Cisco Success Network (CSN) für Cisco Email Security

Inhalt

[Einführung](#)
[Vorteile](#)
[Erfasste Informationen](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Firewall-bezogene Konfiguration](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[CSN- und CTR-Abhängigkeiten](#)
[CSN-Konfiguration mithilfe der Benutzeroberfläche](#)
[CSN-Konfiguration mithilfe der CLI](#)
[Fehlerbehebung](#)

Einführung

Dieses Dokument enthält Informationen zur Cisco Success Network-Funktion, die als Teil der Version AsyncOS 13.5.1 für die Cisco E-Mail Security Appliance (ESA) verfügbar ist. Cisco Success Network (CSN) ist ein benutzerfähiger Cloud-Service. Wenn CSN aktiviert ist, wird eine sichere Verbindung zwischen der ESA und der Cisco Cloud hergestellt (mithilfe der CTR-Verbindung), um Funktionsstatusinformationen zu streamen. Das Streaming von CSN-Daten bietet einen Mechanismus zur Auswahl von Daten, die für die ESA von Interesse sind, und zur Übermittlung dieser Daten in einem strukturierten Format an Remote-Managementstationen.

Vorteile

- Informationen für den Kunden über verfügbare, nicht verwendete Funktionen, die die Effektivität des Produkts verbessern können.
- Informieren des Kunden über zusätzliche technische Support-Services und Überwachung, die für das Produkt verfügbar sein könnten.
- Um Cisco bei der Verbesserung des Produkts zu unterstützen.

Erfasste Informationen

Dies sind die Funktionslisten, die nach der Konfiguration auf dem ESA-Gerät als Teil dieser Funktion erfasst werden:

- Gerätemodell (x90, x95, 000 V, 100 V, 300 V, 600 V)
- Geräte-Seriennummer (UDI)
- UserAccountID (VLN-ID oder SLPIID)

- Softwareversion
- Installationsdatum
- slVAN (Virtual Account Name in Smart Licensing)
- Bereitstellungsmodus
- IronPort Anti-Spam
- Graymail Safe Unsubscribe
- Sophos
- McAfee
- Dateireputation
- Dateianalyse
- Schutz vor Datenverlusten
- Externe Bedrohungs-Feeds
- IronPort-Bildanalyse
- Outbreak-Filter
- Cisco IronPort Email Encryption-Einstellungen (Umschlagverschlüsselung)
- PXE-Verschlüsselung
- Domänenreputation
- URL-Filterung
- Anpassen der Blockseite
- Nachrichtenverfolgung
- Richtlinien-, Virus- und Outbreak-Quarantäne
- Spam-Quarantäne

Voraussetzungen

Anforderungen

Um diese Funktion zu konfigurieren, müssen einige der folgenden Anforderungen erfüllt werden:

- CTR-Konto (Cisco Threat Response)

Firewall-bezogene Konfiguration

Die für die Funktion des CSN erforderliche Firewall-Konfiguration hängt derzeit von der CTR-Kommunikation ab. Weitere Informationen finden Sie in diesem Dokument: Integration der ESA in CTR.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Email Security Appliance (ESA) AsyncOS Version 13.5.1.x und höher

Konfigurieren

Sie können diese Funktion sowohl über die ESA-Benutzeroberfläche als auch über die CLI

konfigurieren. Details zu beiden Schritten finden Sie unten.

CSN- und CTR-Abhängigkeiten

Die CSN-Funktion hängt von der CTR-Feature-Konnektivität ab, damit sie erfolgreich ausgeführt werden kann. Diese Tabelle enthält weitere Informationen zur Beziehung zwischen diesen beiden Prozessen.

Reaktion auf Bedrohungen	CSN	SSE-Anschluss	CSN-Prozess
Deaktiviert	Deaktiviert	Nach unten	Deaktiviert
Deaktiviert (Registrierung entfernen)	Aktiviert	Nach unten	Nach unten
Deaktiviert (registriert)	Aktiviert	Nach oben	Nach oben
Aktiviert	Manuell deaktiviert	Nach oben	Nach unten
Aktiviert	Aktiviert	Nach oben	Nach oben

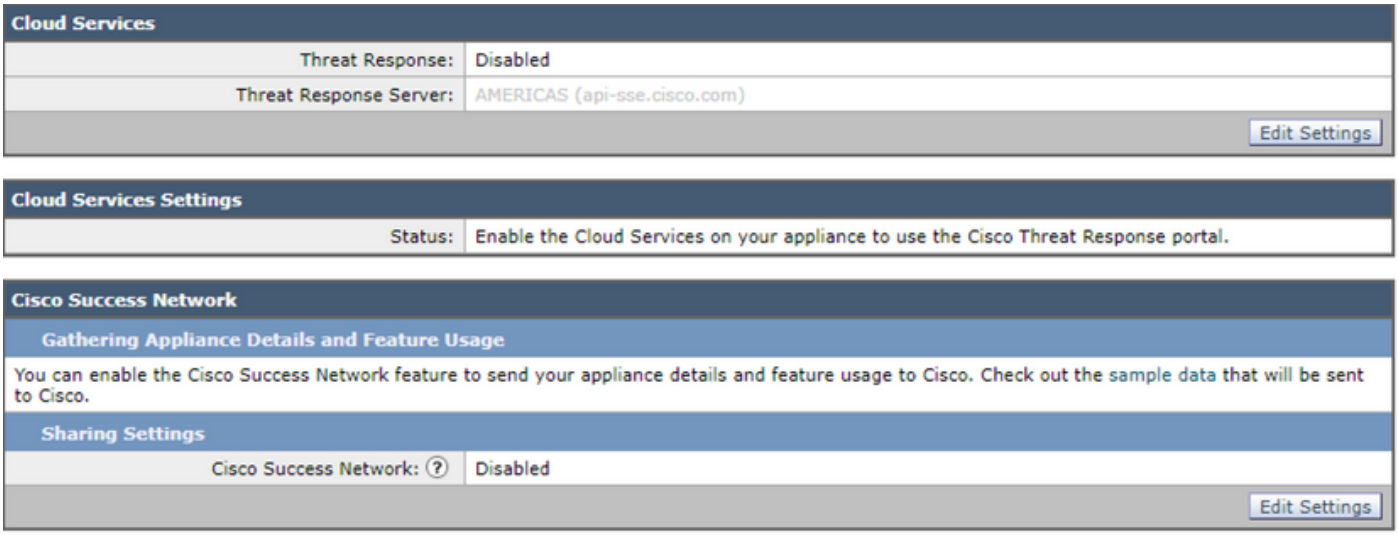
CSN-Konfiguration mithilfe der Benutzeroberfläche

1) Melden Sie sich bei der ESA-Benutzeroberfläche an.

2) Navigieren Sie zu **Network >> Cloud Service Settings** (Ich nehme an, dass CTR deaktiviert war, bevor wir mit dem Upgrade auf 13.5.1.x begonnen haben). Vor dem Upgrade wird CSN ebenfalls standardmäßig aktiviert, wenn CTR aktiviert wurde. Wenn CTR deaktiviert wurde, wird auch CSN deaktiviert.

> **Hinweis**: Wir gehen davon aus, dass CTR deaktiviert wurde, bevor das Upgrade als CTR in einer zentralen Bereitstellung deaktiviert werden soll, da es nur auf dem SMA aktiviert ist, um die Berichtsinformationen an CTR zu senden.

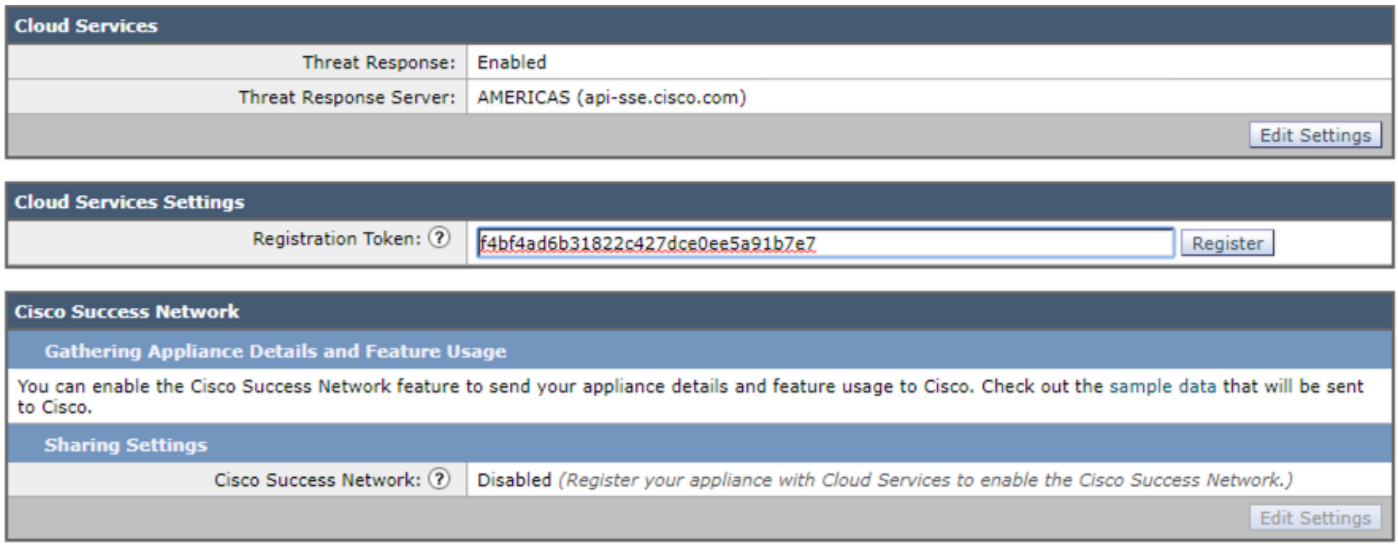
3) Dies ist der Standardwert auf dem ESA-Gerät: -



4) Wir werden diese ESA jetzt registrieren, indem wir zuerst die CTR-Services auf der ESA aktivieren und die Änderungen "einsenden".

5) Dieser Status wird auf der CTR-Seite "Der Cisco Cloud Service ist besetzt. Navigieren Sie nach einiger Zeit zurück zu dieser Seite, um den Status der Appliance zu überprüfen." Bestätigen Sie die Änderungen am Gerät.

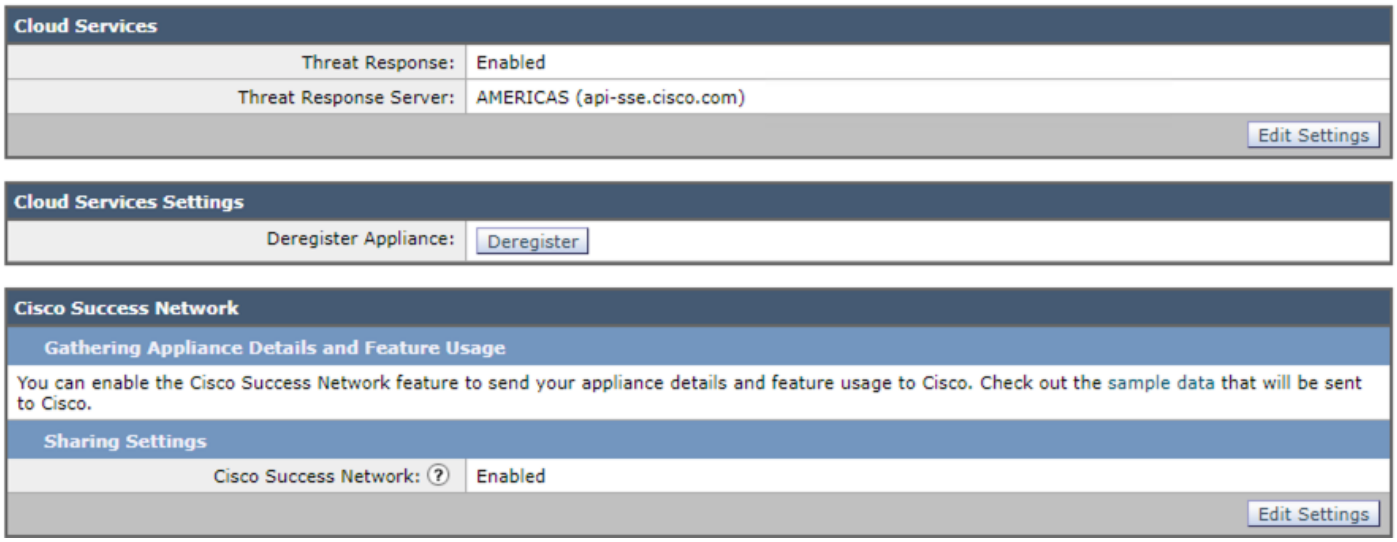
6) Anschließend würden Sie das CTR-Token abrufen und das Gerät für CTR registrieren:



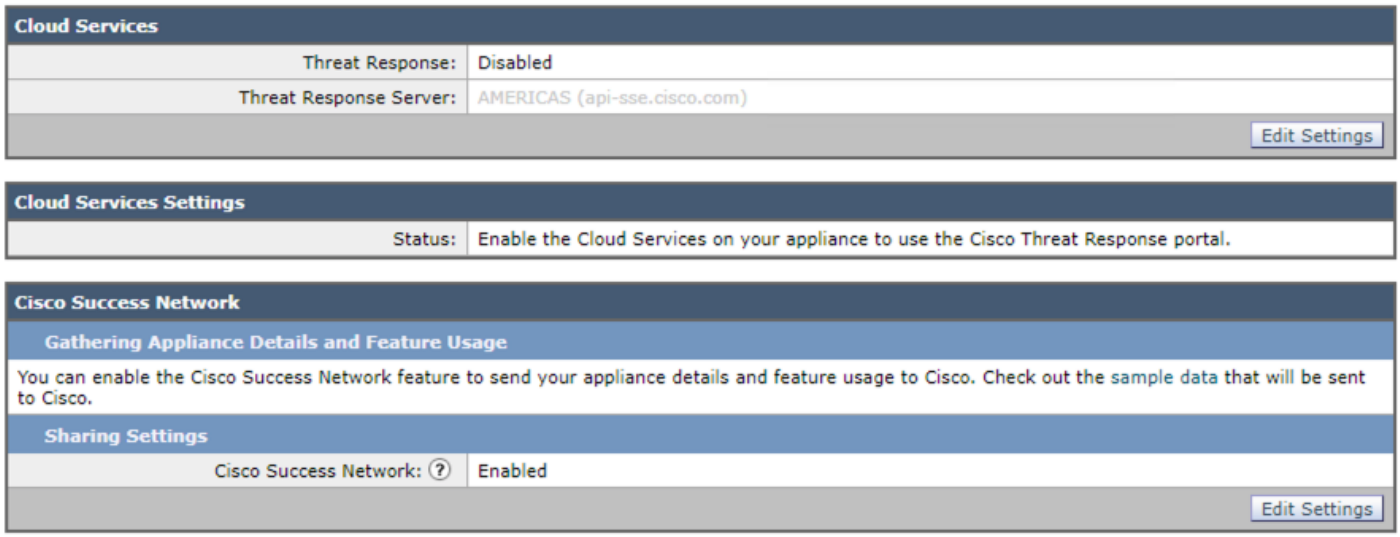
7) Dieser Status sollte angezeigt werden, sobald die Registrierung erfolgreich war:

Success - Eine Anfrage zur Registrierung Ihrer Appliance beim Cisco Threat Response-Portal wird initiiert. Navigieren Sie nach einiger Zeit wieder zu dieser Seite, um den Status der Appliance zu überprüfen.

8) Sobald Sie die Seite aktualisiert haben, werden CTR Registered und CSN Enabled angezeigt:



9) Wie bereits erwähnt, muss CTR in diesem Szenario deaktiviert werden, da diese ESA zentralisiert ist und das CSN weiterhin wie erwartet aktiviert ist. Falls diese ESA nicht von SMA (nicht zentralisiert) verwaltet wird, können Sie die CTR-Funktion aktivieren.



Dies sollte der letzte Status der Konfiguration sein. **Dieser Schritt sollte für jede ESA befolgt werden, da diese Einstellung auf Computerebene festgelegt ist.**

CSN-Konfiguration mithilfe der CLI

```
(Machine esa )> csnconfig

You can enable the Cisco Success Network feature to send your appliance details and feature
usage to Cisco.

Choose the operation you want to perform:
- ENABLE - To enable the Cisco Success Network feature on your appliance.
[]> enable

The Cisco Success Network feature is currently enabled on your appliance.
```

Änderungen müssen im Rahmen der Aktivierung dieser Funktion mithilfe der CLI übernommen werden.

Fehlerbehebung

Zur Fehlerbehebung steht ein PUB-Protokoll (**/data/pub/csn_logs**) zur Verfügung, das die Informationen zu dieser Funktion enthält. Das nachfolgende Beispiel zeigt das Protokoll zum Zeitpunkt der Registrierung auf dem Gerät:

```
(Machine ESA) (SERVICE)> tail

Currently configured logs:
    Log Name            Log Type                            Retrieval           Interval
 ---------------------------------------------------------------------------------------
 1. API                 API Logs                            Manual Download     None
 2. amp                 AMP Engine Logs                     Manual Download     None
 3. amparchive          AMP Archive                         Manual Download     None
 4. antispam            Anti-Spam Logs                      Manual Download     None
 5. antivirus           Anti-Virus Logs                     Manual Download     None
 6. asarchive           Anti-Spam Archive                   Manual Download     None
 7. authentication      Authentication Logs                 Manual Download     None
 8. avarchive           Anti-Virus Archive                  Manual Download     None
 9. bounces             Bounce Logs                         Manual Download     None
10. cli_logs            CLI Audit Logs                      Manual Download     None
11. csn_logs            CSN Logs                            Manual Download     None
12. ctr_logs            CTR Logs                            Manual Download     None
13. dlp                 DLP Logs                            Manual Download     None
14. eaas                Advanced Phishing Protection Logs   Manual Download     None
15. encryption          Encryption Logs                     Manual Download     None
16. error_logs          IronPort Text Mail Logs             Manual Download     None
17. euq_logs            Spam Quarantine Logs                Manual Download     None
18. euqgui_logs         Spam Quarantine GUI Logs            Manual Download     None
19. ftpd_logs           FTP Server Logs                     Manual Download     None
20. gmarchive           Graymail Archive                    Manual Download     None
21. graymail            Graymail Engine Logs                Manual Download     None
22. gui_logs            HTTP Logs                           Manual Download     None
23. ipr_client          IP Reputation Logs                  Manual Download     None
24. mail_logs           IronPort Text Mail Logs             Manual Download     None
25. remediation         Remediation Logs                    Manual Download     None
26. reportd_logs        Reporting Logs                      Manual Download     None
27. reportqueryd_logs   Reporting Query Logs                Manual Download     None
28. s3_client           S3 Client Logs                      Manual Download     None
29. scanning            Scanning Logs                       Manual Download     None
30. sdr_client          Sender Domain Reputation Logs       Manual Download     None
31. service_logs        Service Logs                        Manual Download     None
32. smartlicense        Smartlicense Logs                   Manual Download     None
33. sntpd_logs          NTP logs                            Manual Download     None
34. status              Status Logs                         Manual Download     None
35. system_logs         System Logs                         Manual Download     None
36. threatfeeds         Threat Feeds Logs                   Manual Download     None
37. trackerd_logs       Tracking Logs                       Manual Download     None
38. unified-2           Consolidated Event Logs             Manual Download     None
39. updater_logs        Updater Logs                        Manual Download     None
40. upgrade_logs        Upgrade Logs                        Manual Download     None
41. url_rep_client      URL Reputation Logs                 Manual Download     None
Enter the number of the log you wish to tail.
[]> 11

Press Ctrl-C to stop.
Sun Apr 26 18:16:13 2020 Info: Begin Logfile
Sun Apr 26 18:16:13 2020 Info: Version: 13.5.1-177 SN: 564D2E7007BA223114B8-786BB6AB7179
Sun Apr 26 18:16:13 2020 Info: Time offset from UTC: -18000 seconds
Sun Apr 26 18:16:13 2020 Info: System is coming up.
```

```
Sun Apr 26 18:16:13 2020 Info: DAEMON: Watchdog thread started
Sun Apr 26 18:16:16 2020 Info: The appliance is uploading CSN data
Sun Apr 26 18:16:16 2020 Info: The appliance has successfully uploaded CSN data
```