

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[認証によって署名される要求を生成して下さい](#)

[認証局の認証に署名して下さい](#)

[証明書のインストール](#)

[認証をコピーして下さい](#)

[ローカル コンピュータ ストアに認証をインポートして下さい](#)

[IIS 認証を結合 して下さい](#)

[確認](#)

[計画はキャンセルします](#)

[トラブルシューティング](#)

[関連記事](#)

## 概要

この資料は方法のコンフィギュレーションプロセスを統一されたコンタクトセンター 企業 ( UCCE ) 診断フレームワーク柱廊玄関ツールのための CA 署名入り認証をインストールする説明したものです。

## 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。

- Active Directory
- ドメイン ネーム システム ( DNS ) サーバ
- すべてのサーバおよびクライアントのために展開され、はたらく CA インフラストラクチャ
- 診断フレームワーク柱廊玄関

認証警告を受け取らないでブラウザの IP アドレスの入力によって診断フレームワーク柱廊玄関ツールにアクセスすることはこの技術情報のスコープからあります。

### 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。

- Cisco UCCE 11.0.1
- Microsoft Windows サーバ 2012 R2
- Microsoft Windows サーバ 2012 R2 認証局
- Microsoft Windows 7 SP1 OS

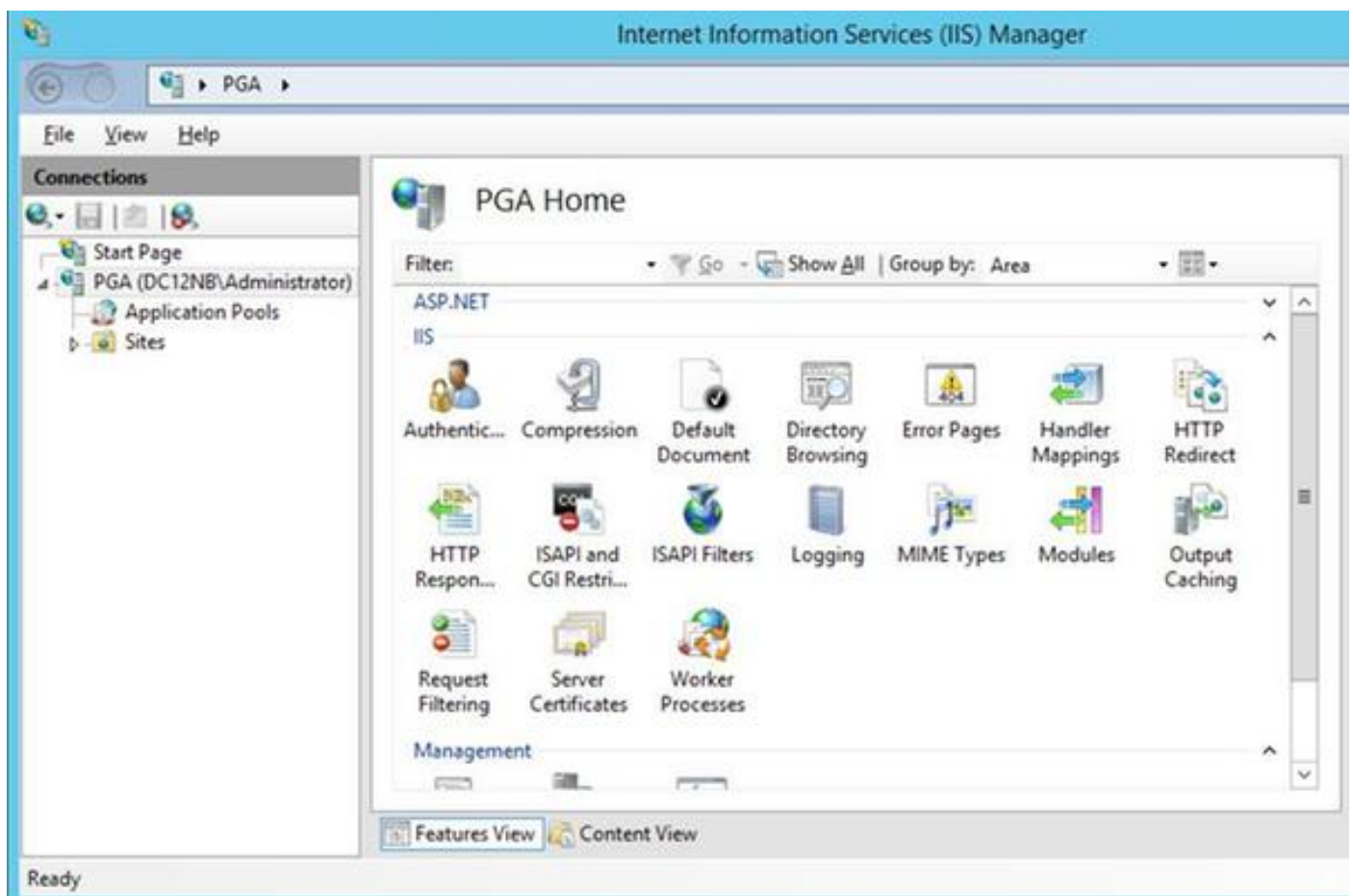
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

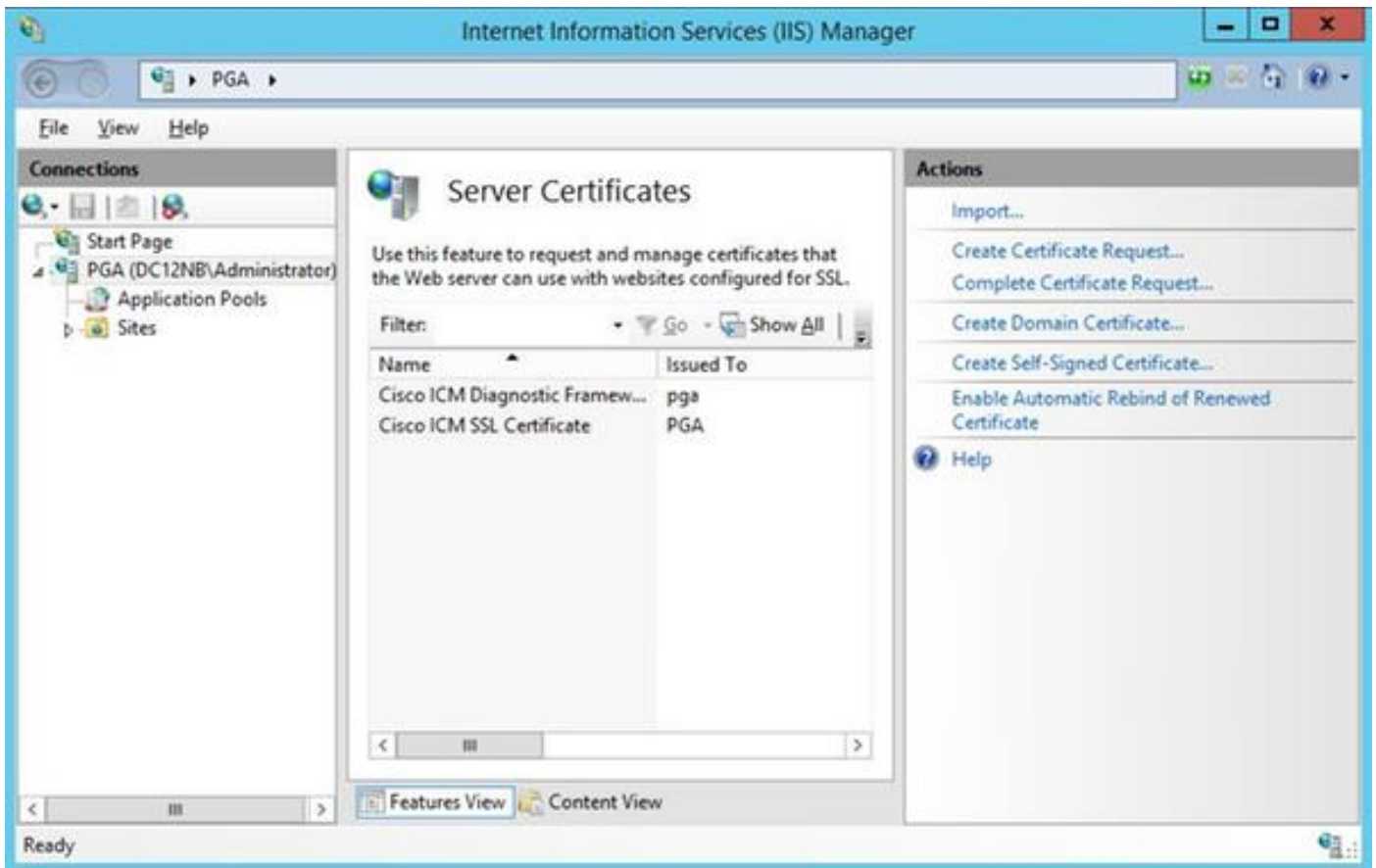
## 設定

### 認証によって署名される要求を生成して下さい

Internet Information Services（IIS）マネージャを開いて下さい、サイトを、例およびサーバ証明の Peripheral Gateway A（PGA）選択して下さい。



アクション パネルの証明書要求を『Create』を選択して下さい。



Common Name (CN) を、組織 (o)、Organization Unit (OU)、局所性 (l)、状態 (ST)、国 (c) フィールド入力して下さい。Common Name は完全修飾ドメイン名 (FQDN) ホスト名 + ドメイン名と同じである必要があります。

Request Certificate

### Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="pga.allevich.local"/>
Organization:	<input type="text" value="Cisco"/>
Organizational unit:	<input type="text" value="TAC"/>
City/locality:	<input type="text" value="Krakow"/>
State/province:	<input type="text" value="Malopolskie"/>
Country/region:	<input type="text" value="PL"/>

Previous Next Finish Cancel

暗号化サービスプロバイダーのデフォルト設定を残し、ビット長を規定して下さい: 2048。

パスをどこに保存するか選択して下さい。たとえば pga.csr 名前のデスクトップで。

テキストエディタの新しく作成された要求を開いて下さい。



```
pga.csr - Notepad
File Edit Format View Help
|-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEYzCCA0sCAQAwbzELMAKGA1UEBhMCUEwxFDASBgNVBAGMC01hbG9wb2xza211
MQ8wDQYDVQQHDAZLcmFr3cx3DjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANUQUx
GzAZBgNVBAMMEBnYS5hbGxldm1jaC5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKbbmpv6sBNMY8LQeaESAna7VDS/572pRMeopNYyohwu72x
z5XYGLsjaMk/qr4yHhd1pP0dQ58V4p/X/gxEZYAbDTyBVmLX3Qufj0KgW5RhBufe
5DizHnWcbUQYwPDiHumCULNSgGNVuh5bjHhYXhj5+hRRJcbldbBHVWwYwNf0GMnf
/+LPRTt81RRQ4YUZ5VxU5eeRvTQTJpK/M/Hli8XSJbgzK1dv96VPTt1qewptJd40
quLU22zIgZpMatnnZix2uFrV2IfwVNu+Pwq0RQt+MdeUQAKLCdtQjqLJs2CZht+r
hYuevF289SGf8oVYuNmD57YKeT1aN2CTZy6y3wECAwEAaCCAA0wGgYKKwYBBAGC
Nw0CAzEMFgo2LjIu0TIwMC4yMEkGCSsGAQQBgjcVFDE8MD0CAQUMENBnYS5hbGx1
dmljaC5sb2NhbAwUREMxMk5CXEFkbWluaXN0cmF0b3IMC0luZXRNZ3IuZXh1MHIG
CisGAQQBgjcNAgIxZDBiAgEBHloATQBpAGMAcGvAHMAbwBmAHQAIABSAFMAQQAg
AFMAQwBoAGEAbgBuAGUAbAAgAEMAcb5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQ
AHIAbwB2AGkAZABIAHIDAQAwwc8GCSqGSIb3DQEJDDjGBwTCBvjaOBgNVHQ8BAf8E
BAMCBPAwEwYDVR01BAwwCgYIKwYBBQUHAwEweAYJKoZIhvcNAQkPBGswaTA0Bggq
hkiG9w0DAGICAIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAF1AwQBKjALBglghkgB
ZQMEAS0wCwYJYIZIAWUDBAECMA5GCWCGSAF1AwQBbTAHBgUrDgMCBzAKBggqhkiG
9w0DBzAdBgNVHQ4EFgQUfj556Gk1SHyFrvNZNNA/CK6gLM0wDQYJKoZIhvcNAQEF
BQADggEBABwz3dTNqqEKTVRJ1dfZu1zY2tS/7tZuBBn1FWF0tP361F0kIgYodUz3
Wn49aA1GVxYpwFrw4wrrwj1Ln17C+LQQMh1bPvwy+IWAgAAGdh2KgXzAVXchnFEE
HY9q8QF7aJnn+Jk+i13atCkRWB+L0leSAx/R/Mv5z1vMli1tkbMkaTUqzR/wvFrm
6RElv+Dwt31zNZeUvt8qrw5YynrEjoSZFPuvdt0oPZ6zUMAYzH8PwribmdGSSWxs
NpJM5DjSwrXQ6r2R6qBItjLhNsVTRZQQtHb/+DIhfLe5neCyRgtW4smmViSg1qb0
/z5CP6gHi8IZ9rrg0xCwzWmsN6mQ18M=
-----END NEW CERTIFICATE REQUEST-----
```

CTRL+C.のバッファに認証をコピーして下さい。

## 認証局の認証に署名して下さい

注: 外部認証局を使用していれば ( GoDaddy のように ) 生成した後 CSR ファイルをもらう  
それらに連絡する必要があります。

Enroll ページ CA サーバ証明に署名して下さい。

[https:// <CA-server-address>/certsrv](https://<CA-server-address>/certsrv)

SELECT 要求 **認証**はバッファに、**高度証明書要求** 証明書署名要求 ( CSR ) コンテンツを貼り付  
け。それから **Webサーバとしてテンプレート**を『Certificate』を選択して下さい。

基礎 64 符号化された認証をダウンロードして下さい。

認証を開き、より遅い使用方法のための拇印フィールド ä® ä³ä³ää³ä をコピーして下さい。拇印からの領域を取除いて下さい。

## 証明書のインストール

### 認証をコピーして下さい

柱廊玄関ツールが見つけられる UCCE VM に最近生成された証明書ファイルをコピーして下さい。

### ローカル コンピュータ ストアに認証をインポートして下さい

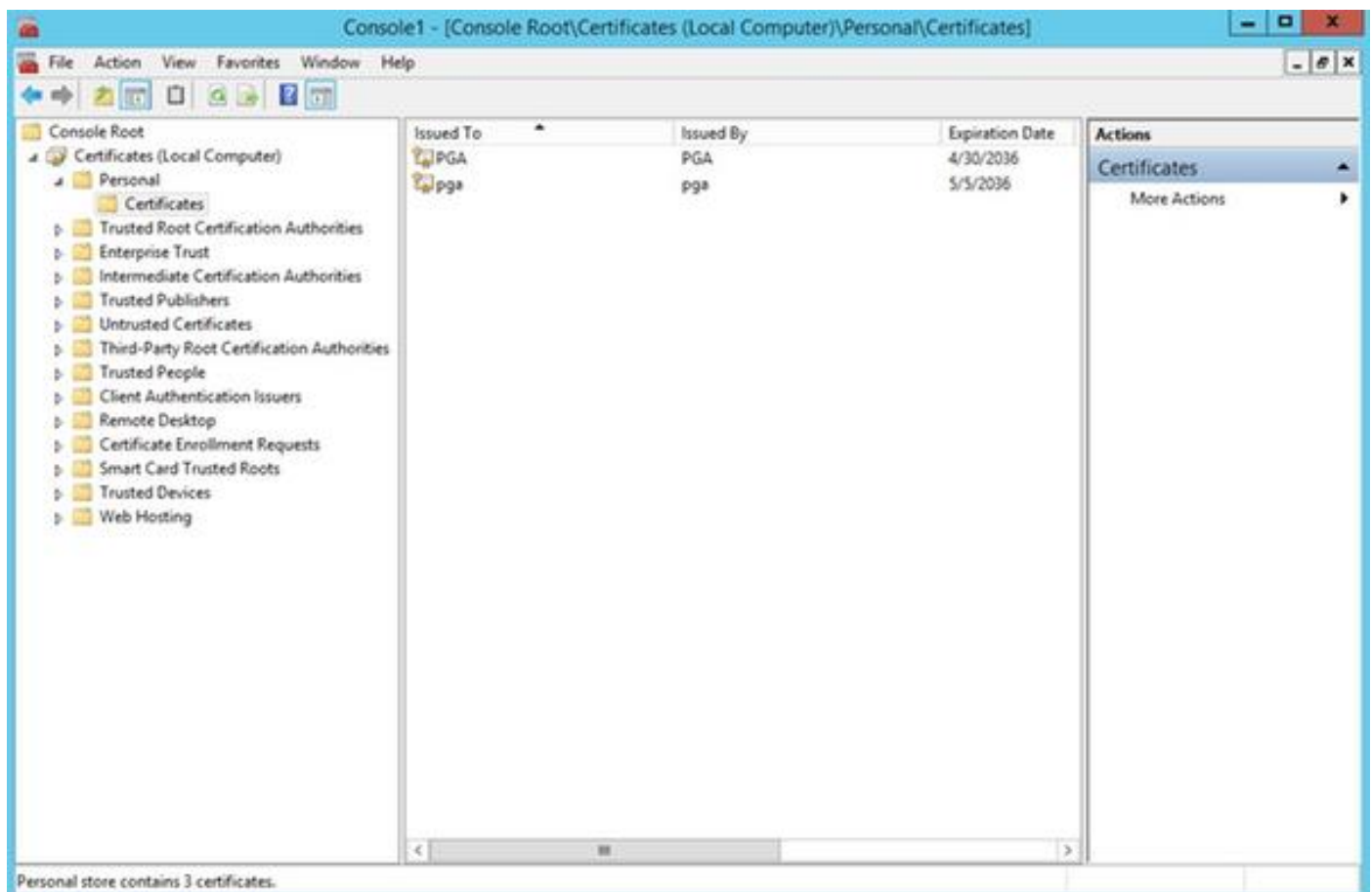
メニュー、タイプ**実行**および **mmc** を『Start』を選択することによる同じ UCCE サーバ起動 Microsoft Management Console ( MMC ) コンソール。

『Add/Remove Snap-in』をクリックすればダイアログボックスで『Add』をクリックして下さい。

それから**認証**メニューを選択し、追加して下さい。

証明書スナップインダイアログボックスで、> **ローカル コンピュータ** > 完了 『Computer Account』をクリックして下さい。

身分証明書 フォルダへのナビゲート。



操作ウィンドウでは操作を > すべてのタスク > インポート 『More』 を選択して下さい。

認証ストアは個人的に設定されたことを以前に生成された Next メニューで確認しなさい認証を 『Next』 をクリックし、参照し、選択すれば。最後の画面で選択される証明書ストアおよび証明書ファイルを確認し、『Finish』 をクリックして下さい。

## IIS 認証を結合して下さい

CMD アプリケーションを開いて下さい。

診断柱廊玄関ホーム フォルダーへのナビゲート。

```
cd c:\icm\serviceability\diagnostics\bin
```

柱廊玄関ツールのための現在の認証 バインディングを取除いて下さい。

```
DiagFwCertMgr /task:UnbindCert
```

CA 署名入り認証を結合して下さい。

ヒント：テキストエディタ ( notepad++ ) をハッシュの領域を取除くのに使用して下さい。

前に保存される取除かれる領域とハッシュを使用して下さい。

```
DiagFwCertMgr /task:BindCertFromStore /certhash:bc6bbe23b8b3a26d8446c252400f9264c5c30a29
```

認証が正常に結合 されれば出力の同じような行を見るはずです。

「認証 バインディングです有効」は

認証 バインディングがこのコマンドを使用して正常だったことを確認して下さい。

```
DiagFwCertMgr /task:ValidateCertBinding
```

再度同じようなメッセージは出力で表示する必要があります。

「認証 バインディングです有効」は

注: DiagFwCertMgr はデフォルトでポート 7890 を使用します。

診断フレームワーク サービスを再開して下さい。

```
sc stop "diagfwsvc"sc start "diagfwsvc"
```

ヒント： Service リストおよび特に柱廊玄関サービス名は CMD ツールの tasklist コマンドによってチェックすることができます。

```
tasklist /v
```

## 確認

FQDN を使用して診断フレームワーク ページを開けば認証 警告メッセージをプロンプト表示するべきではありません。

## 計画はキャンセルします

柱廊玄関ツールにアクセスを失ったら自己署名証明書を再生し、例外を追加できます。それはこのコマンドを使用してすることができます。

```
DiagFwCertMgr /task:CreateAndBindCert
```

## トラブルシューティング

診断フレームワーク柱廊玄関ツールに IP アドレスを時ログオン使用しないで下さい。FQDN が Certificate CN フィールドで規定される値と一致するならないので、まだ認証警告を受け取りません。

すべてのサーバが NTP ソースと同期されることを確認して下さい。

```
w32tm /monitor
```

認証対象代替名 ( SAN ) または楕円曲線デジタル署名アルゴリズムを ( 試みれば EC DSA ) 使用するためにまたは 4096 の変調長さ 認証は-これらの機能の 1 つに特定ではないこと最初に隔離します。

## 関連記事

[UCCE \ PCCE -得るべきプロシージャおよび Upload ウィンドウ サーバ 自己が。2008 のサーバの署名されたまたは認証局 \( CA \) 認証](#)

[設定して下さい Cisco 音声 オペレーティング システム \( VOS \) の CLI によって CA 署名入り認証を](#)