

Uitleggen van de client-id voor bestandsanalyse voor gateway, cloudgateway en e-mail- en webbeheer

Inhoud

[Inleiding](#)

[Client ID voor bestandsanalyse voor gateway, cloudgateway en e-mail- en webbeheer](#)

[Gateway voor cloudgateway](#)

[E-mail- en webbeheer](#)

[Applicatiegroepering voor rapportage van bestandanalyse](#)

[Groepsapplicaties](#)

[Gateway voor cloudgateway](#)

[E-mail- en webbeheer](#)

[Applicaties bekijken](#)

[Gateway voor cloudgateway](#)

[E-mail- en webbeheer](#)

[Aanvullende informatie](#)

[Cisco Secure E-mail gateway-documentatie](#)

[Documentatie voor beveiligde e-mail met Cloud Gateway](#)

[Cisco Secure Email en Web Manager-documentatie](#)

[Cisco Secure Malware-analyses](#)

[Cisco beveiligde productdocumentatie](#)

Inleiding

Dit document beschrijft hoe u de client-ID voor bestandanalyse kunt vinden voor Cisco Secure Email Gateway, Cloud Gateway en Email and Web Manager. De client-ID voor bestandsanalyse is een unieke registratiesleutel van 65 tekens die wordt gebruikt wanneer de Gateway, Cloud Gateway of Email and Web Manager zich registreert bij Cisco Malware Analytics (voorheen Threat Grid) voor het indienen en sandboxen van bestanden. Als u bijvoorbeeld de service Bestandsanalyse hebt ingeschakeld en de reputatieservice geen informatie heeft over de bestandsbijlage die in een bericht is gevonden, en de bestandsbijlage voldoet aan de criteria voor bestanden die kunnen worden geanalyseerd ([zie Ondersteunde bestanden voor bestandsreputatie- en analyseservices](#)), kan het bericht in quarantaine worden geplaatst ([zie Berichten in quarantaine plaatsen met bijlagen die voor analyse worden verzonden](#)), en kan het bestand voor analyse worden verzonden.

Bij "Applicatie Groepering voor Rapportage van Bestandsanalyse" dient u er zeker van te zijn dat u uw Bestandsanalyse-ID(en) kent.

Raadpleeg het hoofdstuk "Bestandsreputatie filtering en bestandsanalyse" van de gebruikershandleiding voor volledige informatie:

- [Cisco Secure Email Gateway-eindgebruikershandleidingen](#)

- [Cisco Secure Email Cloud Gateway-eindgebruikershandleidingen](#)

Client ID voor bestandsanalyse voor gateway, cloudgateway en e-mail- en webbeheer

De client-ID voor bestandsanalyse wordt automatisch gegenereerd voor toestellen wanneer u File Analysis inschakelt.

Zorg ervoor dat u over de benodigde functietoetsen en de bestandsreputatie en bestandsanalyse beschikt voordat u begint met de Gateway of Cloud Gateway. Om de functietoetsen te zien, navigeer u naar **Systeembeheer > Functietoetsen**. Bestandsreputatie en bestandsanalyse worden afzonderlijk vermeld en hebben de actieve status.

Gateway voor cloudgateway

1. Log in op de gebruikersinterface.
2. Ga naar **Security Services > Bestandsreputatie en -analyse**.
3. Klik op **Wereldwijde instellingen bewerken...**
4. Breid **geavanceerde instellingen voor bestandanalyse uit**.

De client-ID voor bestandanalyse wordt hier vermeld.

E Voorbeeld:

Edit File Reputation and Analysis Settings

Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 443 (for File Reputation and File Analysis). Please see the Online Help for additional details.

File Reputation Filtering: Enable File Reputation

File Analysis: Enable File Analysis

Select All Expand All Collapse All Reset

- Archived and compressed
- Configuration
- Database
- Document
- Email
- Encoded and Encrypted
- Executables
- Microsoft Documents
- Miscellaneous

Advanced settings for File Reputation

Advanced Settings for File Analysis

File Analysis Server URL: AMERICAS (https://panacea.threatgrid.com)

File Analysis Client ID: 01_VLNESA _423AA9781B67 -25CC6 _C600V_000000

Proxy Settings: Use File Reputation Proxy

Server: Port:

Username:

Passphrase:

Retype Passphrase:

Advanced settings for Cache

Advanced Settings for File Analysis Threshold Score

Opmerking: Er is een verschil in de File Analysis Client ID voor virtuele apparaten versus hardware-apparaten.

De client-id voor bestandsanalyse voor de gateway of cloudgateway is gebaseerd op een tekenreeksindeling van 65 tekens:

Waarde	Uitleg
01_	"01" is specifiek voor de gateway of cloudgateway.
VLNESAXXYYYY_	Als dit een virtueel apparaat is, gebruikt het de VLN-licentie # (gevonden bij de CLI-opdrachtshowlicentie). Als dit een hardware-apparaat is, is er geen veld.
SERIEEL_	VOLLEDIG serienummer van het apparaat.
CX200V_	Model van het apparaat.
00000000	Veldnullen. Gebaseerd op de vorige velden, variëren deze om het veld van 65 tekens ronden.

E-mail- en webbeheer

1. Log in op de gebruikersinterface.
2. Ga naar **Gecentraliseerd beheer > Security applicatie**.

Onderaan deze pagina staat de sectie Bestandsanalyse. De client-ID voor bestandanalyse wordt hier vermeld.

Voorbeeld:

Security Appliances

Centralized Service Status	
Spam Quarantine:	Enabled, using 1 license
Policy, Virus and Outbreak Quarantines:	Enabled, using 1 license
	Alternate Quarantine Release Appliance (?) : esa5 Specify Alternate Release Appliance...
Centralized Email Reporting:	Enabled, using 1 license
Centralized Email Message Tracking:	Enabled, using 1 license
Centralized Web Configuration Manager:	Service disabled
Centralized Web Reporting:	Service disabled
Centralized Upgrades for Web:	Service disabled

Security Appliances							
Email							
Add Email Appliance...							
Appliance Name	IP Address or Hostname	Services				Connection Established?	Delete
		Spam Quarantine	Policy, Virus and Outbreak Quarantines	Reporting	Tracking		
■	■	✓	✓	✓	✓	Yes	🗑️
Web							
No centralized services are currently available.							

File Analysis	
File Analysis Client ID:	06_VLNSMA ■_420D5DE07A468! -006DAF ■_M300V_00000000
Appliance Group ID/Name:	File Analysis Server URL: <input type="text" value="AMERICAS:https://panacea.threatgrid.com"/> Group Name: <input type="text"/> Group Now <ul style="list-style-type: none"> Typically, this value will be your Cisco Connection Online ID (CCO ID). This Group Name is case-sensitive. It must be configured identically on each appliance. An appliance can belong to only one group per server. <p>This change will take effect immediately, without Commit. Once grouped, this value can only be reset by Cisco support.</p>
Grouping Details:	You can use any appliance in a group to view detailed File Analysis results in the cloud for files uploaded from any appliance in the group. View Appliances in Group

Opmerking: Er is een verschil in de File Analysis Client ID voor virtuele apparaten versus hardware-apparaten.

De client-id voor bestandsanalyse voor e-mail en webbeheer is gebaseerd op een tekenreeksindeling van 65 tekens:

Waarde	Uitleg
06_	"06" is specifiek voor de Email en Web Manager.
VLNSMAXXXYY	Als dit een virtueel apparaat is, gebruikt het de VLN-licentie # (gevonden bij de CLI-opdrachtshowlicentie). Als dit een hardware-apparaat is, is er geen veld.
SERIEEL_	VOLLEDIG serienummer van het apparaat.
MX200V_	Model van het apparaat.
000000	Veldnullen. Gebaseerd op de vorige velden, variëren deze om het veld van 65 tekens a

Applicatiegroepering voor rapportage van bestandanalyse

Als uw licentie toegang tot Cisco Secure Malware Analytics (<https://panacea.threatgrid.com>) omvat, is het de beste praktijk voor uw Gateway of Cloud Gateway om deze aan uw individuele organisatieaccount te koppelen. Om alle content security applicaties in uw organisatie in staat te stellen om gedetailleerde resultaten in de cloud weer te geven over bestanden die voor analyse worden verzonden vanaf elke Gateway of Cloud Gateway in uw organisatie, moet u alle applicaties bij dezelfde apparaatgroep aansluiten. Wanneer u zich aanmeldt bij Malware Analytics, worden uw inzendingen en bedreigingsmonsters die naar de cloud worden gestuurd voor analyse allemaal weergegeven in het Malware Analytics-dashboard voor uw organisatie.

Opmerking: Cloudgateway-klienten hebben dit ingesteld tijdens activeringen en implementaties die door Cisco worden uitgevoerd.

Groepsapplicaties

Opmerking: Als u een Cloud Gateway hebt en dit is niet voltooid, opent u een [ondersteuningscase](#) voordat u een applicatie-groep-id/naam configureert.

Gateway voor cloudgateway

1. Ga vanuit de gebruikersinterface naar **Security Services > File Reputation and Analysis**.
2. Klik op **Klik hier om applicaties te groeperen of weer te geven voor File Analysis rapportage**.
3. Voer uw **apparaatgroep-id/naam** in. De standaardwaarden zijn: Aanbevolen wordt om uw CCOID voor deze waarde te gebruiken. Een apparaat kan tot slechts één groep behoren. Nadat u de functie Bestandsanalyse hebt geconfigureerd, kunt u een machine aan een groep toevoegen.
4. Klik nu op **Groep**.

E-mail- en webbeheer

Opmerking: De optie voor het configureren van een Applicatie Groep ID/Naam is alleen

beschikbaar nadat de E-mail en Web Manager een E-mail applicatie heeft toegevoegd voor gecentraliseerde beheerdoeleinden en het Beleid, Virus, Uitbraak Quarantines heeft gemigreerd.

1. Ga vanuit de gebruikersinterface naar **Gecentraliseerde services > Security applicaties**. Voer uw **apparaatgroep-id/naam** in. De standaardwaarden zijn: Meestal is deze waarde uw Cisco Connection Online ID (CCO-id). Deze groepsnaam is hoofdlettergevoelig. Het moet op elk apparaat identiek worden geconfigureerd. Een apparaat kan tot slechts één groep per server behoren.
2. Klik nu op **Groep**.

Let op:

- Wanneer u een groep-ID toevoegt, wordt het onmiddellijk van kracht, zonder een commit. Als u een groep-ID moet wijzigen, moet u contact opnemen met Cisco TAC.
- Deze naam is hoofdlettergevoelig en moet op elk apparaat in de analysegroep identiek worden geconfigureerd.

Applicaties bekijken

Gateway voor cloudgateway

1. Navigeer vanuit de gebruikersinterface naar **Security Services > File Reputation and Analysis**.
2. Klik op **Klik hier om applicaties te groeperen of weer te geven voor File Analysis rapportage**.
3. Klik op **Applicaties bekijken**.

E-mail- en webbeheer

1. Ga vanuit de gebruikersinterface naar **Gecentraliseerde services > Security applicaties**.
2. Klik op **Toepassingen in groep bekijken** in het gedeelte Bestandsanalyse.

De client-ID voor bestandsanalyse van alle apparaten die bij de applicatiegroep-id/naam zijn aangesloten, wordt hier vermeld.

Voorbeeld:

Appliance Grouping for File Analysis Reporting.

Appliance Grouping for File Analysis Reporting

Appliance Group ID/Name: [?] [] [] []

Cancel Change Group View Appliances

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved.

List of Appliances in the Group: [] [] [] (https://panacea.threatgrid.com)

Number	File Analysis Client ID
1	01_7C0EC []-FCH: []_C380_00000000000000000000000000000000
2	01_EC2B20195 [] -FB7E4 []_C300V_00000000000000000000000000
3	01_VLNESA []_4239CEE15 [] -0EDD []_C100V_00000000
4	01_VLNESA []_564D9931D [] -9-1856 []_C100V_00000000
5	01_VLNESA []_420D4F3 [] -B4F-B9 []_C100V_00000000
6	01_VLNESA []_420DF63 [] -17-A5 []_C100V_00000000
7	01_VLNESA []_423A11C [] -9AA-20 []_C100V_00000000
8	01_VLNESA []_423AA97 [] -AAE-25 []_C600V_00000000
9	01_VLNESA []_564D3DE [] -AFFD-9 []_C100V_00000000
10	01_VLNESA []_564DA24 [] -97E-EA []_C100V_00000000
11	01_VLNESA []_564D78E [] -E52-6C []_C100V_00000000
12	01_VLNESA []_420D39D [] -7D6-62 []_C100V_00000000
13	01_VLNESA []_423A59C [] -22E-8B []_C100V_00000000
14	01_VLNESA []_4239CEE [] -04-0E []_C100V_00000000
15	01_VLNESA []_4216676B [] -28-A95 []_C100V_00000000
16	01_VLNESA []_423F2B99 [] -38-776 []_C100V_00000000
17	01_VLNESA []_420D39DE [] -D6-62 []_C100V_00000000
18	01_VLNESA []_420D4E75 [] -E3-0AA []_C100V_00000000
19	01_VLNESA []_423A09B8 [] -5A-5B6 []_C100V_00000000
20	01_VLNESA []_423A59C6 [] -2E-8BE []_C100V_00000000
21	06_VLNSMA []_420D5DE0 [] -4-006 []_M300V_00000000
22	06_VLNSMA []_420D4B [] -C57-CE []_M100V_00000000
23	06_VLNSMA []_420D538E [] -9F-8FC []_M100V_00000000
24	06_VLNSMA []_420D704E [] -62-17F []_M100V_00000000
25	06_VLNSMA []_420D8737 [] -34-608 []_M100V_00000000
26	06_VLNSMA []_420DEE32 [] -4B-F5C []_M100V_00000000

OK

Aanvullende informatie

Cisco Secure E-mail gateway-documentatie

- [Release-opmerkingen](#)
- [Gebruikershandleiding](#)
- [CLI-referentiegids](#)
- [API-programmeerhandleidingen voor Cisco Secure Email Gateway](#)
- [Open bron die in Cisco Secure Email Gateway wordt gebruikt](#)
- [Installatiehandleiding voor Cisco Content Security virtuele applicatie \(inclusief vESA\)](#)

Documentatie voor beveiligde e-mail met Cloud Gateway

- [Release-opmerkingen](#)
- [Gebruikershandleiding](#)

Cisco Secure Email en Web Manager-documentatie

- [Releaseopmerkingen en compatibiliteitsmatrix](#)
- [Gebruikershandleiding](#)
- [API-programmeerhandleidingen voor Cisco Secure Email and Web Manager](#)
- [Installatiehandleiding voor Cisco Content Security virtuele applicatie](#) (inclusief vSMA)

Cisco Secure Malware-analyses

- [Cisco Secure Malware Analytics \(Threat Grid\)](#)

Cisco beveiligde productdocumentatie

- [Cisco Secure-portfolio-naamgevingsarchitectuur](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.