Erläutern der Dateianalyse-Client-ID für Gateway, Cloud Gateway sowie E-Mail und Web Manager

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die File Analysis Client-ID für Cisco Secure Email Gateway, Cloud Gateway und Email und Web Manager finden. Die File Analysis Client ID ist ein eindeutiger 65-Zeichen-Registrierungsschlüssel, der verwendet wird, wenn sich der Gateway, Cloud Gateway oder E-Mail- und Web-Manager bei Cisco Malware Analytics (ehemals Threat Grid) für die Einreichung von Dateien und das Sandboxing registriert. Wenn Sie z. B. den Dateianalysedienst aktiviert haben und der Reputationsdienst über keine Informationen zum Dateianhang in einer Nachricht verfügt, und der Dateianhang die Kriterien für Dateien erfüllt, die analysiert werden können (sieheUnterstützte Dateien für Dateireputations- und Analysedienste), kann die Nachricht in Quarantäne verschoben werden (sieheQuarantäne von Nachrichten mit zur Analyse gesendeten Anhängen) und die Datei zur Analyse gesendet werden.

Stellen Sie sicher, dass Sie Ihre Analyse-ID(s) für "Appliance Grouping for File Analysis Reporting" kennen.

Ausführliche Informationen finden Sie im Kapitel "File Reputation Filtering and File Analysis" im Benutzerhandbuch:

- Cisco Secure Email Gateway - Benutzerhandbücher

- Cisco Secure Email Cloud Gateway - Benutzerhandbücher

Dateianalyse-Client-ID für Gateway, Cloud-Gateway und E-Mail- und Web-Manager

Die Dateianalyse-Client-ID wird automatisch für Appliances generiert, wenn Sie die Dateianalyse aktivieren.

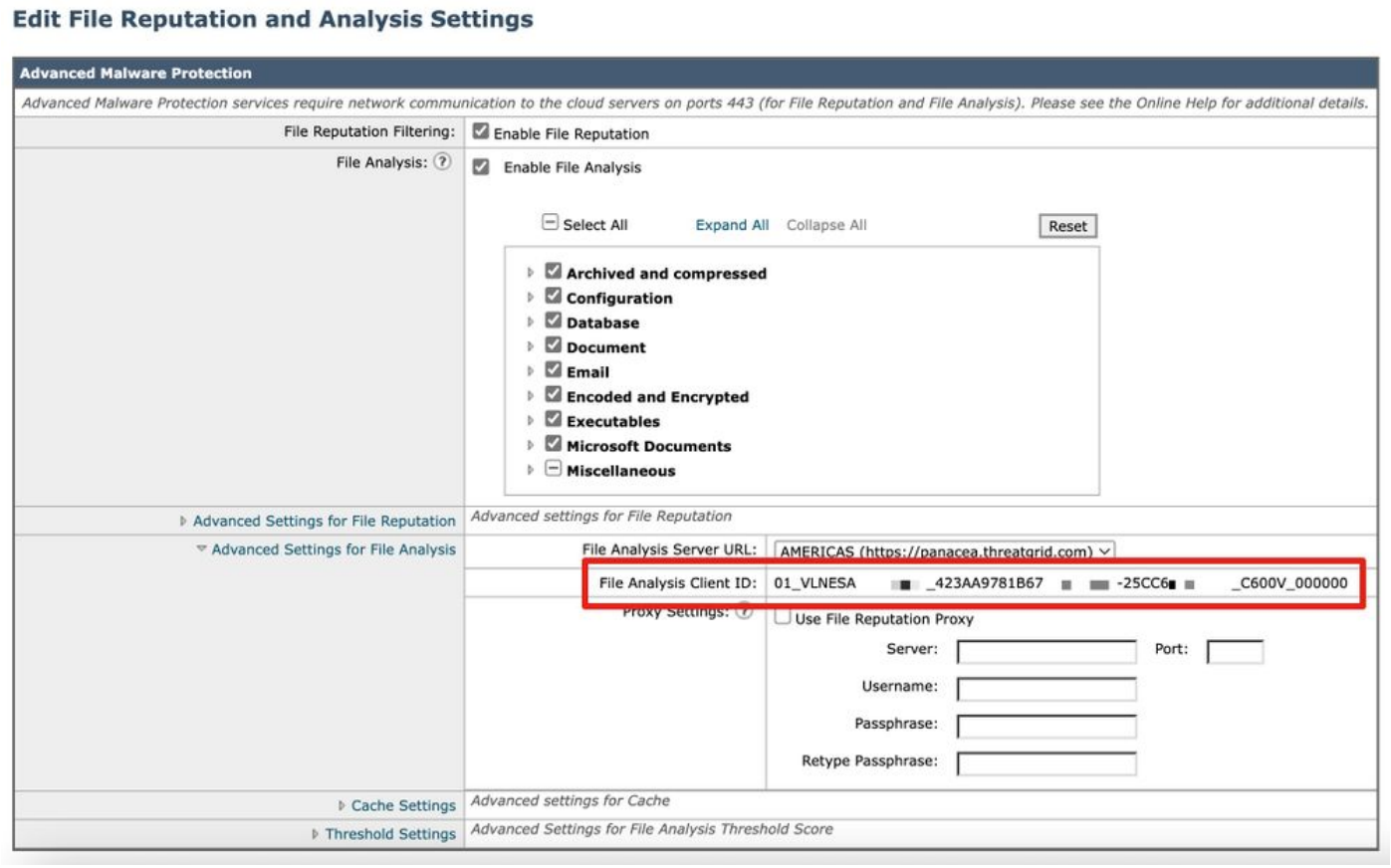
Bevor Sie mit dem Gateway oder Cloud Gateway beginnen, stellen Sie sicher, dass Sie über die erforderlichen Feature-Schlüssel verfügen und Dateireputation und Dateianalyse aktivieren. Um die Feature-Schlüssel anzuzeigen, navigieren Sie zu **Systemverwaltung > Feature-Schlüssel**. Dateireputation und Dateianalyse werden getrennt aufgeführt und haben den Status Aktiv.

Gateway oder Cloud Gateway

1. Melden Sie sich bei der Benutzeroberfläche an.
2. Navigieren Sie zu **Sicherheitsdienste > Dateireputation und -analyse**.
3. Klicken Sie auf **Globale Einstellungen bearbeiten...**
4. Erweitern Sie **Erweiterte Einstellungen für die Dateianalyse**.

Die File Analysis Client ID ist hier aufgelistet.

OBeispiel:



Anmerkung: Es besteht ein Unterschied zwischen der Dateianalyse-Client-ID für virtuelle Appliances und der der Hardware-Appliances.

Die Dateianalyse-Client-ID für das Gateway oder Cloud Gateway basiert auf einem 65 Zeichen langen Zeichenfolgenformat:

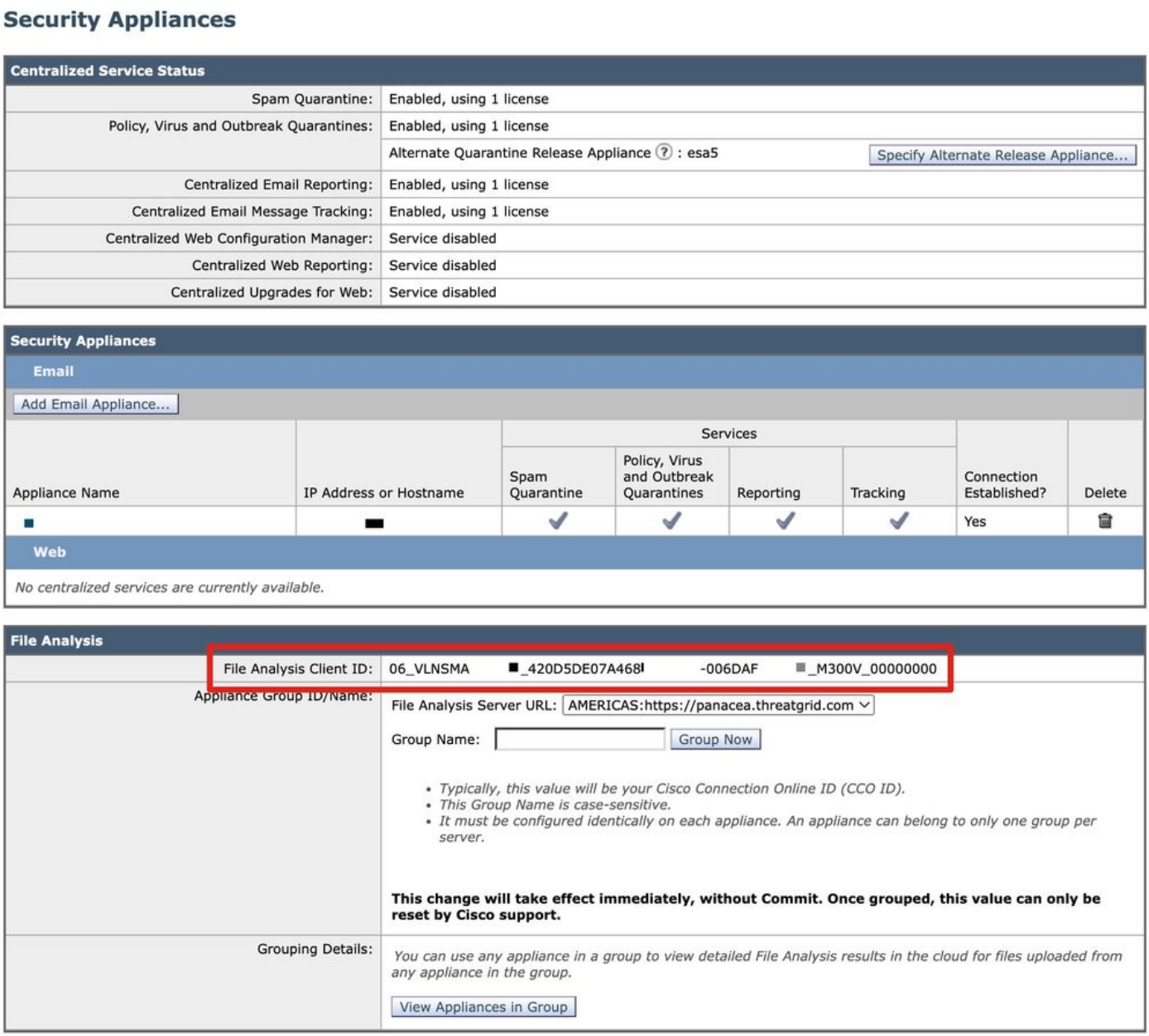
Wert	Erklärung
01_	"01" ist spezifisch für das Gateway oder Cloud Gateway.
VLNESAXXXYYY	Handelt es sich um eine virtuelle Appliance, wird die VLN-Lizenznummer verwendet (z finden über den CLI-Befehl **showlicense**). Wenn es sich um eine Hardware-Appliance handelt, ist kein Feld vorhanden.
SERIELL_	Volle serielle Schnittstelle der Appliance.
CX00V	Modell der Appliance.
00000000	Feldnullen. Basierend auf den vorherigen Feldern variieren diese, um das Feld mit 65 Zeichen zu beenden.

E-Mail- und Web-Manager

1. Melden Sie sich bei der Benutzeroberfläche an.
2. Navigieren Sie zu **Zentrale Verwaltung > Sicherheits-Appliance**.

Unten auf dieser Seite finden Sie den Abschnitt "Dateianalyse". Die File Analysis Client ID ist hier aufgelistet.

Beispiel:



Anmerkung: Es besteht ein Unterschied zwischen der Dateianalyse-Client-ID für virtuelle Appliances und der der Hardware-Appliances.

Die Dateianalyse-Client-ID für den E-Mail- und Web-Manager basiert auf einem 65 Zeichen langen Zeichenfolgenformat:

Wert	Erklärung
06_	"06" bezieht sich speziell auf den E-Mail- und Web-Manager.
VLNSMAXXXYYY_	Handelt es sich um eine virtuelle Appliance, wird die VLN-Lizenznummer verwendet (zu finden über den CLI-Befehl **showlicense**). Wenn es sich um eine Hardware-Appliance handelt, ist kein Feld vorhanden.
SERIELL_	Volle serielle Schnittstelle der Appliance.
MX00V	Modell der Appliance.
000000	Feldnullen. Basierend auf den vorherigen Feldern variieren diese, um das Feld mit 65 Zeichen zu beenden.

Appliance-Gruppierung für Berichte zur Dateianalyse

Wenn Ihre Lizenz den Zugriff auf Cisco Secure Malware Analytics (https://panacea.threatgrid.com) beinhaltet, besteht die Best Practice für Ihr Gateway oder Cloud Gateway darin, diese mit Ihrem individuellen Unternehmenskonto zu verknüpfen. Damit alle Content Security Appliances in Ihrer Organisation detaillierte Ergebnisse zu Dateien anzeigen können, die zur Analyse von einem Gateway oder Cloud Gateway in Ihrer Organisation gesendet wurden, müssen Sie alle Appliances derselben Appliancegruppe angehören. Wenn Sie sich bei Malware Analytics anmelden, werden Ihre Eingaben und Bedrohungsbeispiele, die zur Analyse an die Cloud gesendet werden, im Dashboard für Malware Analytics für Ihr Unternehmen angezeigt.

Anmerkung: Cloud Gateway-Kunden haben dies bei Aktivierungen und Bereitstellungen durch Cisco konfiguriert.

Gruppen-Appliances

Anmerkung: Wenn Sie über ein Cloud Gateway verfügen und dieser Vorgang nicht abgeschlossen ist, öffnen Sie ein Support-Ticket, bevor Sie eine Appliance-Gruppen-ID/-Name konfigurieren.

Gateway oder Cloud Gateway

1. Navigieren Sie auf der Benutzeroberfläche zu **Sicherheitsdienste > Dateireputation und -analyse**.
2. Klicken Sie auf **Klicken Sie hier, um Appliances für das Reporting zur Dateianalyse zu gruppieren oder anzuzeigen**.
3. Geben Sie Ihre **Appliance-Gruppen-ID/-Name ein**. Die Standardwerte sind: Es wird empfohlen, für diesen Wert Ihre CCO-ID zu verwenden.Eine Appliance kann nur einer Gruppe angehören.Nach der Konfiguration der Dateianalyse-Funktion können Sie einen Computer einer Gruppe hinzufügen.
4. Klicken Sie auf **Jetzt gruppieren**.

E-Mail- und Web-Manager

Anmerkung: Die Option zur Konfiguration einer Appliance-Gruppen-ID/-Name ist nur verfügbar, nachdem dem E-Mail- und Web-Manager eine E-Mail-Appliance für zentralisierte Verwaltungszwecke hinzugefügt wurde und die Richtlinien-, Virus- und Outbreak-Quarantänen migriert wurden.

1. Navigieren Sie von der Benutzeroberfläche zu **Centralized Services > Security Appliances**. Geben Sie Ihre **Appliance-Gruppen-ID/-Name ein**. Die Standardwerte sind:Normalerweise ist dieser Wert Ihre Cisco Connection Online ID (CCO ID).Bei diesem Gruppennamen wird die Groß-/Kleinschreibung berücksichtigt.Sie muss auf jeder Appliance identisch konfiguriert sein. Eine Appliance kann nur einer Gruppe pro Server angehören.
2. Klicken Sie auf **Jetzt gruppieren**.

Hinweis:

- Wenn Sie eine Gruppen-ID hinzufügen, wird diese sofort und ohne Commit aktiviert. Wenn Sie eine Gruppen-ID ändern müssen, wenden Sie sich an Cisco TAC.
- Bei diesem Namen wird die Groß-/Kleinschreibung berücksichtigt, und er muss auf jeder Appliance in der Analysegruppe identisch konfiguriert werden.

Appliances anzeigen

Gateway oder Cloud Gateway

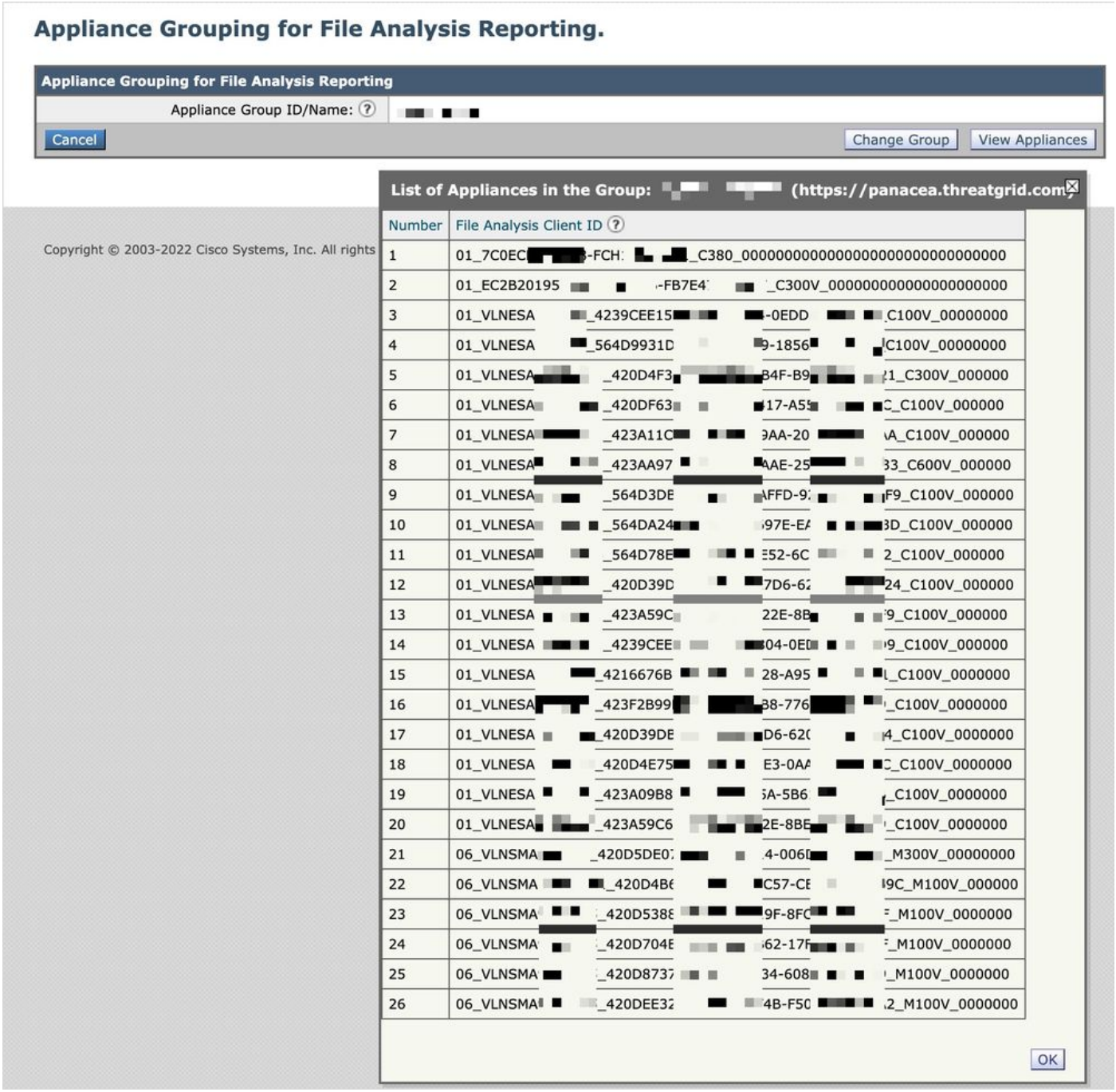
1. Navigieren Sie auf der Benutzeroberfläche zu **Sicherheitsdienste > Dateireputation und -analyse.**
2. Klicken Sie auf **Klicken Sie hier, um Appliances für das Reporting zur Dateianalyse zu gruppieren oder anzuzeigen**.
3. Klicken Sie auf **Einheiten anzeigen**.

E-Mail- und Web-Manager

1. Navigieren Sie von der Benutzeroberfläche zu **Centralized Services > Security Appliances**.
2. Klicken Sie im Abschnitt "Dateianalyse" auf **Einheiten** in **Gruppe anzeigen**.

Die Dateianalyse-Client-ID aller Appliances, die mit der Appliance-Gruppen-ID bzw. dem Appliance-Namen verknüpft sind, werden hier aufgeführt.

Beispiel:



Zusätzliche Informationen

Cisco Secure Email Gateway-Dokumentation

- Versionshinweise
- Benutzerhandbuch
- CLI-Referenzhandbuch
- API-Programmierhandbücher für Cisco Secure Email Gateway
- Open Source für Cisco Secure Email Gateway
- Installationsanleitung für die Cisco Content Security Virtual Appliance (mit vESA)

Secure Email Cloud Gateway - Dokumentation

- Versionshinweise
- Benutzerhandbuch

Cisco Secure Email und Web Manager-Dokumentation

- Versionshinweise und Kompatibilitätsmatrix
- Benutzerhandbuch
- API-Programmierhandbücher für Cisco Secure Email und Web Manager
- Cisco Content Security Virtual Appliance Installationshandbuch (einschl. vSMA)

Cisco Secure Malware Analytics

- Cisco Secure Malware Analytics (Threat Grid)

Cisco Secure-Produktdokumentation

- Cisco Secure Portfolio Naming Architecture

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.