

# Cisco 成功ネットワーク ( CSN ) on Cisco E メールセキュリティ

## 目次

[はじめに](#)

[利点](#)

[収集情報](#)

[前提条件](#)

[要件](#)

[ファイアウォール 関連するコンフィギュレーション](#)

[使用するコンポーネント](#)

[設定](#)

[CSN および CTR 依存関係](#)

[UI を使用する CSN 設定](#)

[CLI を使用する CSN 設定](#)

[トラブルシューティング](#)

## 概要

この資料は Cisco E メールセキュリティ アプライアンス ( ESA ) のために AsyncOS 13.5.1 リリースの一部として利用可能である Cisco 成功ネットワーク 機能で情報を提供したものです。Cisco 成功ネットワーク ( CSN ) はユーザ使用可能なクラウド サービスです。CSN が有効になるとき機能 ステータス情報を流すために、信頼できる接続は ESA と Cisco クラウドの間で ( CTR 接続を使用して )、確立されます。CSN データを流すことは遠隔管理ステーションに ESA からの対象の『Data』を選択し、構造化形式でそれを送信するためにメカニズムを提供します。

## 利点

- 製品の効果を改善できる利用可能な未使用機能に関する顧客を知らせるため。
- 製品のために利用可能であるかもしれないモニタリングおよび追加 Technical Support Services に関する顧客を知らせるため。
- Cisco が製品を改良するのを助けるため。

## 収集情報

これらは一度 ESA デバイスで設定されるこの機能の一部として集められる機能 情報のリストです:

- デバイス モデル ( x90、x95、000v、100v、300v、600v )
- デバイス シリアル番号 ( UDI )
- UserAccountID ( VLN ID ナンバーか SLPIID )
- [Software Version]

- 日付をインストールして下さい
- sIVAN ( スマートな認可のバーチャル アカウント名 )
- 配置モード
- IronPort 反スパム
- Graymail セーフは定期講読を解除します
- Sophos
- McAfee
- ファイル評判
- ファイル分析
- データ損失防止
- 外部からの威圧供給
- Ironport イメージ分析
- 発生フィルター
- Cisco IronPort E メール暗号化設定 ( エンベロープ暗号化 )
- PXE 暗号化
- ドメイン評判
- URL フィルタリング
- Block ページ カスタマイゼーション
- メッセージ トラッキング
- ポリシー、ウイルスおよび発生検疫
- スпам検疫

## 前提条件

### 要件

この機能を設定するために、これらは満たす必要があるいくつかの必要条件です:

- CTR ( Cisco Threat Response ) アカウント

### ファイアウォール 関連するコンフィギュレーション

CSN を機能に CTR 通信に現在依存しています得、詳細についてはこの資料を示すのに必要とされるファイアウォール構成は: [CTR と ESA の統合](#)

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- E メール セキュリティ アプライアンス ( ESA ) AsyncOS バージョン 13.5.1.x および それ以上。

## 設定

ESA UI が CLI 両方を使用してこの機能を設定できます。両方のステップの詳細は下記に示されています。

## CSN および CTR 依存関係

CSN 機能は正常なオペレーションのための CTR 機能 接続によって決まり、この表はこれら二つのプロセス間の関係で詳細を提供したものです。

Threat Response	CSN	SSE コネクタ	CSN プロセス
Disabled	Disabled	下	Disabled
無効 (登録を取り消して下さい)	Enabled	下	下
無効 (登録される)	Enabled	上	上
Enabled	手動で無効にされる	上	下
Enabled	Enabled	上	上

## UI を使用する CSN 設定

1) ESA UI にログインして下さい。

2) 13.5.1.x にアップグレードから開始した前に ) CTR が無効になったとネットワーク >> Cloud サービス設定 ( に仮定します参照して下さい。アップグレードはまた CTR が有効になったら、そして CSN デフォルトで有効になります前に。CTR が無効になった場合、CSN はまた無効になります。

注: 中央集中型配備の CTR としてアップグレードが CTR へのレポート情報を送信するための SMA でだけそれとして無効になるはず有効になるである前に CTR が無効になったことを仮定します。

3) これは ESA デバイスのデフォルトとして観察するものです: -

The screenshot displays three configuration panels from the ESA UI:

- Cloud Services:** Shows Threat Response set to Disabled and Threat Response Server set to AMERICAS (api-sse.cisco.com). An Edit Settings button is visible.
- Cloud Services Settings:** Shows Status set to Enable the Cloud Services on your appliance to use the Cisco Threat Response portal.
- Cisco Success Network:** Under the heading 'Gathering Appliance Details and Feature Usage', it explains that the feature can be enabled to send details to Cisco. Under 'Sharing Settings', Cisco Success Network is set to Disabled. An Edit Settings button is visible.

4) 最初に ESA の CTR サービスを有効に することによって今すぐにこの ESA を登録し、変更を「入れて下さい」。

Edit Cloud Services	
Threat Response:	<input checked="" type="checkbox"/> Enable
Threat Response Server:	AMERICAS (api-sse.cisco.com) ▼

Cancel Submit

5) CTR ページのこのステータス「Cisco Cloud サービスが使用中であることを示します。ナビゲートして下さいアプライアンス ステータスをチェックする時間以降にこのページに戻って」。デバイスへの変更を保存して下さい。

6) それから前方に移動し、CTR トークンを得、CTR にデバイスを登録します:

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

Cloud Services Settings	
Registration Token: (?)	<input type="text" value="f4bf4ad6b31822c427dce0ee5a91b7e7"/> <a href="#">Register</a>

Cisco Success Network	
<b>Gathering Appliance Details and Feature Usage</b>	
You can enable the Cisco Success Network feature to send your appliance details and feature usage to Cisco. Check out the sample data that will be sent to Cisco.	
<b>Sharing Settings</b>	
Cisco Success Network: (?)	Disabled (Register your appliance with Cloud Services to enable the Cisco Success Network.)

[Edit Settings](#)

7) 登録が正常ならこのステータスを見るはずで:

成功— Cisco Threat Response ポータルが付いているアプライアンスを登録する要求は始められます。アプライアンス ステータスをチェックする時間以降にこのページに戻ってナビゲートして下さい。

8) ページをリフレッシュすれば、登録されていた有効になった CTR および CSN を見ます:

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

Cloud Services Settings	
Deregister Appliance:	<a href="#">Deregister</a>

Cisco Success Network	
<b>Gathering Appliance Details and Feature Usage</b>	
You can enable the Cisco Success Network feature to send your appliance details and feature usage to Cisco. Check out the sample data that will be sent to Cisco.	
<b>Sharing Settings</b>	
Cisco Success Network: (?)	Enabled

[Edit Settings](#)

9) 、CTR はこのシナリオで説明されている通りです中央集中型この ESA として無効になる必要があり、まだ予想通り有効になった CSN を見ます。、この ESA が SMA によって ( 非中央集中型 ) 管理されなければ、CTR を有効にしておくことができます。

Cloud Services	
Threat Response:	Disabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
<a href="#">Edit Settings</a>	

Cloud Services Settings	
Status:	Enable the Cloud Services on your appliance to use the Cisco Threat Response portal.

Cisco Success Network	
<b>Gathering Appliance Details and Feature Usage</b>	
You can enable the Cisco Success Network feature to send your appliance details and feature usage to Cisco. Check out the sample data that will be sent to Cisco.	
<b>Sharing Settings</b>	
Cisco Success Network: ?	Enabled
<a href="#">Edit Settings</a>	

これは設定の最終状態であるはずですが。この設定がマシン レベルであるのでこのステップに各 ESA のために従う必要があります。

## CLI を使用する CSN 設定

```
(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.

変更は CLI を使用してこれを有効に することの一部として保存される必要があります。

## トラブルシューティング

この機能を解決するため、利用可能なこの機能の情報がある PUB ( /data/pub/csn\_logs ) ログがあります。 サンプルは下記の登録がデバイスで完了した時ログです:

```
(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

```