
XC CSD セットアップガイド

F5 ネットワークスジャパン合同会社

2024 年 03 月 12 日

目次:

第 1 章	はじめに	1
1.1	XC Client-Side Defense(CSD) とは	1
1.2	XC Console での設定	2
1.3	Google Chrome を使った動作確認	7
1.4	XC Console での確認	10
1.5	運用監視方法	13
1.6	<参考> CSD デモ動画	21

第 1 章

はじめに

このページでは、これらのオフィシャルなドキュメントの補足となる資料や、複数の機能を組合せてソリューションを実現する方法をご紹介します。

F5 のオフィシャルなドキュメントはこちらにあります。

- AskF5: <https://support.f5.com/csp/home>
- F5 Cloud Docs: <https://clouddocs.f5.com/>
- F5 DevCentral (コミュニティ): <https://devcentral.f5.com/>
- F5 Distributed Cloud Tech Docs : <https://docs.cloud.f5.com/docs/>

本資料の画面表示や名称は資料作成時点の画面表示を利用しております。アップデート等より表示が若干異なる場合がございます。

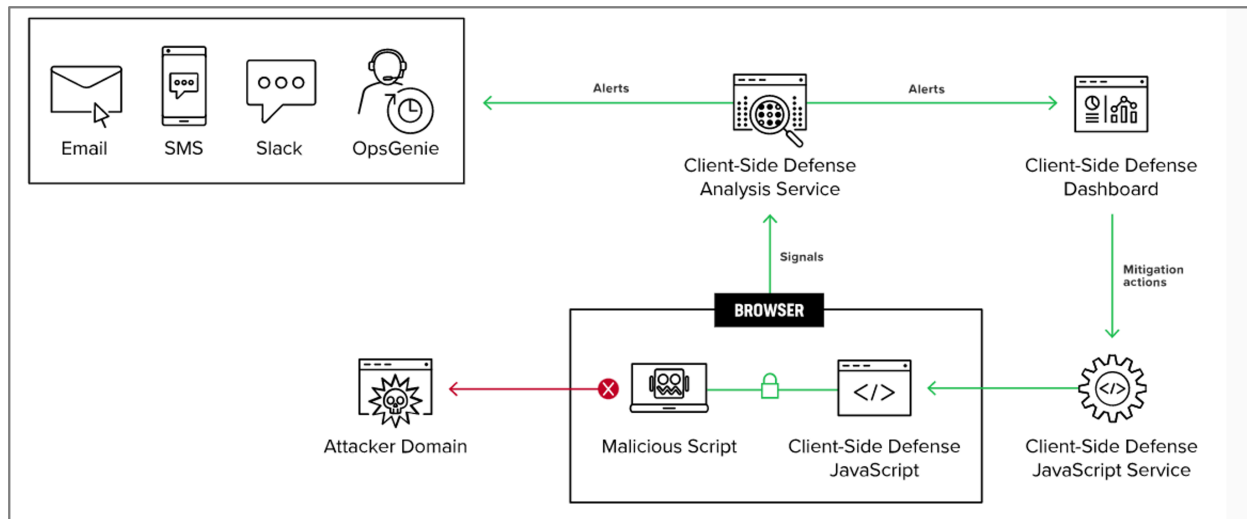
1.1 XC Client-Side Defense(CSD) とは

Client-Side Defense(以下、CSD) は、F5 Distributed Cloud Service(以下、XC) の 1 つとして提供可能な Web スキミング対策用セキュリティ SaaS 型サービスです。

クライアントのブラウザ上で動作する javascript の動作をリアルタイムに監視し、F5 が開発したシグナルに基づいて異常があった場合に管理者にアラートを上げ、データ流出のリスクを軽減することが可能となります。

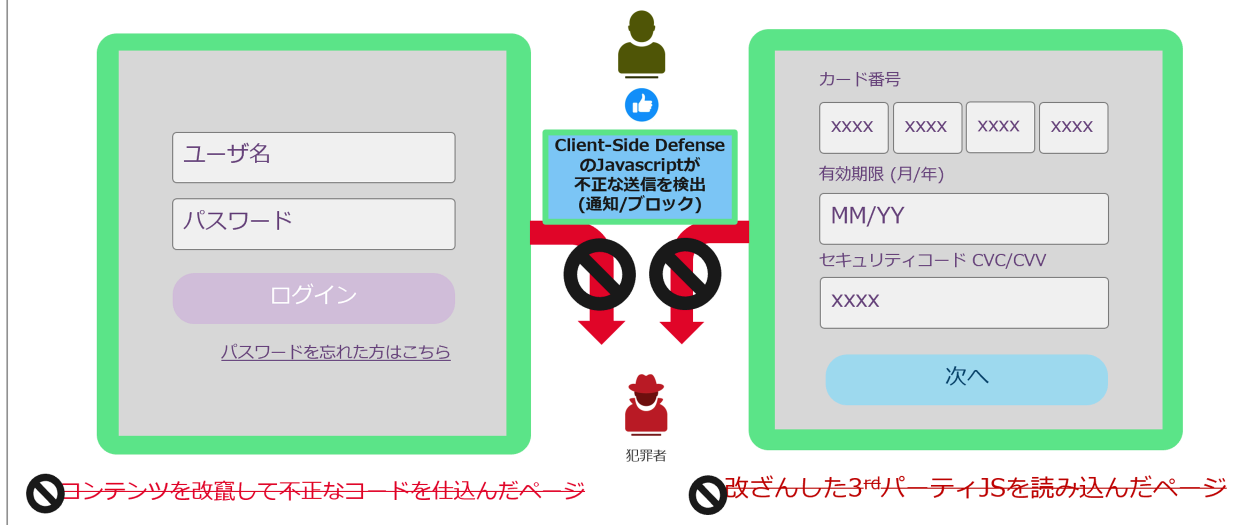
CSD を使用すると、Web サイトにある「ユーザ名/パスワード」を入力するログイン画面や、クレジットカードの情報を入力するページなどに情報奪取のための不正なコードを仕込んだり、javascript を改ざんして重要な情報を抜き取ったりする挙動を検知し、不正とみなした接続先についてブロックすることが可能となります。

- 動作概要構成図



Client-Side Defense : 怪しい動きを検出・保護

WEBページに潜む悪意のあるコードを検出&対処 個人情報への漏洩を防止



1.2 XC Console での設定

1. XC Console にアクセスし、以下の通り、[Home] - [Client-Side Defense] をクリックします。
2. [Dashboard] が表示されます。
3. 保護対象サイトの設定をします。

[Home] - [Client-Side Defense] - [Manage] - [Configuration] から、[Add Domain To Protect] をクリックします。

4. 対象サイトの [Root Domain] を追加し、[Save and Exit] をクリックします。

Welcome to the F5 Distributed Cloud Console

F5 Distributed Cloud Console delivers a set of networking, security, and app management services that can be used to solve various use-cases.

Common services

- Multi-Cloud Network Connect**
Networking & security across clouds, edge and on-premises
- Distributed Apps**
Deploy apps in our global PoPs (REs) or your cloud/edge sites
- Content Delivery Network** Preview
Optimize asset delivery with content caching
- DNS Management**
Configure and manage primary or secondary DNS service
- Multi-Cloud App Connect**
Connect apps across clouds, edge and on-premises using Load Balancers
- Web App & API Protection**
Create a proxy and configure WAF, Bot, and API security services for your apps
- DDoS & Transit Services**
Secure your infrastructure and apps against L3/L4 DDoS attacks
- Bot Defense**
Deploy bot mitigation for F5 BIG-IP and other 3rd party services
- Application Traffic Insight**
Recognize and monitor all client devices that access your applications
- Client-Side Defense** Preview
Monitor and mitigate fraudulent app requests at the client devices
- Account Protection**
Reduce online fraud against web and mobile applications
- Authentication Intelligence**
Identify returning/known users and reduce authentication friction

Client-Side Defense Preview

Monitoring

Dashboard
Script List
Network
Form Fields

Manage
Configuration

Notifications
Alerts
Audit Logs

Service Info
About

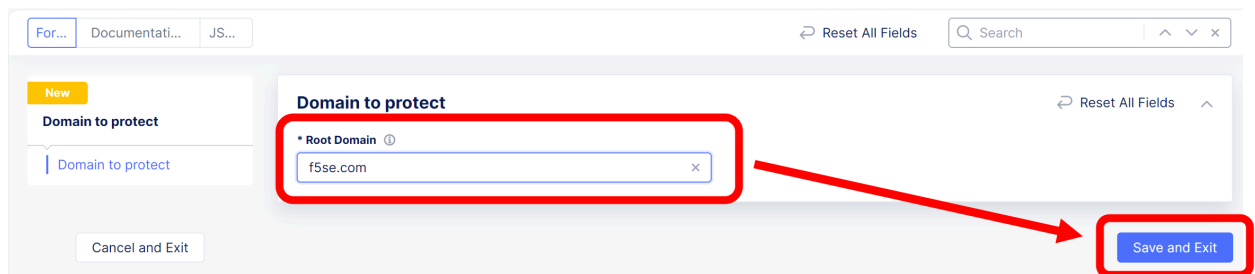
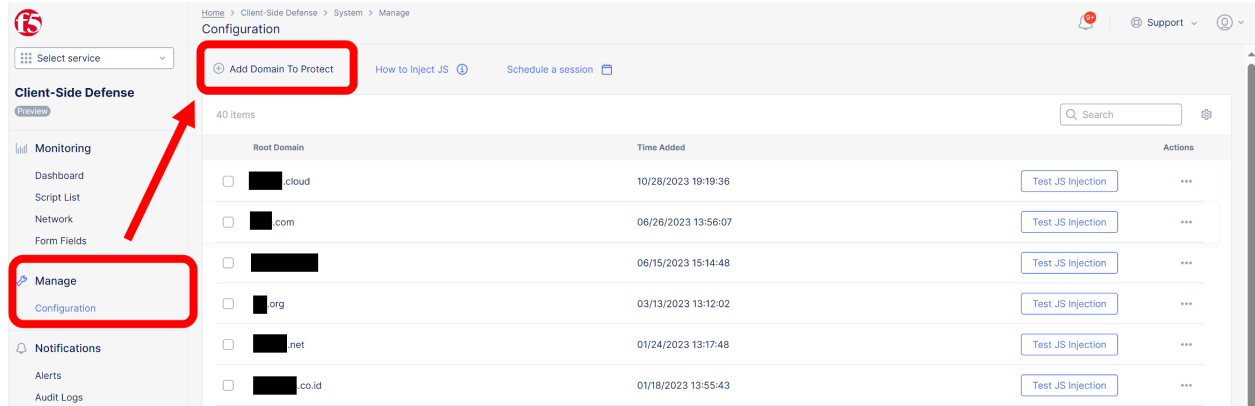
Home > Client-Side Defense > System > Monitoring
Dashboard

Select Location Auto-Refresh: Off Refresh: Updated just now

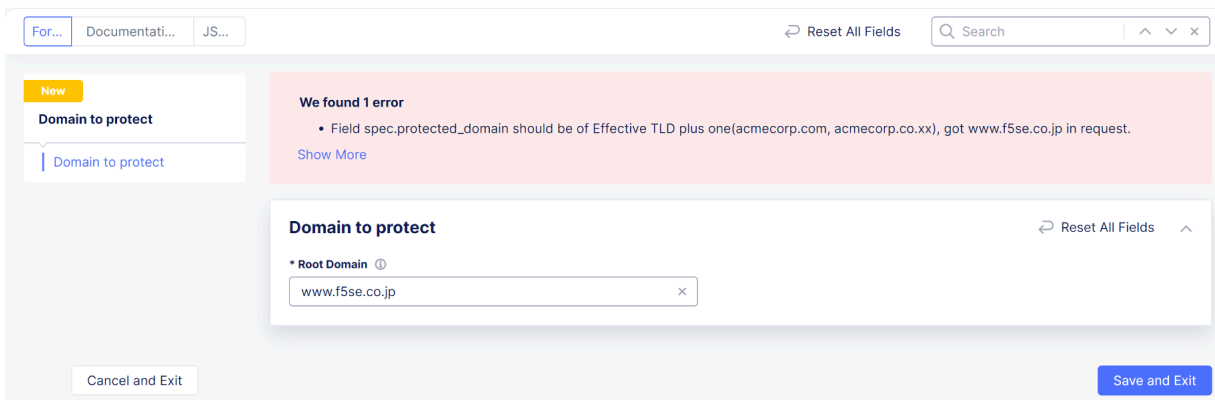
Action Needed: 8 (Since Nov 25, 2023)
Found & Mitigated: 0
Found & Allowed: 0
Total Found: 9 (Since Implemented)
Transactions Consumed: 203 (Since Implemented)

9 items

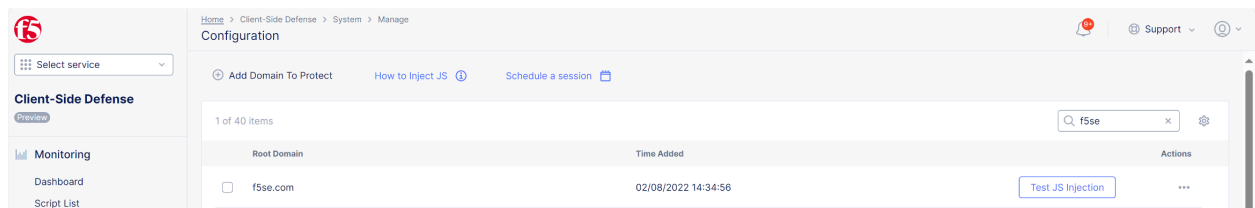
Domain	Status	Last Seen	Domain Category	Locations Found	Actions
ganalltics.com	Action Needed	11/25/2023 03:45:25	Phishing and Other Frauds	https://shop.apac-ent.f5demos.com/	...
gstacis.com	Action Needed	11/25/2023 03:45:25	Search Engines	https://shop.apac-ent.f5demos.com/	...
webfaset.com	Action Needed	11/25/2023 03:45:25	Phishing and Other Frauds	https://shop.apac-ent.f5demos.com/	...
fountm.online	Action Needed	11/25/2023 03:45:25	Unknown	https://shop.apac-ent.f5demos.com/	...
ganalltis.com	Action Needed	11/25/2023 03:45:25	Business and Economy	https://shop.apac-ent.f5demos.com/	...
pixupjqes.tech	Action Needed	11/25/2023 03:45:25	Computer and Internet Security	https://shop.apac-ent.f5demos.com/	...
jqwereid.online	Action Needed	11/25/2023 03:45:25	Computer and Internet Info	https://shop.apac-ent.f5demos.com/	...
[REDACTED].com	Added to Mitigated List	11/11/2023 18:45:25	Computer and Internet Info	https://arcadia.apac-ent.f5demos.com/	...
[REDACTED].com	Action Needed	11/01/2023 11:01:15	Computer and Internet Info	https://bot-demo.apac-ent.f5demos.com/	...



- 参考) Root Domain は、eTDL(effective TLD) + 1 の値でないと以下のようにエラーとなります。

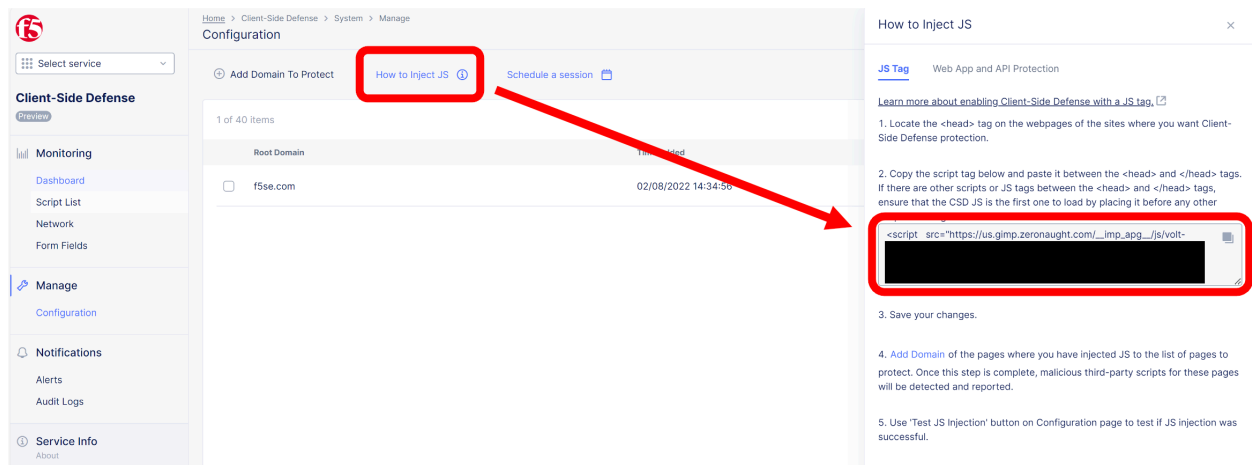


5. 登録後、[Configuration] に反映されていることを確認します。



6. [How to Inject JS] をクリックすると、CSD JS が表示されます。

右の赤枠がスクリプトの内容となりますが、これを挿入する設定を行います。



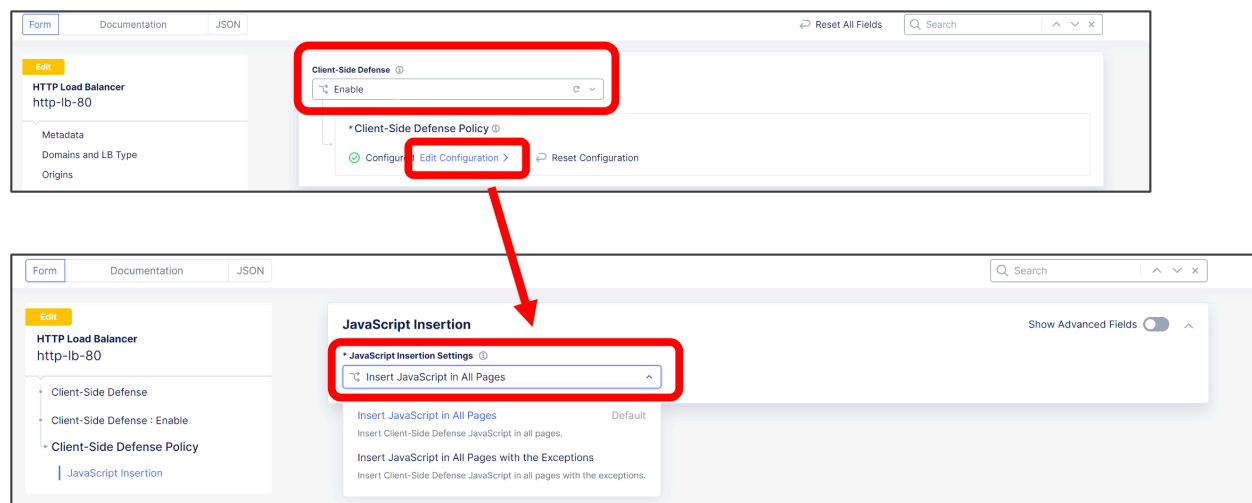
- CSD JS の挿入方法は以下 2 パターンあります。

(1). XC の HTTP LB で設定する場合

CSD 保護が必要な対象 HTTP LB の設定にて、CSD 機能を有効化し、CSD JS を LB で挿入するように設定します。(サーバ側での設定変更不要)

[Home] - [Web App and API Protection] - [Manage] - [Load Balancers] - [HTTP Load Balancers] から対象の HTTP LB の右側 [Action] - [Manage Configuration] をクリックし、右上の [Edit Configuration] をクリックします。

左側タブの [Client-Side Defense] をクリックし、下図の [Client-Side Defense] を Disable から Enable に変更し、[Edit Configuration] から [Insert JavaScript in All Pages] 選択し、[Apply], [Save and Exit] をクリックします。



(2). サーバ側で設定する場合

CSD 保護が必要なサイトの Web ページで<head> タグと </head> タグの間に先ほど XC Console

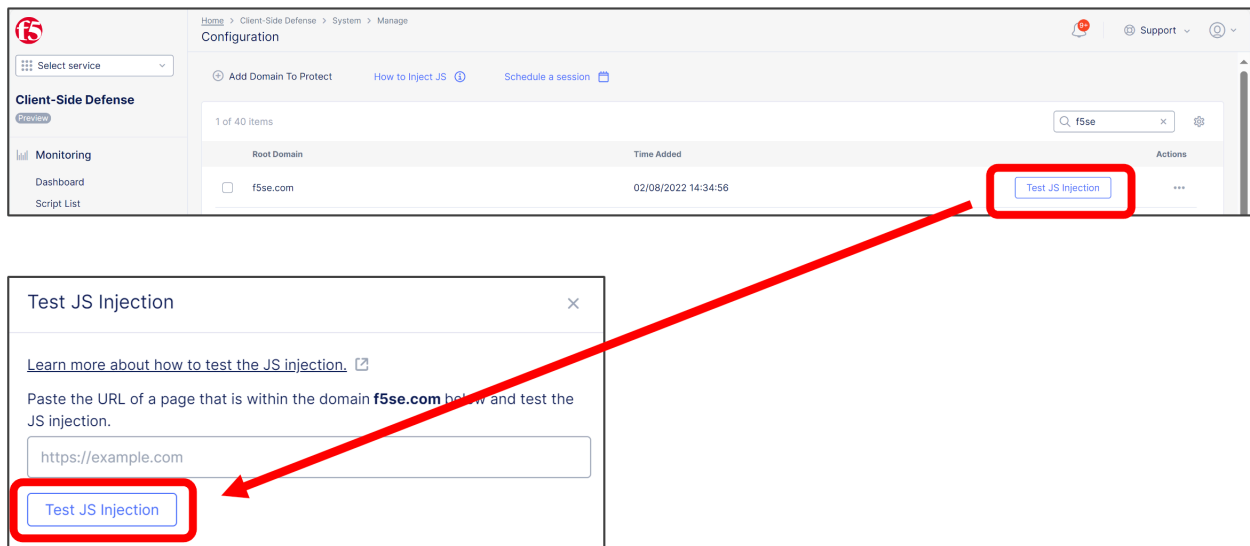
で確認した CSD JS をコピーし、挿入します。

<head> タグと </head> タグの間に他のスクリプトまたは JS タグがある場合は、CSD JS を他のスクリプトまたは JS タグの前に配置して、CSD JS が最初に読み込まれるように挿入してください。

注釈:

- JavaScript をすべてのページに挿入し、保護対象とすることを推奨（デフォルト値）しています。
- 理由は、データの取得とデータの流出が異なるページで起こりうる可能性があるためです。
- 例えば、悪質なスクリプトでは、フォームのあるページでフォームデータをキャプチャし、ローカルストレージや Cookie に保存することが可能です。その後、CSD が有効になっていないページで、スクリプトがこのデータを読み、悪意のあるドメインに送信するような攻撃もあるため、完全に保護するためには、全てのページで CSD を使用することを推奨しています。

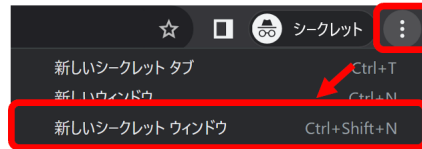
7. 実際にパブリックにアクセスできるサイトへ CSD JS を挿入した場合は、[Test JS Injection] から CSD JS が動作しているか確認できます。



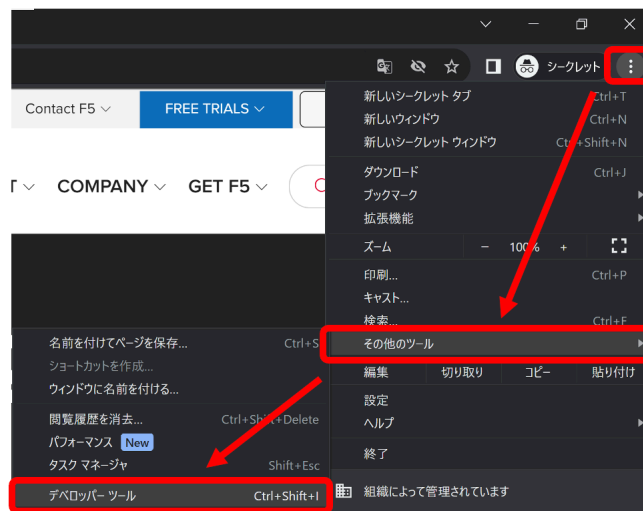
なお、後述の Google Chrome を利用したテストではクライアント側ブラウザで CSD JS を挿入しているため [Test JS Injection] はエラーとなります。

1.3 Google Chrome を使った動作確認

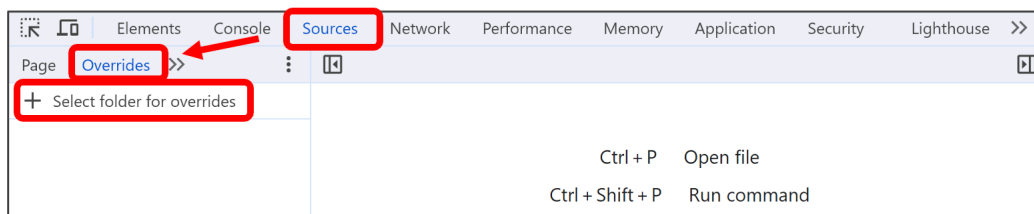
1. クライアント PC で Google Chrome ブラウザを起動します。右上から [シークレットモード] で起動させます。



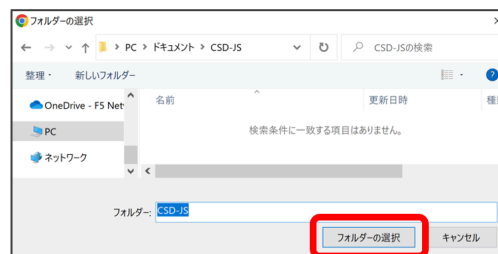
2. 右上から [その他のツール] - [デベロッパー ツール] をクリックします。



3. [Sources] - [Overrides] - [+ Select folder for overrides] をクリックします。



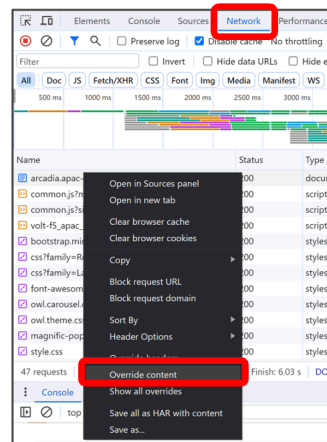
4. 任意のフォルダを作成し、[フォルダーの選択] をクリックします。



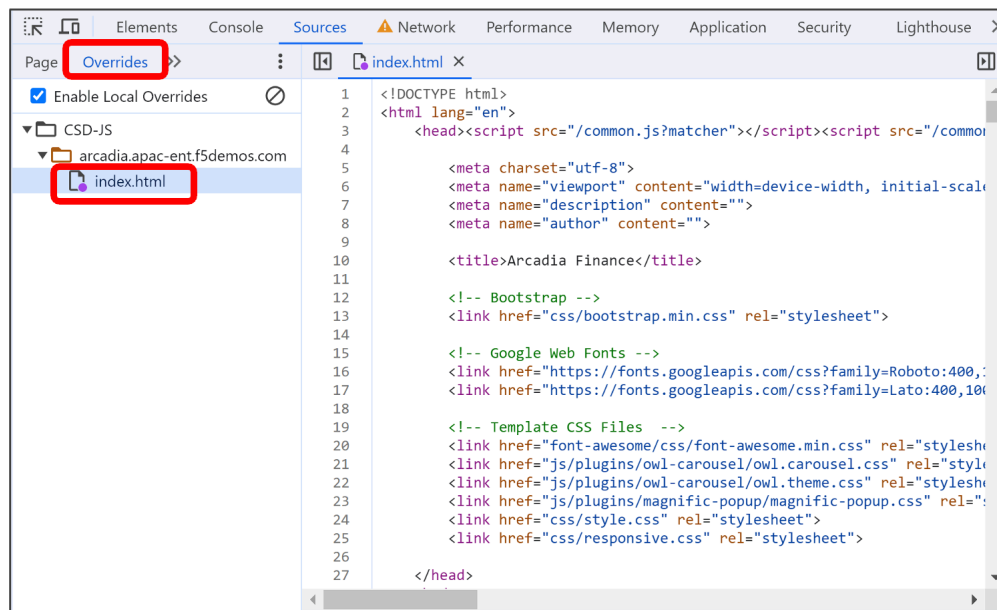
5. 以下のようにフォルダが作成されていることを確認します。



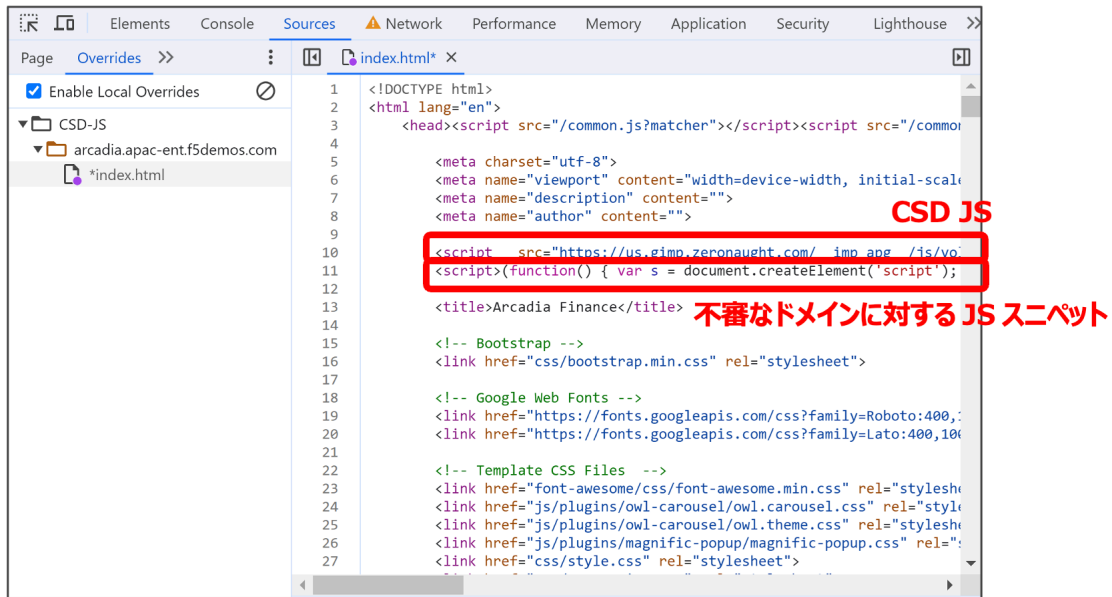
- 対象 URL にアクセスし、[Network] タブをクリックします。対象の通信を選択し、右クリックで [Override content] を選択します。



- [Sources] - [Overrides] に戻ると作成したフォルダ配下に対象サイトのトップページ、本書では [index.html] が表示されます。



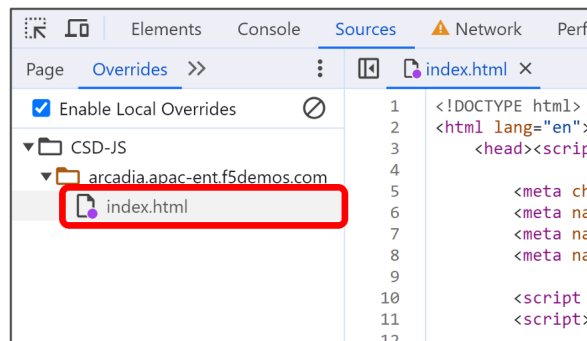
- CSD JS が最初に読み込まれるように、CSD JS と不審なドメインに対する JS スニペットを挿入します。



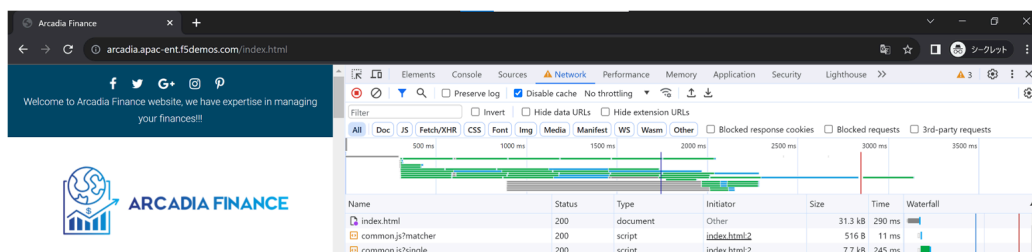
<不審なドメインに対する JS スニペット サンプル>

```
<script>(function() { var s = document.createElement('script'); var domains = [
  ↪ "ganalitis.com", "ganalitics.com", "gstats.com", "webfaset.com", "fountm.online",
  ↪ "pixupjqes.tech", "jqwereid.online"]; for (var i = 0; i < domains.length; ++i) { s.src_
  ↪ = 'https://' + domains[i]; } })();</script>
```

9. 最後に保存することで、[*index.html] から [index.html] になります。



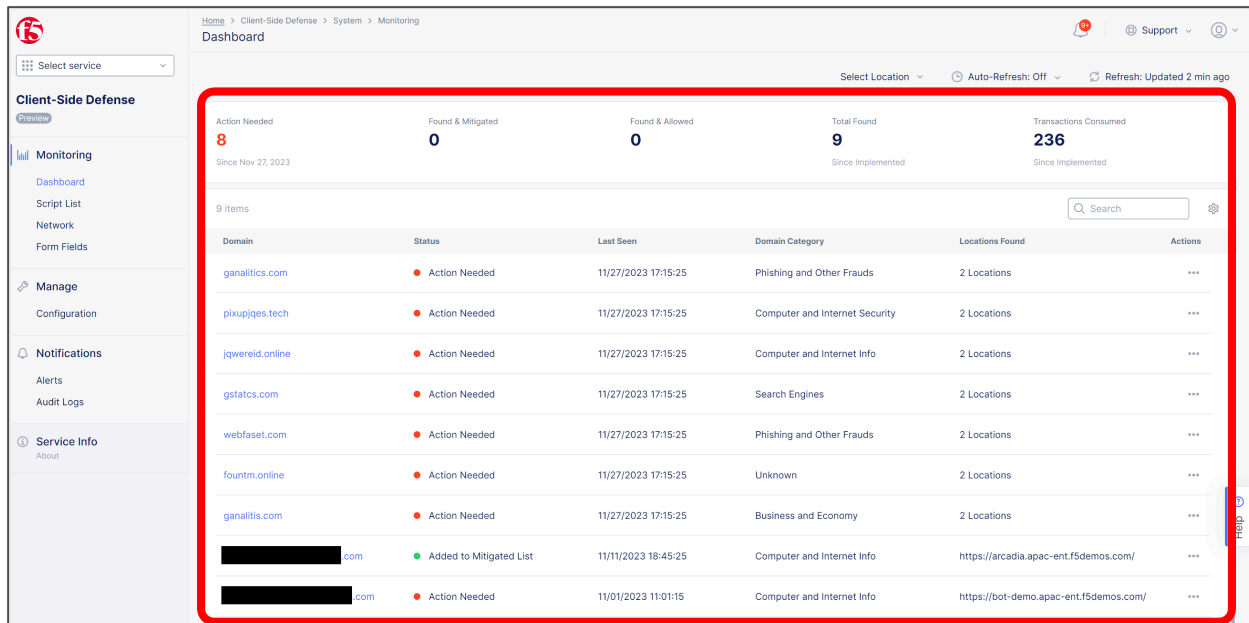
10. 対象サイトに数回アクセスを実施します。



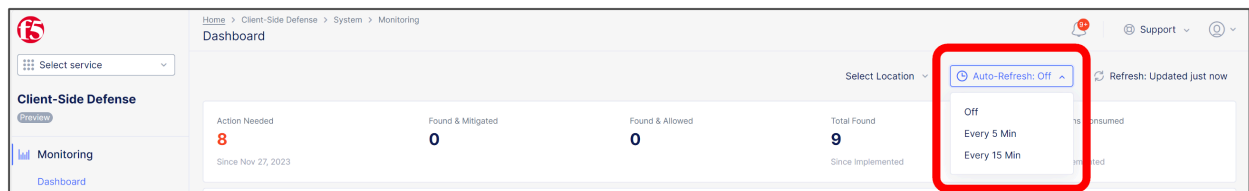
次章で XC CSD で、検知できているかを確認します。

1.4 XC Console での確認

1. 対象アクセスから 5 分以上経過後に [Home] - [Client-Side Defense] - [Dashboard] で確認すると、不正なドメインへのアクセスを検知していることが確認できます。



2. [Dashboard] では [Auto-Refresh] にて 5 分または 15 分でページの自動更新が可能です。



3. [Domain] をクリックすると、Risk Score など詳細情報が確認可能です。

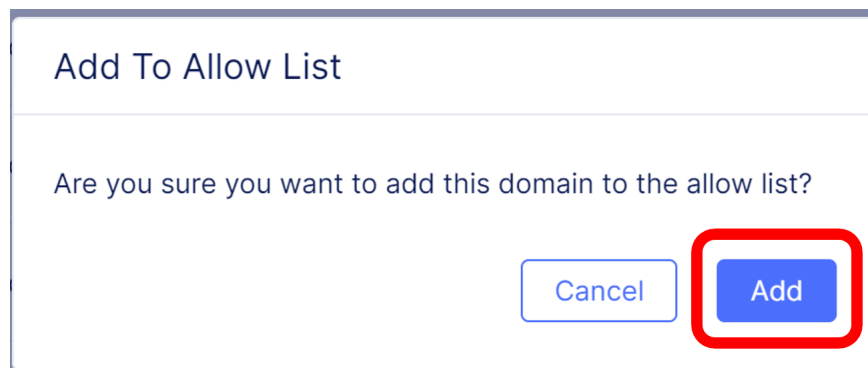
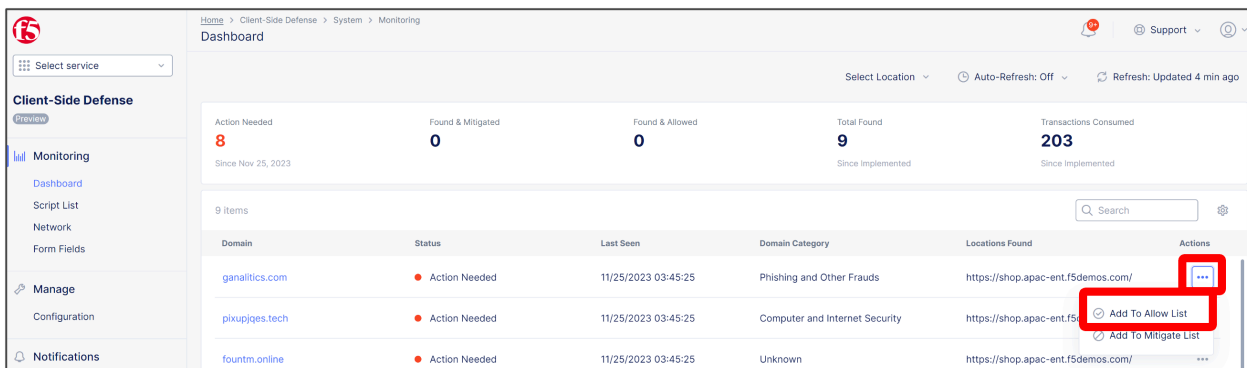
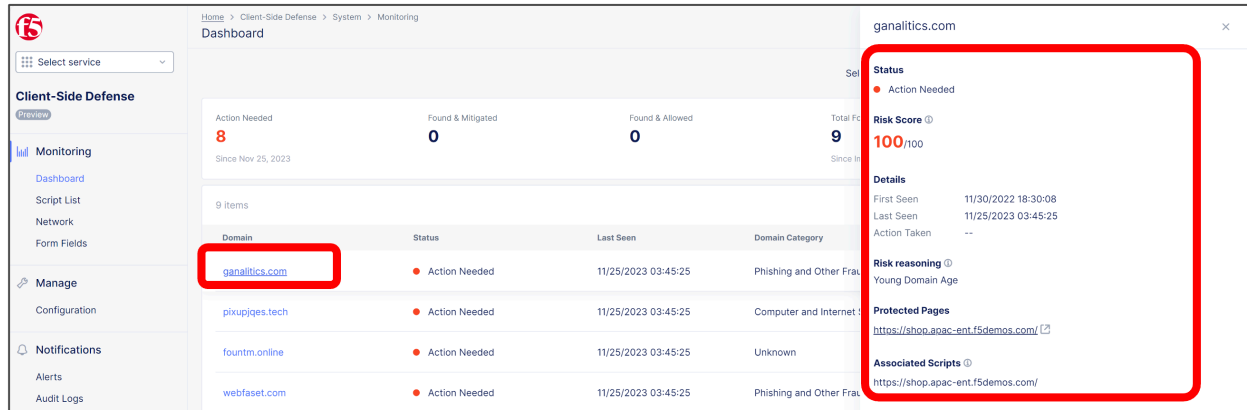
AI/ML による Risk Score 判定が High Risk に分類されると、[Status] が [Action Needed] 表示となるため、意図するドメインへの通信の場合は [Add To Allow List] へ、意図しないドメインへの通信の場合は [Add To Mitigate List] へ追加します。

4. 意図するドメインへの通信許可の設定

- (1). 対象 Domain を Allow List に追加します。

対象 Domain の一番右の [Actions] - [...] から [Add To Allow List] をクリックします。

- (2). 警告を確認し、[Add] をクリックで Allow List への登録は完了です。



(3). [Monitoring] – [Network] - [Allow List] から登録内容を確認可能です。

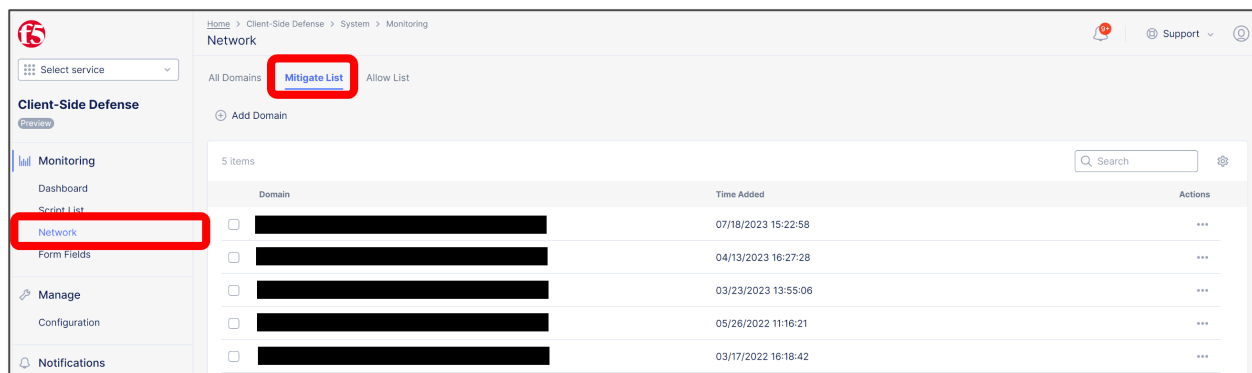
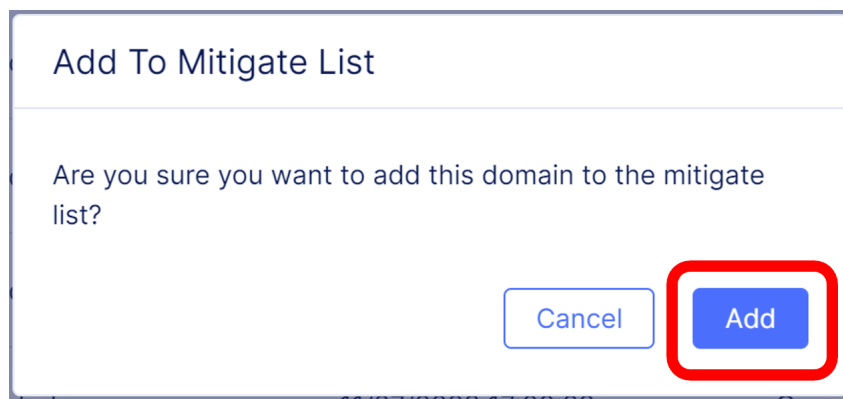
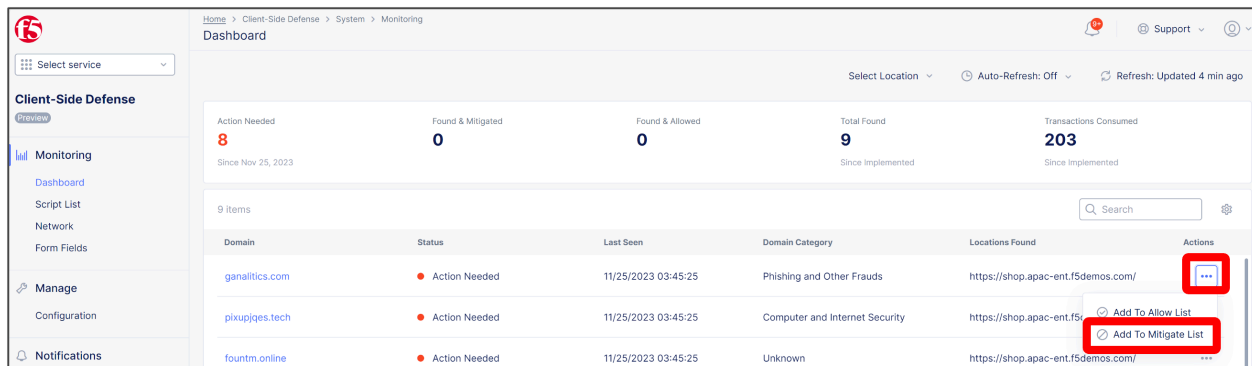
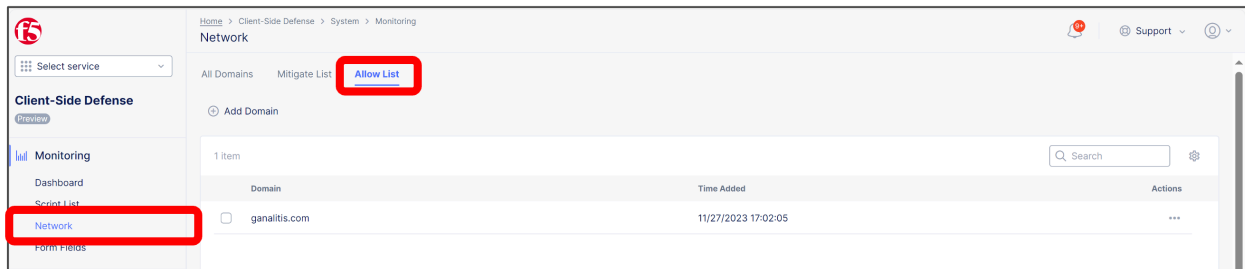
5. 意図しないドメインへの通信遮断の設定

(1). 対象 Domain を Mitigate List に追加します。

対象 Domain の一番右の [Actions] - [...] から [Add To Mitigate List] をクリックします。

(2). 警告を確認し、[Add] をクリックで Mitigate List への登録は完了です。

(3). [Monitoring] – [Network] - [Mitigate List] から登録内容を確認可能です。



1.5 運用監視方法

監視時は検出スクリプト一覧から脅威内容を確認し、スクリプトが意図しないドメインへアクセスしていないか確認することと、意図しない Form Field の読み取りがないかを確認します。

検出スクリプト一覧

[Home] - [Client-Side Defense] - [Monitoring] - [Script List] から保護対象にて検出したスクリプトの一覧を表示可能です。各スクリプトをクリックすることで詳細確認が可能です。

Status の状態の説明は下表のとおりです。

NA - No Action Needed	該当スクリプトでは不審な点を未検出
Resolved - No Action Needed	該当スクリプトでいくつかの不審な動作を検出したが、ユーザがすでにアクションを実行済
AN - Action Needed	注意が必要なスクリプトで不審な動作を検出

検出したスクリプトがどのドメインへ通信を行っているか、どの Form Field の値を読み取ろうとしているかの振る舞いが確認可能です。

意図する通信、意図しない通信のハンドリング

前章 [4. XC Console での確認] の 4 項,5 項 をご参照ください。

Form Field の読み取りを抑止

(1). [Home] - [Client-Side Defense] - [Monitoring] - [Form Fields] から特定のスクリプトによって読み取られる全フォームフィールドを確認することが可能です。

(2). 特定の Form Field に対して、その Field を読み取ろうとする Script があった際に、Risk Score を " High Risk " としてマークし、機微データへのアクセスリスクを管理することが可能です。

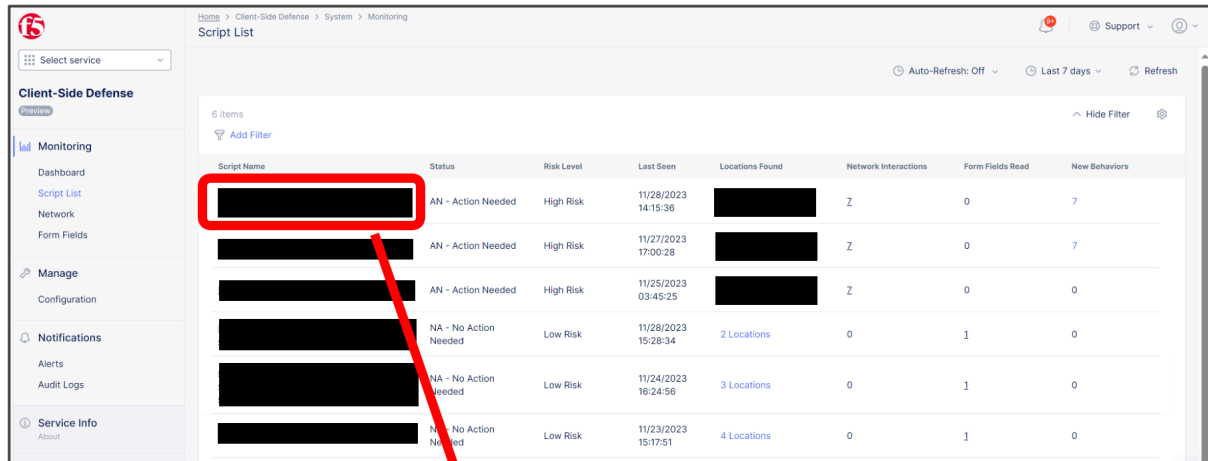
該当 Field の [Actions] から [Mark as Sensitive] を選択し、適用することで、当該 Field を機微データとして取り扱うことが可能です。

(3). Form Field を読み取るスクリプトに対する Mitigation Action として、意図する Form Field の読み取りの場合は [Allow Read] へ、意図しない Form Field の読み取りの場合は [Block Read] へ追加することが可能です。

[Home] - [Client-Side Defense] - [Monitoring] - [Script List] から [Form Fields Read] に数値が記録されているスクリプトを確認し、[Form Fields Read] の数字を選択します。

(4). 該当 Script が読み取っている Form Filed の一覧が表示され、それぞれの Risk Level を確認可能です。

前述の [Mark as Sensitive] にて該当 Field を機微データとして登録しておく、この Field を読み取ろうとする Script は " High Risk " として記録されます。



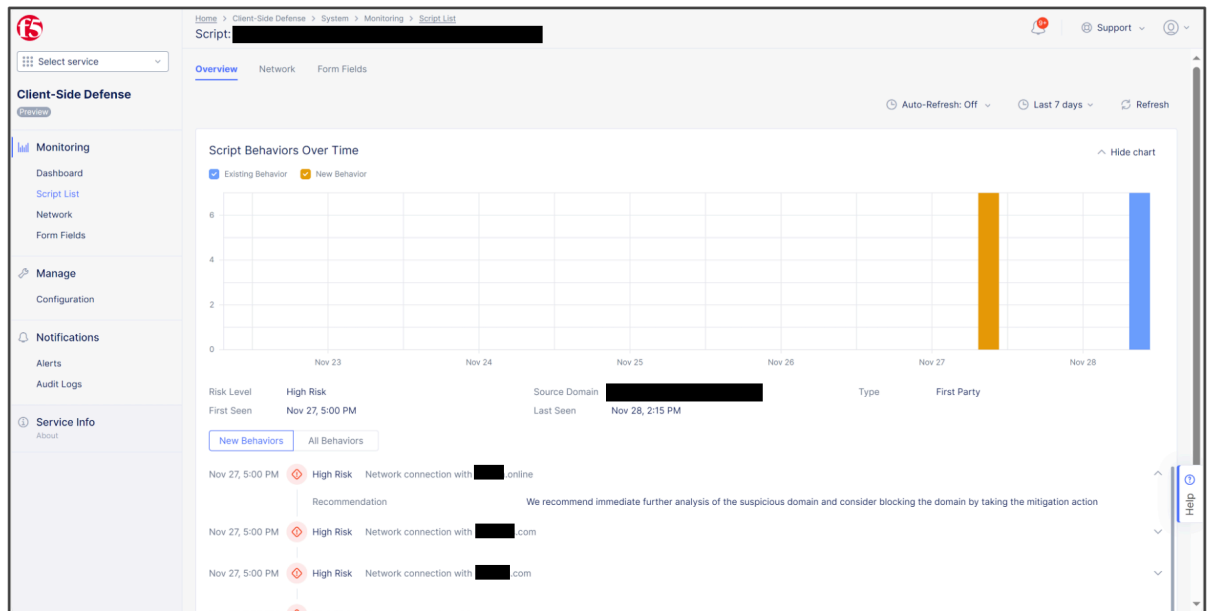
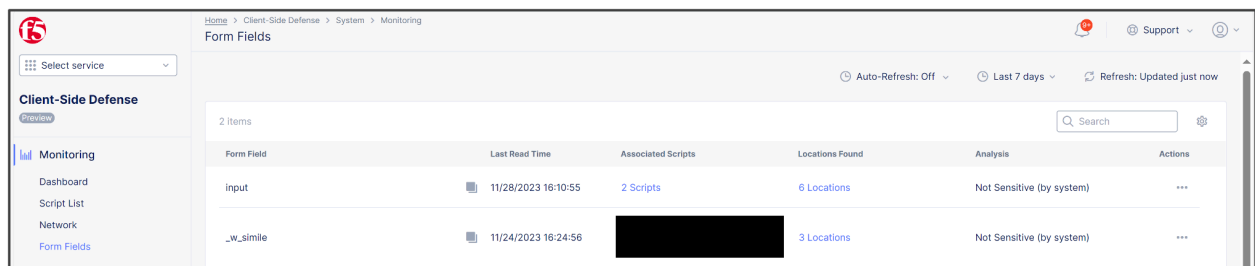
Home > Client-Side Defense > System > Monitoring

Script List

6 Items

Auto-Refresh: Off Last 7 days Refresh

Script Name	Status	Risk Level	Last Seen	Locations Found	Network Interactions	Form Fields Read	New Behaviors
[REDACTED]	AN - Action Needed	High Risk	11/28/2023 14:15:36	[REDACTED]	Z	0	7
[REDACTED]	AN - Action Needed	High Risk	11/27/2023 17:00:28	[REDACTED]	Z	0	7
[REDACTED]	AN - Action Needed	High Risk	11/25/2023 03:45:25	[REDACTED]	Z	0	0
[REDACTED]	NA - No Action Needed	Low Risk	11/28/2023 15:28:34	2 Locations	0	1	0
[REDACTED]	NA - No Action Needed	Low Risk	11/24/2023 16:24:56	3 Locations	0	1	0
[REDACTED]	NA - No Action Needed	Low Risk	11/23/2023 15:17:51	4 Locations	0	1	0

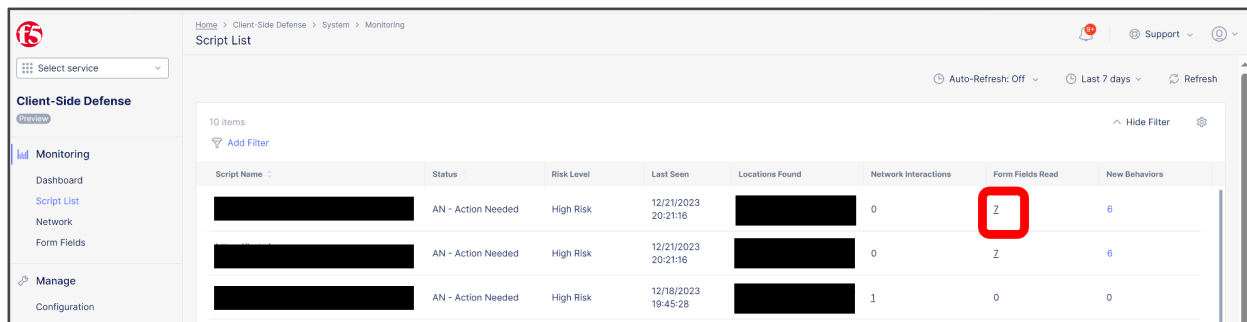
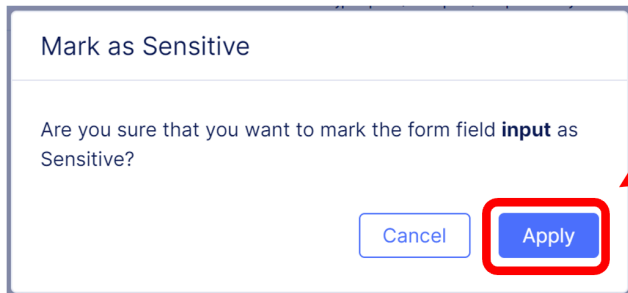
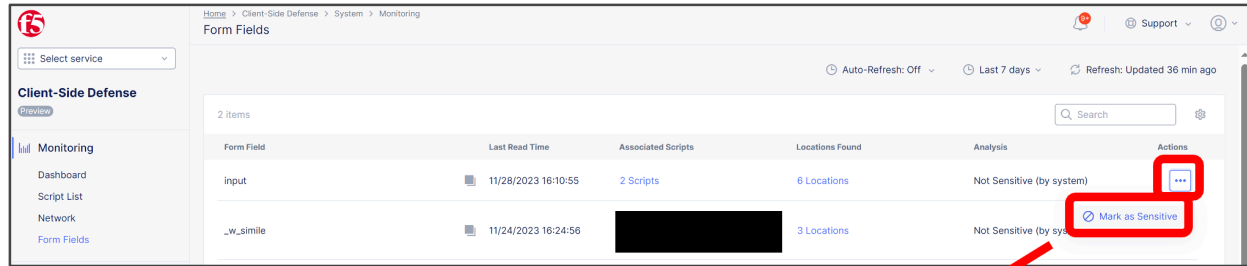
Home > Client-Side Defense > System > Monitoring

Form Fields

2 Items

Auto-Refresh: Off Last 7 days Refresh: Updated just now

Form Field	Last Read Time	Associated Scripts	Locations Found	Analysis	Actions
input	11/28/2023 16:10:55	2 Scripts	6 Locations	Not Sensitive (by system)	...
_w_simile	11/24/2023 16:24:56	[REDACTED]	3 Locations	Not Sensitive (by system)	...



これらの Script による該当 Field の読み取り可否を確認の上、Mitigation Action として [Allow Read] もしくは [Block Read] を設定可能です。

Alert の通知設定

CSD で発生したアラート通知の設定として、[Alert Receivers] ではどこに対し Alert Log を飛ばすかを設定し、[Alert Policies] では何の Alert Log を飛ばすか（ここでは CSD Alert Log）を設定し、最後にそれらの設定内容を [Active Alert Policies] として有効化することで、CSD アラート通知を設定可能です。

(1). Alert Receivers の設定

[Home] - [Audit Logs & Alerts] - [Alerts Management] - [Alert Receivers] にて、[Add Alert Receiver] を選択します。

Receiver は下記から選択することが可能です。(2023/12 時点)

Slack ・ PagerDuty ・ OpsGenie ・ Email ・ SMS ・ Webhook

設定入力後、[Save and Exit] をクリックします。[Alert Receiver] の設定が追加されます。

(2). Alert Policies の設定

Home > Client-Side Defense > System > Monitoring > Script List

Script: [REDACTED]

Overview Network **Form Fields**

Auto-Refresh: Off Last 7 days Refresh **Allow Read Block Read**

7 items

Form Field	Risk Level	Last Read Time	Read Allowed/Blocked
password	High Risk	12/21/2023 20:21:16	-
userName	High Risk	12/21/2023 20:21:16	-
password:nth-child(1)	High Risk	12/21/2023 20:15:16	-
username:nth-child(1)	High Risk	12/21/2023 20:15:16	-
email	High Risk	12/21/2023 20:06:06	-
password_confirmation	High Risk	12/21/2023 20:06:06	-
btn.btn-primary.btn-block.btn-lg	Low Risk	12/21/2023 20:06:06	-

Allow script

Are you sure you want to allow script to read all form fields?

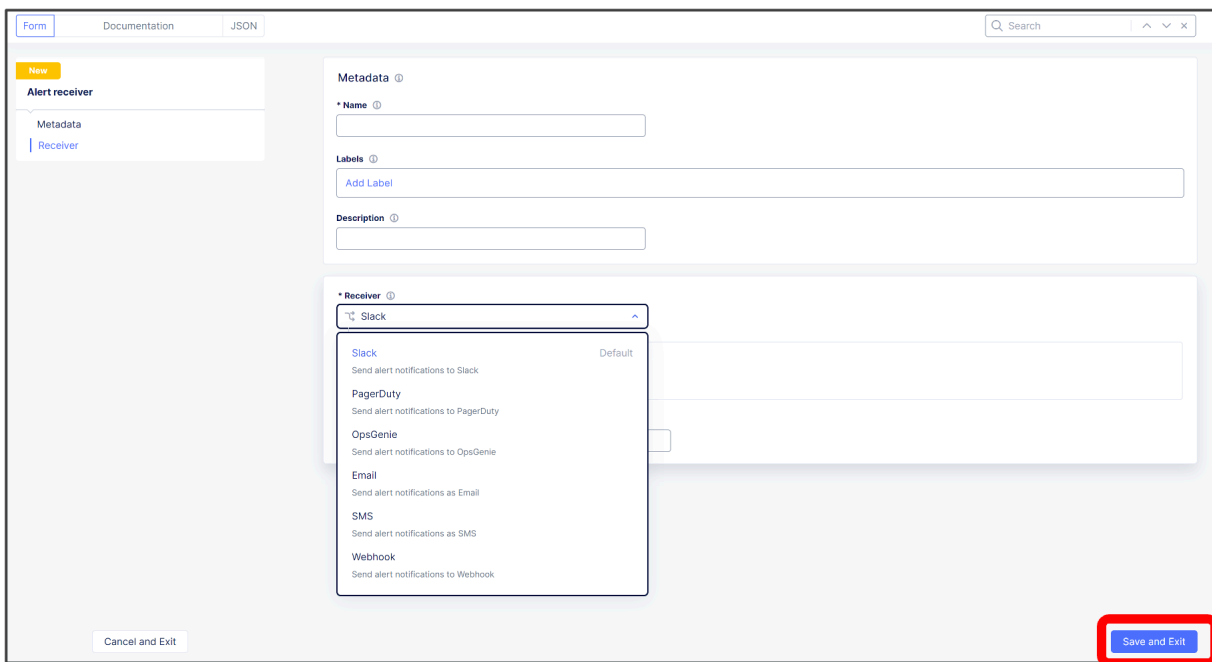
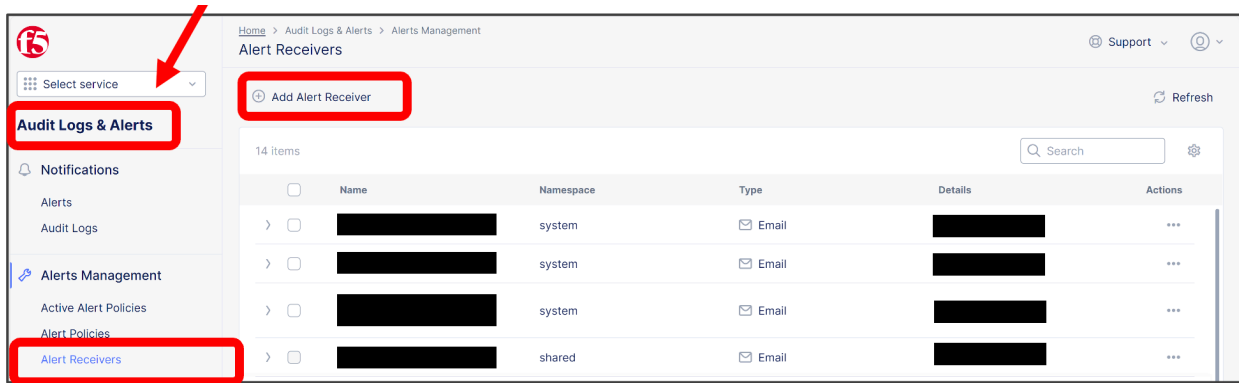
Cancel **Allow**

Welcome to the F5 Distributed Cloud Console

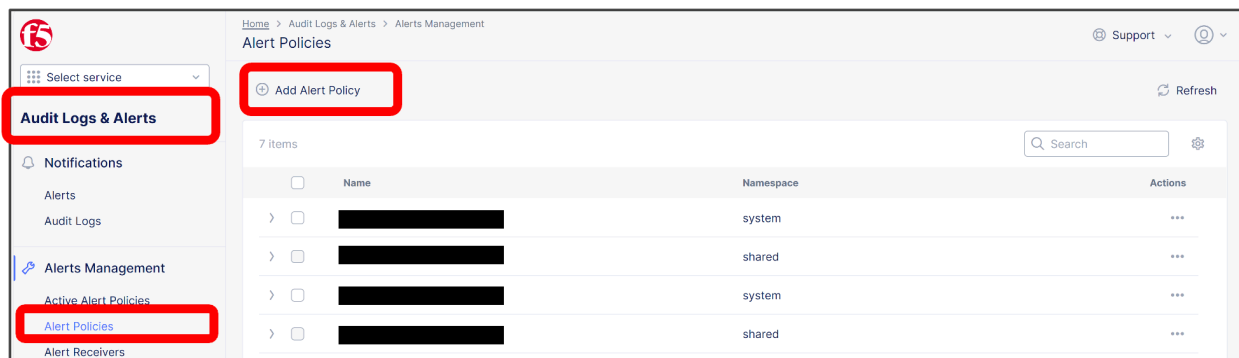
F5 Distributed Cloud Console delivers a set of networking, security, and app management services that can be used to solve various use-cases.

Common services

- Multi-Cloud Network Connect** > Networking & security across clouds, edge and on-premises
- Distributed Apps** > Deploy apps in our global PoPs (REs) or your cloud/edge sites
- Content Delivery Network** > Optimize asset delivery with content caching
- DNS Management** > Configure and manage primary or secondary DNS service
- Multi-Cloud App Connect** > Connect apps across clouds, edge and on-premises using Load Balancers
- Web App & API Protection** > Create a load balancer and configure WAF, Bot, and API security services for your apps
- DDoS & Transit Services** > Secure your infrastructure and apps against L3/L4 DDoS attacks
- Bot Defense** > Deploy bot mitigation for F5 BIG-IP and other 3rd party services
- Application Traffic Insight** > Recognize and monitor all client devices that access your applications
- Client-Side Defense** > Monitor and mitigate fraudulent app requests at the client devices
- Account Protection** > Reduce online fraud against web and mobile applications
- Authentication Intelligence** > Identify returning/known users and reduce authentication friction
- App Infrastructure Protection** > High-efficacy threat detection for your cloud-native workloads
- Observability** > Easily monitor your critical applications and systems from regions around the world
- NGINX Management Suite** > Track, Configure, and Manage NGINX Open Source and NGINX Plus Instances
- Delegated Access** > Control permissions and access to external tenants.
- Shared Configuration** > Create and manage shared configuration objects
- Audit Logs & Alerts** > Review logs and manage alerts
- Billing** > Manage billing and payment settings
- Administration** > Manage tenant settings, users and personal account



[Home] - [Audit Logs & Alerts] - [Alerts Management] - [Alert Policies] にて、[Add Alert Policy] を選択します。



Alert Policy 設定では、先ほど設定した Alert Receiver の設定を紐づけ、Policy Rules から [Security-CSD] を選択します。

以下の通り、[Security Alerts] と [Groups] を選択します。+ Security Alerts : Matching Group + Groups : Security-CSD

[Show Advanced Fields] をクリックすることで、通知間隔を調整可能です。

設定入力後、[Save and Exit] をクリックすることで、[Alert Policy] の設定が追加されます。

(3). Active Alert の設定

[Home] - [Audit Logs & Alerts] - [Alerts Management] - [Active Alert Policies] にて、[Select Active Alert Policies] をクリックします。

[Add Item] をクリックします。

先ほど作成した Alert Policy を選択し、[Save and Exit] をクリックします。

Route

Select Alerts ⓘ

Matching Group

Groups ⓘ

Security-CSD

* Action ⓘ

Send

Policy Rule Notification Parameters ⓘ

⚠ Not configured [Configure >](#)

Notification Parameters

Notify Interval For a Alert ⓘ

4h

Notification Grouping

Reset All Fields Show Advanced Fields ⓘ

* Group Notifications By ⓘ

F5XC Defined Group

Wait to Notify ⓘ

30s

Notify Interval for a Group ⓘ

1m

Form Documentation JSON

Reset All Fields Search

New

Alert policy

Metadata

Alert Receiver Configuration

Policy Rules

Metadata ⓘ

* Name ⓘ

Labels ⓘ

Add Label

Description ⓘ

Alert Receiver Configuration

Reset All Fields Show Advanced Fields ⓘ

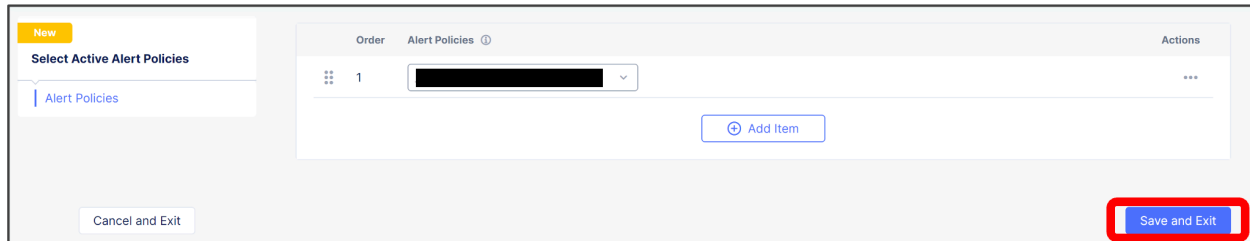
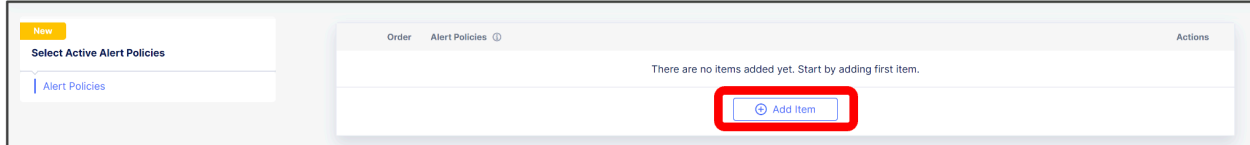
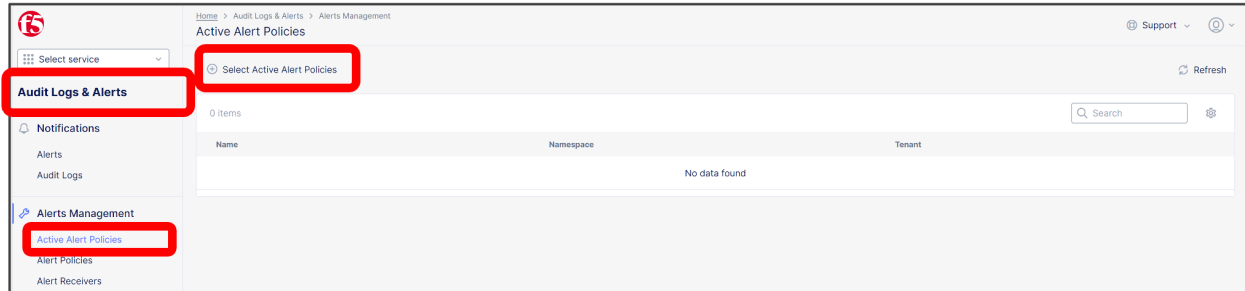
Order	*Alert Receivers ⓘ	Actions
1	csd-alert-...	...

Add Item

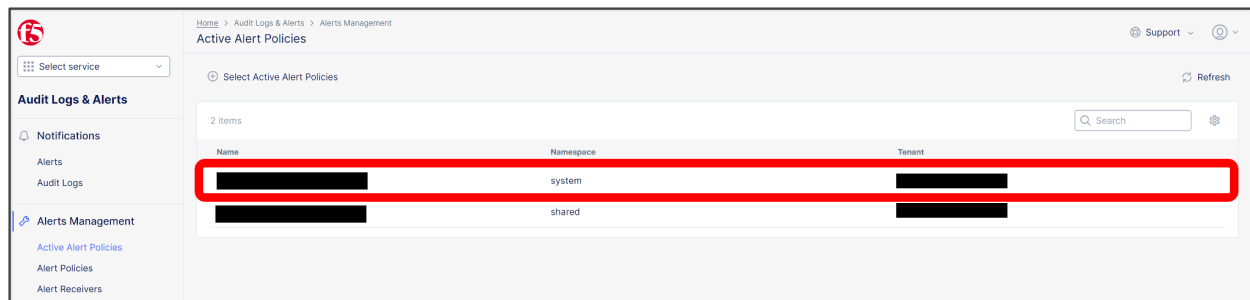
*Policy Rules ⓘ

Configured Edit Configuration > Reset Configuration

Cancel and Exit Save and Exit



Active Alert Policy として追加されます（Namespace は " system " として作成されます）



以上の設定により、CSD アラートが発生した際に、指定した Receiver に対してアラート通知を飛ばすことが可能です。

これで、XC CSD のセットアップガイドは終了となります。

1.6 <参考> CSD デモ動画

F5 XC CSD のデモを公開しています。

注釈: 本資料の画面表示や名称は資料作成時点の画面表示を利用しております。アップデート等より表示が若干異なる場合がございます。
