

CMSでWebbridgeのコンテンツセキュリティポリシーをカスタマイズする方法

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Meeting Server(CMS)バージョン3.2でwebbridge用にカスタマイズされたコンテンツセキュリティポリシーを設定および有効にする手順について説明します。

著者 : Cisco TACエンジニア、Octavio Miralrio

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CMSの一般設定
- Hypertext Transfer Protocol Secure(HTTPS)
- ハイパーテキストマークアップ言語(HTML)
- Webサーバ

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いています。

- CMSバージョン3.2
- Windows Web Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

設定

CMSバージョン3.2以降では、CMS管理者は別のWebサイトにWebアプリを埋め込むことができます。つまり、Webアプリは別のWebページに埋め込まれています。

注：Webアプリは、HTTPを使用するブラウザではなく、HTTPSを必要とするブラウザに組み込まれた場合にメディアを実行できます。

ステップ1:CMSのコマンドラインインターフェイス(CLI)を開き、次のコマンドを実行します。

```
webbridge3 https frame-ancestors
```

<frame-ancestors space-separated string>パラメータは、図に示すように、Webアプリが埋め込まれているフレームのUniform Resource Locator(URL)に置き換える必要があります。ワイルドカードは、https://*.octavio.labのようにサポートされます。

```
cms01> webbridge3
Enabled                               : true
HTTPS listening ports and interfaces  : a:443
HTTPS Key file                         : wbridge3.key
HTTPS Full chain certificate file      : wbridge3bundle.cer
HTTPS Frame-Ancestors                 : https://*.octavio.lab
HTTP redirect                         : Enabled, Port:80
C2W listening ports and interfaces    : a:9999
C2W Key file                          : wbridge3.key
C2W Full chain certificate file        : wbridge3bundle.cer
C2W Trust bundle                      : root.cer
Beta options                          : none
cms01>
cms01>
```

Webアプリは、ヘッダーの内容をチェックせず、文字が有効であることを確認します。管理者は、コンテンツセキュリティポリシーヘッダーに有効な文字列が含まれていることを確認する必要があります。文字列のサイズは1000文字に制限され、使用できる文字はa-z A-Z 0-9_ (1000文字) です。/:?#[]@!\$&'()*+ -= ~ %。

ステップ2:Webページ内でiFrameの埋め込みを設定します。

次の手順は、iframe要素をWebページに埋め込むことです。iframe要素は、HTML文書内の<iframe>タグによって認識されます。メディアをサポートするには、次の属性が必要です。

注：WebAppメディアを実行するにはHTTPSが必要です。iframeでサポートされている他の属性(高さや幅など)も含めることができます。

iFrameコンテンツの作成はWebページ管理者が行います。必要に応じてカスタマイズできます。次に、デモ用に作成されたiFrameの例を示します。

This is the title of the Content Security Policy

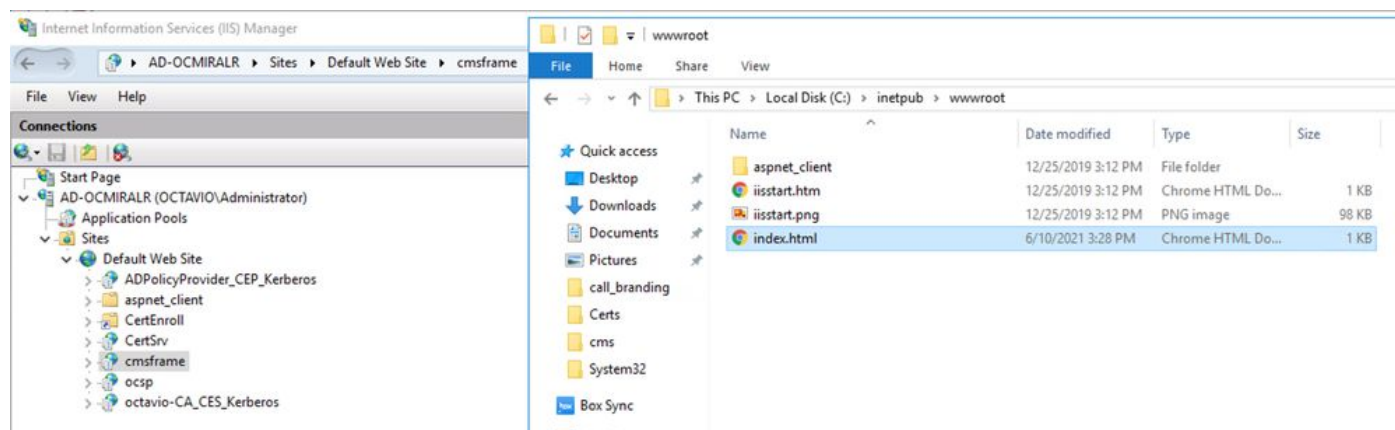
Welcome to the CMS Content Security Policy Demonstration.

All this text is not part of the webbridge itself.

Below you will see the embedded webapp page, <https://join.octavio.lab>.

ステップ3:Webサーバに導入します。

HTMLドキュメントにiframeが埋め込まれると、ページをWebサーバにロードする必要があります。このドキュメントの目的のために、HTMLファイルはindex.htmlと呼ばれて、図に示すようにWindows Webサーバに保存されます。



注：Webサーバの追加設定とWebページで使用可能なオプションは、このドキュメントの範囲外です。Webサーバ管理者は、Webページの展開を完了する必要があります。

確認

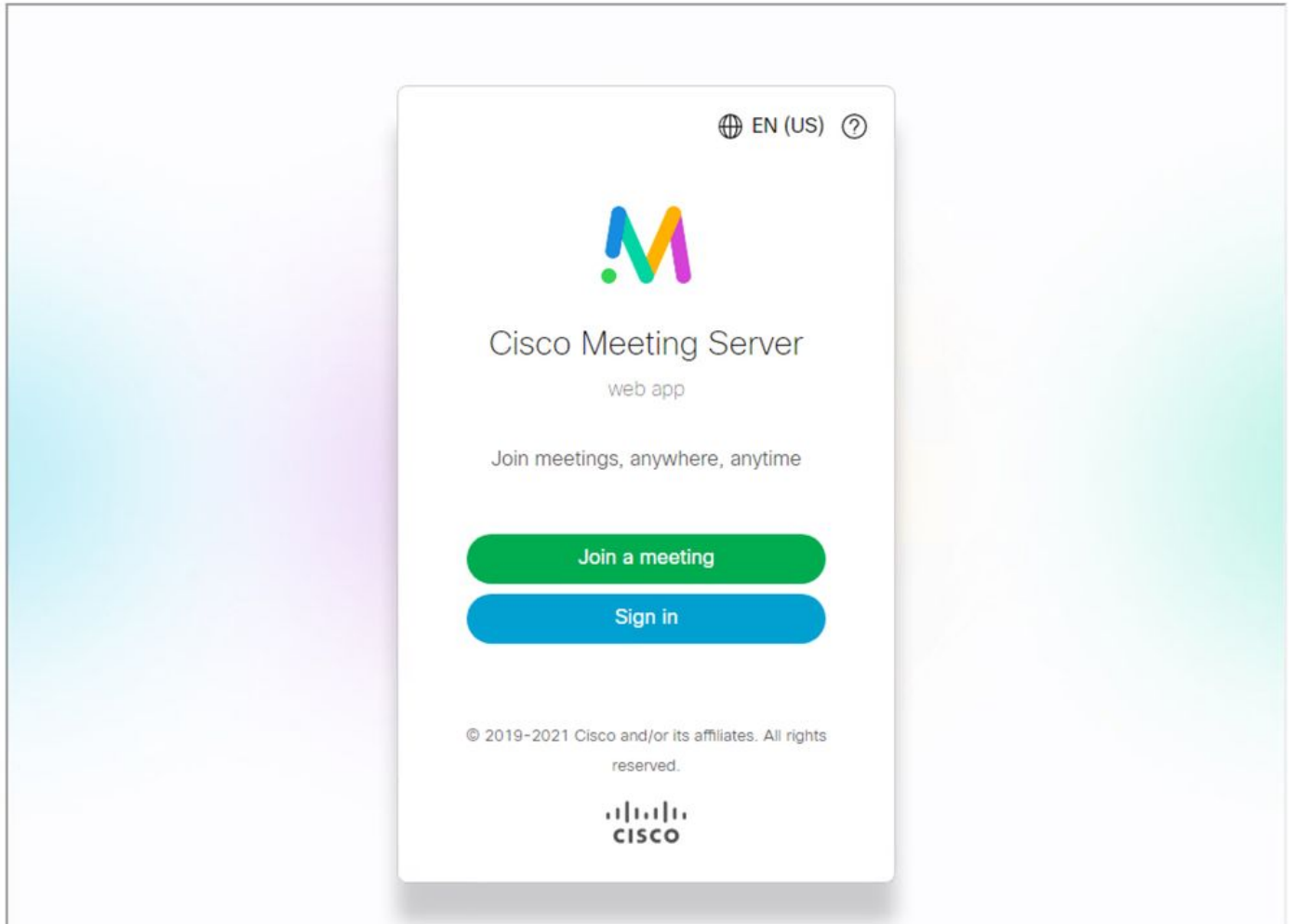
構成が正しく動作していることを確認するには、Webブラウザを開き、iFrameが構成されたWebページに移動します。このドキュメントの<https://ad-ocmiralr.octavio.lab/cmsframe/index.html>です。

This is the title of the Content Security Policy

Welcome to the CMS Content Security Policy Demonstration.

All this text is not part of the webbridge itself.

Below you will see the embedded webapp page, <https://join.octavio.lab>.



CMSで利用可能な会議にアクセスし、音声とビデオが正常に動作していることを確認します。

トラブルシューティング

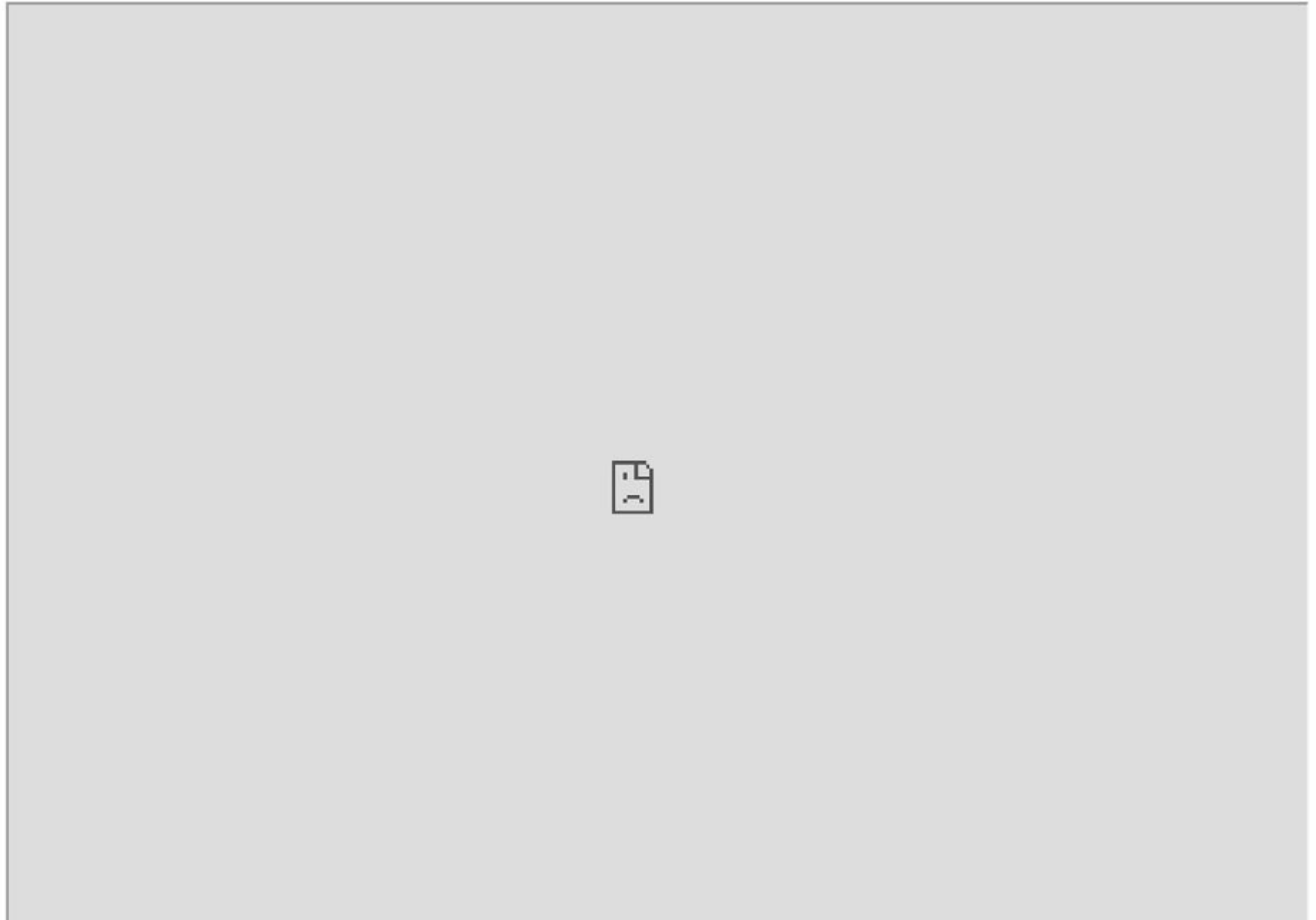
1. Webページが表示されますが、Webアプリはロードされません。

This is the title of the Content Security Policy

Welcome to the CMS Content Security Policy Demonstration.

All this text is not part of the webbridge itself.

Below you will see the embedded webapp page, <https://join.octavio.lab>.



この種の問題を解決するには、次の手順を実行します。

ステップ1:CMSのCLIを開きます。

ステップ2 : 次のコマンドを実行します。 **webbridge**。

ステップ3:webbridgeの設定から、**Frame-Ancestors**が正しいことを確認します。これは、作成されたWebページで設定された**iframe src**である必要があります。

```
cms01> webbridge3
Enabled : true
HTTPS listening ports and interfaces : a:443
HTTPS Key file : wbridge3.key
HTTPS Full chain certificate file : wbridge3bundle.cer
HTTPS Frame-Ancestors : https://*.cms.lab
HTTPS Redirect : Enabled, Port:80
C2W listening ports and interfaces : a:9999
C2W Key file : wbridge3.key
C2W Full chain certificate file : wbridge3bundle.cer
C2W Trust bundle : root.cer
Beta options : none
cms01>
```

この場合、webbridgeで設定されているFrame-Ancestorsは、図に示すように、Webページで設定されているものと異なります。

```
index.html
<!DOCTYPE html>
<html lang="en">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<html>
<head>
<title>Customized Content Security Policy</title>
</head>
<body>
<h1>This is the title of the Content Security Policy</h1>
<p>Welcome to the CMS Content Security Policy Demonstration.</p>
<p>All this text is not part of the webbridge itself.</p>
<p>Subsequent you will see the embedded web page, https://join.octavio.lab.</p>
<iframe src="https://join.octavio.lab" width="1024" height="768" title="CMS 3.2 Customizable CSP" allowusermedia allow="microphone; camera; display-capture"></iframe>
</body>
</html>
```

ステップ4：必要に応じて、webbridge設定またはWebページコードでFrame-Ancestor値を修正します。

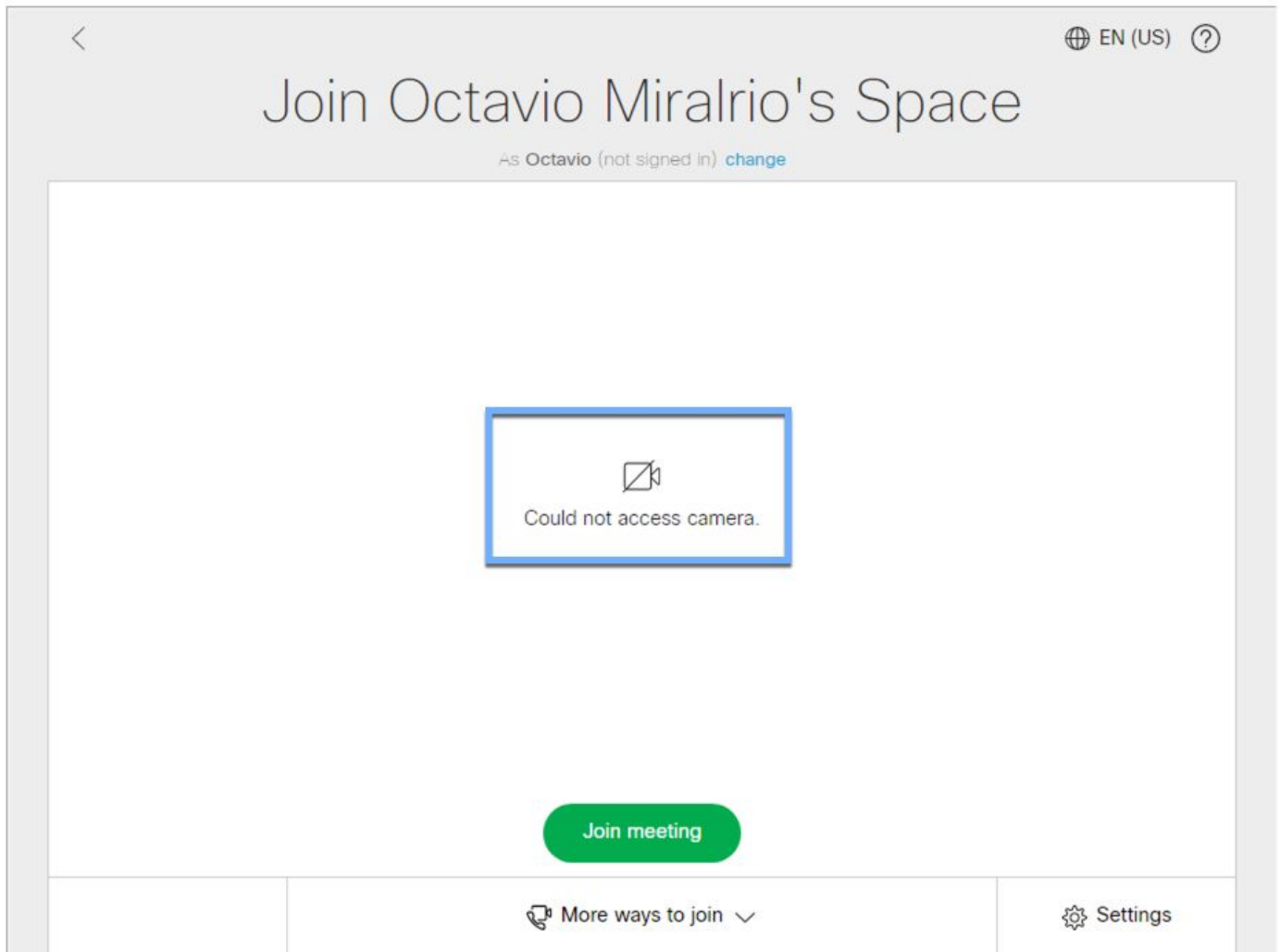
2. Webアプリが読み込まれていますが、カメラやマイクにアクセスできません。

This is the title of the Content Security Policy

Welcome to the CMS Content Security Policy Demonstration.

All this text is not part of the webbridge itself.

Below you will see the embedded webapp page, <https://join.octavio.lab>.



この問題は、iframeが正しく設定されていないために発生します。オーディオとビデオをサポートするには、iframeに`allowusermedia allow="microphone;カメラ;display-capture"`と入力します。

この問題を解決するには、次の手順を実行します。

ステップ1: Webサーバを開き、メインページのHTMLファイルを見つけます。

ステップ2 : テキストエディタを使用してHTMLファイルを編集します。

ステップ3 : 次のコードに示すように、メディア属性をiframeに追加します。