



Unified CVP のインストール後

Unified CVP のインストール後、すべての CVP コンポーネントが正常にインストールされたことを確認するためにインストール後のタスクを実行します。さらに、ポートブロッキングをディセーブルにし、セキュリティの問題に対処し、CVP コンポーネントにライセンスを適用します。



(注) インストール後のタスクには、CVP コンポーネントの設定は除外されます。CVP コンポーネントの設定については、『*Configuration Guide for Cisco Unified Customer Voice Portal (Cisco Unified Customer Voice Portal 設定ガイド)*』を参照してください。

この章では、次のインストール後のタスクについて説明します。

- [ポートブロックのディセーブル化, 1 ページ](#)
- [セキュリティ, 2 ページ](#)
- [Unified CVP REST API のメタデータの同期の開始, 2 ページ](#)

ポートブロックのディセーブル化

ポートの妨害するように設定されたアンチウイルスソフトウェアがあるコンピュータ上に Unified CVP Server コンポーネントをインストールした場合は、Unified CVP プロセスと Tomcat 実行ファイルを除外します。



(注) McAfee VirusScan 専用のポートをディセーブルにするには、次の手順を使用します。McAfee VirusScan 以外のアンチウイルスソフトウェアを使用している場合は、そのアンチウイルスソフトウェアのポートブロッキングルールで同等の除外を実行します。

手順

-
- ステップ 1** VirusScan コンソールで、[Access Protection] をダブルクリックし、[Port Blocking] タブをクリックします。
- ステップ 2** [Prevent IRC communication] チェックボックスがオンになっている場合は、次の手順を実行します。
- a) [Prevent IRC communication] のプロパティを編集するには、[Edit] をクリックします。
 - b) [Add or edit a port blocking range] ダイアログボックスで、**VoiceBrowser.exe** と Tomcat 実行ファイルを [Excluded Process] テキストボックスに追加し、[OK] をクリックします。
- 重要** CVP Server の音声ブラウザと Tomcat 実行ファイルの文字列のスペースを削除し、正しく動作するようにします。
-

セキュリティ

選択した Unified CVP 展開によっては、特定のセキュリティ上の考慮事項に対処する必要があります。セキュリティについては、『*Configuration Guide for Cisco Unified Customer Voice Portal (Cisco Unified Customer Voice Portal 設定ガイド)*』を参照してください。



(注) Windows 2008 R2 に対するセキュリティ強化の追加は推奨されません。

Unified CVP REST API のメタデータの同期の開始

CVP REST API アーキテクチャでは、メディア サーバのメディア ファイルおよび VXML Server の VXML アプリケーションの情報は、Derby データベースのメタデータとして WSM Server に保存されます。これらのメタデータ情報は、REST API コールによって作成、更新、削除されます。メタデータが VXML Server およびメディア サーバのファイルと同期していない可能性がある場合があります。CVP Server の追加および削除、REST API 以外のツールによるアプリケーションおよびメディア ファイルの展開、VXML Server、REST API がサポートされていない 10.0 よりも前のバージョンからアップグレードした VXML Server の例を示します。

VXML Server とメディア サーバのファイルとメタデータの同期を有効にするには、新しいコマンドライン ツール「metasynch.cmd」（C:\Cisco\CVP\wsm\CLI で入手可能）を使用できます。内部的にツールは Synch Up API を使用して同期を実行します。これには 3 つの引数、つまり、WSM ユーザ名、WSM ユーザパスワード、およびサーバタイプ（MEDIA、VXML、または VXML_STANDALONE）が使用されます。サーバタイプの情報に基づいて、それぞれのサーバタイプのすべてのサーバが同期されます。サーバタイプ引数を入力しないと、メタデータは OAMP で設定されているすべてのメディア サーバおよび VXML Server と同期されます。

アップグレードの場合、メディア ファイルおよび VXML アプリケーションはメディア サーバと VXML Server にありますが、対応するメタデータ情報は、WSM Server にはありません。メタデータ情報がないと、ユーザは REST API を使用できず、メディア サーバと VXML Server の既存のメディア ファイルと VXML アプリケーションへのアクセス、更新、および削除ができなくなります。

Sync-up ツールを使用したメタデータ ファイルの同期

`metasynch.cmd` を呼び出すには、次の手順を実行します。

手順

-
- ステップ 1** C:\Cisco\CVP\wsm\CLI の場所に移動します。
- ステップ 2** 次の引数を指定して `metasynch.cmd` ファイルを実行します。
- `wsm` のユーザ名
 - `wsm` のパスワード

例 :

```
metasynch.cmd wsmusername wsmpassword MEDIA
```

```
Usage : metasynch [オプション] username password [サーバ タイプ]
```

```
servertype : MEDIA/VXML/VXML_STANDALONE
```

```
options : -help -? print this help message
```

(注) サーバタイプの引数は、MEDIA、VXML、または VXML_STANDALONE タイプである必要があります。サーバタイプ引数を指定しないと、メタデータは、VXML Server 上のすべての VXML アプリケーションと、メディア サーバ上のすべてのメディア ファイルと同期されます。synch コマンド ツールのログは次の場所にあります。

```
C:\Cisco\CVP\wsm\CLI\log\SyncTool.log
```

