Explain the File Analysis Client ID for Gateway, Cloud Gateway, and Email and Web Manager

Contents

Introduction
File Analysis Client ID for Gateway, Cloud Gateway, and Email and Web Manager
Gateway or Cloud Gateway
Email and Web Manager
Appliance Grouping for File Analysis Reporting
Group Appliances
Gateway or Cloud Gateway
Email and Web Manager
View Appliances
Gateway or Cloud Gateway
Email and Web Manager
Additional Information
Cisco Secure Email Gateway Documentation
Secure Email Cloud Gateway Documentation
Cisco Secure Email and Web Manager Documentation
Cisco Secure Malware Analytics
Cisco Secure Product Documentation

Introduction

This document describes how to find the File Analysis Client ID for Cisco Secure Email Gateway, Cloud Gateway, and Email and Web Manager. The File Analysis Client ID is a unique 65-character registration key used when the Gateway, Cloud Gateway, or Email and Web Manager registers with Cisco Malware Analytics (formerly Threat Grid) for file submission and sandboxing. For example, if you have enabled the File Analysis service, and the reputation service has no information about the file attachment found in a message, and the file attachment meets the criteria for files that can be analyzed (seeSupported Files for File Reputation and Analysis Services), then the message can be quarantined (seeQuarantining Messages with Attachments Sent for Analysis), and the file sent for analysis.

For "Appliance Grouping for File Analysis Reporting," please be sure you know your File Analysis ID(s).

For complete details, please see the "File Reputation Filtering and File Analysis" chapter of the User Guide:

- Cisco Secure Email Gateway End User Guides
- Cisco Secure Email Cloud Gateway End-User Guides

File Analysis Client ID for Gateway, Cloud Gateway, and Email and Web Manager

The File Analysis Client ID is automatically generated for appliances when you enable File Analysis.

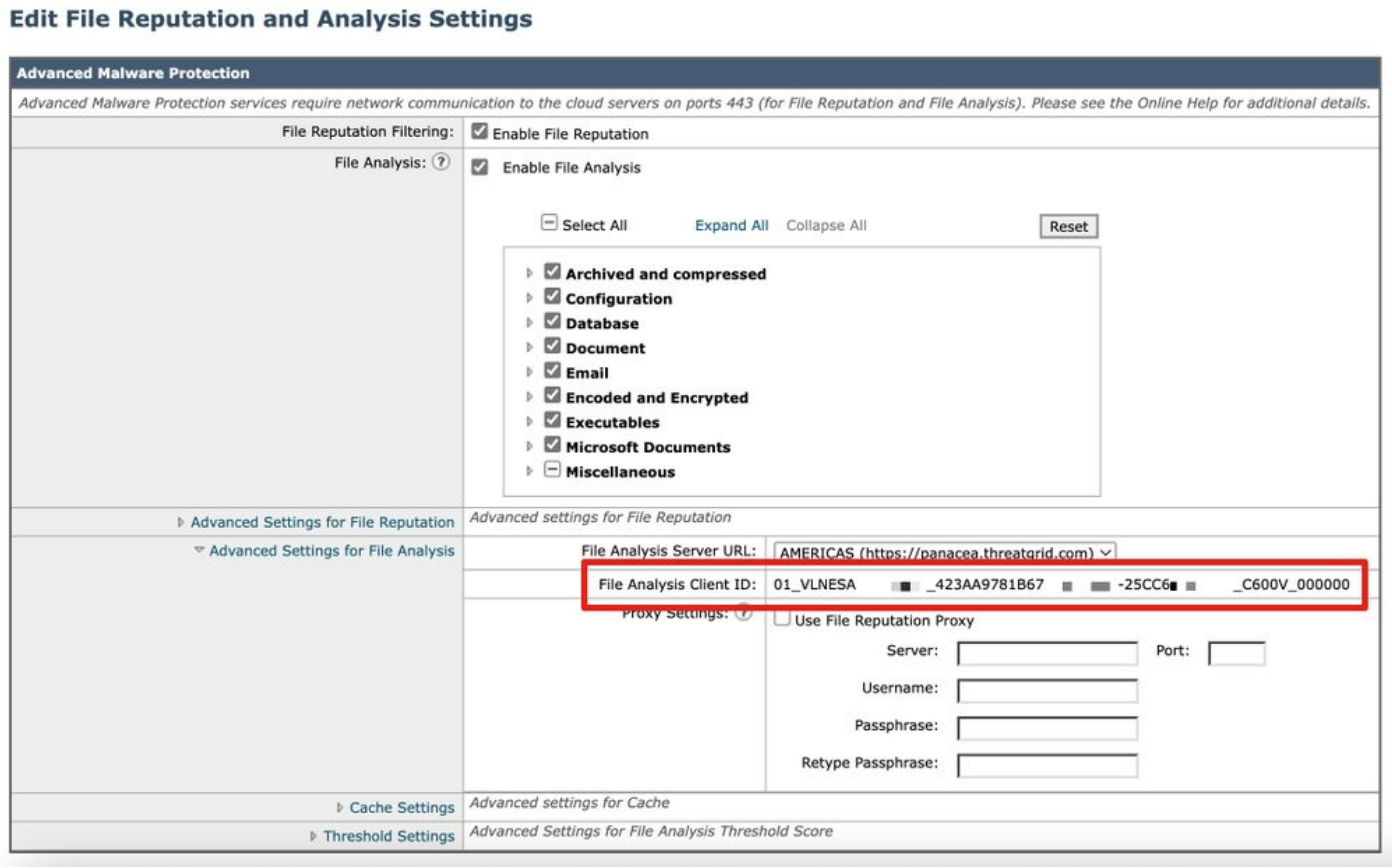
Before you begin from the Gateway or Cloud Gateway, please ensure you have the needed feature keys and enabled File Reputation and File Analysis. To see your feature keys, navigate to **System Administration > Feature Keys**. File Reputation and File Analysis are listed separately and have Active status.

Gateway or Cloud Gateway

1. Log in to the user interface.
2. Navigate to **Security Services > File Reputation and Analysis**.
3. Click **Edit Global Settings…**
4. Expand **Advanced Settings for File Analysis**.

The File Analysis Client ID is listed here.

Example:



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 Reputation*

Advanced Settings for File Analysis:

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

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

Proxy Settings: □ Use File Reputation Proxy

Server: Port:

Username:

Passphrase:

Retype Passphrase:

Cache Settings: *Advanced settings for Cache*

Threshold Settings: *Advanced Settings for File Analysis Threshold Score*

Note: There is a difference in the File Analysis Client ID for virtual appliances vs. hardware appliances.

The File Analysis Client ID for the Gateway or Cloud Gateway is based on a 65-character string format:

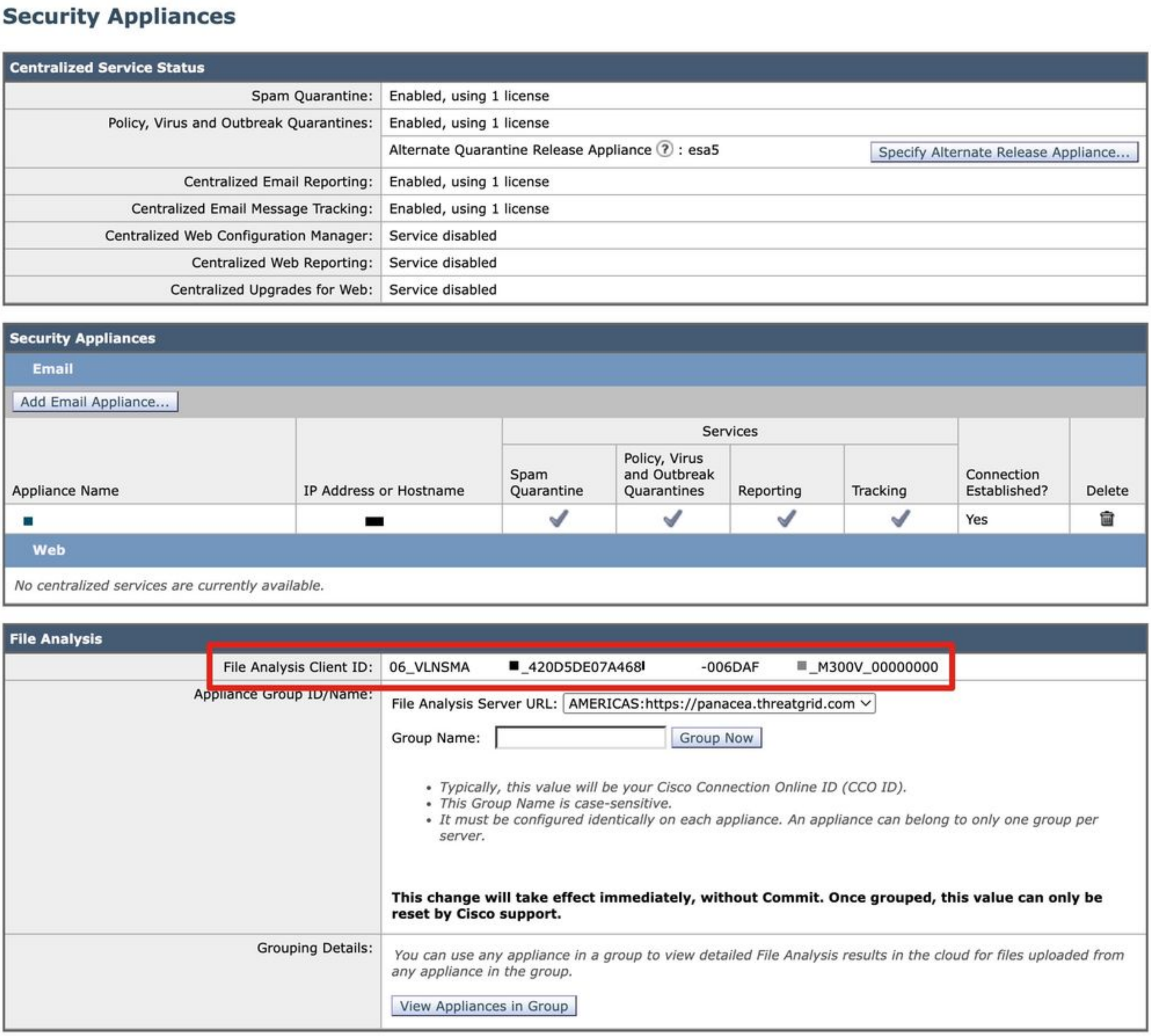
Value	Explanation
01_	"01" is specific to the Gateway or Cloud Gateway.
VLNESAXXXYYY_	If this is a virtual appliance, it uses the VLN license # (found from the CLI command **showlicense**). If this is a hardware appliance, there is no field.
SERIAL_	FULL serial of the appliance.
CX00V_	Model of the appliance.
00000000	Field zeros. Based on the previous fields, these vary to finish out the field of 65 chara

Email and Web Manager

1. Log in to the user interface.
2. Navigate to **Centralized Management > Security Appliance**.

At the bottom of this page is the File Analysis section. The File Analysis Client ID is listed here.

Example:



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...

		Services					
Appliance Name	IP Address or Hostname	Spam Quarantine	Policy, Virus and Outbreak Quarantines	Reporting	Tracking	Connection Established?	Delete
[redacted]	[redacted]	✓	✓	✓	✓	Yes	🗑

Web

No centralized services are currently available.

File Analysis	
File Analysis Client ID:	06_VLNSMA [redacted] _420D5DE07A468 [redacted] -006DAF [redacted] _M300V_00000000
Appliance Group ID/Name:	File Analysis Server URL: AMERICAS:https://panacea.threatgrid.com Group Name: Group Now • *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.* **This change will take effect immediately, without Commit. Once grouped, this value can only be reset by Cisco support.**
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

Note: There is a difference in the File Analysis Client ID for virtual appliances vs. hardware appliances.

The File Analysis Client ID for the Email and Web Manager is based on a 65-character string format:

Value	Explanation
06_	"06" is specific to the Email and Web Manager.
VLNSMAXXXYYY_	If this is a virtual appliance, it uses the VLN license # (found from the CLI command **showlicense**). If this is a hardware appliance, there is no field.
SERIAL_	FULL serial of the appliance.
MX00V_	Model of the appliance.
000000	Field zeros. Based on the previous fields, these vary to finish out the field of 65 characte

Appliance Grouping for File Analysis Reporting

If your license includes access to Cisco Secure Malware Analytics (https://panacea.threatgrid.com), the best practice for your Gateway or Cloud Gateway is to have them associated with your individual organization account. To allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Gateway or Cloud Gateway in your organization, you need to join all appliances to the same appliance group. When you log in to Malware Analytics, your submissions and threat samples sent to the cloud for analysis are all displayed in the Malware Analytics dashboard for your organization.

> **Note**: Cloud Gateway customers have this configured during activations and deployment performed by Cisco.

Group Appliances

> **Note**: If you have a Cloud Gateway and this is not completed, please open a support case before you configure an Appliance Group ID/Name.

Gateway or Cloud Gateway

1. From the user interface, navigate to **Security Services > File Reputation and Analysis**.
2. Click on **Click here to group or view appliances for File Analysis reporting**.
3. Enter your **Appliance Group ID/Name**. The default values are: It is suggested to use your CCOID for this value.An appliance can belong to only one group.After you configure the File Analysis feature, you can add a machine to a group.
4. Click **Group Now**.

Email and Web Manager

> **Note**: The option to configure an Appliance Group ID/Name is only available after the Email and Web Manager has an Email Appliance added for centralized management purposes and

has the Policy, Virus, Outbreak Quarantines migrated.

1. From the user interface, navigate to **Centralized Services > Security Appliances**. Enter your **Appliance Group ID/Name**. The default values are:Typically, this value is 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.
2. Click **Group Now**.

Please note:

- When you add a Group ID, it takes effect immediately, without a commit. If you need to change a Group ID, you must contact Cisco TAC.
- This name is case-sensitive and must be configured identically on each appliance in the Analysis Group.

View Appliances

Gateway or Cloud Gateway

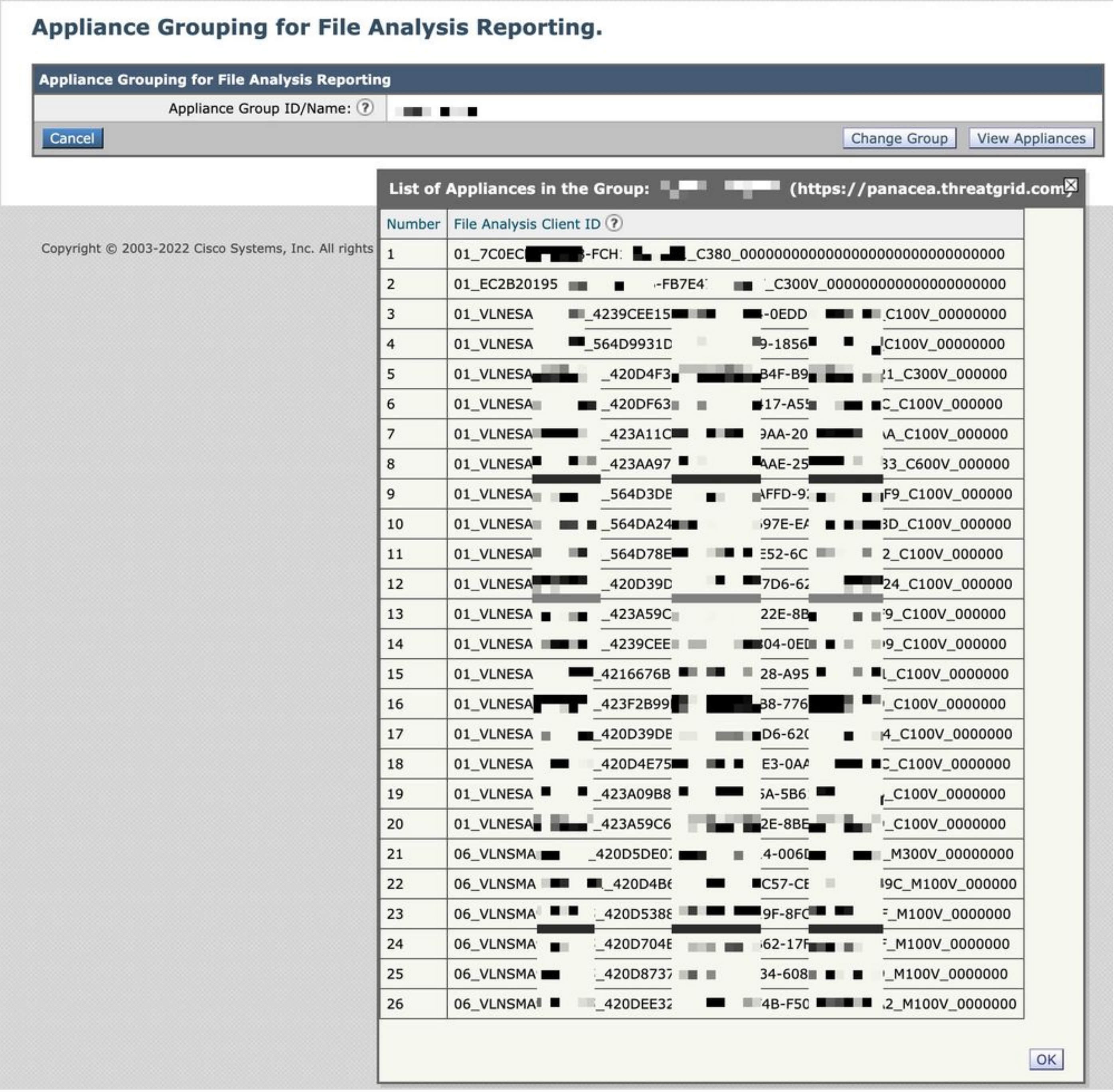
1. From the user interface, navigate to **Security Services > File Reputation and Analysis.**
2. Click on **Click here to group or view appliances for File Analysis reporting**.
3. Click on **View Appliances**.

Email and Web Manager

1. From the user interface, navigate to **Centralized Services > Security Appliances**.
2. Click on **View Appliances in Group** in the File Analysis section.

The File Analysis Client ID of all appliances associated with the Appliance Group ID/Name are listed here.

Example:



Appliance Grouping for File Analysis Reporting.

Appliance Grouping for File Analysis Reporting

Appliance Group ID/Name: [redacted]

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

Number	File Analysis Client ID
1	01_7C0EC[redacted]-FCH[redacted]_C380_00000000000000000000000000000000
2	01_EC2B20195[redacted]-FB7E4[redacted]_C300V_000000000000000000000
3	01_VLNESA[redacted]_4239CEE15[redacted]-0EDD[redacted]C100V_00000000
4	01_VLNESA[redacted]_564D9931D[redacted]9-1856[redacted]C100V_00000000
5	01_VLNESA[redacted]_420D4F3[redacted]B4F-B9[redacted]1_C300V_000000
6	01_VLNESA[redacted]_420DF63[redacted]17-A5[redacted]_C100V_000000
7	01_VLNESA[redacted]_423A11C[redacted]AA-20[redacted]A_C100V_000000
8	01_VLNESA[redacted]_423AA97[redacted]AAE-25[redacted]33_C600V_000000
9	01_VLNESA[redacted]_564D3DE[redacted]AFFD-9[redacted]F9_C100V_000000
10	01_VLNESA[redacted]_564DA24[redacted]97E-E[redacted]3D_C100V_000000
11	01_VLNESA[redacted]_564D78E[redacted]52-6C[redacted]2_C100V_000000
12	01_VLNESA[redacted]_420D39D[redacted]7D6-6[redacted]24_C100V_000000
13	01_VLNESA[redacted]_423A59C[redacted]22E-8B[redacted]9_C100V_000000
14	01_VLNESA[redacted]_4239CEE[redacted]04-0E[redacted]9_C100V_000000
15	01_VLNESA[redacted]_4216676B[redacted]28-A95[redacted]_C100V_0000000
16	01_VLNESA[redacted]_423F2B99[redacted]38-776[redacted]_C100V_0000000
17	01_VLNESA[redacted]_420D39DE[redacted]D6-62[redacted]4_C100V_0000000
18	01_VLNESA[redacted]_420D4E75[redacted]E3-0A[redacted]_C100V_0000000
19	01_VLNESA[redacted]_423A09B8[redacted]A-5B6[redacted]_C100V_0000000
20	01_VLNESA[redacted]_423A59C6[redacted]2E-8BE[redacted]_C100V_0000000
21	06_VLNSMA[redacted]_420D5DE0[redacted]4-006[redacted]_M300V_00000000
22	06_VLNSMA[redacted]_420D4B[redacted]C57-C[redacted]9C_M100V_000000
23	06_VLNSMA[redacted]_420D538[redacted]9F-8FC[redacted]_M100V_0000000
24	06_VLNSMA[redacted]_420D704[redacted]62-17[redacted]_M100V_0000000
25	06_VLNSMA[redacted]_420D873[redacted]34-608[redacted]_M100V_0000000
26	06_VLNSMA[redacted]_420DEE3[redacted]4B-F5[redacted]2_M100V_0000000

Additional Information

Cisco Secure Email Gateway Documentation

- Release Notes
- User Guide
- CLI Reference Guide
- API Programming Guides for Cisco Secure Email Gateway
- Open Source Used in Cisco Secure Email Gateway
- Cisco Content Security Virtual Appliance Installation Guide(includes vESA)

Secure Email Cloud Gateway Documentation

- Release Notes
- User Guide

Cisco Secure Email and Web Manager Documentation

- Release Notes and Compatibility Matrix
- User Guide
- API Programming Guides for Cisco Secure Email and Web Manager
- Cisco Content Security Virtual Appliance Installation Guide(includes vSMA)

Cisco Secure Malware Analytics

- Cisco Secure Malware Analytics (Threat Grid)

Cisco Secure Product Documentation

- Cisco Secure portfolio naming architecture