JCiDt7D6orNwAA
.
```

.
.

## Benutzerauthentifizierung mit Hilfe der CLI konfigurieren

Verwenden Sie die Befehle in diesem Abschnitt, um Authentifzierungsparameter für den remote Benutzer zu konfigurieren, die die verwaltete Appliance verwendet, um sich auf der Central Management Appliance anzumelden, um sich anzukündigen. Dies ist ein existierender "admin" Benutzer auf der Central Management Appliance.

**HINWEIS:** Sehen Sie die `ssh` und `cmc` Befehle in der *CLI Befehlsreferenz* für fortgeschrittene Authentifizierungsoptionen.

**Um Passwortauthentifizierung zu konfigurieren:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Legen Sie den "Passwort" Authentifizierungstypen fest:

   ```
   hostname (config) # cmc client server auth authtype password
   ```

3. Legen Sie den remote Benutzer für die Anmeldung auf der Central Management Appliance fest:

   ```
   hostname (config) # cmc client server auth password username <username>
   ```

4. Legen Sie das Passwort für die Authentifizierung des remote Users fest:

   ```
   hostname (config) # cmc client server auth password password <password>
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um SSH-DSA2 Authentifizierung zu konfigurieren:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Legen Sie den SSH-DSA2 Authentifizierungstyp fest:

   ```
   hostname (config) # cmc client server auth authtype ssh-dsa2
   ```

3. Legen Sie den remote User für die Anmeldung auf der Central Management Appliance fest:

   ```
   hostname (config) # cmc client server auth ssh-dsa2 username <username>
   ```

4. Legen Sie die benannte Identität fest, die für die Authentifizierung des remote Benutzers verwendet werden soll:

   ```
   hostname (config) # cmc client server auth ssh-dsa2 identity
   <identityName>
   ```

   wobei <identityName> der Name einer vorhandenen Identität ist.

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um SSH-RSA2 Authentifizierung zu konfigurieren:**

1. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Legen Sie den SSH-RSA2 Authentifizierungstypen fest:

   ```
   hostname (config) # cmc client server auth authtype ssh-rsa2
   ```

3. Legen Sie den remote User für die Anmeldung auf der Central Management Appliance fest:

   ```
   hostname (config) # cmc client server auth ssh-rsa2 username <username>
   ```

4. Legen Sie die benannte Identität fest, die für die Authentifizierung des remote Benutzers verwendet werden soll:

   ```
   hostname (config) # cmc client server auth ssh-rsa2 identity
   <identityName>
   ```

   wobei <identityName> der Name einer vorhandenen Identität ist.

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiel:

Im folgenden Beispiel werden SSH-DSA2 Authentifizierungsparameter für die Anmeldung auf der Central Management Appliance konfiguriert.

```
hostname (config) # cmc client server auth authtype ssh-dsa2
hostname (config) # cmc client server auth ssh-dsa2 username cmcadmin3
hostname (config) # cmc client server auth ssh-dsa2 identity admin3
```

# Hostschlüssel-Authentifizierung

Hostschlüssel Authentifizierung kann verwendet werden, um Man-in-the Middle Angriffe zu verhindern, bei denen sich ein anderer Server als die Network Security Appliance oder Central Management Plattform ausgibt und den Datenverkehr zwischen ihnen abfängt. Wenn die Network Security Appliance und die Central Management Appliance das erste

Mal mit Hilfe einer Client-initiierten Verbindung verbunden werden, findet ein Schlüsselaustausch statt. Die Central Management Appliance sendet eine Kopie ihres Hostschlüssels an die Appliance, wo er mit den Schlüsseln in der Hostschlüssel Datenbank der Appliance verglichen wird.

Wenn eine strenge Hostschlüssel-Überprüfung aktiviert ist, kann die Verbindung nur hergestellt werden, wenn der gesendete Schlüssel mit einem Eintrag in der lokalen Hostschlüssel Datenbank für den Network Security remote Benutzer übereinstimmt. Wenn die globale Hostschlüssel-Überprüfung aktiviert ist, kann die Verbindung nur hergestellt werden, wenn der gesendete Schlüssel mit einem Eintrag in der globalen Hostschlüssel Datenbank der Network Security übereinstimmt.

Sie können strenge Hostschlüssel-Überprüfung, globale Hostschlüssel-Überprüfung oder beides durchsetzen.

**WICHTIG:** Hostschlüssel werden in der Konfigurationsdatenbank gespeichert, und sind somit in der Sicherungsdatei enthalten.

**HINHWEIS:** Im Compliance-Modus werden sowohl strenge als auch globale Hostschlüssel-Überprüfung durchgesetzt. Details finden Sie unter *FIPS 140-2 und Common Criteria Anhang*.

Details finden Sie in den folgenden Themen:

- Einen Hostschlüssel mit Hilfe der CLI erhalten auf der nächsten Seite
- Einen Hostschlüssel in die Global Host-Keys Datenbank mit Hilfe der CLI importieren auf Seite 439
- Strenge und globale Hostschlüssel-Überprüfung mit Hilfe der CLI aktivieren auf Seite 441

## Voraussetzungen

- Admin-Zugriff, um Authentifizierung zu konfigurieren und Schlüssel zu erstellen.
- Monitor-, Operator- oder Admin-Zugriff zum Abrufen von Central Management Appliance Hostschlüsseln.
- Der private Schlüssel verbleibt auf der Network Security Appliance und kann nicht aus dem public Key errechnet werden.

## Einen Hostschlüssel mit Hilfe der Web-UI erhalten

Verwenden Sie die **Certificate Management** Seite, um den Hostschlüssel der Central Management Appliance zu erhalten. Dies ist der Schlüssel, den Sie in die globale Hostschlüssel-Datenbank der verwalteten Network Security Appliance importieren müssen.


**WICHTIG!** Die Hostschlüssel-Zeichenfolge muss möglicherweise in einem Network Address Translation (NAT) Deployment verändert werden. Details finden Sie unter Globale Hostschlüssel-Authentifizierung in einem NAT Deployment konfigurieren auf Seite 467.

**Um einen Hostschlüssel abzurufen:**

1. Melden Sie sich auf der Web-UI der Central Management an.
2. Klicken Sie auf das **Settings** Register.
3. Klicken Sie auf der Seitenleiste auf **Certificates/Keys**.
4. Finden Sie die **Appliance Public Key** Zeichenfolge im **Keys** Abschnitt.
5. Kopieren Sie die Zeichenfolge mit der IP-Adresse beginnend.
6. Führen Sie einen der folgenden Schritte aus:
   - Fügen Sie den Schlüssel in die verwaltete Network Security CLI ein, wie unter Einen Hostschlüssel in die Global Host-Keys Datenbank mit Hilfe der CLI importieren auf Seite 439 beschrieben.
   - Fügen Sie den Schlüssel in eine Textdatei ein und speichern sie für später.

## Einen Hostschlüssel mit Hilfe der CLI erhalten

Verwenden Sie den Befehl in diesem Abschnitt, um den Hostschlüssel der Central Management Appliance zu erhalten. Dies ist der Schlüssel, den Sie in die globale Hostschlüssel-Datenbank der verwalteten Network Security Appliance importieren müssen.

**WICHTIG!** Sie müssen den RSA v2 Schlüssel erhalten.

**WICHTIG!** Die Hostschlüssel-Zeichenfolge muss möglicherweise in einem Network Address Translation (NAT) Deployment verändert werden. Details finden Sie unter Globale Hostschlüssel-Authentifizierung in einem NAT Deployment konfigurieren auf Seite 467.

**Um den Hostschlüssel abzurufen:**

1. Melden Sie sich in der Central Management CLI an.
2. Zeigen Sie die Schlüssel an:

   `hostname > show ssh server host-keys interface ether1`
3. Finden Sie den RSA v2 Hostschlüsseleintrag.
4. Kopieren Sie die Schlüsselzeichenfolge, einschließlich der doppelten Anführungszeichen.
5. Führen Sie einen der folgenden Schritte aus:
   - Fügen Sie den Schlüssel in die Network Security CLI ein, wie unter Einen Hostschlüssel in die Global Host-Keys Datenbank mit Hilfe der CLI importieren auf der nächsten Seite beschrieben.
   - Fügen Sie den Schlüssel in eine Textdatei ein und speichern sie für später.

## Beispiel:

Dieses Beispiel zeigt die Central Management Hostschlüssel an. Der RSA v2 Schlüssel ist zu Illustrationszwecken hervorgehoben.

```
CM-08 > show ssh server host-keys interface ether1

SSH server configuration:
   SSH server enabled:      yes
   .
   .
   .
   Interface listen enabled: yes
   Listen Interfaces:
     Interface: ether1

Host Key Finger Prints and Key Lengths:
    RSA v1 host key: 37:20:5f:af:65:33:e8:62:26:3c:25:d0:1f:2d:8a:54 (2048)
    RSA v2 host key: c7:64:12:8a:71:a6:da:14:3c:05:37:aa:7a:2e:2a:8c (2048)
    DSA v2 host key: 85:59:a8:a1:d8:3e:df:2e:74:fc:6a:be:be:d2:62:32 (1024)

Host Keys:
 RSA v1 host key: "10.11.121.13 2048 65537 27678927235571051433944923436127639420072994239434197952617478790730883193561581892416574428382880076651052317847902037474895252247975570054315595358600142845914848782710493540937857691486699538042052007295602744764036681566020303332538223563825872378195559416466034473245176374751379653304184889304215755398717002961974218227773055287228117309728679472422744200184844597327452806661880313000836518022137675657765205670872217927843062157032172499589577136315879700789083029147987588619557961691104204933846230076323566554605149466931434034062601876531156968025568815192986073498446108395753542572032093143856912019598"

 RSA v2 host key: "10.11.121.13 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDZZJLE/ftkUddyNW6KdqEQXjsOPjbtzTn3OB51QgOfdeQHrJgFHM2/4C9WtDkwuX5jd7gdWnSWYwrXDv657thlyRPIt4WxjfObpOolPKAe6shgYq35NxalYDt7Pa/oym51SN/x9dGaaTFOHvvdAfOGu5E7nv3YjLjmSgdpSp7auHnYsyJ5O+xlYocXtoBq6jOueyxm8qm76IWLOO7JIJ7ZLgMI8FjZ5gp48r+Hnjrdio2rhKKUP/6BOjpHRxsd8yPxMgJpyz2Dwv9ZIJha67f6sgWYdt4yxfBc9yr7yG3iVWVJcLE+83aY24X7DBUXFnG3AeciDpEqAit2dPF586hJ"

    DSA v2 host key: "10.11.121.13 ssh-dss AAAAB3NzaC1kc3MAAACBAMY7tSZt46Qrv/hqL1tazYjXNzkyLTWp54DjfkxzE//+qjEOAUr9hTU3ZmHYChzUVTEKj7syaxd+4Y+8IZ94eRVcnrH/jrqtEaJ64SvoUqGkbKKezUbCVfSrzGgTV/AOdUzLYMLbOEMrTMcXki+DnaUSd8OPCWLvqOMcgOIpXAAAAFQDItRIv/iH3AAy23h3cnWzp3dpOXQAAAIASOAONTiOO8A+f1HNOm3PzSO2ZQ9ittHxA1ISs7yE6dcbj9JrWVf1w2lJTEZAJPQz/c9NysGVJusll6Aj1aqQ6EKuhKlPcpYOPyCVKT3TGgY93i648umYZSs9+HzoLY1/aTnnkBGDQ8mFbjhyw3UdeiFjamVVr+4o8QwMbDXAfXAAAAIEAjBMXsp4gK5yvsAgBqcZeZm3vW4zYUpZZ
```

```
374A3ANXENWTh2yyQd8Ig1gB0YKDBhSHD6sZpPg88WSDxK3IAdifYGx+FAhowiuWcI+kA0UeiAb9/C+A
653zii1Nc85/fsIwl3GIjmp/xO23b+9YmHY8V5CsT+mmSIYQutCIzUVWbcYvEc="
```

# Einen Hostschlüssel in die Global Host-Keys Datenbank mit Hilfe der CLI importieren

Verwenden Sie die Befehle in diesem Abschnitt, um den Hostschlüssel von einer Central Management Appliance in die globale Host-Keys Datenbank der Network Security zu importieren. Diese Vorgang ist für die globale Hostschlüsselauthentifizierung erforderlich, bei der die Verbindung nur zulässig ist, wenn der Hostschlüssel, den die Central Management sendet, bereits in dieser Datenbank enthalten ist.

**VORSICHT!** Wenn Sie globale Hostschlüsselauthentifizierung verwenden wollen, müssen Sie diese Funktion ausdrücklich zusätzlich zum Importieren des Hostschlüssels aktivieren. Details finden Sie unter Strenge und globale Hostschlüssel-Überprüfung mit Hilfe der CLI aktivieren auf Seite 441.

**WICHTIG!** Bevor Sie diesen Vorgang ausführen, müssen Sie den Hostschlüssel von der Central Management Appliance abrufen. Diesen Schlüssel können Sie von der Central Management Web-UI oder CLI erhalten. Details finden Sie unter Einen Hostschlüssel mit Hilfe der Web-UI erhalten auf Seite 436 oder Einen Hostschlüssel mit Hilfe der CLI erhalten auf Seite 437.

**WICHTIG!** Die Hostschlüssel-Zeichenfolge muss möglicherweise in einem Network Address Translation (NAT) Deployment verändert werden. Details finden Sie unter Globale Hostschlüssel-Authentifizierung in einem NAT Deployment konfigurieren auf Seite 467.

**HINWEIS:** Sehen Sie die `ssh` Befehle in der *CLI Befehlsreferenz* für erweiterte Authentifizierungsoptionen.

**Um einen Hostschlüssel zu importieren:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Importieren Sie den Schlüssel in die globale Host-Keys Datenbank:

   ```
   hostname (config) # ssh client global known-host "<keyString>"
   ```

   **WICHTIG!** Der Schlüssel muss mit der Central Management IP-Adresse starten und in doppelte Anführungszeichen eingeschlossen sein. Wenn der Schlüssel mit dem Hostnamen beginnt, ersetzen Sie den Hostnamen mit der IP-Adresse.

4. Bestätigen Sie Ihre Änderung:

   ```
   hostname (config) # show ssh server host-keys
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um einen Hostschlüssel zu entfernen:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Entfernen Sie den Schlüssel:

   ```
   hostname (config) # no ssh client global known-host "<keyString>"
   ```

4. Bestätigen Sie Ihre Änderung:

   ```
   hostname (config) # show ssh server host-keys
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**ACHTUNG!** Wenn Sie einen eingesetzten Hostschlüssel löschen, wird die Verbindung zwischen der Central Management Appliance und der verwalteten Appliance abgebrochen.

## Beispiel:

In diesem Beispiel wird der Hostschlüssel von einer Central Management Plattform auf die globale Hostschlüssel Datenbank der Network Security Appliance importiert.

```
hostname (config) # ssh client global known-host "10.11.121.13 ssh-rsa AAAAB3
NzaC1yc2EAAAADAQABAAABAQDZZJLE/ftkUddyNW6KdqEQXjS0PjbtzTn3OB51Qg0fdeQHrJgFHM2
/4C9WtDkwuX5jd7gdWnSWYwrXDv657thlyRPIt4WxjfObpOolPKAe6shgYq35NxalYDt7Pa/oym51
SN/x9dGaaTFOHvvdAf0Gu5E7nv3YjLjmSgdpSp7auHnYsyJ5O+xlYocXtoBq6jOueyxm8qm76IWL0
O7JIJ7ZLgMI8FjZ5gp48r+Hnjrdio2rhKKUP/6BOjpHRxsd8yPxMgJpyz2Dwv9ZIJha67f6sgWYdt
4yxfBc9yr7yG3iVWVJcLE+83aY24X7DBUXFnG3AeciDpEqAit2dPF586hJ"
hostname (config) # show ssh server host-keys
SSH client Strict Hostkey Checking: ask
Minimum protocol version: 2
Cipher list: compatible
Minimum key length: 1024 bits


SSH Global Known Hosts:
    Entry 1:
          Host:              10.11.121.13
          Finger Print:      c7:64:12:8a:71:a6:da:14:3c:05:37:aa:7a:2e:2a:8c
          Key Length (bits): 2048
...
```

# Strenge und globale Hostschlüssel-Überprüfung mit Hilfe der CLI aktivieren

Verwenden Sie die Befehle in diesem Abschnitt, um strenge Hostschüssel Überprüfung, globale Hostschüssel Überprüfung oder beides zu aktivieren.

- Bei **strenger Hostschlüssel-Überwachung** wird die Verbindung nur zugelassen, wenn nur die lokale Hostschlüssel Datenbank für den Network Security remote Benutzer bereits einen Eintrag enthält, der mit dem Schlüssel übereinstimmt, den die Central Management Appliance sendet.
- Mit **globaler Hostschlüssel Überprüfung** wird die Verbindung nur genehmigt, wenn die globale Hostschlüssel Datenbank der Network Security bereits einen Eintrag enthält, der mit dem Schlüssel übereinstimmt, den die Central Management Appliance sendet.

**VORSICHT!** Wenn Sie die globale Hostschlüssel-Authentifizierung aktivieren, werden alle vorhandenen Verbindungen unterbrochen, bis Sie den Hostschlüssel ausdrücklich der globalen Hostschlüssel-Datenbank hinzufügen. Anleitungen finden Sie unter Einen Hostschlüssel in die Global Host-Keys Datenbank mit Hilfe der CLI importieren auf Seite 439.

**HINWEIS:** Sehen Sie die `ssh` und `cmc` Befehle in der *CLI Befehlsreferenz* für erweiterte Authentifizierungsoptionen.

**Um strenge Hostschlüssel-Überprüfung zu aktivieren:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Aktivieren Sie strenge Hostschlüssel Überprüfung:

   ```
   hostname (config) # cmc auth ssh host-key strict
   ```

4. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show cmc auth ssh
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um globale Hostschlüssel Überprüfung zu aktivieren:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Aktivieren Sie globale Hostschlüssel Überprüfung:

   ```
   hostname (config) # cmc auth ssh host-key global-only
   ```

4. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show cmc auth ssh
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

**Um strenge oder globale Hostschüssel Überprüfung Authentifizierung zu deaktivieren:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

3. Führen Sie die folgenden Aufgaben nach Bedarf aus.
   - Um strenge Hostschlüssel Überprüfung zu deaktivieren:

     ```
     hostname (config) # no cmc auth ssh host-key strict
     ```

   - Um globale Hostschlüssel Überprüfung zu deaktivieren:

     ```
     hostname (config) # no cmc auth ssh host-key global
     ```

4. Bestätigen Sie Ihre Änderungen:

   ```
   hostname (config) # show cmc auth ssh
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

## Beispiel:

Dieses Beispiel setzt sowohl strenge als auch globale Hostschlüssel Überprüfung auf einer verwalteten Network SecurityAppliance durch.

```
hostname (config) # cmc auth ssh host-key strict
hostname (config) # cmc auth ssh host-key global-only
hostname (config) # show cmc auth ssh

CMC SSH configuration:
   Strict host key checking enabled:  yes
   Global only known hosts enabled:   yes
   Minimum protocol version:          2
   Cipher list:                       compatible
   Minimum key length:                1024 bits
```

# ANHANG B: Network Address Translation (NAT) konfigurieren

In den folgenden Abschnitten wird beschrieben, wie eine Appliance zu der Central Management Plattform zur Verwaltung in einem Deployment hinzugefügt wird, in dem die Central Management Plattform, die Appliance oder beide sich hinter einem NAT Gateway befinden.



## Informationen über NAT-Adressenabbildung

Um NAT-Deployment in einem Central Management Netzwerk zu implementieren, muss ein Netzwerkadministrator Quelle-zu Ziel IP-Adressen- und Portpaare zuordnen, so dass eine Verbindung mit der verwalteten Network Security Appliance hinter dem NAT-Gateway hergestellt werden kann. Verwaltete Appliances können entweder einen oder zwei Ports für die Verbindung und die Verwaltung und DTI Netzwerkverkehr verwenden. Standardmäßig wird ein Port benutzt. Die Schritte zum Wechseln von Single-Port und Dual-Port Kommunikation in einem NAT-Deployment sind unter Single-Port Kommunikation mit Hilfe der CLI wiederherstellen auf Seite 424 beschrieben.

## Portzugriff für Single-Port Kommunikation

Für eine **Single-Port** Konfiguration muss der remote Management (SSH) Port zugänglich sein. Dieser Port wird zum Initiieren der Verbindung, der Konfiguration und Überwachung der Appliance und Anfordern von Sicherheitsaktualisierungen (z.B. Sicherheitsinhalt, Guest Images und System Images) vom DTI-Quellserver verwendet. Port 22 ist der Standardwert.

## Portzugriff für Dual-Port Kommunikation

Für **Dual-Port** Konfiguration müssen die folgenden Ports zugänglich sein:

- Remote Management (SSH) Port—Der Management-Port, über den die Verbindung hergestellt wird und den die Central Management Appliance für die Konfigurierung und Überwachung der Appliance verwendet. Port 22 ist der Standardwert.
- DTI Network Service (HTTPS) Port—Der Port, der zum Anfordern von Softwareaktualisierungen (z.B. Sicherheitsinhalt, Guest Images, und System Images) vom DTI-Quellserver verwendet wird. Port 443 ist der Standardwert.
- DTI-Adresse für die Central Management Plattform—Wenn sich die Central Management Appliance hinter einem NAT befindet, muss der Netzwerkadministrator eine zugängliche DTI-Server IP-Adresse und HTTPS-Port zuordnen. Details finden Sie unter Eine zugängliche DTI-Serveradresse konfigurieren und aktivieren auf Seite 453.

# Zuordnungen, die verwendet werden, wenn die Central Management Appliance die Verbindung initiiert

In diesem Thema wird die NAT-Adresszuordnung für jede unterstützte Topologie beschrieben, in der die Central Management Appliance den Prozess zum Hinzufügen einer Appliance für die Verwaltung initiiert.

Einige Topologien verwenden virtuelle IP-Adressen. Diese Adressen werden auf dem NAT-Gateway zugeordnet, um eine Central Management Plattform oder verwaltetes Gerät zu erreichen, das sich auf einem internen Netzwerk hinter dem Gateway befindet.

**HINWEIS:**Es werden nur die Adressen angezeigt, die zugeordnet werden müssen. Wenn keine Zuordnung angezeigt wird, werden die Standard IP-Adressen und Standard-Ports (22 oder 22 und 443) verwendet.

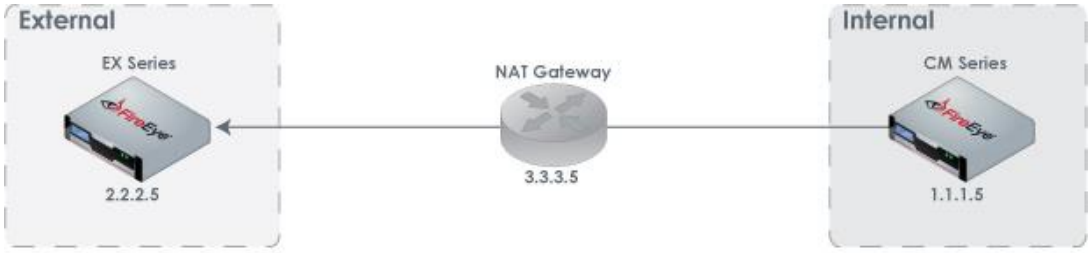
# Central Management Appliance befindet sich hinter einem NAT-Gateway

In diesem Abschnitt werden die Zuordnungen beschrieben, die für Deployments benötigt werden, in denen sich die Central Management Plattform hinter dem Gateway befindet und die Verbindung für die Konfigurierung und Verwaltung der Appliance initiiert.

**HINWEIS:**Die folgenden Single-Port Diagramme verwenden die Email Security — Server Edition Appliance als verwaltete Appliance und die Dual-Port Diagramme verwenden die Network Security Appliance als verwaltete Appliance. Sie repräsentieren allerdings auch andere Appliances.

## Single-Port Kommunikation

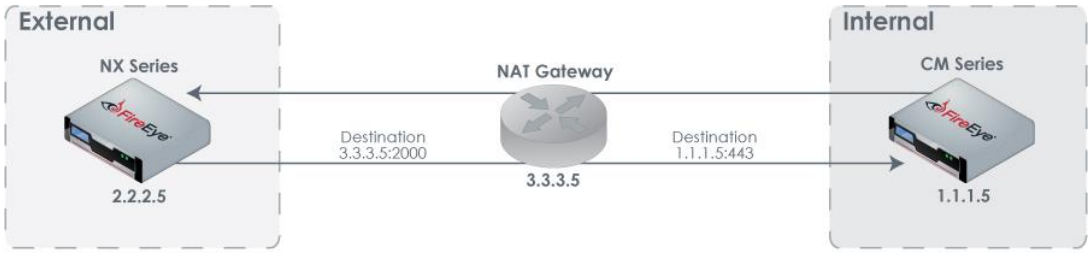
Wenn die Central Management Appliance die Verbindung initiiert und die Network Security Appliance sich in einem externen Netzwerk befindet und für Single-Port Kommunikation konfiguriert ist, ist keine NAT-Adresszuordnung erforderlich.



## Dual-Port Kommunikation

Wenn die Central Management Appliance die Verbindung initiiert und die Network Security Appliance sich in einem externen Netzwerk befindet und für Dual-Port Kommunikation konfiguriert ist, ist keine NAT-Adresszuordnung erforderlich.

Da sich die Central Management Appliance allerdings in einem internen Netzwerk befindet, müssen die zugängliche DTI-Server IP-Adresse und der HTTPS-Port der Central Management internen IP-Adresse und Port 443 zugeordnet werden, so dass die Network Security Appliance Softwareaktualisierungen anfordern kann.




# Network Security Appliance befindet sich hinter einem NAT Gateway

NAT Adressabbildung ist für Deployments erforderlich, in denen die Central Management Appliance die Verbindung initiiert, um die Network Security Appliance, die sich hinter einem NAT Gateway befindet, zu konfigurieren und zu verwalten. Die Zuordnungsdetails hängen davon ab, ob die Network Security Appliance für Single-Port oder Dual-Port Kommunikation konfiguriert ist.

## Single-Port Kommunikation

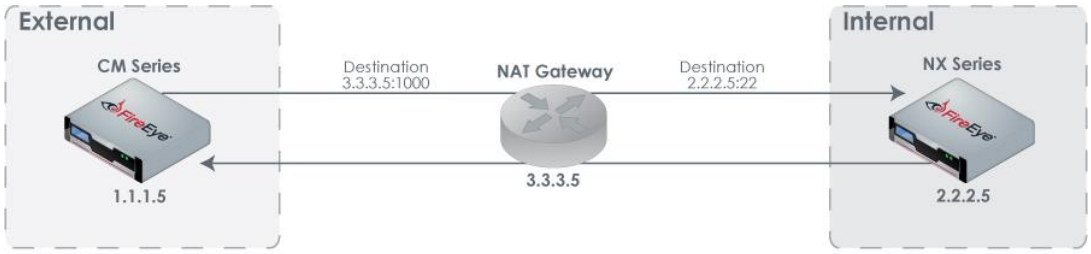
Wenn die Central Management Appliance die Verbindung mit der Network Security Appliance initiiert, die sich hinter einem NAT-Gateway befindet und für Single-Port Kommunikation konfiguriert ist, müssen eine virtuelle NAT IP-Adresse und Port der internen IP-Adresse und Port 22 der Network Security Appliance zugeordnet werden.

Die Zuordnung ermöglicht der Central Management Appliance, die Verbindung zu initiieren und dann die Network Security Appliance zu konfigurieren und zu überwachen. Die Network Security Appliance verwendet die Zuordnung, um Softwareaktualisierungen anzufordern.


## Dual-Port Kommunikation

Wenn die Central Management Appliance die Verbindung mit der Network Security Appliance initiiert, die sich hinter einem NAT-Gateway befindet und für Dual-Port Kommunikation konfiguriert ist, müssen eine virtuelle NAT IP-Adresse und Port der internen IP-Adresse und Port 22 der Network Security Appliance zugeordnet werden.

Die Central Management Appliance verwendet Mapping, um die Verbindung zu initiieren und dann die Network Security Appliance zu konfigurieren und zu verwalten. Da sich die Central Management Appliance in einem externen Netzwerk befindet ist keine Abbildung für die Network Security Appliance erforderlich, um Softwareaktualisierungen anzufordern.




# Central Management und Network Security Appliances befinden sich hinter verschiedenen NAT Gateways

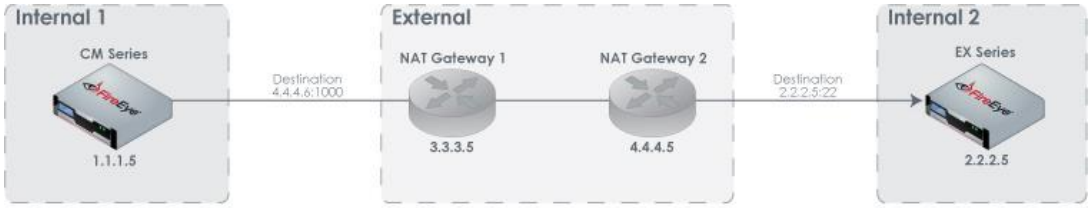
NAT Adressenabbildungen sind für Deployments erforderlich, in denen die Central Management Appliance eine Verbindung mit der Network Security Appliance initiiert und

sich die beiden Geräte hinter verschiedenen NAT-Gateways befinden. Die Abbildungsdetails hängen davon ab, ob die Network Security Appliance für Single-Port oder Dual-Port Kommunikation konfiguriert ist.

## Single-Port Kommunikation

Wenn die Central Management Appliance die Verbindung initiiert, die Network Security Appliance für Single-Port Kommunikation konfiguriert ist und sich die beiden Geräte hinter verschiedenen NAT-Gateways befinden, müssen die virtuelle IP-Adresse und Port von NAT-Gateway 2 auf die interne IP-Adresse und Port 22 der Network Security Appliance abgebildet werden.

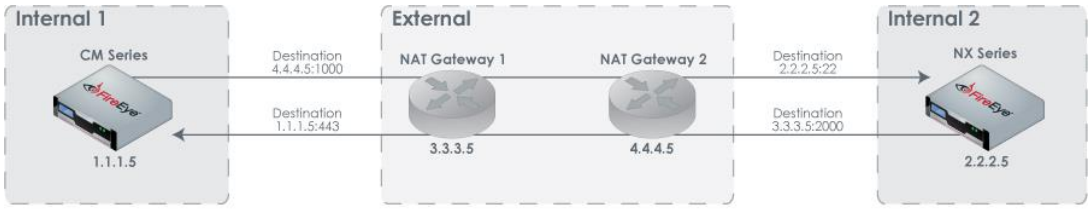
Die Abbildung ermöglicht der Central Management Appliance, eine Verbindung zu initiieren und die Network Security Appliance zu konfigurieren und zu überwachen, und der Network Security Appliance, Software Aktualisierungen zu beantragen.




## Dual-Port Kommunikation

Wenn die Network Security Appliance für Dual-Port Kommunikation konfiguriert ist und sich die Network Security Appliance und die Central Management Appliance hinter verschiedenen NAT-Gateways befinden, sind die folgenden NAT-Adressabbildungen erforderlich:

- Eine virtuelle NAT-Gateway 2 IP-Adresse und Port müssen auf der internen IP-Adresse und Port 22 der Network Security Appliance abgebildet werden. Mapping ermöglicht der Central Management Appliance, die Verbindung zu initiieren und dann die Network Security Appliance zu konfigurieren und zu überwachen.
- Die zugängliche DTI Server IP-Adresse und der HTTPS Port müssen einer virtuellen NAT-Gateway 1 IP-Adresse und Port zugeordnet sein und die virtuelle NAT-Gateway 1 IP-Adresse und Port müssen der internen IP-Adresse und Port 443 der Central Management zugeordnet sein. Diese Abbildungen ermöglichen der Network Security Appliance, Softwareaktualisierungen anzufordern.



## Central Management und Network Security Appliance befinden sich in einem externen Netzwerk

Wenn die Central Management Appliance die Verbindung initiiert und sich die Network Security Appliance in einem externen Netzwerk befindet, ist keine NAT-Adressenabbildung erforderlich.

# Abbildungen, die verwendet werden, wenn die Network Security Appliance die Verbindung initiiert

In diesem Abschnitt wird die NAT Adresszuordnung angezeigt, die für jede unterstützte Topologie erforderlich ist, in der die Network Security Appliance die Verbindung mit der Central Management Appliance initiiert:

- Central Management Appliance befindet sich hinter einem NAT-Gateway unten
- Network Security Appliance befindet sich hinter einem NAT Gateway auf Seite 451
- Central Management und Network Security Appliance befinden sich hinter verschiedenen NAT Gateways auf Seite 451
- Central Management und Network Security Appliance befinden sich in externen Netzwerken auf Seite 452

Einige Topologien verwenden virtuelle IP-Adressen. Diese Adressen werden auf dem NAT-Gateway zugeordnet, um eine Central Management Appliance oder verwaltete Appliance zu erreichen, die sich auf einem internen Netzwerk hinter dem Gateway befindet.

**HINWEIS:**Es werden nur die Adressen angezeigt, die zugeordnet werden müssen. Wenn keine Zuordnung angezeigt wird, werden die Standard IP-Adressen und Standard-Ports (22 oder 22 und 443) verwendet.

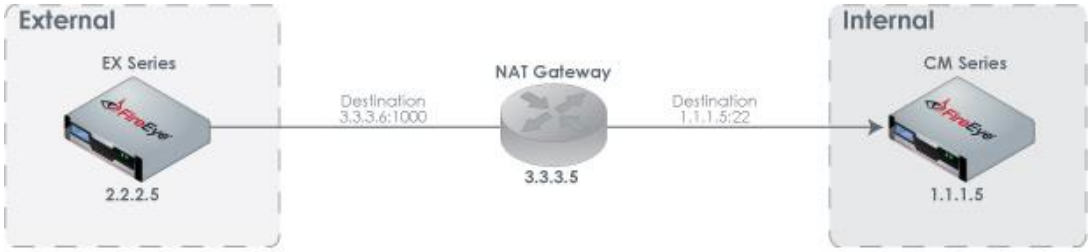
## Central Management Appliance befindet sich hinter einem NAT-Gateway

NAT-Adresszuordnungen sind für Deployments erforderlich, in denen die Network Security Appliance eine Verbindung mit der Central Management Appliance hinter einem NAT-Gateway initiiert. Die Zuordnungsdetails hängen davon ab, ob die Network Security Appliance für Single-Port oder Dual-Port Kommunikation konfiguriert ist.

## Single-Port Kommunikation

Wenn die Network Security Appliance für Single-Point Kommunikation konfiguriert ist und eine Verbindung mit der Central Management Appliance hinter einem NAT Gateway initiiert hat, müssen eine virtuelle NAT IP-Adresse und Port der internen Central Management IP-Adresse und Port 22 zugeordnet sein.

Die Network Security Appliance verwendet die Zuordnung, um eine Anfrage zu senden, zur Central Management Appliance für das Management hinzugefügt zu werden sowie Softwareaktualisierungen anzufordern.

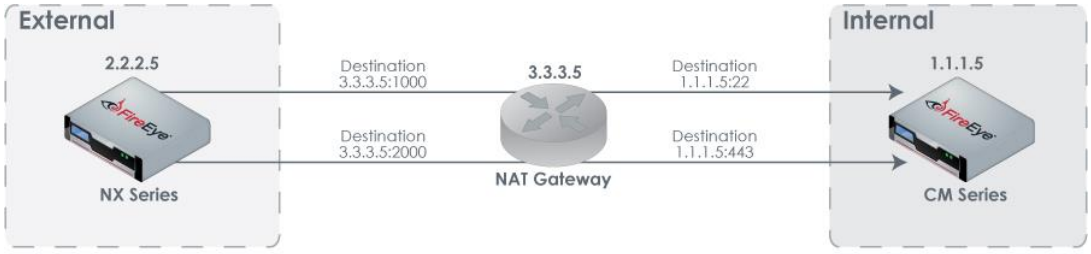



## Dual-Port Kommunikation

Wenn die Network Security  Appliance für Dual-Port Kommunikation konfiguriert ist und eine Verbindung mit der Central Management Appliance hinter einem NAT Gateway initiiert, müssen eine virtuelle NAT IP-Adresse und Port mit der internen Central Management IP-Adresse und Port zugeordnet sein.

Die Network Security Appliance verwendet die Zuordnung, um eine Anfrage zu senden, zur Central Management Appliance für das Management hinzugefügt zu werden sowie Softwareaktualisierungen anzufordern.

Da sich die Central Management Appliance allerdings in einem internen Netzwerk befindet, müssen die zugängliche DTI-Server IP-Adresse und der HTTPS-Port der Central Management internen IP-Adresse und Port 443 zugeordnet werden, so dass die Network Security Appliance Softwareaktualisierungen anfordern kann.



# Network Security Appliance befindet sich hinter einem NAT Gateway

Zuordnung ist nicht erforderlich, weil sich die Central Management Appliance in einem externen Netzwerk befindet und für die Network Security Appliance zugänglich ist.

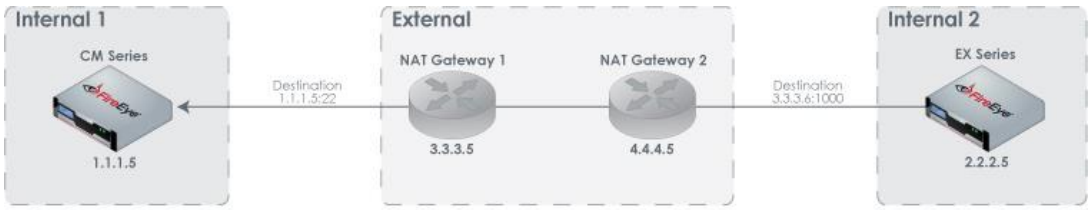
# Central Management und Network Security Appliance befinden sich hinter verschiedenen NAT Gateways

NAT Adresszuordnungen sind für Deployments erforderlich, in denen die Network Security Appliance eine Verbindung mit der Central Management Appliance initiiert und sich zwei Geräte hinter verschiedenen NAT Gateways befinden. Die Zuordnungsdetails hängen davon ab, ob die Network Security Appliance für Single-Port oder Dual-Port Kommunikation konfiguriert ist.

## Single-Port Kommunikation

Wenn die Network Security Appliance für Single-Port Kommunikation konfiguriert ist und sich die Network Security Appliance und die Central Management Appliance hinter verschiedenen NAT Gateways befinden, müssen die virtuelle NAT Gateway 1 IP-Adresse und Port der Central Management internen IP-Adresse und Port 22 zugeordnet werden.

Die Central Management Appliance verwendet die Zuordnung, um die Network Security Appliance zu konfigurieren und zu überwachen. Die Network Security Appliance verwendet die Zuordnung, um eine Anfrage zu senden, zur Central Management Appliance für das Management hinzugefügt zu werden sowie Softwareaktualisierungen anzufordern.



## Dual-Port Kommunikation

Wen die Network Security Appliance für Dual-Port Kommunikation konfiguriert ist und sich die Network Security Appliance und die Central Management Appliance hinter verschiedenen NAT Gateways befinden, sind die folgenden NAT Adresszuordnungen erforderlich:

- Die virtuelle NAT-Gateway 1 IP-Adresse und Port müssen der Central Management internen IP-Adresse und Port 22 zugeordnet werden. Die Zuordnung ermöglicht der Network Security Appliance, eine Anfrage zu senden, zur Central Management Appliance zur Verwaltung hinzugefügt zu werden und der Central Management Appliance, die Network Security Appliance zu konfigurieren und zu verwalten.
- Die interne IP-Adresse und Port 443 der Network Security Appliance müssen einer virtuellen NAT Gateway 2 IP-Adresse und Port zugeordnet sein. Die virtuelle NAT-Gateway 1 IP-Adresse und Port müssen der Central Management internen IP-Adresse und Port 443 für die Network Security Appliance zugeordnet werden. Die Zuordnungen ermöglichen der Network Security Appliance, Softwareaktualisierungen anzufordern.


# Central Management und Network Security Appliance befinden sich in externen Netzwerken

Wenn sich die beiden Geräte in externen Netzwerken befinden und die Network Security Appliance die Verbindung initiiert, ist keine NAT-Adresszuordnung erforderlich.

# Eine zugängliche DTI-Serveradresse konfigurieren und aktivieren

Die Central Management Appliance kann als die DTI-Quelle für ihre verwalteten Appliances fungieren, um Softwareaktualisierungen (wie z.B. Sicherheitsinhalt, Guest Images und System Images) herunterzuladen. In einer Dual-Port Konfiguration läuft der Managementverkehr durch den SSH Port und der DTI Verkehr läuft durch den HTTPS Port. Wenn sich die Central Management Appliance hinter einem NAT-Gateway befindet, besitzt sie eine interne IP-Adresse, die verwaltete Appliances nicht erreichen können.

In dieser Umgebung müssen Sie eine zugängliche Adresse konfigurieren und aktivieren, die die verwaltete Appliance als die DTI-Quelle für Softwareaktualisierungen verwenden wird. Diese Adresse ist die virtuelle NAT IP-Adresse und Port, die der Central Management internen IP-Adresse und Port 443 zugeordnet ist. Details finden Sie unter Auf Single-Port oder Dual-Port Kommunikation in einem NAT-Deployment wechseln auf Seite 457.

Die zugängliche DTI-Server Adresse muss auf jeder verwalteten Appliance konfiguriert und aktiviert werden. Zusätzlich muss auf verwalteten Appliances, die eine unterstützte Version ausführen (siehe Hinweis unten), eine "no override" Markierung eingestellt werden, um zu verhindern, dass die Standard Central Management Adresse die zugängliche Adresse überschreibt.

**WICHTIG!** Alle verwalteten Appliances hinter dem gleichen NAT-Gateway wie die Central Management Appliance verwenden die Standard Central Management Appliance als ihre DTI-Quelle und erfordern keine zusätzliche Konfiguration.

**WICHTIG!** Eine zugängliche DTI-Serveradresse ist nur in einer Dual-Port Konfiguration erforderlich. Wenn Sie von der Dual-Port zur Single-Port-Kommunikation wechseln, müssen Sie die "no override" Markierung entfernen und stattdessen eine "override" Markierung einstellen, um der Central Management Appliance zu genehmigen, die Single-Port-Einstellungen auf die verwaltete Appliance zu pushen. Details finden Sie unter Auf Single-Port oder Dual-Port Kommunikation in einem NAT-Deployment wechseln auf Seite 457.

## Voraussetzungen

- Admin Zugriff

# Eine zugängliche DTI-Serveradresse mit Hilfe der CLI konfigurieren und aktivieren

Verwenden Sie die CLI Befehle in diesem Abschnitt, um eine benutzerdefinierte DTI-Quelle zu konfigurieren und aktivieren Sie sie als eine zugängliche DTI-Serveradresse für verwaltete Network Security Appliances mit Hilfe des dual-Port Adresstypen.

**WICHTIG!** Verwenden Sie dieses Verfahren nur für das in Den Adresstyp für DTI-Network Serviceanfragen ändern auf Seite 423 beschriebene Szenario.

**WICHTIG!** Sie müssen die Befehle in der angezeigten Reihenfolge eingeben.

**HINWEIS:** Diese Konfiguration muss auf jeder verwalteten Appliance durchgeführt werden. Sie können den Vorgang auf jeder Appliance wiederholen oder Appliance Gruppenfunktionen verwenden, um die zugängliche Adresse auf mehreren Appliances gleichzeitig zu konfigurieren.

**HINWEIS:** Nur eine benutzerdefinierte DTI-Adresse kann konfiguriert werden.

**Um die benutzerdefinierte Adresse zu konfigurieren:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

```
appl-hostname > enable
appl-hostname # configure terminal
```

3. Konfigurieren Sie die zugängliche Adresse für die DTI `source`:

   a. Verhindern Sie, dass die lokale Adresse die zugängliche Adresse überschreibt:

      ```
      appl-hostname (config) # no fenet dti source override enable
      ```

   b. Konfigurieren Sie die IP-Adresse und Port:

      ```
      appl-hostname (config) # fenet dti source type <name> address
      <ipAddress> [port <port>]
      ```

      wobei `name` der Name Ihrer Wahl und `ipAddress` die NAT IPv4- oder IPv6-Adresse ist. Der `port` Parameter ist optional und fällt auf 443 zurück, wenn er nicht festgelegt ist.

   c. Bestimmen Sie den User und das Passwort des DTI-Servers:

      ```
      appl-hostname (config) # fenet dti source type <name> username
      <username> password <password>
      ```

   d. Stellen Sie `CUSTOM` als den Standard DTI-Quelltyp ein:

      ```
      appl-hostname (config) # fenet dti source default <name>
      ```

4. Konfigurieren Sie die zugängliche Adresse für die DTI `upload destination`:

   a. Verhindern Sie, dass die lokale Adresse die zugängliche Adresse überschreibt:

      ```
      appl-hostname (config) # no fenet dti upload destination override
      enable
      ```

   b. Konfigurieren Sie die Adresse und Port:

      ```
      appl-hostname (config) # fenet dti upload destination type
      <name> address <ipAddress> [port <port>]
      ```

      wobei `name` der Name Ihrer Wahl und `ipAddress` die NAT Gateway IPv4- oder IPv6-Adresse ist. Der `port` Parameter ist optional und fällt auf 443 zurück, wenn er nicht festgelegt ist.

   c. Bestimmen Sie den User und das Passwort des DTI-Servers:

      ```
      appl-hostname (config) # fenet dti upload destination type
      <name> username <username> password <password>
      ```

   d. Stellen Sie `CUSTOM` als den Standard Zieltyp für das DTI-Upload ein:

      ```
      appl-hostname (config) # fenet dti upload destination default
      <name>
      ```

5. Konfigurieren Sie die zugängliche Adresse für den `enrollment`, `faude`, `mil`, `helix` oder `virtual` Service:

   a. Verhindern Sie, dass die lokale Adresse die zugängliche Adresse überschreibt:

   ```
   appl-hostname (config) # no fenet dti <service> service override enable
   ```

   b. Konfigurieren Sie die Adresse und den Port:

   ```
   appl-hostname (config) # fenet dti <service> service type <name> address <ipAddress> [port <port>]
   ```

   wobei `name` ein Name Ihrer Wahl und `ipAddress` die virtuelle NAT IPv4- oder IPv6 Adresse ist. Der `port` Parameter ist optional und fällt auf 443 zurück, wenn er nicht festgelegt ist.

   c. Bestimmen Sie den User und das Passwort des DTI-Servers:

   ```
   appl-hostname (config) # fenet dti <service> service type <name> username <username> password <password>
   ```

   d. Stellen Sie `CUSTOM` als den Standard DTI-Servicetyp ein:

   ```
   appl-hostname (config) # fenet dti mil service default <name>
   ```

6. Bestätigen Sie die Konfiguration:

   ```
   appl-hostname (config) # show fenet
   ```

7. Speichern Sie Ihre Änderungen:

   ```
   appl-hostname (config) # write memory
   ```

## Die benutzerdefinierte DTI-Quelle löschen

Sie können die benutzerdefinierte DTI-Quelle löschen, wodurch sie von der Liste der verfügbaren Optionen entfernt wird.

**HINWEIS:** Sie können die benutzerdefinierte DTI-Quelle nicht löschen, wenn es sich um eine aktive DTI-Quelle für verwaltete Appliances handelt.

**Um die benutzerdefinierte DTI Quelle zu löschen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

2. Löschen Sie die benutzerdefinierte DTI-Quelle:

   ```
   appl-hostname (config) # no fenet dti source type <name>
   ```

3. Bestätigen Sie Ihre Änderungen:

   ```
   appl-hostname (config) # show fenet dti configuration
   ```

4. Speichern Sie Ihre Änderungen:

```
appl-hostname (config) # write memory
```

## Beispiel:

Im folgenden Beispiel wird eine benutzerdefinierte Adresse mit dem Namen "CUSTOM" konfiguriert und verhindert, dass die Central Management Appliance sie mit der Central Management lokalen Adresse überschreibt.

```
appl-hostname (config) # no fenet dti source override enable
appl-hostname (config) # fenet dti source type CUSTOM address 10.3.3.5 port
2000
appl-hostname (config) # fenet dti source type CUSTOM username user8 password
123ABCXYZ
appl-hostname (config) # fenet dti source default CUSTOM
appl-hostname (config) # no fenet dti upload destination override enable
appl-hostname (config) # fenet dti upload destination type CUSTOM address
3.3.3.5 port 2000
appl-hostname (config) # fenet dti upload destination type CUSTOM username
user8 password 123ABCXYZ
appl-hostname (config) # fenet dti upload destination default CUSTOM
...

appl-hostname (config) # show fenet
DTI CLIENT CONFIGURATION:
  Download source    :  CUSTOM (user8@10.3.3.5)
  Upload destination :  CUSTOM (user8@10.3.3.5)
  Update channel     :  CUSTOM (user8@10.3.3.5)
  Http proxy         :  None
  Connect timeout    :  30 (max tries: 3)
  Speed Time         :  60
  Max Time           :  14400
  Rate Limit         :  None
  Lockdown enabled   :  No
  SSL minimum version:  tls1
  SSL cipher list    :  compatible
```

# Auf Single-Port oder Dual-Port Kommunikation in einem NAT-Deployment wechseln

Verwaltete Network Security Appliances können mit der Central Management Appliance über einen einzelnen Port oder mit Hilfe von zwei Ports kommunizieren. (Details finden Sie unter Informationen über die Änderung des Adresstyps für DTI-Network Serviceanfragen auf Seite 423.)

In der Dual-Port Konfiguration muss eine benutzerdefinierte DTI-Quelladresse konfiguriert werden, wenn sich die Central Management Appliance in einem internen Netzwerk hinter einem NAT Gateway befindet. Die benutzerdefinierte Adresse ermöglicht der verwalteten Appliance Zugriff auf den HTTPS-Port auf der Central Management Appliance, um Softwareaktualisierungen von dem DTI-Netzwerk anzufordern. (Details finden Sie unter Eine zugängliche DTI-Serveradresse konfigurieren und aktivieren auf Seite 453.)

Um die benutzerdefinierte Adresse zu konfigurieren, müssen Sie eine Markierung einstellen, um zu verhindern, dass die Central Management Appliance die benutzerdefinierten Adresseneinstellungen überschreibt. Wenn Sie von Dual-Port auf Single-Port Kommunikation wechseln, müssen Sie diese Markierung entfernen, so dass die Central Management Applinace die Single-Port Einstellungen auf die Network Security Appliance gepusht werden können.

**Um von Dual-Port auf Single-Port Kommunikation zu wechseln:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

3. Gestatten Sie der Central Management Appliance die Single-Port Einstellungen zu pushen:

   ```
   appl-hostname (config) # fenet dti source override enable
   appl-hostname (config) # fenet dti upload destination override enable
   appl-hostname (config) # fenet dti mil service override enable
   appl-hostname (config) # fenet dti avsuite service override enable
   ```

4. Bestätigen Sie Ihre Änderungen:

   ```
   appl-hostname (config) # show fenet
   ```

5. Speichern Sie Ihre Änderungen:

   ```
   appl-hostname (config) # write memory
   ```

**Um von Single-Port auf Dual-Port Kommunikation zu wechseln:**

1. Führen Sie das Verfahren in Dual-Port Kommunikation mit Hilfe der CLI konfigurieren auf Seite 426 aus.
2. Wenn sich die Central Management Appliance hinter einem NAT-Gateway befindet, führen Sie das Verfahren in Eine zugängliche DTI-Serveradresse mit Hilfe der CLI konfigurieren und aktivieren auf Seite 454 aus.

## Beispiel:

Das folgende Beispiel ermöglicht der Central Management Appliance, die Single-Port Einstellungen auf die Network Security Appliance zu pushen, nachdem der Adresstyp von Dual-Port auf Single-Port geändert wurde.

```
appl-hostname (config) # fenet dti source override enable
appl-hostname (config) # fenet dti upload destination override enable
appl-hostname (config) # fenet dti mil service override enable
appl-hostname (config) # fenet dti avsuite service override enable
appl-hostname (config) # write memory
appl-hostname (config) # show fenet dti configuration


DTI CLIENT CONFIGURATION:
  Download source    :  CMS (DTIUser@10.2.0.0 : singleport) - Managed by CMS
```

```
  Upload destination :  CMS (DTIUser@10.2.0.0 : singleport) - Managed by CMS
  Mil service        :  CMS (DTIUser@10.2.0.0 : singleport) - Managed by CMS

  AVSuite service    : CMS (DTIUser@10.2.0.0 : singleport)  - Managed by CMS
...
```

# Eine Managementanfrage in einem NAT-Deployment senden

Ein Network Security Administrator kann eine Anfrage senden, um die Appliance zur Central Management Appliance hinzuzufügen. Ein Rendezvous-Vorgang ermöglicht der Network Security Appliance, die Anfrage zu versuchen und gestattet dem Central Management Administrator, die Liste der ausstehenden Anfragen zu sehen.

## Voraussetzungen für die Erstellung einer erfolgreichen Verbindung

Um eine Managementanfrage zu senden und die Verbindung erfolgreich zu erstellen und beizubehalten, muss folgendes vorhanden sein:

- **Automatische Rendezvous-Versuche werden** auf der anfragenden Network Security Appliance aktiviert (standardmäßig deaktiviert).
- **Die automatische Verbindungsfunktion ist** auf der anfragenden Network Security Appliance aktiviert, so dass die automatisch versucht, sich mit der Central Management Appliance zu verbinden, nachdem der Rendezvous-Versuch erfolgreich ist (standardmäßig aktiviert).

  **HINWEIS:** Sehen Sie Eine Network Security Appliance vorbereiten, eine Managementanfrage in einem NAT-Deployment zu senden auf der nächsten Seite, um diese Einstellungen zu bestätigen und zu aktivieren.

- **Die Network Security Appliance besitzt einen einzigartigen und permanenten Hostnamen**. Ausstehende Anfragen von Appliances mit dem gleichen Hostnamen oder IP-Adresse werden abgelehnt. Wenn der Hostname geändert wird, wird die Verbindung unterbrochen und kann nicht zurückgesetzt werden. In diesem Fall muss die Appliance von der Central Management Appliance entfernt und dann erneut mit dem neuen Hostnamen hinzugefügt werden.

- **Die Central Management Appliance und die Network Security Appliance haben denselben Rendezvous-Service Namen**. Der Rendezvous-Vorgang hat eine Kennung (bekannt als *Servicename*), die standardmäßig auf "cmc" eingestellt ist. Die Central Management Appliance und die anfragende Appliance müssen den gleichen Servicenamen haben; wenn Sie den Servicenamen auf einer ändern, müssen Sie ihn auch auf der anderen ändern. Der `cmc rendezvous service-name <hostname>` Befehl ändert den Servicenamen; der `no cmc rendezvous service-name` Befehl stellt den Standardwert wieder her. Details finden Sie in der *CLI Befehlsreferenz*.

  **WICHTIG!** Appliance-initiierte Verbindungen werden in Central Management High Availability (HA) Deployments nicht untestützt.

## Voraussetzungen

- Operator oder Admin Zugriff
- Network address translation (NAT) Zuordnung, wie in Informationen über NAT-Adressenabbildung auf Seite 443 beschrieben
- *Wenn sich die anfordernde Appliance hinter einem NAT-Gateway befindet*: Die virtuelle NAT-Adresse und Port, die der internen IP-Adresse und SSH-Port der anfordernden Appliance zugeordnet ist.
- Wenn sich die Central Management Appliance hinter einem NAT-Gateway befindet:
  - Die virtuelle NAT-Adresse und Port, die der Central Management internen IP-Adresse und SSH-Port zugeordnet ist.
  - Eins der folgenden:
    - die zugängliche Central Management IP-Adresse und Port, beschrieben inEine zugängliche DTI-Serveradresse konfigurieren und aktivieren auf Seite 453
    - Auf der Appliance aktivierte Single-Port Kommunikation, wie in Den Adresstyp für DTI-Network Serviceanfragen ändern auf Seite 423 beschrieben

## Eine Network Security Appliance vorbereiten, eine Managementanfrage in einem NAT-Deployment zu senden

Verwenden Sie die Befehle in diesem Abschnitt, um eine Appliance in einem NAT-Deployment vorzubereiten, eine Managementanfrage an die Central Management Appliance zu senden.

**Um das Senden einer Anfrage vorzubereiten:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

3. Aktivieren Sie automatische Rendezvous-Versuche:

   ```
   appl-hostname (config) # cmc rendezvous client auto
   ```

   **WICHTIG:**Nachdem automatisches Rendezvous aktiviert ist, wird die lokale IP-Adresse der Appliance in der Anfrage anstelle der zugeordneten Adresse eingeschlossen, wenn sich die anfragende Network Security Appliance hinter einem NAT-Gateway befindet. Sie müssen verhindern, dass die lokale IP-Adresse der Appliance Teil der Anfrage ist und dann erzwingen, dass die Anfrage erneut mit Hilfe der zugeordneten Adresse gesendet wird. Diese Befehle sind in den relevanten Vorgängen eingeschlossen.

4. Bestätigen Sie, dass die automatische Verbindungsfunktion aktiviert ist:
   a. Zeigen Sie die Network Security (Client) Informationen an:

      ```
      appl-hostname (config) # show cmc client
      ```

   b. Wenn `Autoconnect: no` angezeigt wird, aktivieren Sie automatische Verbindung:

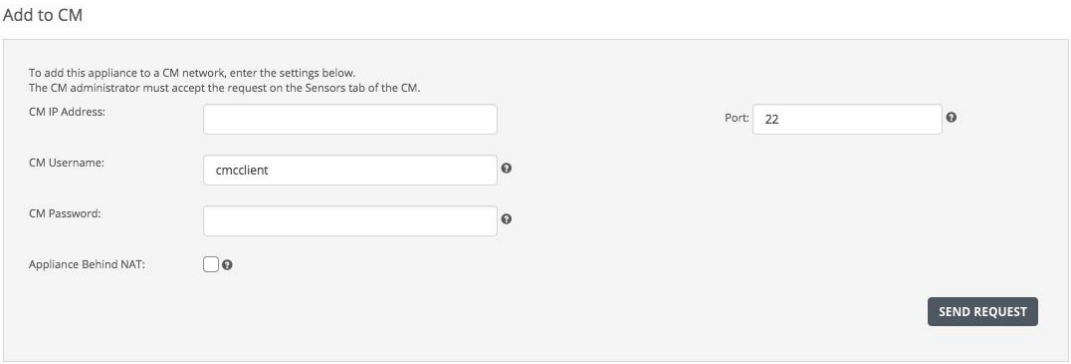
      ```
      appl-hostname (config) # cmc client connection auto
      ```

5. Speichern Sie Ihre Änderungen:

   ```
   hostname (config) # write memory
   ```

# Eine Managementanfrage in einem NAT-Deployment mit Hilfe der Appliance Web-UI senden

Verwenden Sie die **Add to CM** Seite in der Network Security Web-UI, um eine Anfrage zu initiieren, zu einer Central Management Appliance hinzugefügt zu werden.




**Um eine Managementanfrage zu senden:**

1. Wenn die Network Security Appliance noch nie eine Managementanfrage gesendet hat, stellen Sie sicher, dass die in Eine Network Security Appliance vorbereiten, eine Managementanfrage in einem NAT-Deployment zu senden auf Seite 460 beschriebenen Voraussetzungen erfüllt sind.
2. Melden Sie sich auf der Network Security Web-UI an.
3. Klicken Sie auf den **Settings** Tab.
4. Klicken Sie auf der Seitenleiste auf **CM Network**.
5. In den **CM IP Address** und **Port** Feldern, führen Sie einen der folgenden Schritte aus:
   - *Wenn sich die* Central Management *nicht hinter einem NAT-Gateway oder hinter dem gleichen NAT-Gateway wie die Appliance befindet*: Geben Sie die Central Management IP-Adresse und den remote Management-Port ein. Der Standardport ist 22.
   - *Wenn sich die* Central Management *hinter einem anderen NAT-Gateway als dem Appliance NAT-Gateway befindet*: Geben Sie die zugängliche Central Management IP-Adresse und Port ein.
6. In den **CM Username** und **CM Password** Felden geben Sie die Admin-Berechtigungen ein, die die Appliance zum Anmelden auf der Central Management Appliance verwenden soll, um sich anzukündigen.
7. Wenn sich die Network SecurityAppliance hinter einem NAT-Gateway befindet, wählen Sie das **Appliance Behind NAT** Kontrollkästchen.

8. Klicken Sie auf **Send Request**.

   In einer Nachricht werden Sie darüber informiert, ob die Anfrage erfolgreich war oder nicht oder dass die Network Security Appliance bereits von der Central Management Appliance verwaltet wird. Wenn die Anfrage erfolgreich ist, kann ein Central Management Administrator die Anfrage annehmen oder ablehnen. Ein Beispiel für eine Erfolgsmeldung wird nachfolgend angezeigt:


**HINWEIS:** Informationen über die Annahme der Anfragen und Hinzufügen der Appliance zur Central Management Appliance finden Sie im *Central ManagementAdministrationshandbuch*.

## Eine Managementanfrage in einem NAT-Deployment mit Hilfe der Network Security CLI senden

Verwenden Sie die Befehle in diesem Abschnitt, um eine Managementanfrage von einer Network Security Appliance in einem NAT Deployment an die Central Management Appliance zu senden.

Die folgenden Topologien werden unterstützt:

- Central Management und Network Security Appliance hinter dem gleichen NAT-Gateway auf der nächsten Seite
- Network Security Appliance hinter NAT-Gateway und Central Management in externem Netzwerk auf der nächsten Seite
- Central Management hinter NAT-Gateway und Network Security Appliance in externem Netzwerk auf Seite 465
- Central Management und Network Security Appliances hinter verschiedenen NAT-Gateways auf Seite 466

**VORSICHT!** Wenn die Network Security Appliance noch nie eine Managementanfrage gesendet hat, stellen Sie sicher, dass die in Eine Network Security Appliance vorbereiten, eine Managementanfrage in einem NAT-Deployment zu senden auf Seite 460 beschriebenen Voraussetzungen vorhanden sind bevor Sie versuchen, die Anfrage zu senden.

## Central Management und Network Security Appliance hinter dem gleichen NAT-Gateway

**Um eine Managementanfrage zu senden:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

3. Bestimmen Sie den Hostnamen oder die IPv4- oder IPv6-Adresse der Central Management Appliance:

   ```
   appl-hostname (config) # cmc client server address <hostname, IPv4 or
   IPv6 address>
   ```

4. Bestimmen Sie den Authentifizierungstyp und Admin-Berechtigungen, die die Appliance für die Anmeldung auf der Central Management Appliance verwenden soll, um sich anzukündigen.

   ```
   appl-hostname (config) # cmc client server auth authtype <authType>
   appl-hostname (config) # cmc client server auth <authType> username
   <username>
   appl-hostname (config) # cmc client server auth <authType> password
   <password>  | identity <identity>
   ```

   wobei <authType> **password**, **ssh-dsa2** oder **ssh-rsa2** sein kann. (Sehen Sie Benutzerauthentifizierung mit Hilfe der CLI konfigurieren auf Seite 434 für Details.)

5. Speichern Sie Ihre Änderungen:

   ```
   appl-hostname (config) # write memory
   ```

## Network Security Appliance hinter NAT-Gateway und Central Management in externem Netzwerk

**Um eine Managementanfrage zu senden:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

3. Bestimmen Sie den Hostnamen oder die IPv4- oder IPv6-Adresse der Central Management Appliance:

   ```
   appl-hostname (config) # cmc client server address <hostname, IPv4 or
   IPv6 address>
   ```

4. Bestimmen Sie den Authentifizierungstyp und Admin-Berechtigungen, die die Appliance für die Anmeldung auf der Appliance verwenden soll, um sich anzukündigen.Central Management

   ```
   appl-hostname (config) # cmc client server auth <authType>
   appl-hostname (config) # cmc client server auth <authType> username
   <username>
   appl-hostname (config) # cmc client server auth <authType> password
   <password> | identity <identity>
   ```

   wobei <authType> **password**, **ssh-dsa2** oder **ssh-rsa2** sein kann. (Sehen Sie Benutzerauthentifizierung mit Hilfe der CLI konfigurieren auf Seite 434 für Details.)

5. Verwenden Sie, dass die lokale IP-Adresse der Appliance hinter dem NAT-Gateway Teil der Anfrage wird:

   ```
   appl-hostname (config) # no cmc rendezvous client send-client-address
   ```

6. Speichern Sie Ihre Änderungen:

   ```
   appl-hostname (config) # write memory
   ```

## Central Management hinter NAT-Gateway und Network Security Appliance in externem Netzwerk

**Um eine Managementanfrage zu senden:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

3. Bestimmen Sie den virtuellen NAT-Hostnamen oder die IPv4- oder IPv6 Adresse und den Port, die der Central Management internen IP-Adresse und SSH Port zugeordnet sind:

   ```
   appl-hostname (config) # cmc client server address <hostname, IPv4 or
   IPv6 address>
   ```

   wobei <IPv4 or IPv6 address> die zugeordnete IPv4 oder IPv6 Adresse ist.

4. (Optional) Bestimmen Sie den virtuellen NAT-Port, der dem Central Management internen SSH Port zugeordnet ist:

   ```
   appl-hostname (config) # cmc client server port <port>
   ```

   Der Port fällt auf 22 zurück, wenn dies nicht festgelegt ist.

5. Bestimmen Sie den Authentifizierungstyp und Admin-Berechtigungen, die die Appliance für die Anmeldung auf der Central Management Plattform verwenden soll, um sich anzukündigen.

   ```
   appl-hostname (config) # cmc client server auth <authType>
   appl-hostname (config) # cmc client server auth <authType> username
   <username>
   appl-hostname (config) # cmc client server auth <authType> password
   <password> | identity <identity>
   ```

   wobei <authType> **password**, **ssh-dsa2** oder **ssh-rsa2** sein kann. (Sehen Sie Benutzerauthentifizierung mit Hilfe der CLI konfigurieren auf Seite 434 für Details.)

6. Speichern Sie Ihre Änderungen:

   ```
   appl-hostname (config) # write memory
   ```

## Central Management und Network Security Appliances hinter verschiedenen NAT-Gateways

**Um eine Managementanfrage zu senden:**

1. Melden Sie sich auf der Network Security CLI an.
2. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   appl-hostname > enable
   appl-hostname # configure terminal
   ```

3. Bestimmen Sie den virtuellen Central Management NAT Hostnamen oder die IPv4- oder IPv6-Adresse, die der Central Management internen IP-Adresse zugeordnet ist:

   ```
   appl-hostname (config) # cmc client server address <hostname, IPv4 or
   IPv6 address>
   ```

   wobei `<IPv4 or IPv6 address>` die zugeordnete IPv4-oder IPv6-Adresse ist.

4. (Optional) Bestimmen Sie den virtuellen Central Management NAT-Port, der dem Central Management internen SSH Port zugeordnet ist:

   ```
   appl-hostname (config) # cmc client server port <port>
   ```

   Der Port fällt auf 22 zurück, wenn dies nicht festgelegt ist.

5. Bestimmen Sie den Authentifizierungstyp und Admin-Berechtigungen, die die Appliance für die Anmeldung auf der Central Management Plattform verwenden soll, um sich anzukündigen.

   ```
   hostname (config) # cmc client server auth authtype <authType>
   hostname (config) # cmc client server auth <authType> username
   <username>
   hostname (config) # cmc client server auth <authType> password
   <password> |  identity <identity>
   ```

   wobei `<authType>` **password**, **ssh-dsa2** oder **ssh-rsa2** sein kann. (Sehen Sie Benutzerauthentifizierung mit Hilfe der CLI konfigurieren auf Seite 434 für Details.)

6. Verwenden Sie, dass die lokale IP-Adresse der Appliance hinter dem NAT-Gateway Teil der Anfrage wird:

   ```
   appl-hostname (config) # no cmc rendezvous client send-client-address
   ```

7. Senden Sie die Anfrage erneut, ohne die lokale IP-Adresse der Appliance einzuschließen.

   ```
   appl-hostname (config) # cmc rendezvous client force
   ```

8. Speichern Sie Ihre Änderungen:

   ```
   appl-hostname (config) # write memory
   ```

# Globale Hostschlüssel-Authentifizierung in einem NAT Deployment konfigurieren

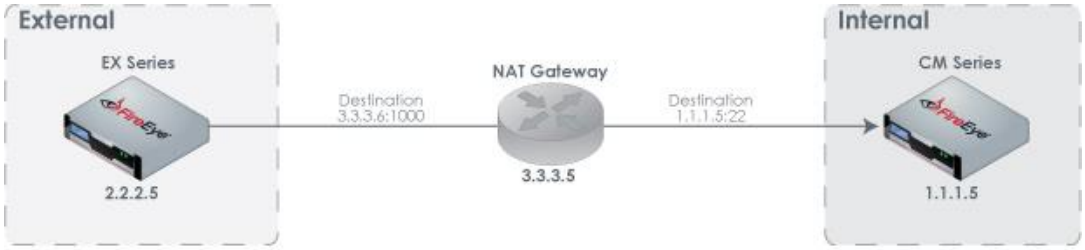
Wenn globale Hostschlüssel Authentifizierung auf einer verwalteten Network Security Appliance erzwungen wird, müssen Sie den öffentlichen Hostschlüssel von der Central Management Appliance erhalten und in die globale Hostschlüssel-Datenbank der Network Security Appliance importieren. Dies ist in Secure Shell (SSH) Authentifizierung konfigurieren auf Seite 431 beschrieben.

Die Central Management Hostschlüssel-Zeichenfolge enthält ihre IP-Adresse. Wenn sich die Central Management Appliance in einem internen Netzwerk hinter einem NAT Gateway befindet, muss die IP-Adresse in der Schlüssel-Zeichenfolge, die Sie von der Central Management Web-UI oder CLI erhalten, mit der virtuellen IP-Adresse ersetzt werden, die der Central Management auf dem NAT Gateway zugeordnet ist.

## Beispiel:

In diesem Beispiel befindet sich die Central Management Plattform hinter dem NAT Gateway. Ihre IP-Adresse ist 1.1.1.2 und die virtuelle Adresse ist 3.3.3.5.

**HINWEIS:** Dieses Beispiel stammt von einer Email Security — Server Edition Appliance, trifft aber auch auf Network Security Appliances zu.



Die Hostschlüssel-Zeichenfolge, die Sie von der Central Management Web-UI oder CLI erhalten haben, beginnt mit "1.1.1.5". Zum Beispiel:

```
1.1.1.5 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzd5JwKBjHLe/jxkF0JzWcXOTw9l0
bz2SctkQrihkqg/zXqrmxAfgbzYulDSIxOKZTh2VBnKsy0qRWrCps64Itlh6iRlr7Jxa+jAtTAGsy
...
```

Bevor Sie den Hostschlüssel in die Email Security — Server Edition globale Hostschlüssel-Datenbank importieren, müssen Sie "1.1.1.5" mit "3.3.3.5" ersetzen. Zum Beispiel:

```
3.3.3.5 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzd5JwKBjHLe/jxkF0JzWcXOTw9l0
bz2SctkQrihkqg/zXqrmxAfgbzYulDSIxOKZTh2VBnKsy0qRWrCps64Itlh6iRlr7Jxa+jAtTAGsy
...
```

# ANHANG C: Die NX Appliance konfigurieren, Datenverkehr von einem Spiegelport weiterzuleiten

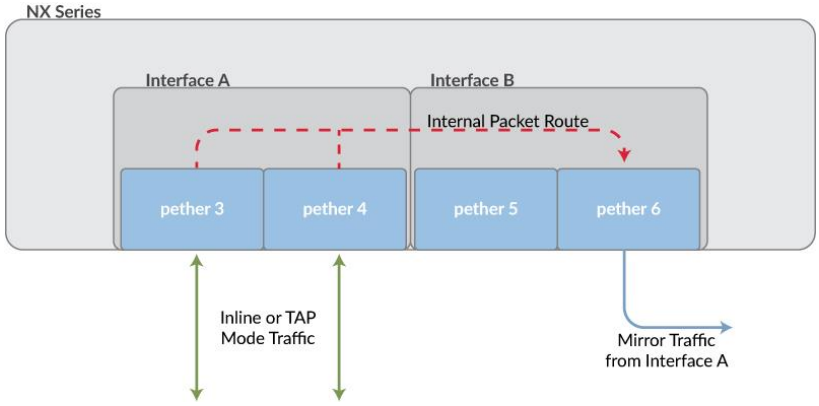
Sie können die Network Security Appliance als ein SPAN Gerät konfigurieren. In diesem Szenario leitet ein Network Security Überwachungsschnittstellenpaar eine Kopie des Netzwerkverkehrs, den es verarbeitet, an einen anderen Port auf der gleichen Appliance weiter, der als ein dedizierter SPAN- (oder *Spiegel*) Port konfiguriert ist. Der Spiegelport kann mit einem anderen Analysegerät verbunden werden, z.B. der Packet Capture Appliance. Mit Hilfe dieses Beispiels empfängt die Packet Capture Appliance den Verkehr vom Network Security Spiegelport und führt eine tiefere forensische Analyse aus den Paketen durch.

Das Schnittstellenpaar mit dem Spiegelport muss im Tap-Modus konfiguriert werden. Das Überwachungsschnittstellenpaar kann im Inline-Modus (Monitor- oder Blockierungsmodus) oder Tap-Modus konfiguriert werden. Im inline Blockiermodus wird aller Verkehr (einschließlich der blockierte Verkehr), auf das andere Analysegerät weitergeleitet.

**HINWEIS:** Wenn ein Schnittstellenpaar im Tap Modus konfiguriert ist, kann ein Port ein Überwachungsport und der andere Port ein Mirror Port sein. Allerdings kann der Überwachungsport seinen Verkehr nicht auf den Spiegelport in seinem eigenen Schnittstellenpaar weiterleiten.

Es besteht eine 1:1-Beziehung zwischen einem Spiegelport auf der Network Security Appliance und dem SPAN-Port auf dem empfangenden Gerät. Sie können mehrere Spiegelports auf der Network Security Appliance und mehrere SPAN-Ports auf dem empfangenden Gerät konfigurieren, aber jeder Network Security Spiegelport kann Verkehr nur auf einen SPAN-Port auf dem anderen Gerät weiterleiten.

Das folgende Diagramm zeigt den Verkehrsfluss in der Konfiguration einer Network Security Portspiegelung an. In diesem Beispiel spiegelt Interface A den Netzwerkverkehr auf pether6 und pether6 leiten den Verkehr an das andere Analysegerät weiter.




Beachten Sie Folgendes:

- Pakete werden verworfen, wenn sie nicht bearbeitet werden können. Pakete werden beispielsweise verworfen, wenn Sie Hardware- oder Medienfehler enthalten oder das Verkehrsvolumen die Kapazität des Spiegelports überschreitet.
- Übergroße Pakete (Pakete, die größer als 1700 Byte sind) und Jumbopakete können auf der Packet Capture Appliance gespiegelt werden. (Beachten Sie, dass die Network Security Appliance keine Erkennung und Analyse auf diesen Paketen durchführt.)

**HINWEIS:** Sie können eine Network Security Appliance nicht konfigurieren, sowohl Verkehr von einem Spiegelport, wie in diesem Thema beschrieben, weiterzuleiten und ein Mitglied eines Network Security High Availability (HA) Paars zu sein. (Details über Network Security HA finden Sie im *Network Security High-Availability Handbuch*.)

## Voraussetzungen

- Operator oder Admin Zugriff
- Mindestens zwei Schnittstellenpaare auf der Network Security Appliance
- Im Tap-Modus konfiguriertes Spiegelport-Schnittstellenpaar

# Die NX konfigurieren, Verkehr von einem Spiegelport mit Hilfe der CLI weiterzuleiten

Verwenden Sie die Befehle in diesem Abschnitt, um Portspiegelung zu konfigurieren.

**Um einen Spiegelport auf einer Schnittstelle zu konfigurieren:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Zeigen Sie die Schnittstellenkonfiguration an:

   ```
   hostname (config) # show policymgr interfaces
   ```

3. Wenn sich das Schnittstellenpaar mit dem Mirror-Port noch nicht im Tap-Modus befindet, ändern Sie es:

   ```
   hostname (config) # policymgr interface <interfacePair> op-mode tap
   hostname (config) # policymgr interface <interfacePair> re-configure
   ```

   wobei `<interfacePair>` die Kennzeichnung des Schnittstellenpaars ist.

4. Konfigurieren Sie den Spiegelport:

   ```
   hostname (config) # policymgr interface <interfacePair> mirror port
   <portName>
   ```

   wobei `<interfacePair>` das Schnittstellenpaar ist, von dem Verkehr weitergeleitet wird und `<portName>` der Port, der den gespiegelten Verkehr empfangen soll.

5. Bestätigen Sie Ihre Änderung:

   ```
   hostname (config) # show policymgr interfaces
   ```

6. Speichern Sie Ihre Änderung:

   ```
   hostname (config) # write memory
   ```

**HINWEIS:** Wenn Sie mehrere Spiegelports für das gleiche Schnittstellenpaar in der gleichen Sitzung konfigurieren, wird der letzte Port, den Sie konfigurieren, wirksam. Im folgenden Beispiel wird pether6 von pether9 überschrieben.

```
hostname (config) # policymgr interface A mirror port pether6
hostname (config) # policymgr interface A mirror port pether9
```

**Um einen Spiegelport von einer Schnittstelle zu löschen:**

1. Gehen Sie auf den CLI-Konfigurationsmodus.

   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Löschen Sie den Spiegelport:

   ```
   hostname (config) # policymgr interface <interfacePair> mirror clear
   ```

3. Bestätigen Sie Ihre Änderung:

   ```
   hostname (config) # show policymgr interfaces
   ```

4. Speichern Sie Ihre Änderung:

   ```
   hostname (config) # write memory
   ```

## Beispiele

Das folgende Beispiel zeigt die aktuellen Schnittstellenpaare und ihr Status an und konfiguriert dann pether6 auf Schnittstelle B als den Spiegelport für die Überwachung des Datenverkehrs auf Schnittstelle A.

```
hostname (config) # show policymgr interfaces

Policy enabled : yes

Interface A
  Active       : yes
  op mode      : monitor (permissive)
  fail-safe    : close
  policy       : mixed
  tolerance    : 1
  mirror-port  :
  Ports        : pether3 pether4
  QinQ         : no
  QinQ-evet    : 0x88a8

Interface B
  Active       : yes
  op-mode      : tap (tapping)
  fail-safe    : close
  policy       : mixed
  tolerance    : 1
  mirror-port  :
  Ports        : pether5 pether6
  QinQ         : no
  QinQ-evet    : 0x88a8

Interface C
  Active       : yes
  op mode      : tap (tapping)
  fail-safe    : close
  policy       : mixed
  tolerance    : 1
  mirror-port  :
  Ports        : pether7 pether8
  QinQ         : no
  QinQ-evet    : 0x88a8

Interface D
  Active       : yes
  op mode      : tap (tapping)
  fail-safe    : close
  policy       : mixed
  tolerance    : 1
  mirror-port  :
  Ports        : pether9 pether10
  QinQ         : no
  QinQ-evet    : 0x88a8

hostname (config) # policymgr interface A mirror port pether6
hostname (config) # show policymgr interfaces

Policy enabled : yes

Interface A
  Active       : yes
  op mode      : monitor (permissive)
```

```
  fail-safe    : close
  policy       : mixed
  tolerance    : 1
  mirror-port  : pether6
  Ports        : pether3 pether4
  QinQ         : no
  QinQ-evt     : 0x88a8
...
```

Das folgende Beispiel löscht Portspiegelung auf Schnittstelle A.

```
hostname (config) # policymgr interface A mirror clear
```

Das folgende Beispiel konfiguriert pether6 als den Spiegelport sowohl für Schnittstelle A als auch für Schnittstelle D.

```
hostname (config) # policymgr interface A mirror port pether6
hostname (config) # policymgr interface D mirror port pether6
```

Das folgende Beispiel konfiguriert pether6 als den Spiegelport für Schnittstelle A und pether9 als Spiegelport für Schnittstelle C.

```
hostname (config) # policymgr interface A mirror port pether6
hostname (config) # policymgr interface C mirror port pether9
```

# Technischer Support

Für technische Unterstützung wenden Sie sich an FireEye über das Support Portal:

https://csportal.fireeye.com

# Dokumentation

Dokumentation für alle FireEye Produkte ist im FireEye Dokumentationsportal (Anmeldung erforderlich) verfügbar.

https://docs.fireeye.com/

FireEye, Inc. | 601 McCarthy Blvd. | Milpitas, CA | 1.408.321.6300 | 1.877.FIREEYE | www.fireeye.com/company/contact-us.html