

HP Enterprise Collaboration

Windows®オペレーティングシステム向け

ソフトウェアバージョン: 1.1

インストールおよび構成ガイド

ドキュメントリリース日: 2012年8月(英語版)

ソフトウェアリリース日: 2012年8月(英語版)



ご注意

保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密性のあるコンピュータソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピュータソフトウェア、コンピュータソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

© Copyright 2012 Hewlett-Packard Development Company, L.P.

商標について

Adobe™は、Adobe Systems Incorporated (アドビシステムズ社) の商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

本製品には 'zlib' 汎用圧縮ライブラリのインタフェースが使用されています。'zlib': Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアのバージョン番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに更新されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新の更新のチェック、またはご使用のドキュメントが最新版かどうかの確認には、次のサイトをご利用ください。

<http://support.openview.hp.com/selfsolve/manuals>

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDの取得登録は、次のWebサイトから行なうことができます。

<http://h20229.www2.hp.com/passport-registration.html>(英語サイト)

または、HP Passport のログインページの [**New users - please register**] リンクをクリックします。

適切な製品 サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPの営業担当にお問い合わせください。

サポート

HPソフトウェアサポートオンラインWebサイトを参照してください。

<http://support.openview.hp.com>

HPソフトウェアが提供する製品、サービス、サポートに関する詳細情報をご覧ください。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HPソフトウェアサポートWebサイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポートケースとエンハンスメント要求の登録とトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HP サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部を除き、サポートのご利用には、HP Passportユーザとしてご登録の上、ログインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDの登録は、次の場所で行います。

<http://h20229.www2.hp.com/passport-registration.html>(英語サイト)

アクセスレベルに関する詳細は、以下のWebサイトにアクセスしてください。

http://support.openview.hp.com/access_level.jsp

目次

インストールおよび構成ガイド.....	1
目次.....	5
はじめに.....	7
HP Enterprise Collaborationドキュメントライブラリ.....	7
前提条件.....	9
データベースと表領域の権限.....	9
電子メールの構成.....	9
Enterprise Collaborationのインストールと構成.....	10
Enterprise Collaborationのインストール.....	10
ユーザーリポジトリとユーザーの役割の構成.....	24
リバースプロキシ使用時のセキュアログインの構成.....	27
Office Communicator ServerおよびMS Lync Serverとの統合の設定.....	29
ルート証明機関 (CA) の証明書のインストール.....	29
OCSエージェントマシンでのサーバー証明書のインストール.....	37
エージェントのプロビジョニング.....	44
OCS 2007でのエージェントプロビジョニング.....	44
Lync 2010のエージェントプロビジョニング.....	47
リッチコンテンツをサポートするOCSの設定.....	48
リッチコンテンツをサポートするOCクライアントの設定.....	51
ECとOCSの統合のサニティテスト.....	51
追加の構成手順.....	53
メールクライアントの証明書のインストール.....	53
カスタマー証明書のインストール.....	53
デフォルトの安全な認証を無効化 (オプション).....	54
Deployment Managerでの構成の更新.....	55
アダプターの設定.....	59
EC構成の1.0から1.1へのアップグレード.....	61

デスクトップクライアントのインストール.....	63
付録A: HP Enterprise Collaborationでのネットワーク構成スキーマ.....	68
付録B: external-ldap.propertiesファイルの更新.....	69
基本的なLDAPプロパティ.....	69
ユーザープロバイダーの構成.....	69
ユーザーオブジェクトクラスの構成.....	70
グループ検索.....	71
グループオブジェクトクラス (LDAPベンダー固有).....	72
グループ階層.....	73
詳細構成.....	73
Apache Directory Studio LDAPブラウザによるLDAPへのログイン.....	74

第1章

はじめに

Enterprise Collaboration (EC) は、HP製品を使用するIT組織を対象にしたコラボレーションプラットフォームであり、ほぼすべてのフローで発生するコラボレーションを効率化し、円滑にします。ECは、ITワークスペースにあるアプリケーションで管理する構造化データと、それをサポートする非構造的なコラボレーションを連携します。

このガイドでは、Enterprise Collaborationのインストールと構成の方法について説明します。

Enterprise Collaborationのインストールと構成は、次の手順で行います。

1. 「Enterprise Collaborationのインストールと構成」(10ページ)
2. 「ユーザーリポジトリとユーザーの役割の構成」(24ページ)
3. 「Office Communicator ServerおよびMS Lync Serverとの統合の設定」(29ページ) この手順は、ECとOffice Communicatorを組み合わせて使用する場合に実行します。
4. 「Deployment Managerでの構成の更新」(55ページ) この手順は、初期インストールで指定したデータベースまたはOCS設定を変更する場合や、ECをOffice Communicator Serverで使用するための構成を行う場合 (手順3のOCS統合設定を行った場合) に実行します。
5. 「アダプターの設定」(59ページ) この手順は、ECと他のアプリケーションを統合する場合に実行します (コンテキストオブジェクトを会話に追加する機能や、既存のコンテキストオブジェクトをファセットで表示する機能など)。
6. 「追加の構成手順」(53ページ): システム設定によっては、構成作業を追加で実行する必要があります。使用中のシステムが次のいずれかに合致する場合、この項を参照してください。
 - メールサーバーへのアクセスにセキュリティ保護された接続と自己署名の証明書を使用する場合
 - スタンドアロンのWebアプリケーションを使用するネットワーク構成を行う場合
 - リバースプロキシを使用するネットワーク構成を行う場合
 - 認証時のhttpsへのリダイレクトを無効にする場合 (セキュリティが低下するのでお勧めしません)

HP Enterprise Collaborationドキュメントライブラリ

HP Enterprise Collaborationは、次のガイドとリファレンスがPDF形式で付属しています。HP Enterprise Collaborationのドキュメントの最新版については、次のHPソフトウェアの製品マニュアルウェブサイトにアクセスしてください。<http://support.openview.hp.com/selfsolve/manuals>このサイトにアクセスするにはHP Passportへの登録とサインインが必要です。

ガイド名	説明
HP Enterprise Collaborationインストールおよび構成ガイド	HP Enterprise Collaborationのインストールと構成方法を説明しています。
HP Enterprise Collaborationコンセプトガイド	HP Enterprise Collaboration の概念、コンポーネント、会話ワークフローについて詳しく説明しています。
HP Enterprise Collaboration Integration Guide	カスタマイズしたアプリケーションコンテンツを追加するアダプターの開発方法と、Enterprise Collaborationをサードパーティアプリケーションに統合する方法について説明しています。
HP Enterprise Collaboration Developers Guide	HP Enterprise Collaborationをユーザーが開発したアプリケーションに統合する方法について説明しています。
HP Enterprise Collaborationリリースノート	HP Enterprise Collaborationに関する最新情報を紹介します。
HP Enterprise Collaboration Support Matrix	HP ECのシステム要件と、HP Enterprise Collaborationで現在サポートされるHP製品とバージョンのリストを掲載します。
HP Enterprise Collaboration Open Sources and Third-Party Software Agreements	HP Enterprise Collaborationに付属するオープンソースコンポーネントとサードパーティコンポーネントのライセンスのリストを掲載します。

さらに、DVDの次の場所にHP Enterprise Collaborationのムービーがあります。

Documentation\Movies\HPEC_1.wmv

前提条件

Enterprise Collaborationをインストールする前に、Windows UAC (ユーザーアカウント制御) を無効にする必要があります。UACが有効になった状態でインストールを行うと、検証ページでエラーメッセージが表示されます。

UACを無効にするには、次の手順を実行します。

1. [スタート] メニューから [ファイル名を指定して実行] を選択し、**msconfig** と入力します。
2. [システム構成] ウィンドウが開いたら、[ツール] タブを選択します。
3. ツールリストから [UAC設定の変更] を選択して [起動] をクリックします。
4. [ユーザー アカウント コントロール] ウィンドウが開いたら、[通知しない] までスクロールして [OK] をクリックします。

データベースと表領域の権限

Enterprise Collaborationデータベースのインストールと構成は、一般ユーザー (特殊な権限が必要) で実行でき、DBAユーザーで実行する必要はありません。

インストールを行うユーザー <ユーザー名> を作成する際には、次の権限を割り当ててください。

```
GRANT CREATE USER TO <ユーザー名> WITH ADMIN OPTION;
```

```
GRANT CONNECT TO <ユーザー名> WITH ADMIN OPTION;
```

```
GRANT UNLIMITED TABLESPACE TO <ユーザー名> WITH ADMIN OPTION;
```

```
GRANT CREATE VIEW TO <ユーザー名> WITH ADMIN OPTION;
```

```
GRANT RESOURCE TO <ユーザー名> WITH ADMIN OPTION;
```

```
GRANT CREATE JOB TO <ユーザー名> WITH ADMIN OPTION;
```

インストール中に表領域の有無をチェックするので、インストールユーザーにはさらに次の権限を割り当てる必要があります。

```
GRANT SELECT ON DBA_TABLESPACES TO <ユーザー名>;
```

電子メールの構成

Enterprise Collaborationでは、会話の進行中、ユーザーの電子メールアドレス宛に電子メールを送信します。

ただし、一部のメールサーバーでは**EmailGeneralFromName** パラメーターがデフォルトでFalseに設定されているため、メールを送信できません。

この場合、JMXコンソールで**EmailGeneralFromName** パラメーターの値をTrueに変更してください。

第2章

Enterprise Collaborationのインストールと構成

ここでは、Enterprise Collaborationをインストールおよび構成する方法について詳しく説明します。インストールの前に、「前提条件」と「データベースと表領域の権限」の内容をよく読み、前提条件を満たして権限設定が正しく行われていることを確認してください。

Enterprise Collaborationのインストール

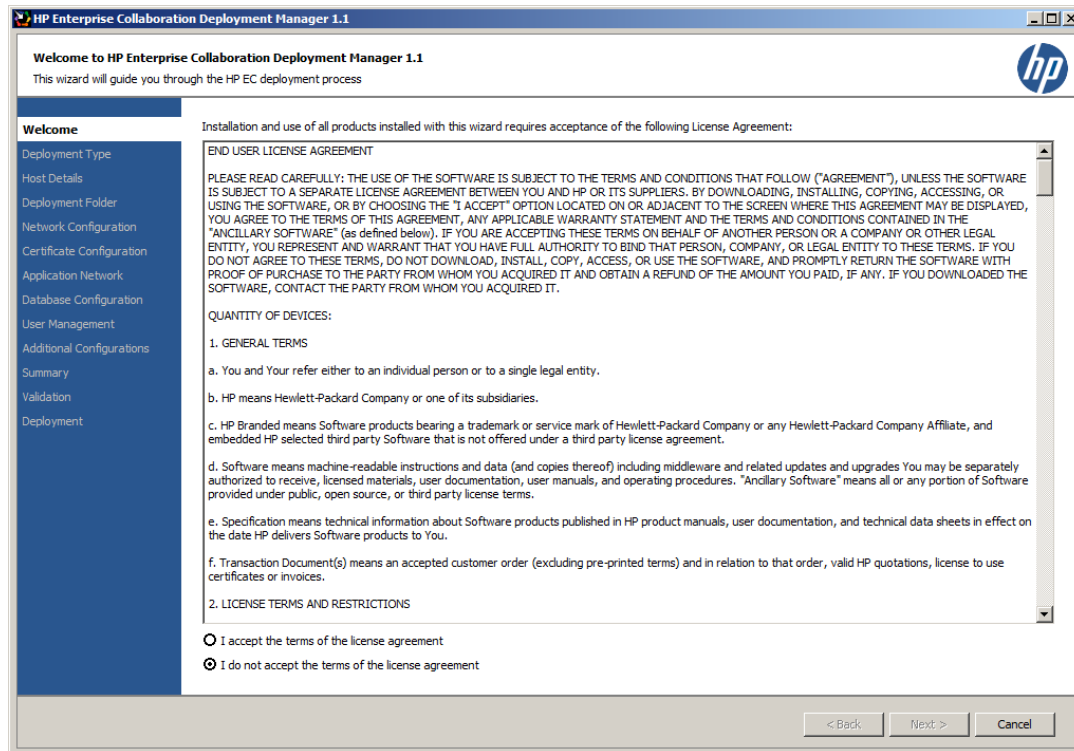
ここでは、Enterprise Collaboration (EC) のインストール手順について説明します。ECのインストール後に構成を変更する場合は、「Deployment Managerでの構成の更新」(55ページ)を参照してください。

Enterprise Collaborationをインストールするには、次の手順を実行します。

1. **ECのインストール用.zipファイルをHP Webサイトからダウンロードする場合**：ECインストール用.zipファイルを、ECが通信するすべてのECTポロジエントリティ (MSSQLや、メールサーバー、OCSなどオプションエントリティ) にアクセスできる場所に解凍します。

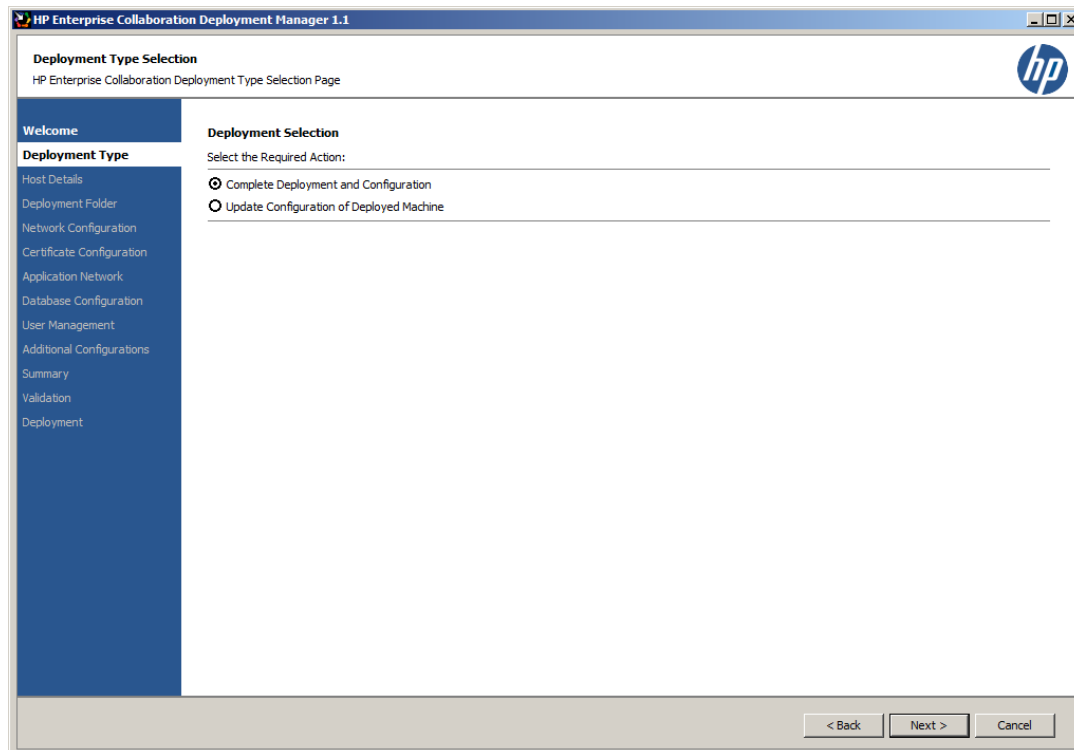
インストール作業にDVDを使用する場合：DVDの内容をすべてハードドライブ上のディレクトリにコピーします。

2. **Windows_Setup**フォルダーを開き、**EC.exe**をダブルクリックします。
3. Enterprise Collaboration Deployment Manager Wizardが起動します。



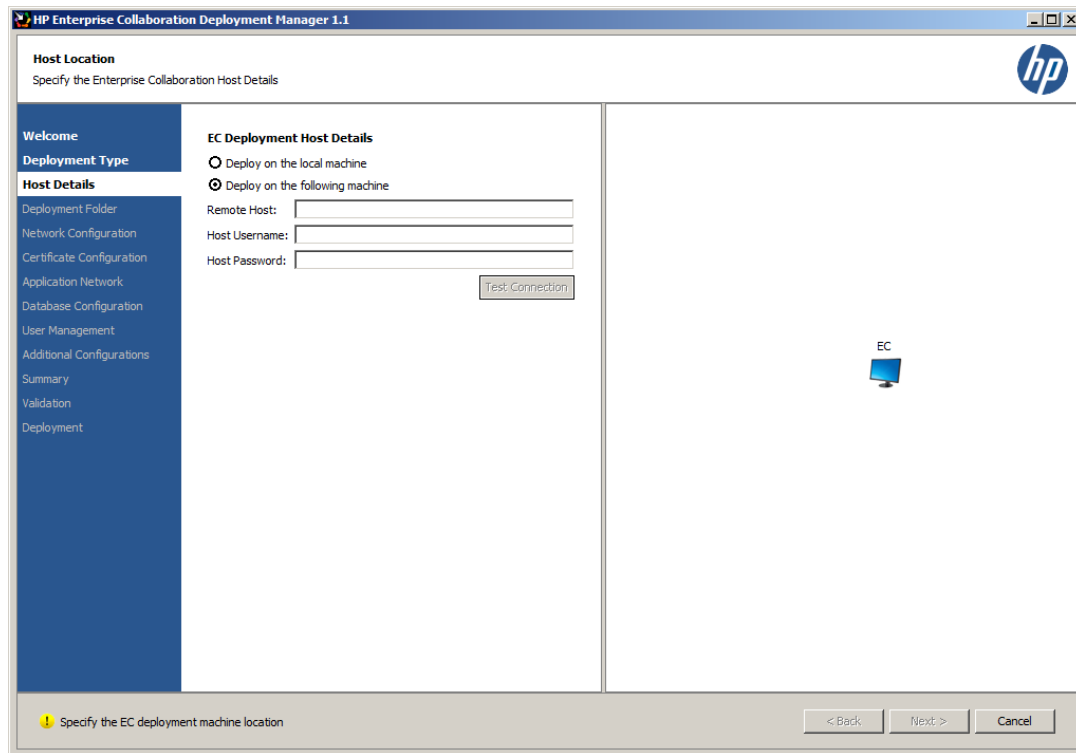
使用許諾契約書の内容を読み、[I accept the terms of the license agreement] を選択します。[Next] をクリックします。

4. [Deployment Type Selection] ページが開きます。



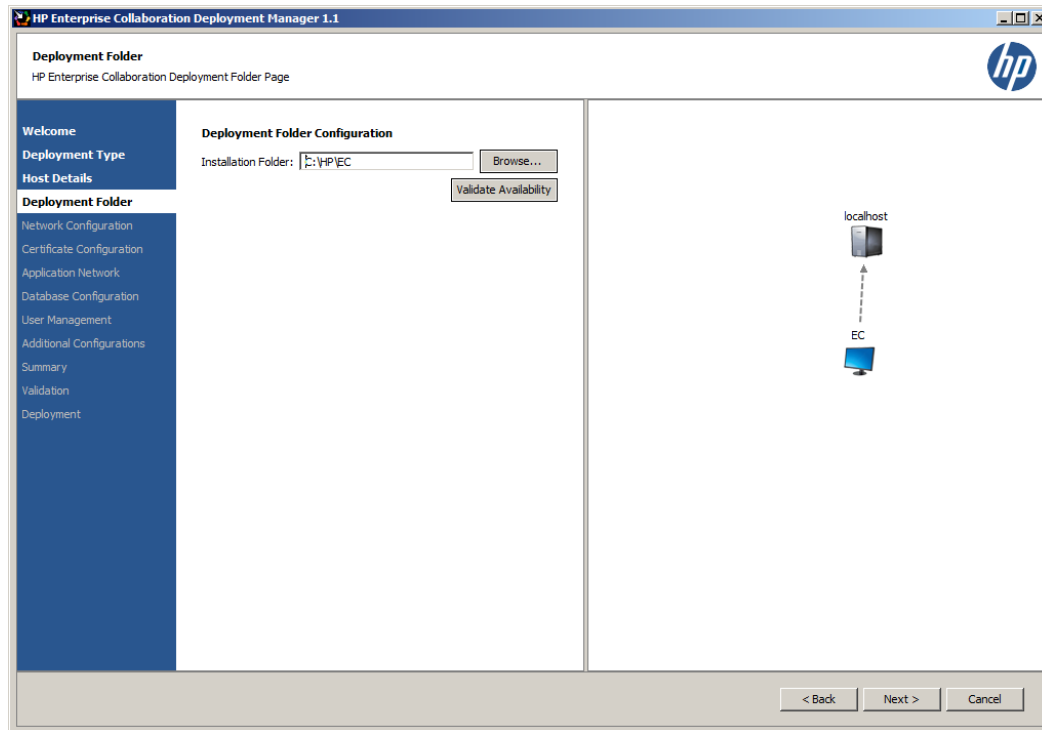
[Complete Deployment and Configuration] を選択します。[Next] をクリックします。

5. [EC Deployment Host Details] ページが開きます。



[Deploy on the local machine] または [Deploy on the following machine] のいずれかを選択します。

- [Deploy on the local machine] を選択すると、[Deployment Folder Configuration] ページが開きます。



[Browse] ボタンでインストールフォルダーを選択するか、デフォルトパスを使用します。[Next] をクリックします。

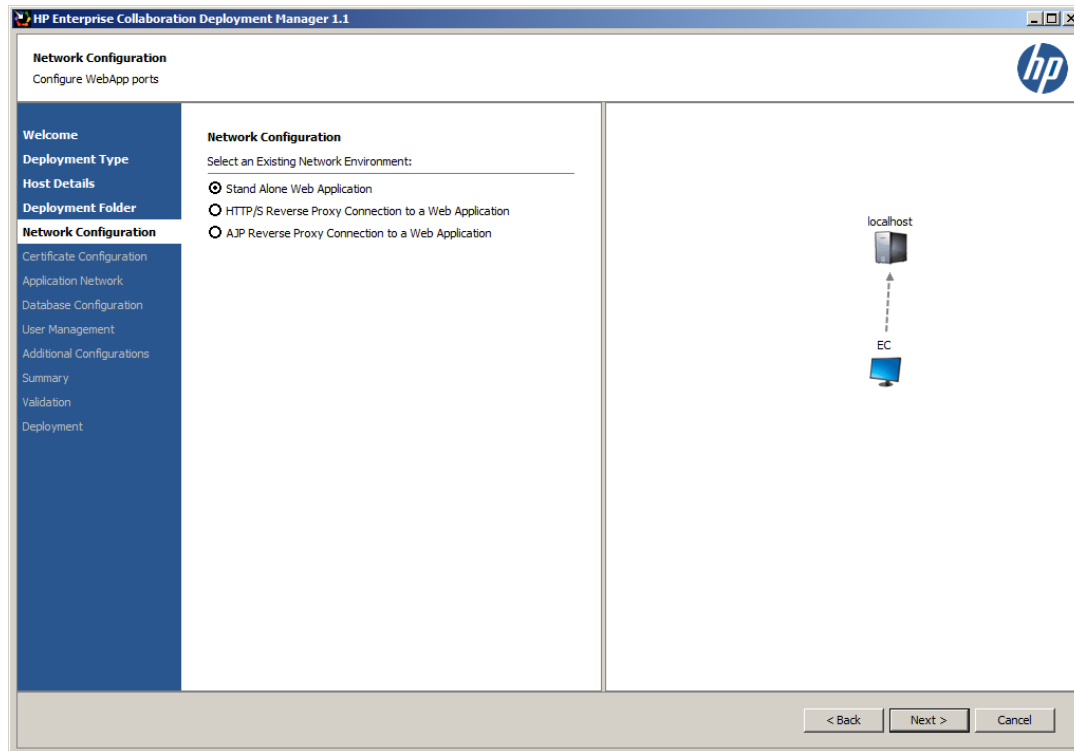
注： [Validate Availability] ボタンをクリックすると、インストールフォルダーパスが有効かどうかをチェックできます。このチェックでは、フォルダーパスがすでに存在し、内容の上書きが可能かどうかを確認します。オプションですが、実行することをお勧めします。

- [Deploy on the following machine] を選択した場合、リモートホストの場所、ホストのユーザー名、ホストのパスワード (オプション) を入力します。[Next] をクリックします。

注：

- リモートホストにデプロイする場合は、ここで [Test Connection] ボタンをクリックすると、PCとリモートホスト間の接続をテストできます。このテストはオプションですが、実行することをお勧めします。
- デプロイメント先のマシンを選択すると、これ以降のウィザードページで、サーバーマシンアイコンの上にマウスカーソルを置くと検証情報 (メモリ要件、使用可能なポートなど) が表示されます。構成プロセスでは、検証に影響を与えるデータ (使用済みのポートを選択するなど) を入力すると、サーバーマシンに「X」記号が赤色で表示され、競合ポートがポップアップウィンドウに表示されます。

6. [Network Configuration] ページが開きます。

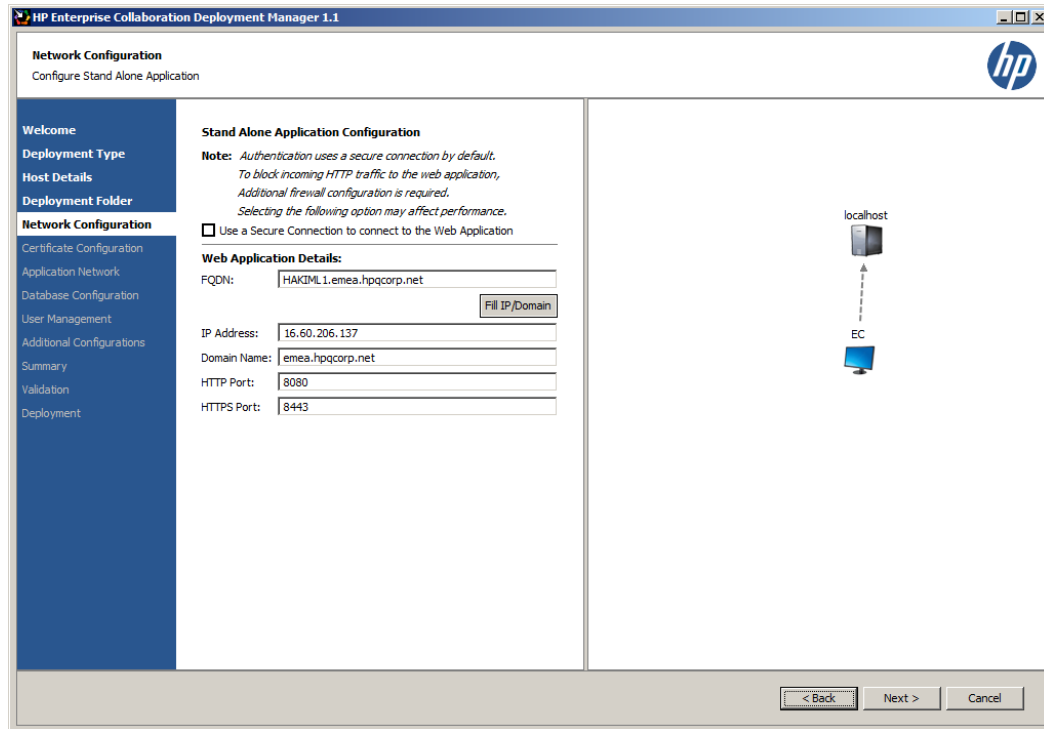


- a. ネットワーク環境として、次のいずれかを選択します。
- Stand Alone Web Application
 - HTTP/S Reverse Proxy Connection to a Web Application
 - AJP Reverse Proxy Connection to a Web Application

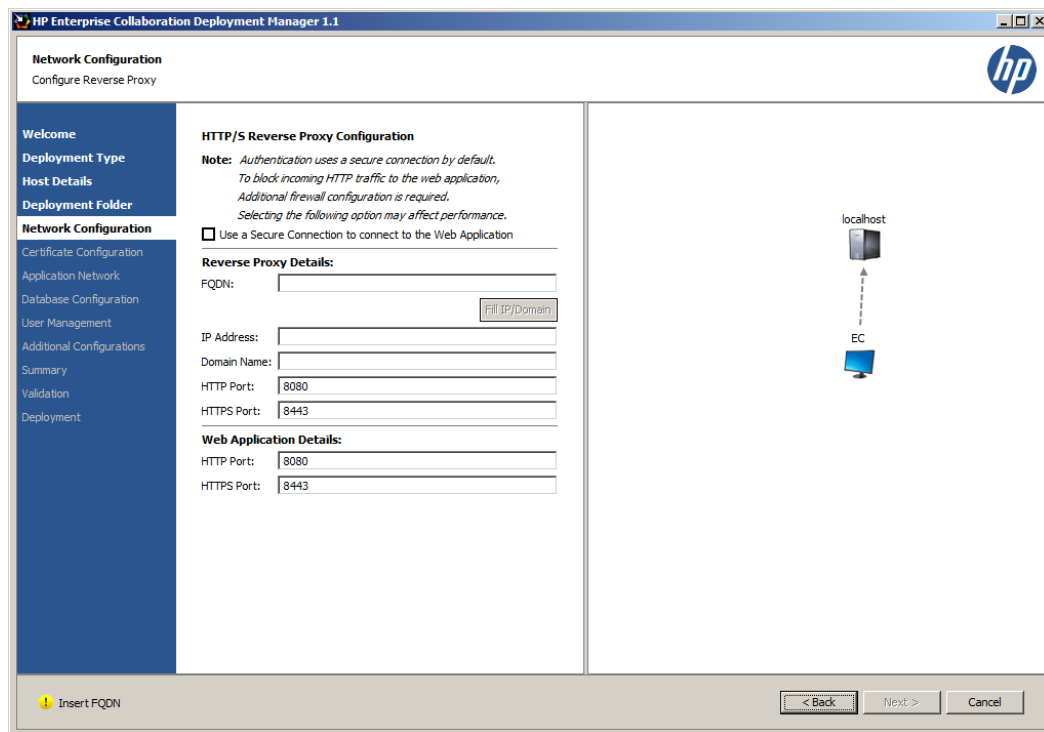
注: その他のネットワーク環境構成については、「付録A: HP Enterprise Collaborationでのネットワーク構成スキーマ」(68ページ)の図を参照してください。

- b. [Next] をクリックします。
7. 選択したネットワーク環境に応じて、次のページのいずれかが開きます。

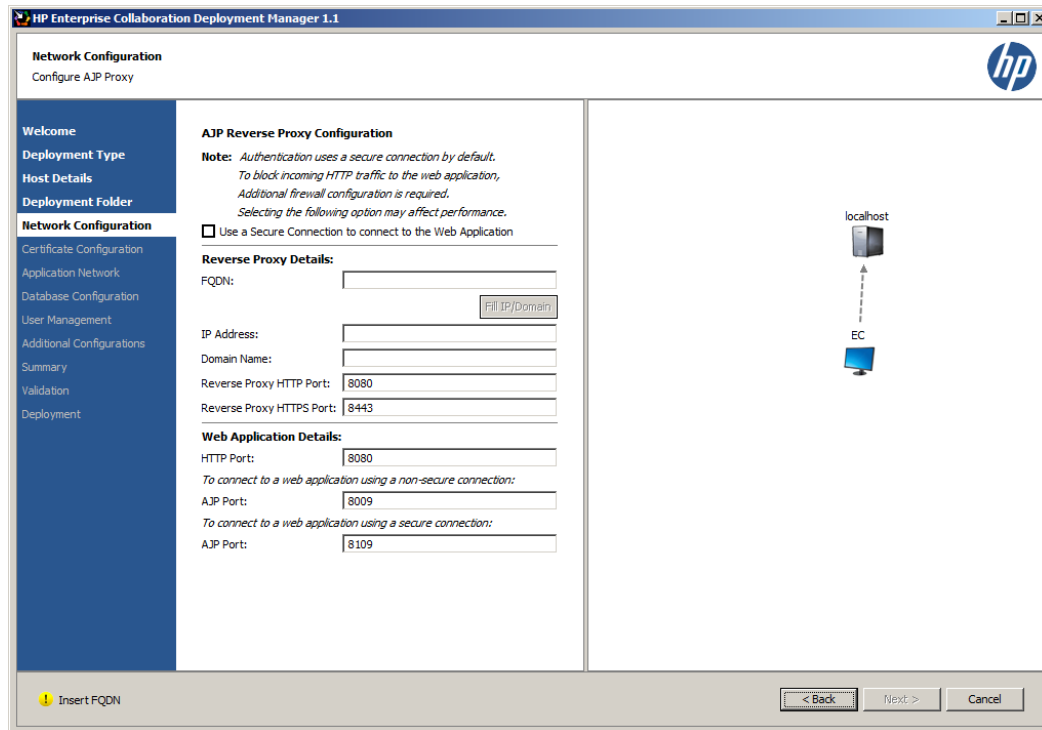
■ Stand Alone Application Configuration



■ HTTP/S Reverse Proxy Configuration



■ AJP Reverse Proxy Configuration



- a. ログイン認証の後にもセキュリティで保護された接続のみを使用してWebアプリケーションにアクセスするには、**[Use a Secure Connection to connect to the Web Application]** を選択します。デフォルトでは、セキュリティで保護された接続はログイン認証に使用されます。ログイン認証後、Webアプリケーションへのアクセスと同じレベルのセキュリティが、クライアントに適用されます。

Webアプリケーションへの着信HTTPトラフィックをブロックするには、さらにファイアウォールを構成する必要があります。

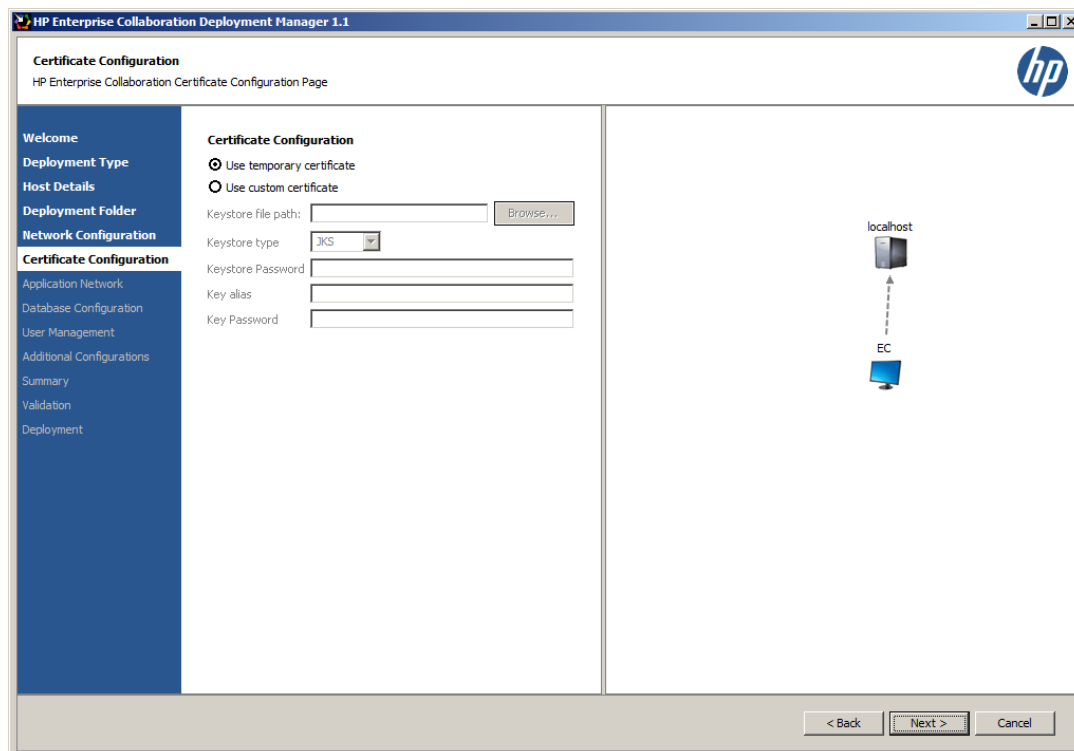
注： Webアプリケーションへの接続にセキュリティで保護された接続を使用する場合、すべての接続にSSLを使用すると、パフォーマンスが低下する可能性があります。

- b. ネットワーク構成ページで、次の内容を入力します。
- **[FQDN]:** WebアプリケーションまたはリバースプロキシのFQDNを入力します。スタンドアロン構成を行っている場合、デプロイするマシンのFQDNがデフォルト値です。

注： FQDNを入力したら、**[Fill IP/Domain]** をクリックすると、IPアドレスとドメイン名が自動入力されます。

- **[IP Address]:** WebアプリケーションまたはリバースプロキシのIPアドレスを入力します。スタンドアロン構成を行っている場合、デプロイするマシンのIPアドレスがデフォルト値です。
- **[Domain Name]:** Webアプリケーションまたはリバースプロキシのドメイン名を入力します。スタンドアロン構成を行っている場合、デプロイするマシンのドメイン名がデフォルト値です。

- **[HTTP Port (for Web Application)]**: デフォルト値は8080です。
 - **[HTTPS Port (for Web Application)]**: デフォルト値は8443です (このポートは、AJPリバースプロキシには関係ありません)。
 - **[HTTP Port (for Reverse Proxy)]**: デフォルト値は8080です。
 - **[HTTPS Port (for Reverse Proxy)]**: デフォルト値は8443です。
 - **[AJP Port (non-secure connection)]**: AJPリバースプロキシ専用です。デフォルト値は8009です。
 - **[AJP Port (secure connection)]**: AJPリバースプロキシ専用です。デフォルト値は8109です。
- c. **[Next]** をクリックします。
8. **[Certificate Configuration]** ページが開きます。



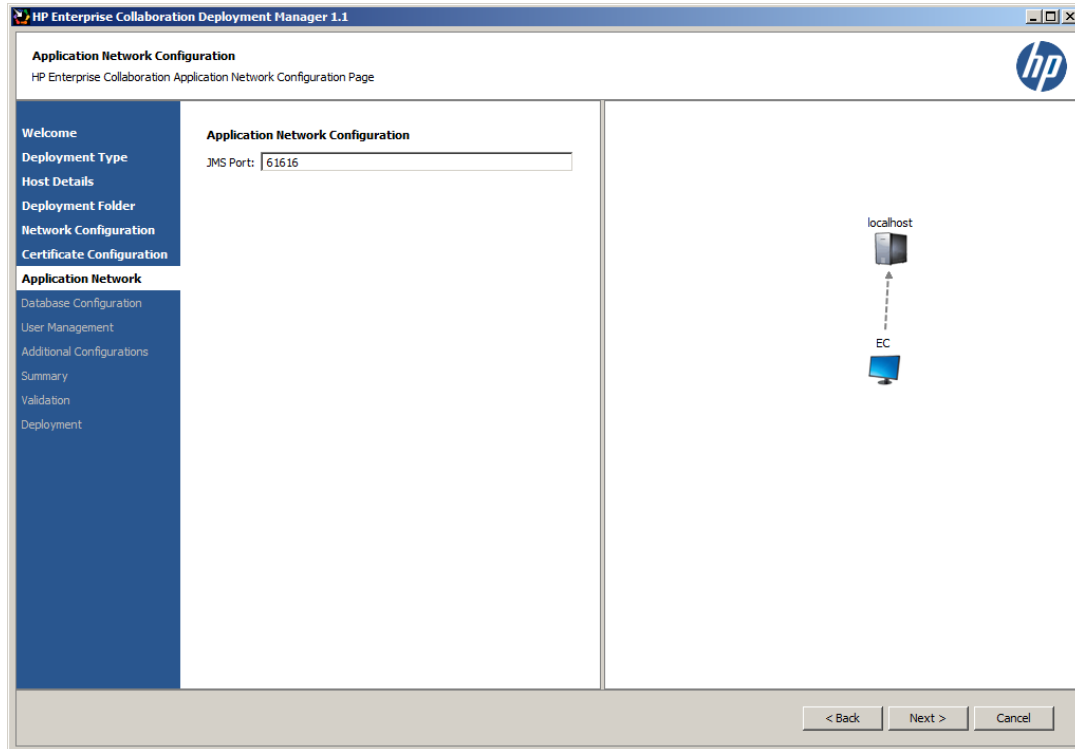
このページでは、セキュリティで保護された接続を使用してWebアプリケーションにアクセスする場合に使用するサーバー証明書をECに追加します。既存のキーストアから証明書をインポートする場合は、キーストアパス、キーストアタイプ、キーストアパスワードの入力が必要になります。

[Key alias] フィールドには、ECに追加する証明書のエイリアスを入力します。

[Key Password] フィールドには、キーストア内の証明書のパスワードを入力します。証明書に別のパスワードがない場合は、キーストアのパスワードを入力します。

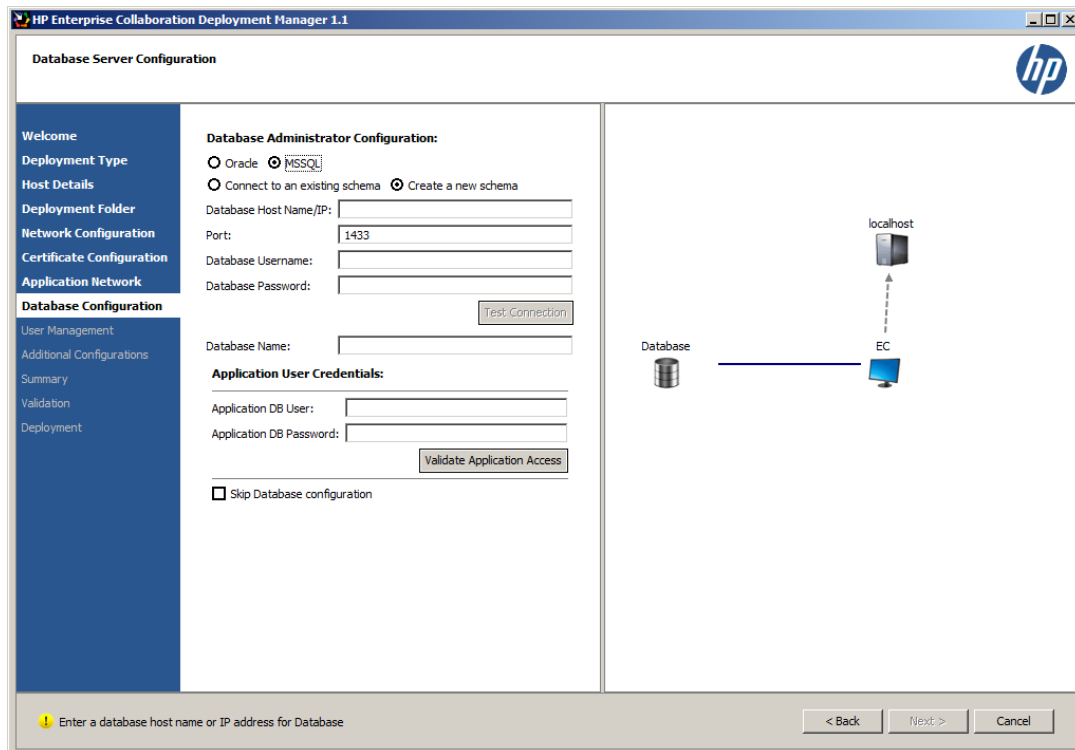
ECは、デフォルトで、自己署名の一時証明書を生成します。

9. **[Next]** をクリックします。
- [Application Network Configuration]** ページが開きます。



JMSポートを入力するか、デフォルト値の61616を使用します。[Next] をクリックします。

10. [Database Server Configuration] ページが開きます。



11. [Oracle] または [MSSQL] を選択します。

Oracleデータベース管理者の構成

HP Enterprise Collaboration Deployment Manager 1.1

Database Server Configuration

hp

Welcome

Deployment Type

Host Details

Deployment Folder

Network Configuration

Certificate Configuration

Application Network

Database Configuration

User Management

Additional Configurations

Summary

Validation

Deployment

Database Administrator Configuration:

Oracle Microsoft

Connect to an existing schema Create a new schema

Database Host Name/IP:

Port:

SID/Service:

Admin Username:

Admin Password:

Application Username:

Application User Password:

Confirm Password:

Default Tablespace:

... Validate Application Access

Skip Database configuration

localhost

Database

EC

Enter a database host name or IP address for Database

< Back Next > Cancel

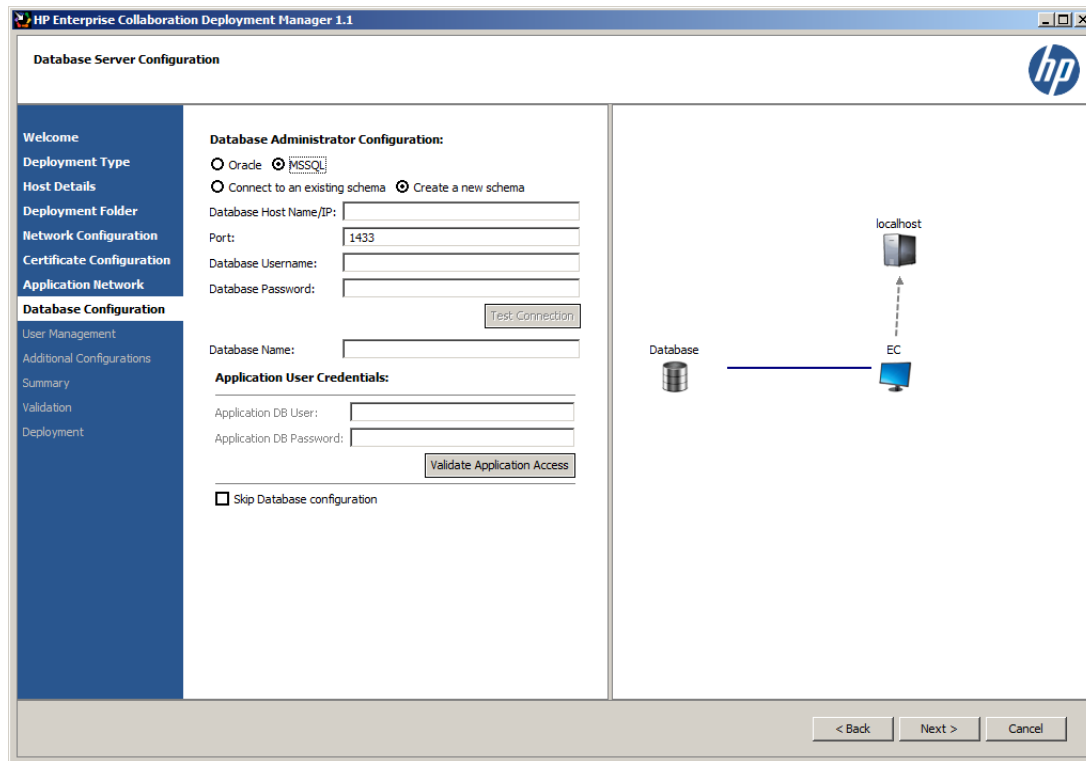
■ スキーマ:

[Connect to an existing schema] または [Create a new schema] のいずれかを選択します。

12. 次の内容を入力します。

- [Database Host Name/IP]
- [Port]: デフォルト値として1521が表示されます。
- [SID/Service]: システムID。
- [Admin Username]
- [Admin Password]
- [Application Username]: アプリケーションがデータベース接続に使用するスキーマの名前。
- [Application User Password]
- [Confirm Password]
- [Default Tablespace]: スキーマの表領域。スキーマに表領域がない場合は [System] と入力します。

13. MSSQLデータベース管理者の構成



- [Connect to an existing schema] または [Create a new schema] のいずれかを選択します。
- 次の内容を入力します。
 - [Database Host Name/IP]
 - [Port]: デフォルト値として1433が表示されます。

注：サポートされるデータベース資格情報の形式はSQL認証です。

- [Database Username]: 作成権限などの管理者権限を持つユーザー名を選択します。
- [Database Password]
- 上記の内容を入力してから、[Test Connection] ボタンをクリックします。

注：テストが失敗した場合は、このページに入力した内容を変更するか、[Skip Database configuration] を選択します。

- [Database Name]: [Connect to an existing schema] を選択した場合、接続するデータベースの名前を入力します。[Create a new schema] を選択した場合、新しいデータベースの名前を入力します。

14. アプリケーションユーザーの資格情報を入力します。

[Application DB User]: アプリケーションがデータベースとの通信に使用するユーザーの名前。

[Application DB Password]: アプリケーションがデータベースとの通信に使用するパスワード。

15. **[Validate Application Access]** ボタンをクリックします。

注：チェックが失敗した場合は、ユーザー資格情報が有効かどうか確認してください。

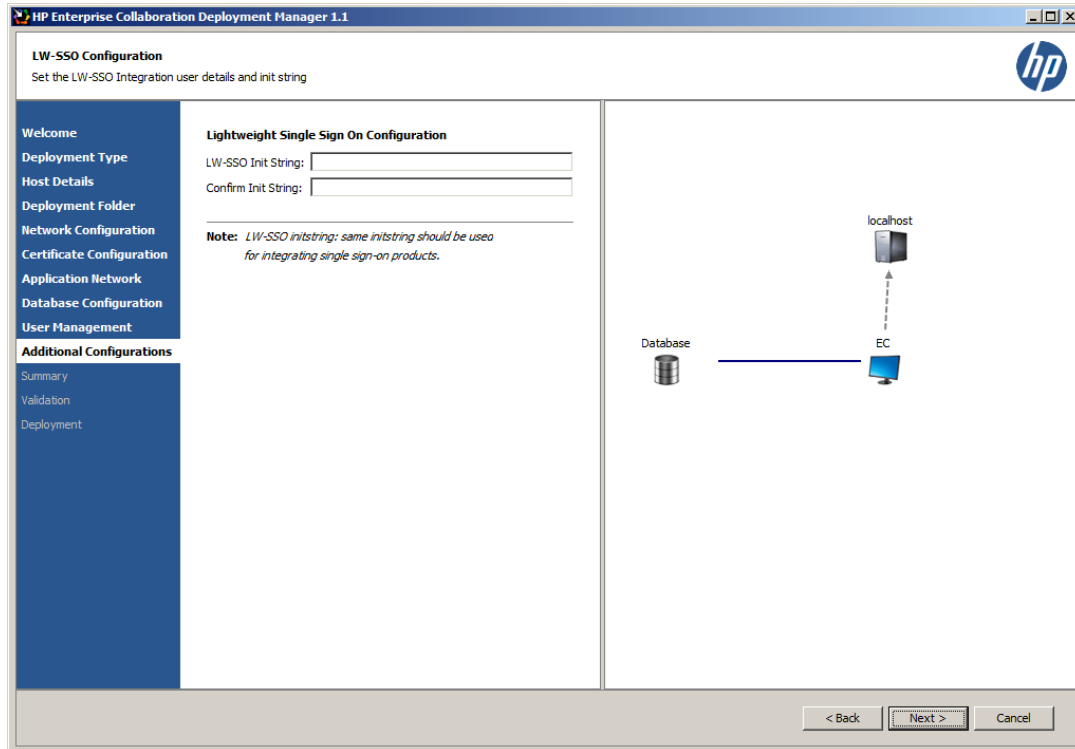
16. **[Next]** をクリックします。
 17. **[User Management Configuration]** ページが開きます。

注：データベース構成をスキップした場合、**[User Management Configuration]** ページも自動的にスキップされます。

- a. 次の内容を入力します。
- **[Temporary Administrator Login Name]:** 既存のユーザーリポジトリ内に存在する名前はログイン名として指定できません。また、「スキーマ: 」(19ページ)で **[Connect to existing schema]** を選択した場合は、以前のインストール作業で使用したログイン名も使用できません。
 - **[Temporary Administrator Password]**
 - **[Confirm Password]**
- b. **[Next]** をクリックします。
18. **[Lightweight Single Sign-On (LW-SSO) Configuration]** ページが開きます。

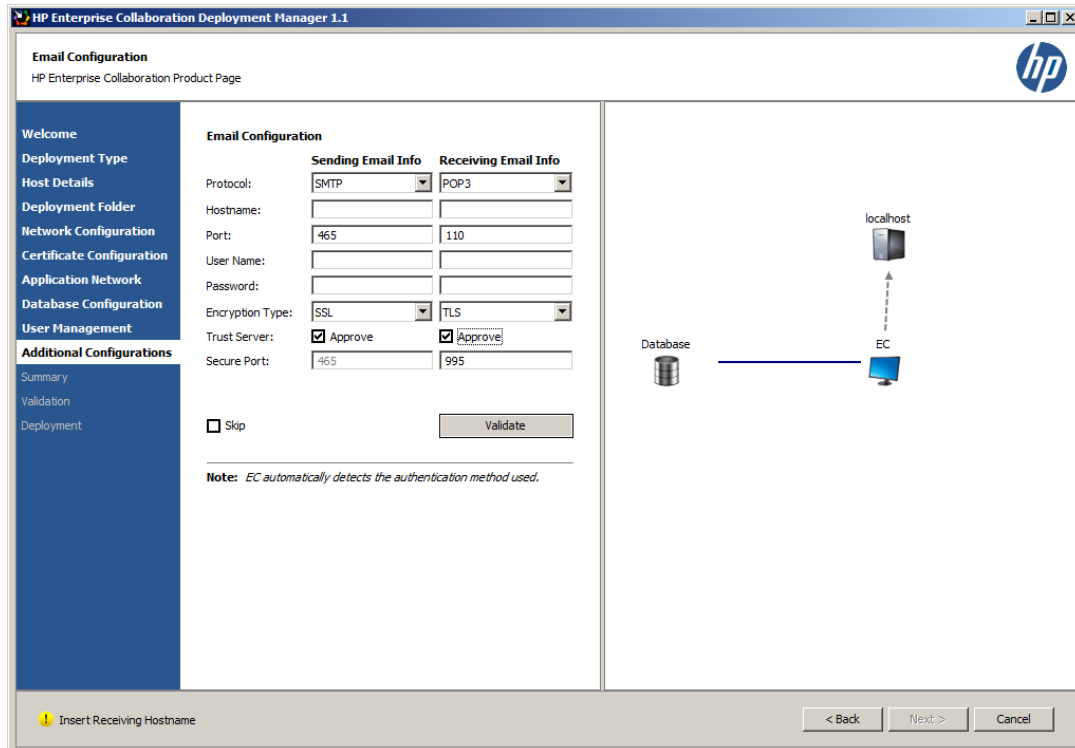
インストールおよび構成ガイド

第2章：Enterprise Collaborationのインストールと構成



[LW-SSO Init String] を入力し、確認のためにもう一度入力してから [Next] をクリックします。

19. [Email Configuration] ページが開きます。



このページは、送信メールの設定と受信メールの設定の2つに分割されています。それぞれについて、次の内容を入力します。

- a. **[Protocol]**: データの送受信に使用するプロトコルを選択します。データ送信にはSMTPを使用します。データ受信にはPOP3またはIMAP4のいずれかを選択します。
- b. **[Hostname]**: 着信と発信のメールサーバーのホスト名。
- c. **[Port]**: 着信データと発信データのポート番号。
- d. **[Username]**: 電子メールの送信と受信に使用するECメールボックスのユーザー名。
- e. **[Password]**: ECメールボックスのパスワード。
- f. **[Encryption Type]** - 電子メールサーバーで使用する暗号化を選択します。プロトコルのセキュリティ保護が必要な場合は、電子メールサーバー構成に応じてSSLまたはTLSを選択してください。
 - [SSL]: SSL暗号化の場合、**[Secure Port]** フィールドにはポート番号が自動入力され、変更できません。
 - [TLS] - Trust Server。 **[Secure Port]** フィールドにポート番号を入力します。

それぞれの暗号化タイプで **[Approve]** を選択し、セキュリティ保護されたポートを追加します。

上記の定義に基づいて、ECが使用する証明書の検証とインストールが行われます。

オプション: すべての構成内容を入力した後に **[Validate]** ボタンをクリックすると、電子メール構成のテストが実行されます。このボタンをクリックすると、ECのインストーラーは、電子メールサーバーがサーバー証明書を使用するかどうかをチェックし、必要に応じて証明書をECキーストアに追加します。

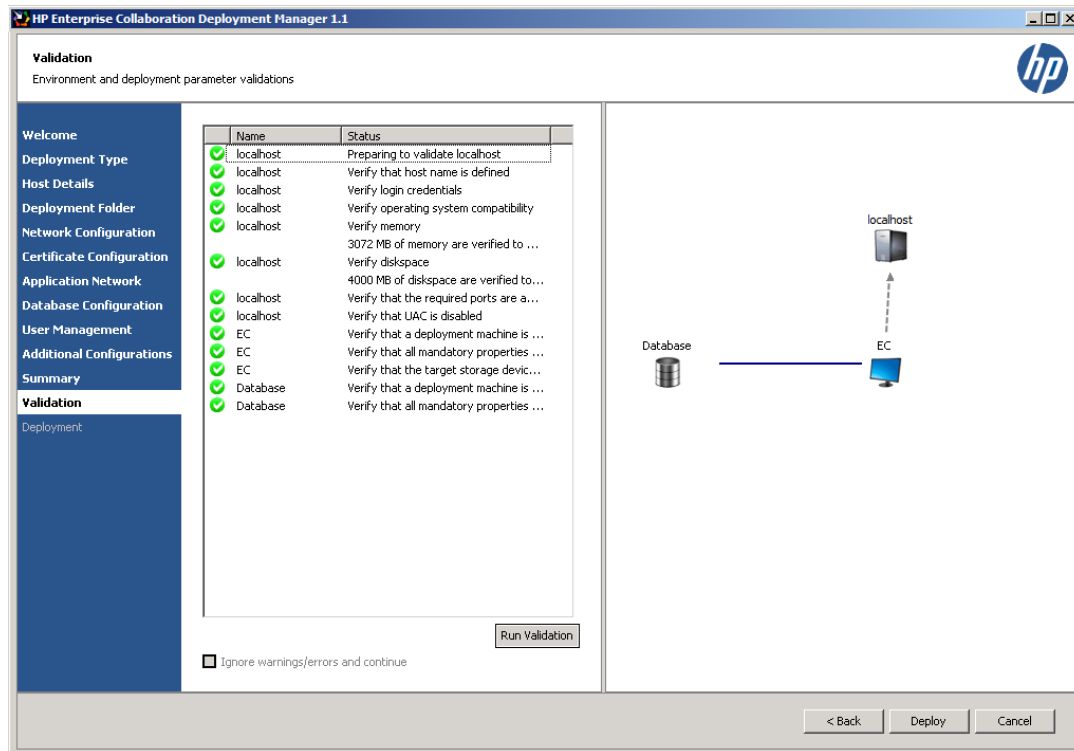
[Next] をクリックします。

注: **[Email Configuration]** ページの内容はすべてオプションです。したがって、**[Skip]** ボタンをクリックすれば入力を省略できます。

20. **[Summary]** ページが開きます。

ここでは、入力した内容をすべて確認できます。変更が必要な場合は、**[Back]** ボタンをクリックすると、ページに戻って内容を変更できます。入力内容がすべて正しいことを確認したら、**[Next]** をクリックします。

21. **[Validation]** ページが開きます。



[Summary] ページで [Next] をクリックすると、検証が自動的に実行されます。

- 検証が成功すると、アイコンはすべて緑色になります。
- 構成に問題があるか、データベース設定をスキップした場合には、赤いアイコンが表示されます。[Ignore warnings/errors and continue] を選択するか、問題を修正してから [Run Validation] ボタンをクリックし、構成上の問題が解消されたかどうかを確認します。

22. [Deploy] をクリックします。

23. デプロイメントが完了したら、[Finish] をクリックします。

デプロイメントが完了すると、プログラム・メニューのHP ECフォルダーの下に次のショートカットが表示されます。

- Start HP EC
- Stop HP EC
- Uninstall HP EC

ユーザーリポジトリとユーザーの役割の構成

インストールが完了したら、ユーザーリポジトリとユーザーの役割の構成を行います。この手順は、ECへのログインに不可欠です。

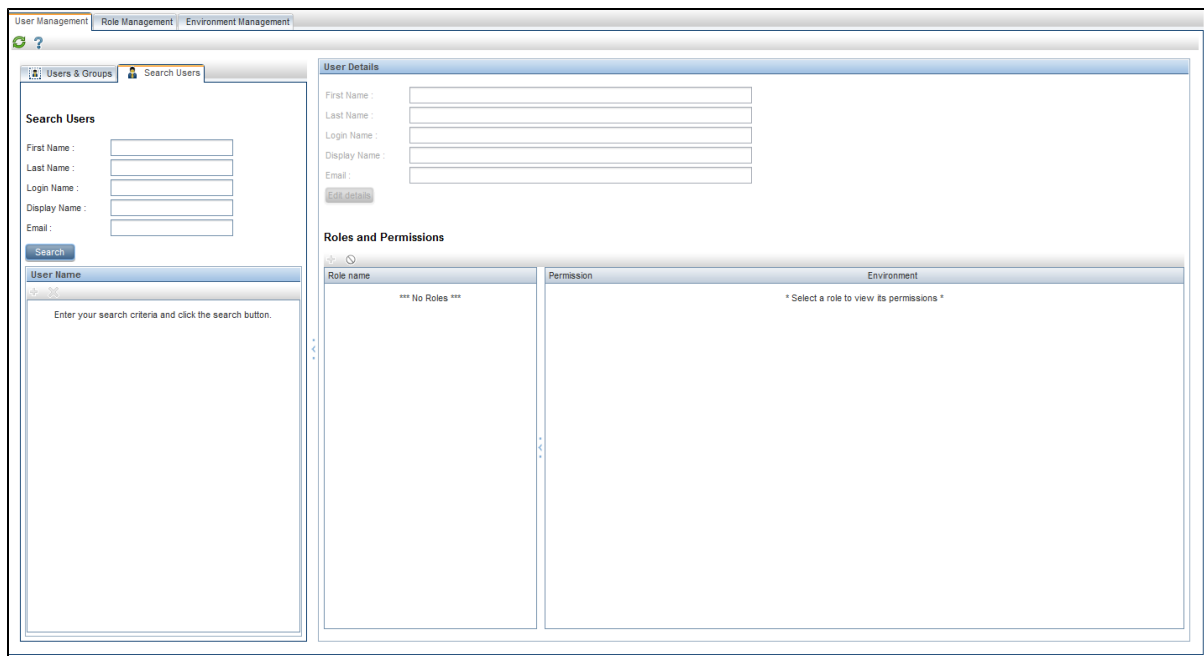
ユーザーリポジトリとユーザーの役割を構成するには、次の手順を実行します。

1. /confディレクトリにあるexternal-ldap.propertiesファイルを、「付録B: external-ldap.propertiesファイルの更新」(69ページ)の手順に従って更新します。

2. **オプション:** SSL経由でLDAPを使用する場合、次のバッチファイルを実行してLDAPサーバー証明書をキーストアにインポートします。

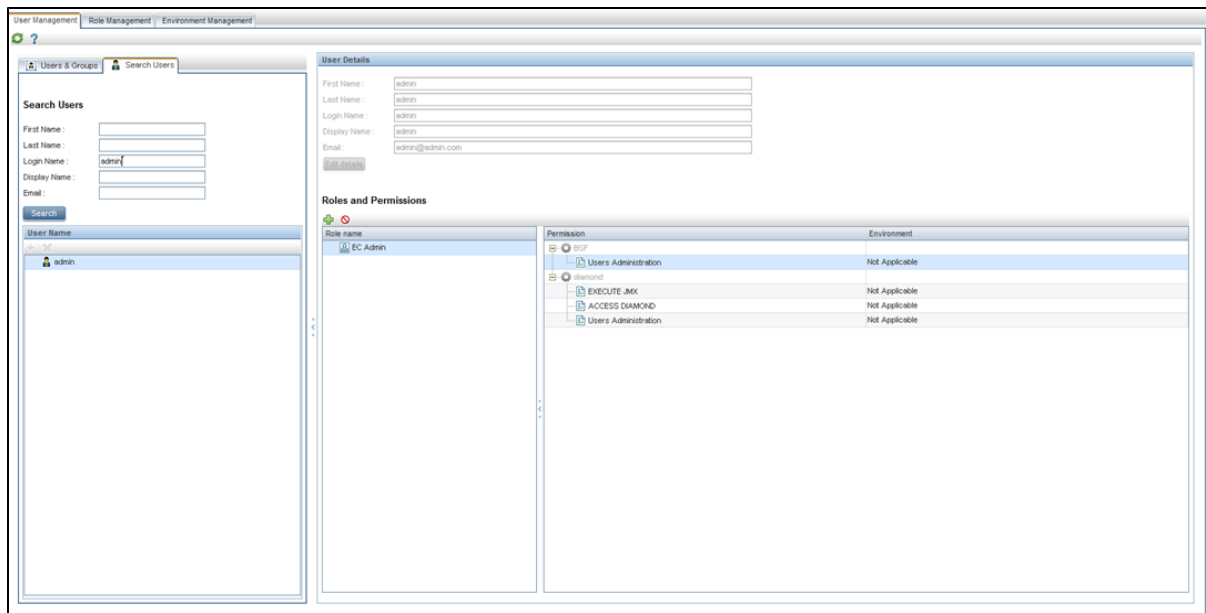
C:\HP\EC\diamond-deploy\set-ldap-certificate.bat <証明書ファイルのパス>

3. \confフォルダーの**bsf.properties**ファイルで、次のようにプロパティの値を設定して保存します。
 - authentication.provider=SHARED
 - personalization.provider=SHARED
 - users.provider=EXTERNAL
 - groups.provider=EXTERNAL
 - roles.provider=SHARED
 - roles.relations.provider=SHARED
4. [スタート] > [すべてのプログラム] > [HP EC] > [Start HP EC] アイコンを選択してECを起動します。
5. **http://<サーバーFQDN>:<ポート>/bsf**にアクセスして、ユーザー管理UIを開きます。
6. インストールプロセスで定義した一時的なユーザー管理者の資格情報を使って、ログインします。
7. ユーザー管理UIが開きます。



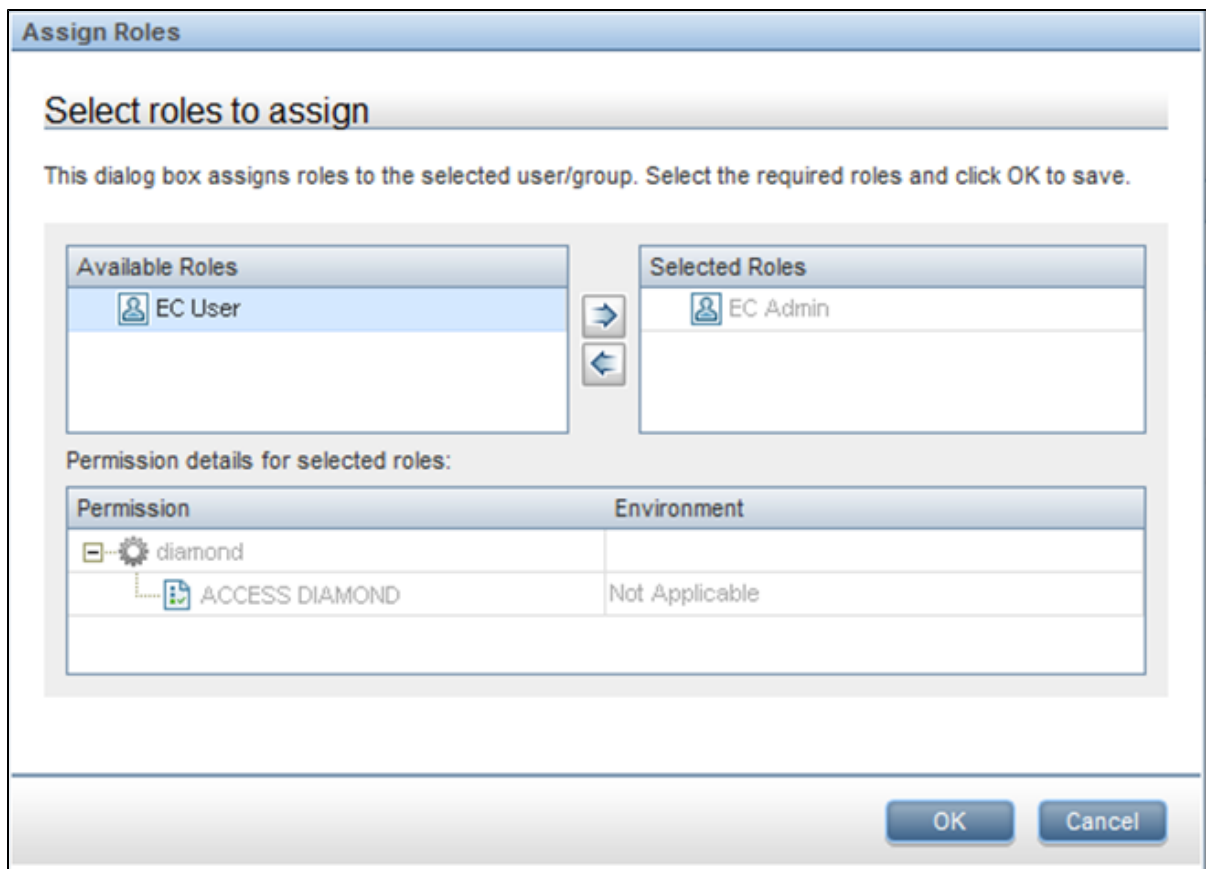
[User Management] セクションで、ユーザーまたはグループを検索します。たとえば、ユーザーを検索するには、[Search Users] タブをクリックして検索条件を入力し、[Search] ボタンをクリックします。

8. [Roles and Permissions] セクションの内容と一致するユーザーとグループが一覧表示されます。



目的のユーザーを選択します。[Add Role] アイコン (👤) をクリックします。

9. [Assign Roles] ダイアログボックスが開きます。



次の役割がユーザーに追加されます。

- EC管理者: EC、JMX、ユーザー管理にアクセスする権限
- ECユーザー: ECにアクセスする権限

注: 少なくとも1人のEC管理者ユーザーに、ユーザー管理UIとJMXへのアクセス権を必ず割り当ててください。

10. [プログラム]メニュー > [HP EC] > [Stop HP EC] アイコンを選択してECを停止します。
11. **bsf.properties** ファイルを次のように変更します。
 - authentication.provider=EXTERNAL
 - personalization.provider=SHARED
 - users.provider=EXTERNAL
 - groups.provider=EXTERNAL
 - roles.provider=SHARED
 - roles.relations.provider=SHARED
12. [プログラム]メニュー > [HP EC] > [Start HP EC] アイコンを選択してECを再開します。

リバースプロキシ使用時のセキュアログインの構成

リバースプロキシでセキュアログイン (HTTPS) を使用する場合は、インストールの完了後、サーバーを起動する前に次の手順を実行します。

1. **bsf.war** パッケージを7zipやWinRARなどの解凍プログラムで開き、内容を編集します。
2. **C:\HP\EC\servers\server-0\webapps\bsf.war\WEB-INF\applicationContext-security.xml** ファイルを開きます。
3. 次のように、**forceHttps**の値をtrueに変更します (変更箇所を太字で示します)。

```
<bean id="authenticationProcessingFilterEntryPoint"
      class="com.hp.sw.bto.security.springsecurity.
      BSFAuthenticationProcessingFilterEntryPoint">

<property name="loginFormUrl">
  <value>/login.form</value>
</property>

<property name="forceHttps">
<value>true</value>
</property>
</bean>
```

4. **C:\HP\EC\servers\server-0\webapps\diamond\WEB-INF\classes\diamond\wssofmconf.xml** ファイルのwebuiセクションに、太字で示した行を追加します。

```
<nonsecureURLs>
  <url>.*\/images\/.*<\/url>
  <url>.*\/desktopClient\/.*<\/url>
<\/nonsecureURLs>

<reverseProxy enabled="true">

<fullServerURL>https:\/\/your.reverse.proxy.fqdn:8443<\/fullServerURL>
<\/reverseProxy>
```

5. 認証ポイントがreverseProxyを指定していることを確認します。C:\HP\EC\conf\client-config.propertiesファイルを編集し、太字部分の値 (reverseProxy FQDN) をチェックしてください。

```
bsf.server.url=https:\/\/your.reverse.proxy.fqdn:8443\/bsf
```

第3章

Office Communicator ServerおよびMS Lync Serverとの統合の設定

Enterprise Collaborationでは、次のバージョンのMS Communicator Serverを統合できます。

- Office Communicator Server 2007 (OCS)
- MS Lync 2010 Server

ルート証明機関 (CA) の証明書のインストール

注: ここに掲載する手順は、Microsoft CA発行者向けの手順です。これ以外の発行システムを使用している場合、以下の手順はルートCA証明書のインストールの参考にはなりますが、異なる内容も含まれているのでご注意ください。

ルートCA証明書のインストールは、次の2つの部分に分かれています。

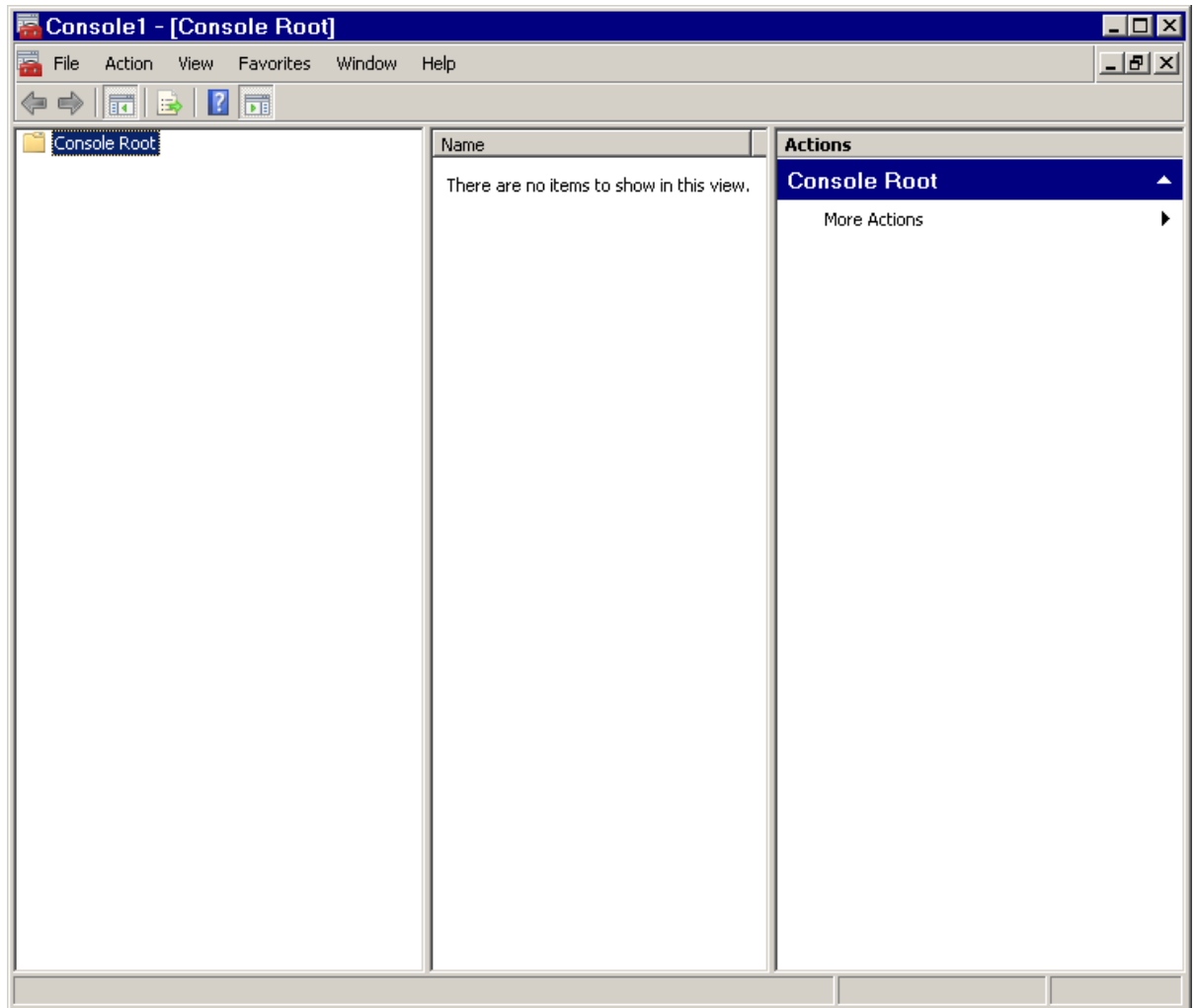
- 「OCSで使用するCAの確認」(29ページ)
- 「ルートCA証明書のダウンロードとインストール」(34ページ)

CAのURLがわかっている場合、最初の手順は省略し、2番目の手順に進んでください。

OCSで使用するCAの確認

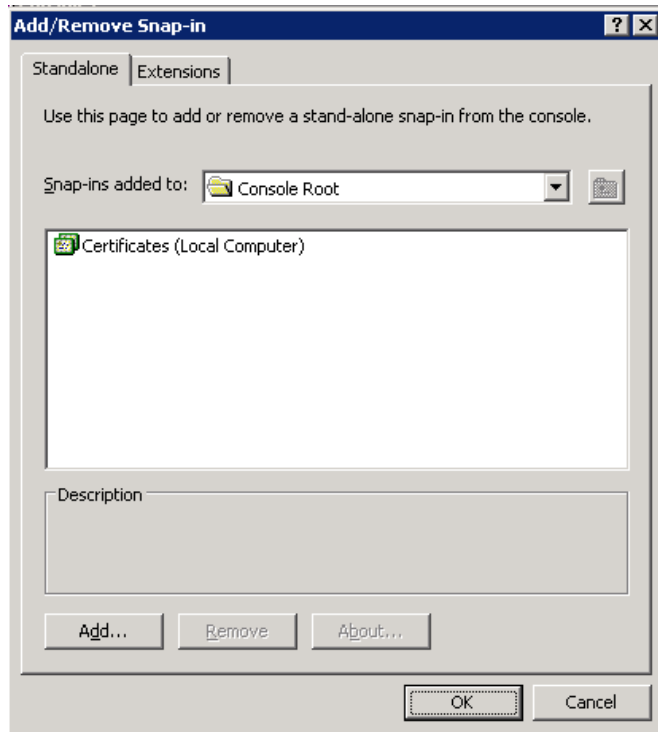
OCSが使用するCAをチェックするには、次の手順を実行します。

1. OCSサーバーにログインし、**mmc.exe**を実行します。
2. [Console Root] が開きます。



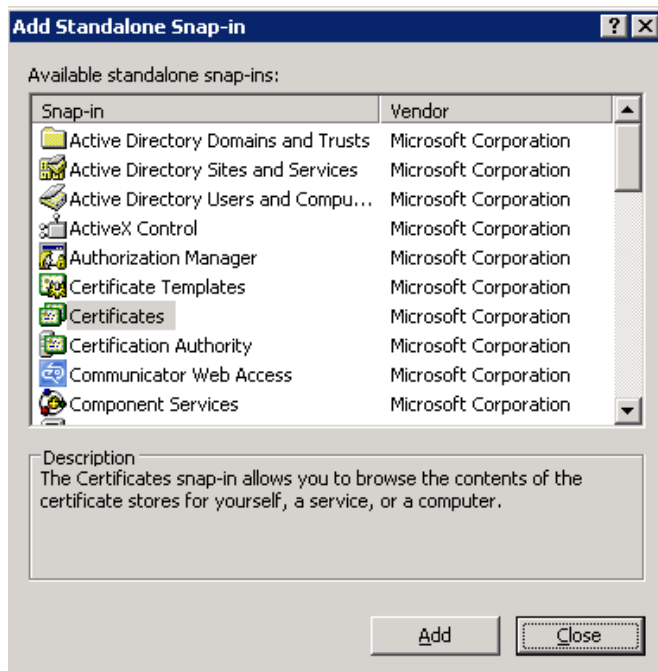
[Console Root] で [File] > [Add/Remove Snap-in] を選択します。

3. [Add/Remove Snap-In] ダイアログボックスが開きます。

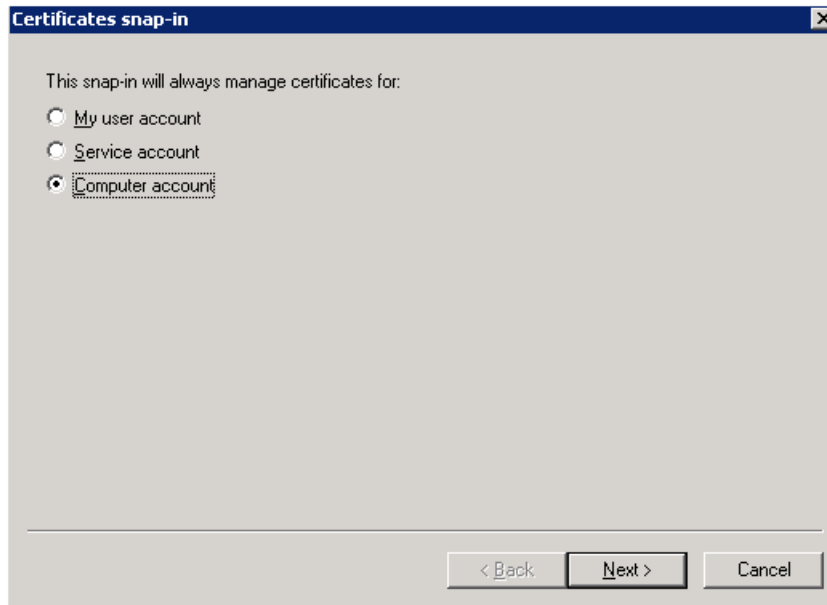


[Certificates] を選択します。[Add] をクリックします。

4. [Add Standalone Snap-In] ダイアログボックスが開きます。[Add] をクリックします。

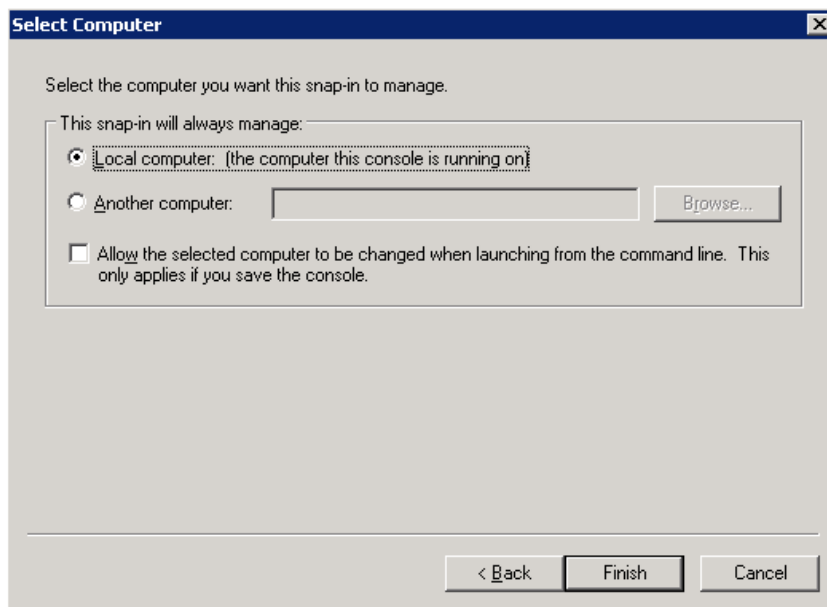


5. [Certificates snap-in] ダイアログボックスが開きます。



[Computer Account] を選択します。[Next] をクリックします。

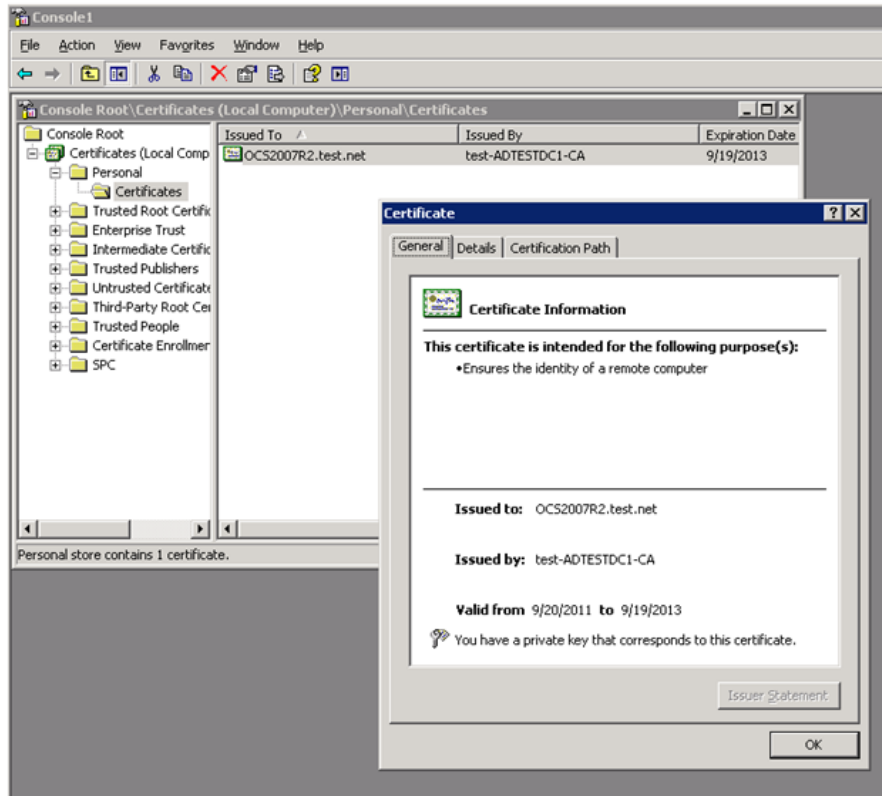
6. [Select Computer] ダイアログボックスが開きます。



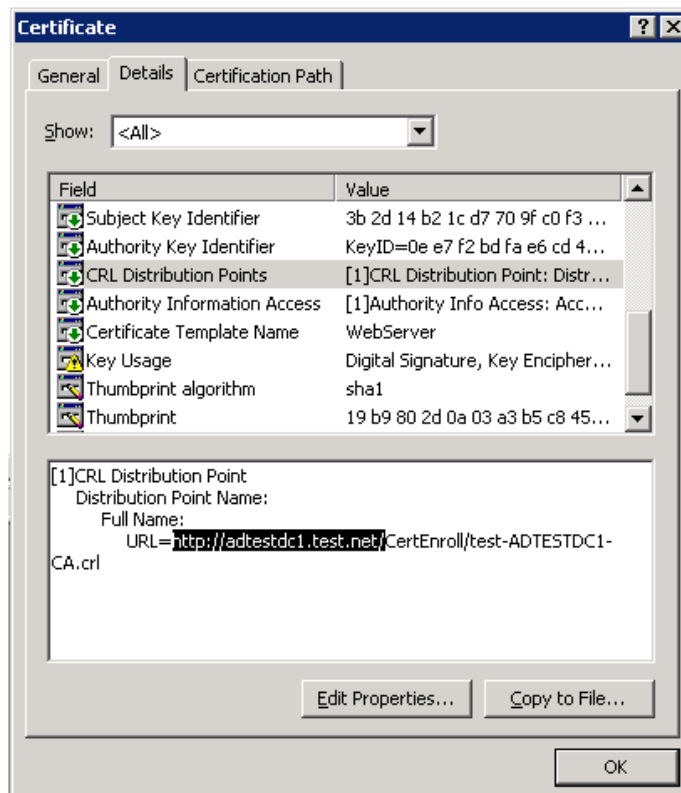
[Local Computer] を選択します。[Finish] をクリックします。

7. [Add Standalone Snap-In] ダイアログボックスが再度開きます。[Close] をクリックします。
8. [Add/Remove Snap-In] ダイアログボックスが再度開きます。[OK] をクリックします。
9. [Console Root] が再度開きます。

[Personal] > [Certificates] (下の図を参照) を選択すると、ルートCA証明書と発行元のCAが表示されます。



10. [Details] タブを選択します。

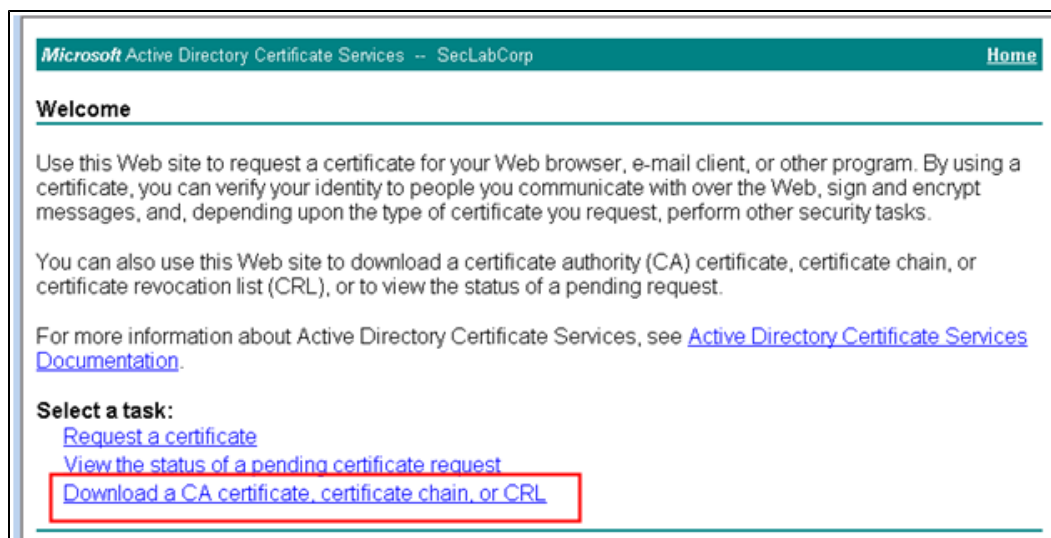


11. 次の手順では、URL行の証明機関名を使って、ルートCA証明書をダウンロードします。証明機関名は、URLの '=' から最初の '/' までに示されています。たとえば、上の図の場合、証明機関名は `http://adtestdc1.test.net` です。

ルートCA証明書のダウンロードとインストール

ルートCA証明書をダウンロードおよびインストールするには、次の手順を実行します。

1. OCSエージェントマシンにログインします。
2. [Details] タブで確認したURLの証明機関名を使って、証明機関のWebサーバーにアクセスします。証明機関名を `/certsrv` に追加してください。たとえば、上の図の [Details] タブの場合、証明機関名は `http://adtestdc1.test.net` なので、証明機関のWebサーバーにはURL `http://adtestdc1.test.net/certsrv` でアクセスできます。
3. [Welcome] ページが開きます。



[Download a CA certificate, certificate chain, or CRL] をクリックします。

4. 次のページが開きます。



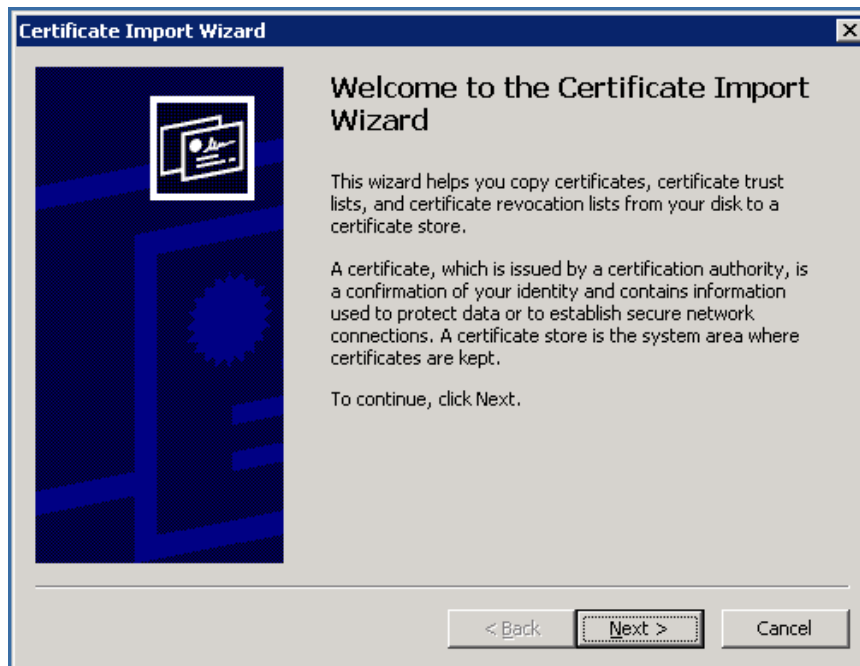
[Download CA certificate chain] をクリックします。

5. [File Download] プロンプトが開き、ルートCA証明書 (*.p7bファイル) の保存に関するメッセージが表示されます。

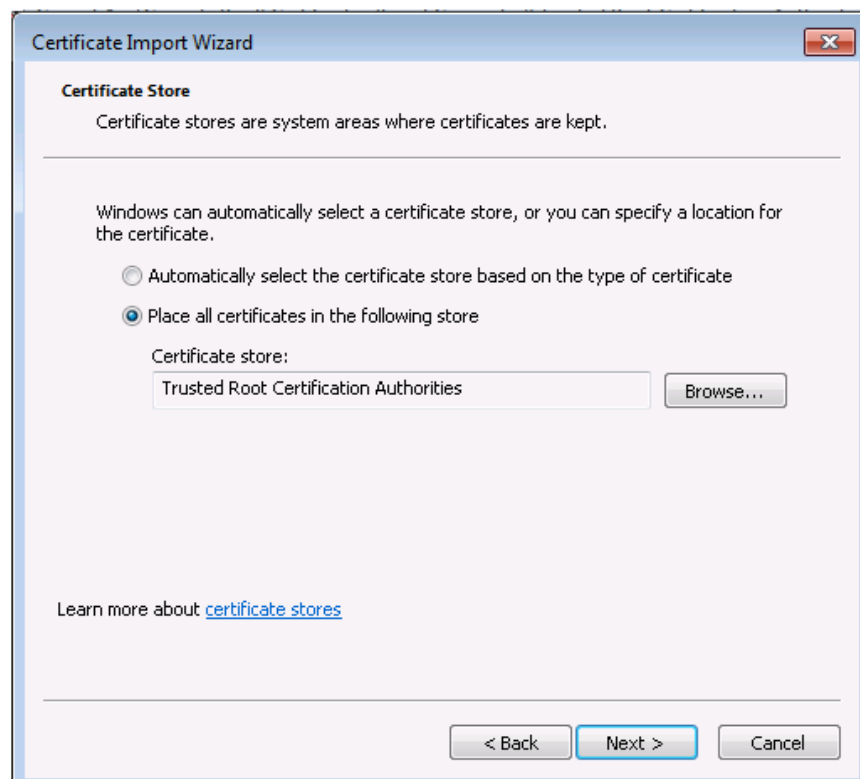
ルートCA証明書をファイルシステム上の任意の場所に保存します。

6. **mmc.exe**を実行します。
7. [Console Root] で [File] > [Add/Remove Snap-in] を選択します。
8. [Add/Remove Snap-In] ウィンドウが開いたら、[Add] をクリックします。
9. [Add Standalone Snap-In] ウィンドウが開いたら、リストから [Certificates] を選択します。[Add] をクリックします。
10. [Certificates snap-in] ウィンドウが開いたら、[Computer Account] を選択します。[Next] をクリックします。
11. [Select Computer] ウィンドウで、[Local Computer] を選択します。[Finish] をクリックします。
12. [Add Standalone Snap-In] ウィンドウで、[Close] をクリックします。
13. [Add/Remove Snap-In] ウィンドウで、[OK] をクリックします。

Certificate Import Wizardが起動します。



14. ウィザードで **[Next]** をクリックします。
15. **[Certificate Store]** ウィンドウが開いたら、**[Place all certificates in the following store]** (下の図を参照) を選択します。 **[Next]** をクリックします。

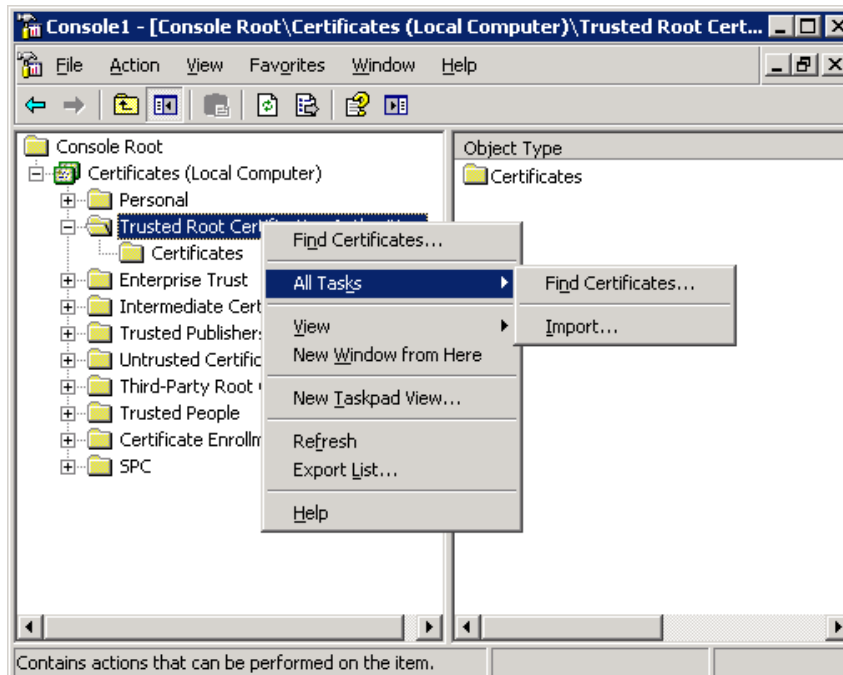


16. ウィザードが完了したら、**[Console Root]** に移動して **[Trusted Root Certification**

Authorities] フォルダーを右クリックします。

17. ポップアップメニューが開きます。

[All Tasks] > [Import] を選択し、ルートCA証明書をインポートします。



OCSエージェントマシンでのサーバー証明書のインストール

サーバー証明書を発行してOCSエージェントマシンにインストールするには、次の手順を実行します。

1. OCSエージェントマシンから(重要)、証明書の証明機関名を使ってCA Webサイトにアクセスします。証明機関名に/certsrvを追加してください。たとえば、証明機関名がhttp://adtestdc1.test.netの場合、証明機関のWebサーバーにアクセスするURLはhttp://adtestdc1.test.net/certsrvとなります。
2. [Welcome] 画面が開きます。[Request a certificate] を選択します。

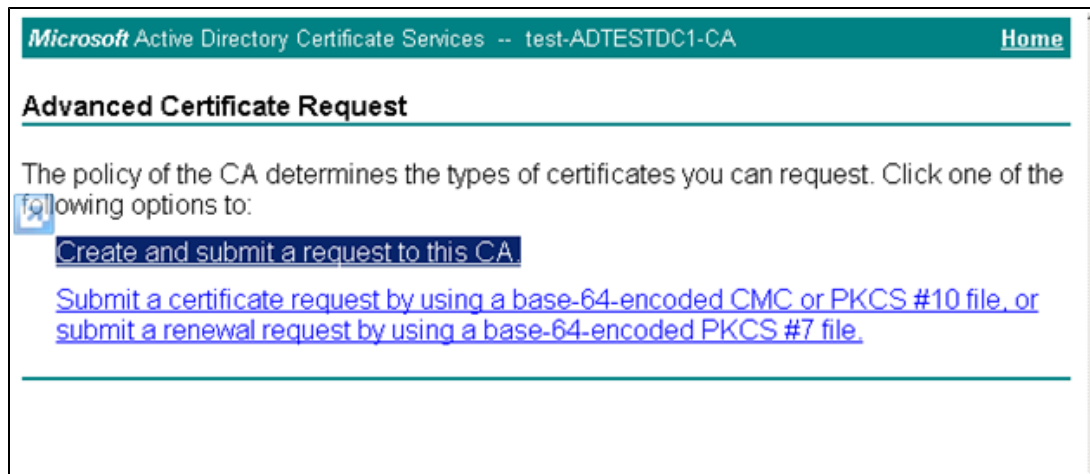


3. [Request a Certificate] 画面が開きます。



[advanced certificate request] を選択します。

4. [Advanced Certificate Request] 画面が開きます。



[Create and submit a request to this CA] を選択します。

5. [Advanced Certificate Request] 画面が開きます。

Microsoft Active Directory Certificate Services -- test-ADTESTDC1-CA Home

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OCS agent machine FQDN goes here

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP: Microsoft RSA SChannel Cryptographic Provider

Key Usage: Exchange

Key Size: 2048 Min: 384 Max: 16384 (common key sizes: 512 1024 2048 4096 8192 16384)

Automatic key container name User specified key container name

Mark keys as exportable

Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: SHA-1 Only used to sign request.

Save request

Attributes:

Friendly Name:

Submit >

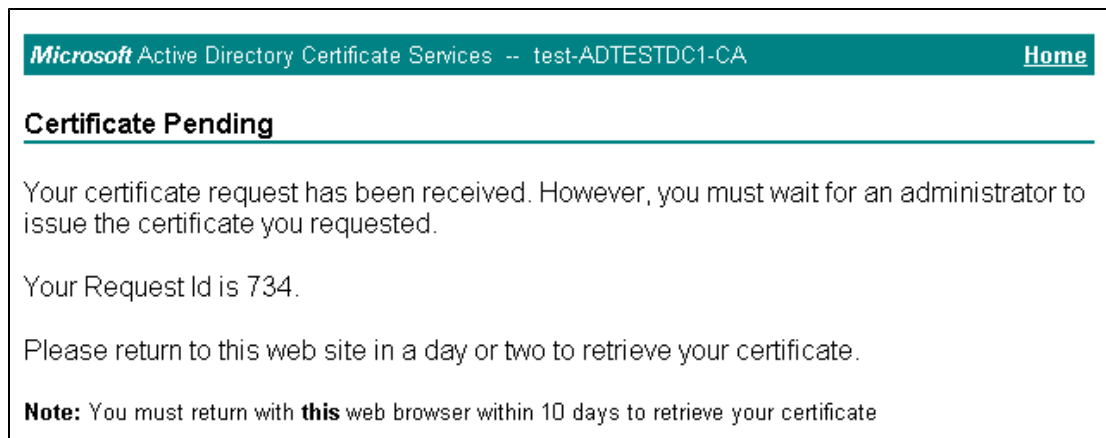
必要な内容を入力します。[Mark keys as exportable] チェックボックスは無効になっていることがありますが、OCSエージェントマシンからアクセスする場合、このチェックボックスを有効にする必要はありません。

6. 入力完了したら、[Submit] ボタンをクリックします。

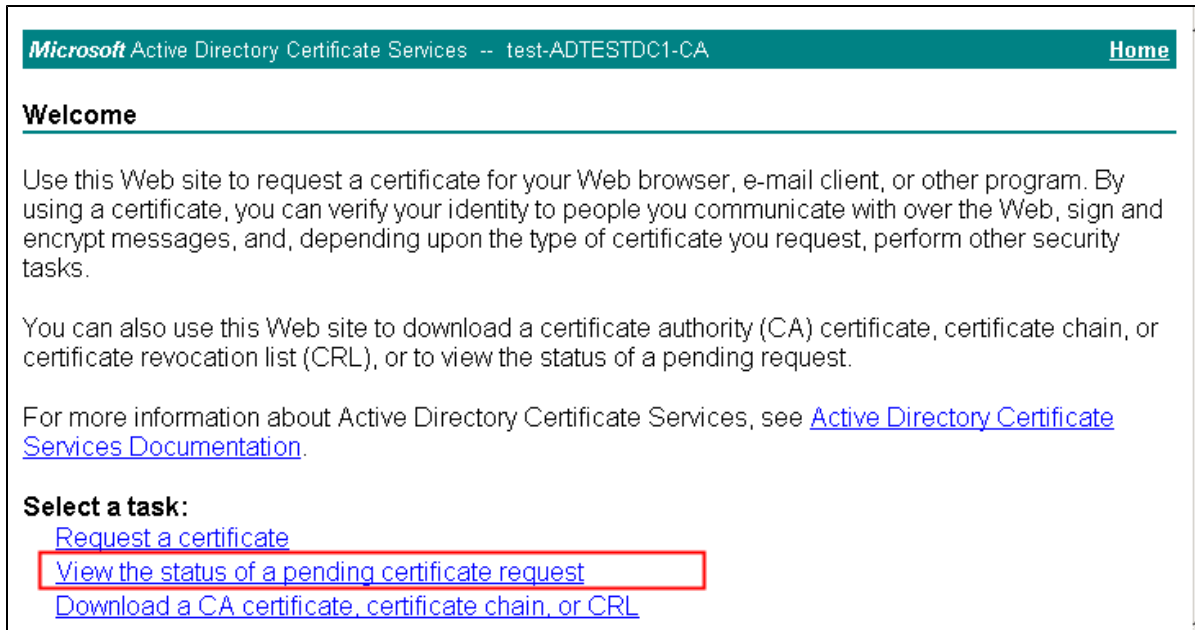
- 証明機関サービスで証明書の自動発行が有効になっている場合、[Certificate Issued] 画面 (下記を参照) が開きます。[Install this certificate] をクリックし、次の手順に進みます。



- 証明機関サービスで証明書の自動発行が有効になっていない場合、CA管理者に証明書の要求を発行することを依頼してください。この場合、[Certificate Issued] 画面ではなく、[Certificate Pending] 画面が表示されます。



- 証明書が発行されたことを通知するメッセージが表示されたら、証明機関名 (重要) を使って、OCSエージェントマシンからCA Webサイトにアクセスします (手順1を参照してください)。
- [Welcome] 画面が開いたら、[View the status of a pending certificate request] をクリックします。



Microsoft Active Directory Certificate Services -- test-ADTESTDC1-CA [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

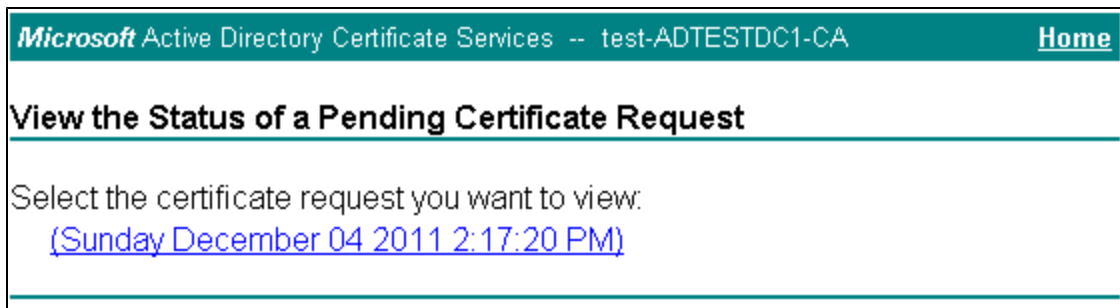
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

iii. 次のページが開きます。発行済みの証明書を選択します。



Microsoft Active Directory Certificate Services -- test-ADTESTDC1-CA [Home](#)

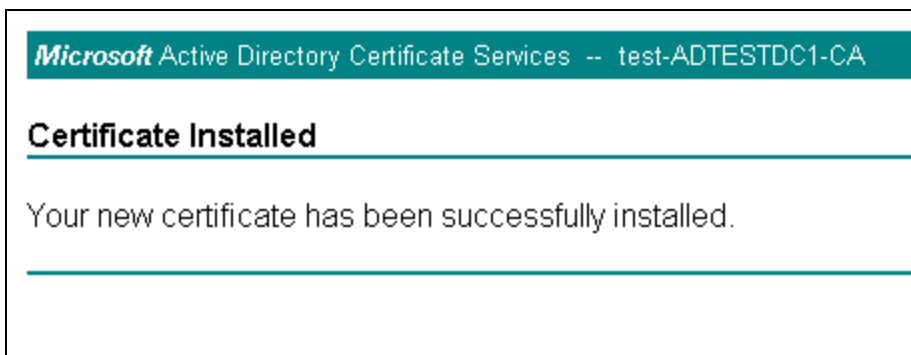
View the Status of a Pending Certificate Request

Select the certificate request you want to view:

[\(Sunday December 04 2011 2:17:20 PM\)](#)

iv. [Certificate Issued] 画面が開きます。[Install this certificate] を選択します。

7. 次のメッセージが表示されます。



Microsoft Active Directory Certificate Services -- test-ADTESTDC1-CA

Certificate Installed

Your new certificate has been successfully installed.

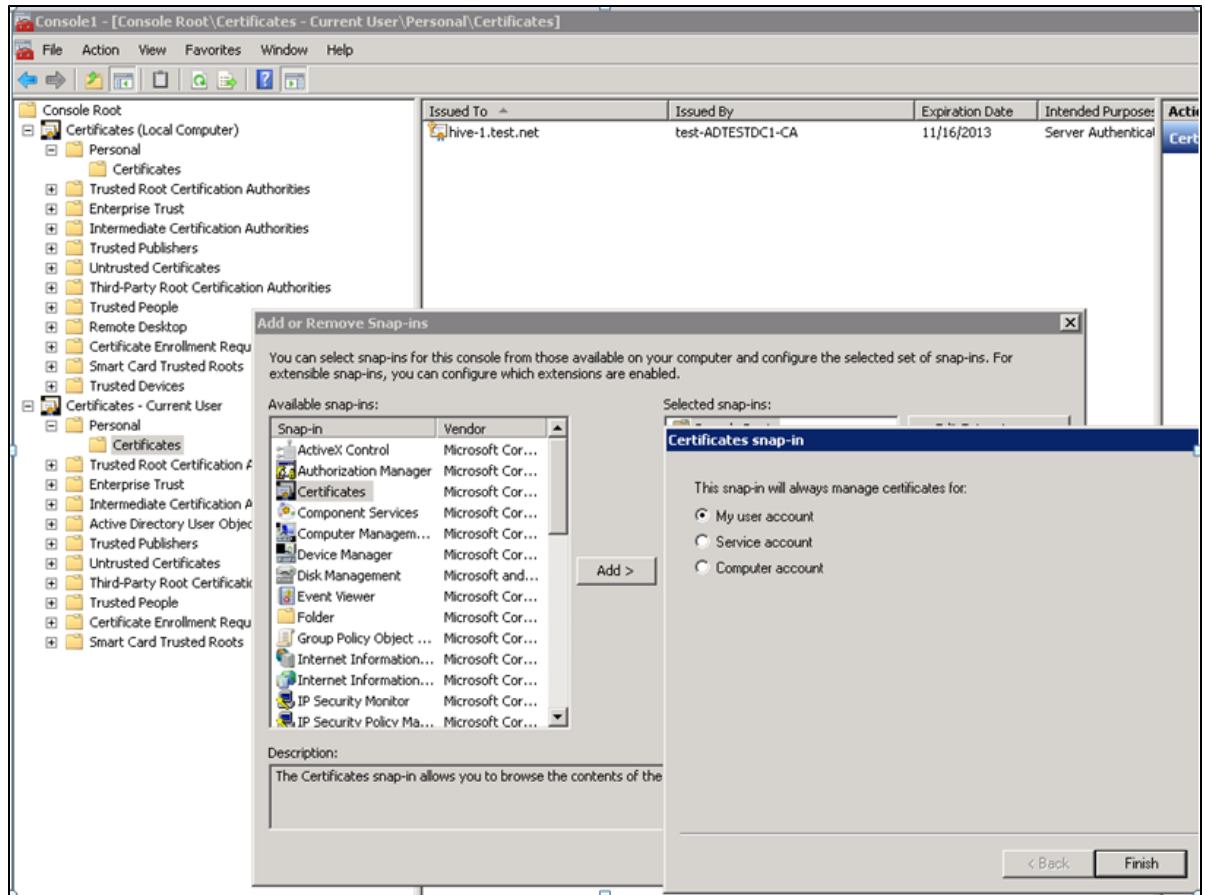
8. OCSサーバーにログインし、**mmc.exe**を実行します。

9. [Console Root] が開きます。[File] > [Add/Remove Snap-in] を選択します。

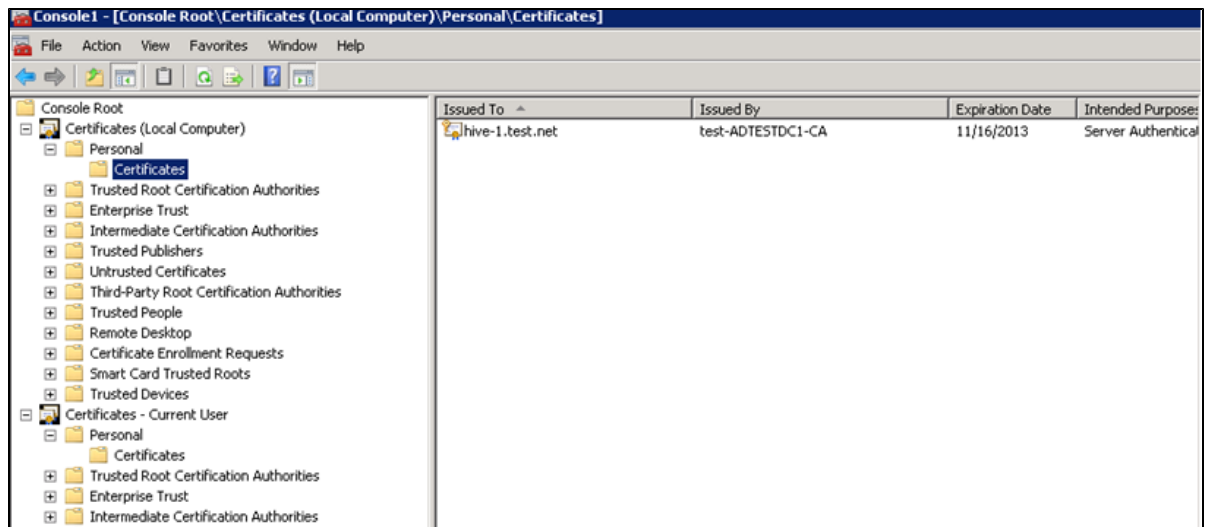
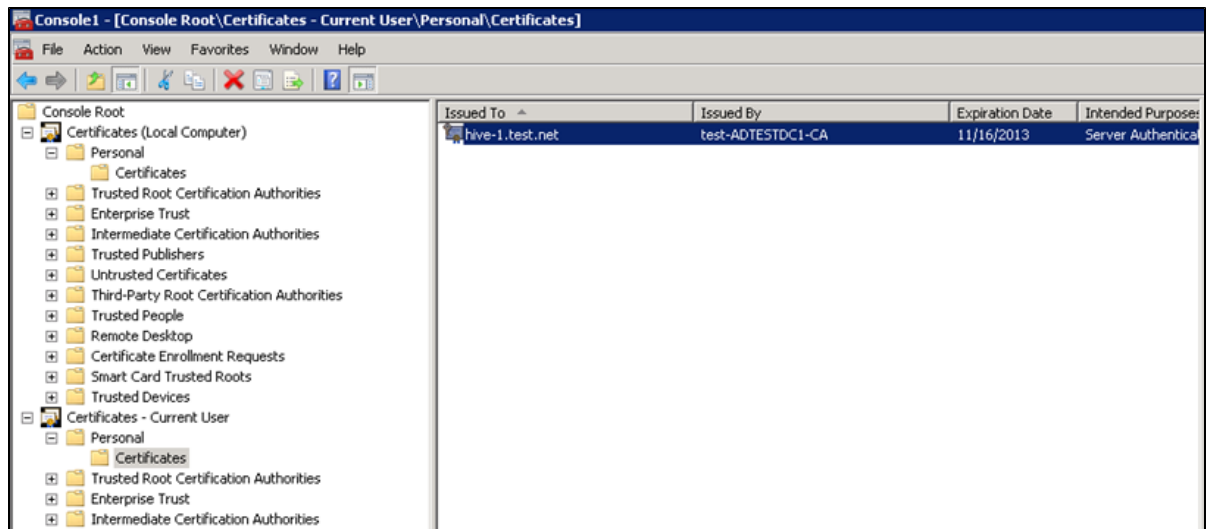
10. [Add/Remove Snap-In] ダイアログボックスが開きます。[Certificates] を選択します。[Add] をク

リックします。

11. **[Add Standalone Snap-In]** ダイアログボックスが開きます。**[Add]** をクリックします。
12. **[Certificates snap-in]** ダイアログボックスが開きます。**[My user account]** (次の図を参照) を選択し、**ユーザーアカウントの証明書スナップイン**を追加します。**[Finish]** をクリックします。



13. OCSエージェントプロセスを別のユーザーアカウントから実行する場合は、**[Certificates - Current User] > [Personal] > [Certificates]** (下の最初の図) から、**[Certificates (Local Computer)/Personal/Certificates]** (下の2番目の図) に、発行済み証明書をドラッグします。



エージェントのプロビジョニング

ここでは、Office Communicator Server 2007とLync Server 2010でのエージェントプロビジョニングの方法について説明します。

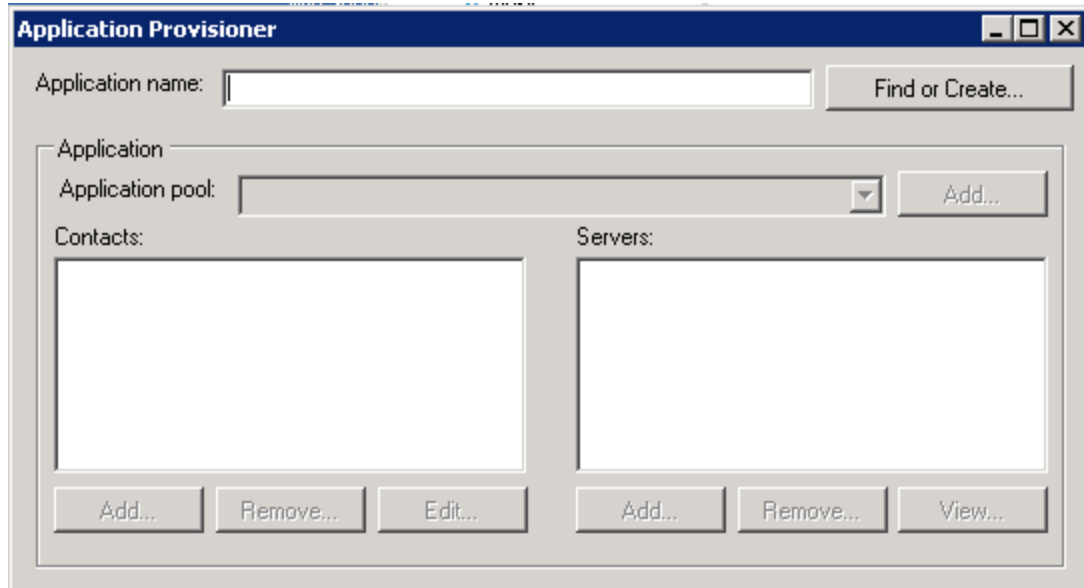
OCS 2007でのエージェントプロビジョニング

前提条件

- OCSエージェントマシンからの通信用に、OCSサーバーポートを開放します。
- OCSエージェント設定を行うドメインユーザーは、OCSエージェントマシン上でRTCUniversalServerAdminsグループのメンバーとLocal/Administratorsグループのメンバーである必要があります。

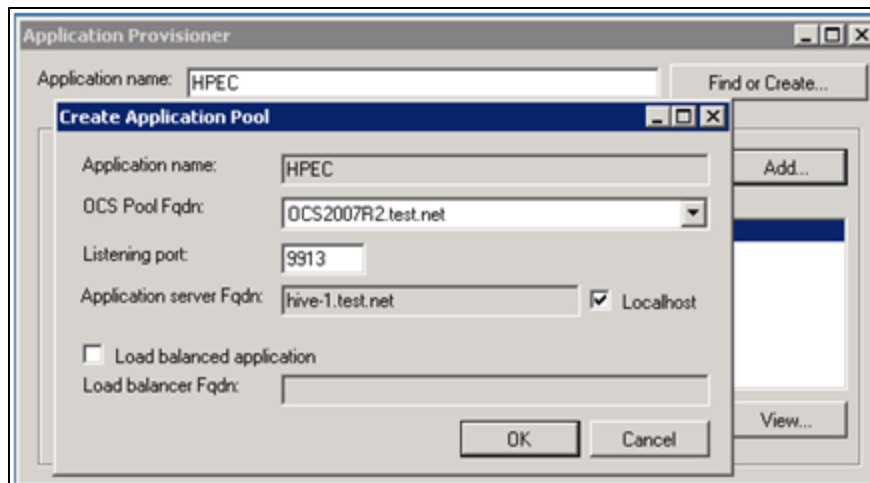
Office Communicator Server 2007のエージェントプロビジョニングを設定するには、次の手順を実行します。

1. OCSエージェントマシンに、RTCUniversalServerAdminsグループのメンバーのユーザーでログインします。
2. **ocs-agent**フォルダーにあるMicrosoftのユーティリティ、**ApplicationProvisioner.exe** (Enterprise Collaborationのインストール時にデプロイ済み)をダブルクリックします。
3. **[Application Provisioner]** ダイアログボックスが開きます。



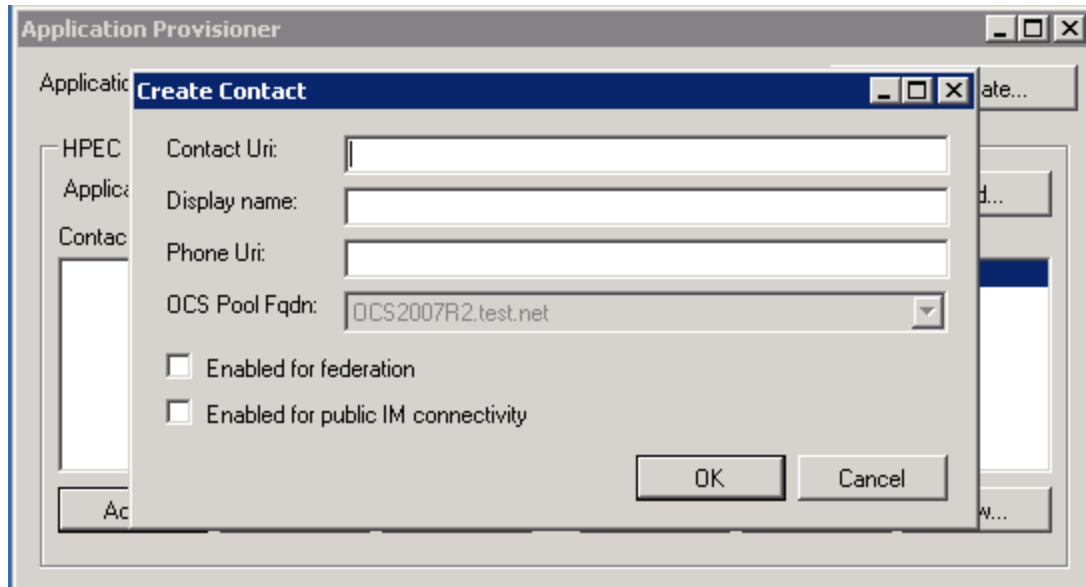
[Application Name] にHPECと入力し、**[Find or Create...]** をクリックします。

4. **[Create Application Pool]** ダイアログボックスが開きます。



- a. 次の内容を入力します。
 - **[OCS Pool Fqdn:]** ドロップダウンリストからOCSサーバーの**[FQDN]**を選択します。
 - リスニングポートの値を入力するか、デフォルト値を使用します。

- [Localhost]チェックボックスを選択します。
 - b. [OK] をクリックします。
 5. [Application Provisioner] ダイアログボックスが開きます。
[Contacts] セクションの [Add...] をクリックし、連絡先オブジェクトを作成します。
 6. [Create Contact] ダイアログボックスが開きます。



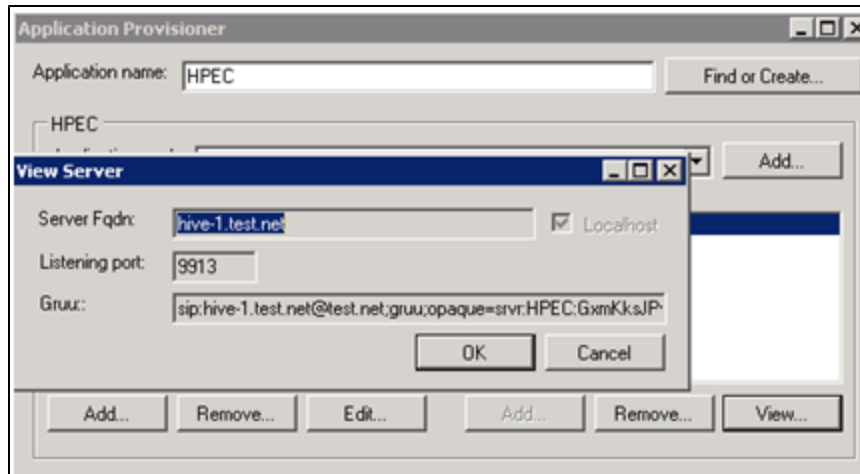
- a. 次の連絡先情報を入力します。
 - **[Contact Uri]:** HPEC OCSエージェントのSIPアドレスを入力します。形式は、**sip:<名前>@<ドメイン名>**です。たとえば、**sip:HPEC@hp.com**のようになります。

注: <名前>には、Active Directory内に存在し、電子メール権限とOCS権限を持つユーザー名を指定してください。

- **[Display name]:** OCでは、ECから受信したOCメッセージの送信者はこの表示名で表示されます。たとえば、**HPEC**と入力します。

注: [Phone Uri] には何も入力しないでください。また、2つのチェックボックスは選択しないでください。

- b. [OK] をクリックします。
7. [Application Provisioner] で、[Contact] を選択します。[Servers] セクションの [View...] をクリックします。
8. [View Server] ダイアログボックスが開きます。



[View Server] ダイアログボックスで、GRUUを保存します。これは、OCSエージェントの詳細設定で使用します。

Lync 2010のエージェントプロビジョニング

1. Lync Serverマシンで、次のように選択します。

```
[スタート] > [Microsoft Lync Server 2010] > [Lync Server Management Shell]
```

2. 次のコマンドを実行し、信用済みアプリケーションを作成します。

```
New-CsTrustedApplication -ApplicationId <アプリケーションID> -Port <アプリケーションポート> -TrustedApplicationPoolFqdn <OCSエージェント FQDN>
```

次に例を示します。

```
New-CsTrustedApplication -ApplicationId EeApplicationId -Port 6000 -TrustedApplicationPoolFqdn exum.fabrikam.com
```

エラーが発生しないことを確認します。

```
Administrator: Lync Server Management Shell
PS C:\Users\Administrator\FABRIKAM> new-cstrustedapplication -applicationid EeApplicationId -trustedapplicationpoolfqdn exum.fabrikam.com -port 6000
WARNING: The following changes must be made in order for the operation to be complete.
Enable-CsTopology must still be run for all changes to take effect.

Identity           : exum.fabrikam.com/urn:application:eeapplicationid
ComputerGruids    : (exum.fabrikam.com sip:exum.fabrikam.com@fabrikam.com;gruu;opaque=srvr:eeapplicationid:hr10ogJNF10kKB9UaVsC7AAA)
ServiceGruids     : sip:exum.fabrikam.com@fabrikam.com;gruu;opaque=srvr:eeapplicationid:hr10ogJNF10kKB9UaVsC7AAA
Protocol          : Mtls
ApplicationId     : urn:application:eeapplicationid
TrustedApplicationPoolFqdn : exum.fabrikam.com
Port              : 6000
LegacyApplicationName : eeapplicationid
```

3. ServiceGruidsの値を保存します。これは、OCSエージェントの詳細設定で使用されます。
4. 次のコマンドを実行し、トポロジを有効にします。

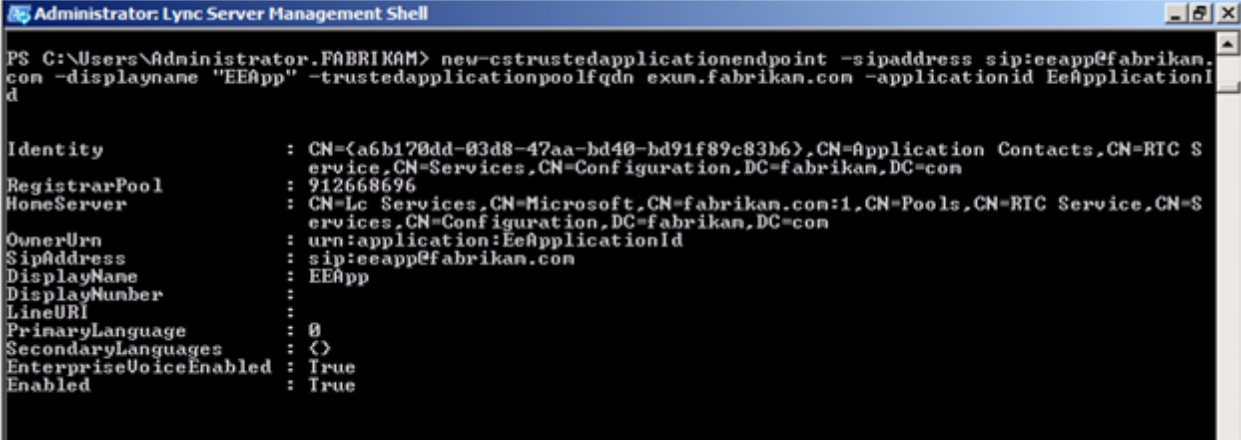
```
Enable-CsTopology
```

5. 次のコマンドを実行し、信用済みアプリケーションエンドポイントを作成します。

```
New-CsTrustedApplicationEndpoint -SipAddress <アプリケーションSIP> -  
DisplayName <アプリケーション表示名> -TrustedApplicationPoolFqdn <OCSエー  
ジェントFQDN> -ApplicationId <アプリケーションID>
```

次に例を示します。

```
New-CsTrustedApplicationEndpoint -SipAddress sip:ee@fabrikam.com -  
DisplayName EE -TrustedApplicationPoolFqdn exum.fabrikam.com -  
ApplicationId EeApplicationId
```



```
Administrator: Lync Server Management Shell  
PS C:\Users\Administrator.FABRIKAM> new-ctrustedapplicationendpoint -sipaddress sip:eeapp@fabrikam.  
com -displayname "EEApp" -trustedapplicationpoolfqdn exum.fabrikam.com -applicationid EeApplicationI  
d  
  
Identity           : CN={a6b170dd-03d8-47aa-bd40-bd91f89c83b6},CN=Application Contacts,CN=RTC S  
ervice,CN=Services,CN=Configuration,DC=fabrikam,DC=com  
RegistrarPool     : 912668696  
HomeServer        : CN=Lc Services,CN=Microsoft,CN=fabrikam.com:1,CN=Pools,CN=RTC Service,CN=S  
ervices,CN=Configuration,DC=fabrikam,DC=com  
OwnerUrn          : urn:application:EeApplicationId  
SipAddress        : sip:eeapp@fabrikam.com  
DisplayName       : EEApp  
DisplayNumber     :  
LineURI          :  
PrimaryLanguage   : 0  
SecondaryLanguages : (< >)  
EnterpriseVoiceEnabled : True  
Enabled          : True
```

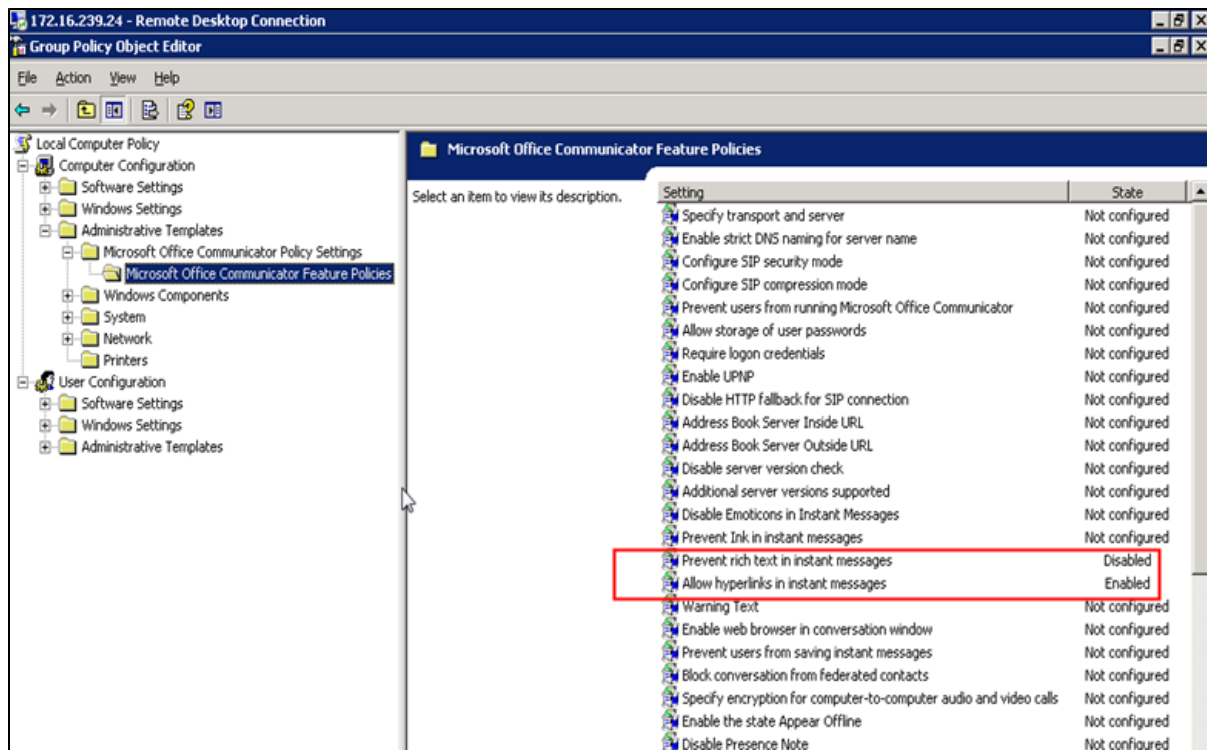
リッチコンテンツをサポートするOCSの設定

注: OCSでは、オプションで、リッチコンテンツのサポートを設定できます。OCSですでにリッチコンテンツのサポートを設定している場合や、リッチコンテンツのサポートが不要な場合は、ここで掲載する手順は省略してください。

リッチコンテンツをサポートするようにOCSを設定するには、次の手順を実行します。

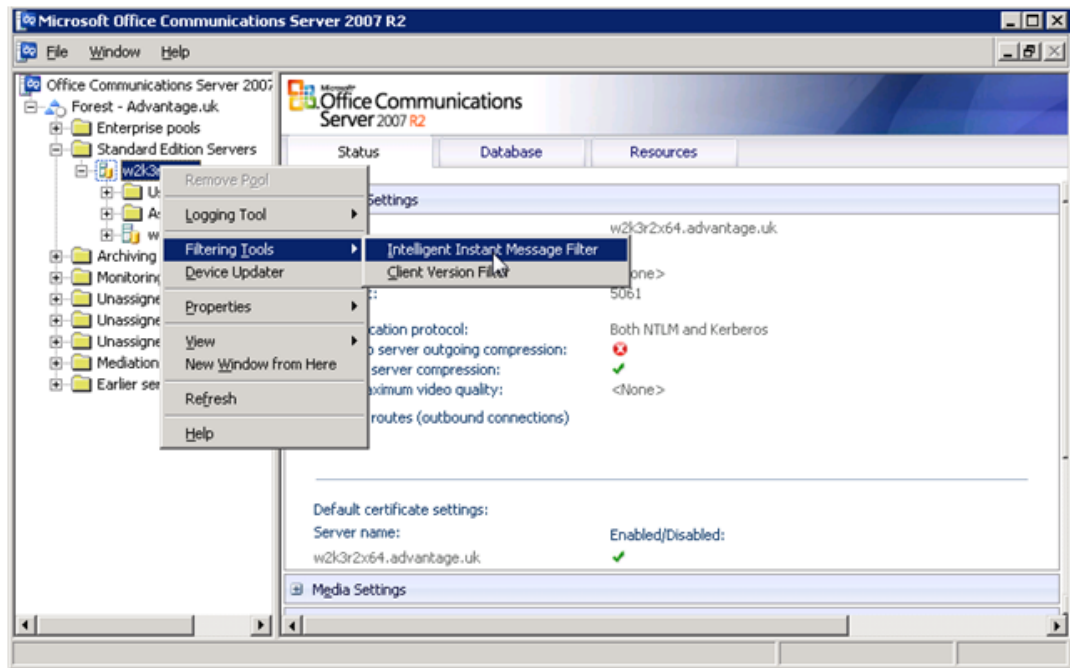
1. Enterprise Collaborationのインストールフォルダーから、Communicator.admファイルをOCSマシンにコピーします。
2. 次のようにgpedit.mscを実行します。
 - a. [Computer Configuration]に移動します。[Administrative Templates]を右クリックし、[Add/Remove Templates...]を選択します。
 - b. ダイアログで[Add...]を選択し、Communicatorの.admファイルのパスを指定します。
 - c. [Computer Configuration] > [Administrative Templates] > [Microsoft Office Communicator Policy Settings] > [Microsoft Office Communicator Feature Policies]を選択します。
 - d. [Prevent rich text in instant messages]を[Disabled]に変更し、[Allow hyperlinks in

instant messages] を **[Enabled]** に設定します。

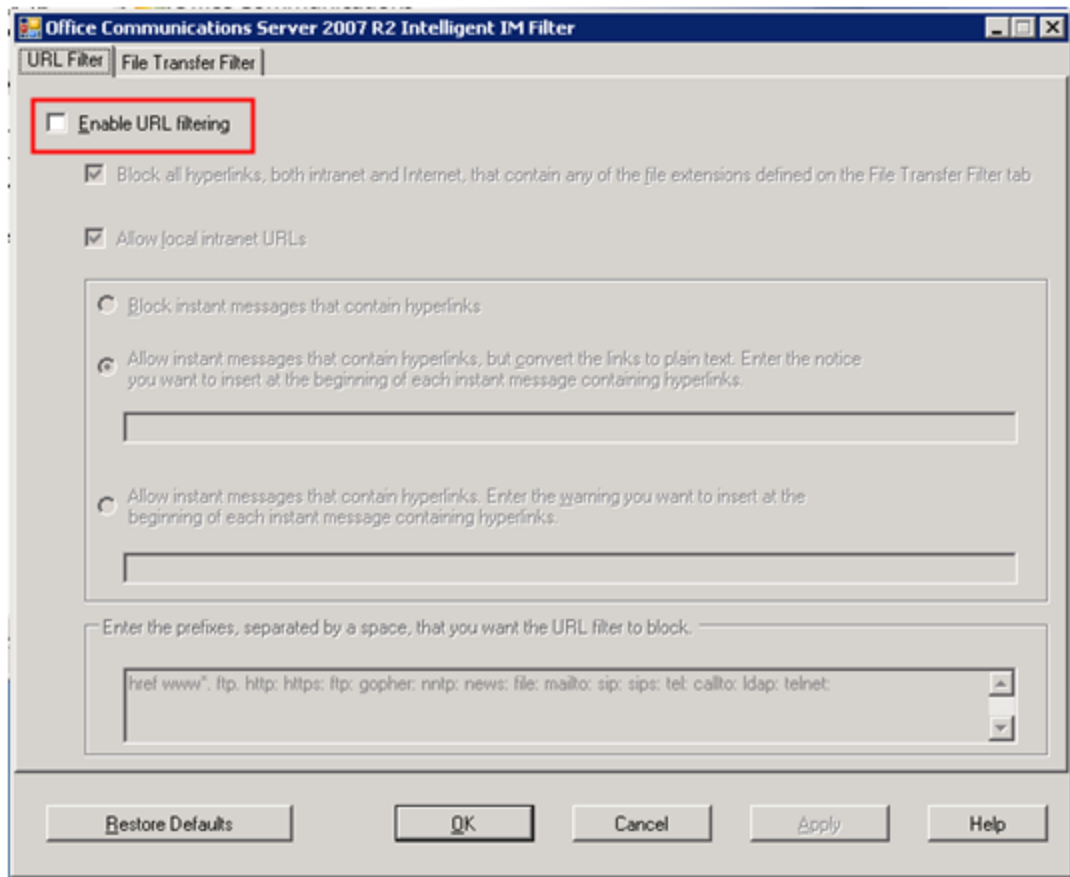


3. **C:\Program Files\Common Files\Microsoft Office Communications Server 2007 R2\WRTCSnap2.msc**を実行して、Microsoft管理コンソールを起動します。

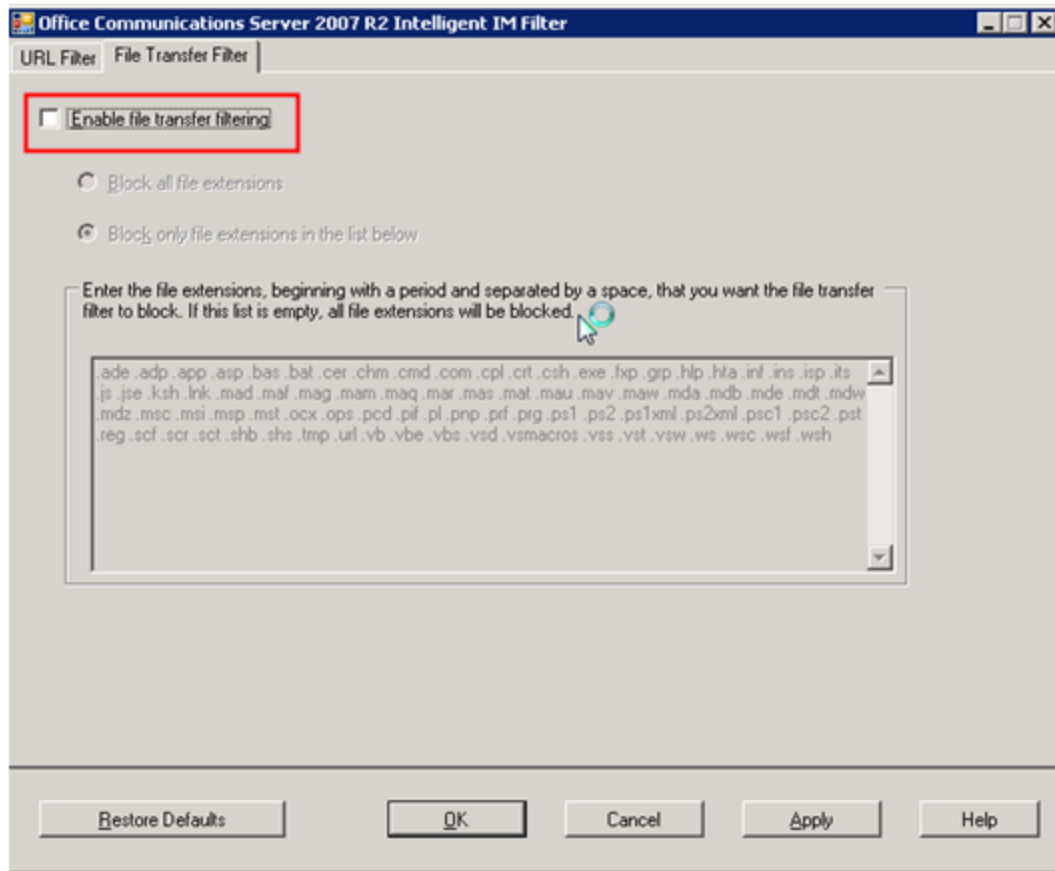
- [Forest - ...]** > **[Standard Edition Servers]** に移動し、OCSサーバーのホスト名を持つポータルを右クリックします。
- ポップアップメニューが開くので、**[Filtering Tools]** > **[Intelligent Instant Message Filter]** を選択します(下の図を参照)。



- c. [URL Filter] タブにある [Enable URL filtering] チェックボックスの選択を解除します (下の図を参照)。



- d. [File Transfer Filter] タブにある [Enable file transfer filtering] チェックボックスの選択を解除します (下の図を参照)。



4. OCSサーバーマシンを再起動します。

リッチコンテンツをサポートするOCクライアントの設定

注: OCクライアントでは、オプションで、リッチコンテンツのサポートを設定できます。OCクライアントですでにリッチコンテンツのサポートを設定している場合や、リッチコンテンツのサポートが不要な場合は、ここで掲載する手順は省略してください。

1. Enterprise Collaborationのインストールフォルダーから、**OCSCClient.reg**ファイルをOCクライアントがインストールされているマシンにコピーします。
2. クライアントマシン (OCクライアントのインストール場所) で**OCSCClient.reg**ファイルを実行し、OCクライアントアプリケーションを再起動します。

ECとOCSの統合のサニティテスト

1. サーバーマシンでHP ECサーバーを起動します。
2. サーバーマシンでOCSエージェントを起動します。

3. クライアントマシンでOCクライアントを起動します。user2でログインします。
4. ブラウザーを起動し、HP ECサイトにアクセスします。user1でログインします。
5. 新しい会話を作成します。user2を会話に追加します。
6. user2を必須の参加者 (緊急)として指定します。user2は、OCクライアントで通知を受信します。
7. OCクライアントからの応答を送信します。user2からの応答が会話に追加されます。

第4章

追加の構成手順

ここでは、インストールでの自動プロセスが失敗した場合、手動で実行する2つのプロセスについて説明します。

メールクライアントの証明書のインストール

メールクライアントの証明書は、2つの方法でインストールできます。ここで掲載するインストール手順が必要になるのは、セキュリティで保護された接続を使ってメールサーバーにアクセスし、証明書が自己署名の場合です。

方法1

1. ECのインストールは完了しており、電子メールの構成データは入力済みですが、電子メール構成の検証は実行していません。
2. 電子メールサーバーのポートの中で、セキュリティ保護されているポートを確認します。
3. ECサーバーで、**diamond-deploy/add-email-certificates.bat**を次のパラメーターで実行します。
**add-email-certificates.bat <電子メールの送信ホスト>:<電子メールの送信用セキュアポート>
<電子メールの受信ホスト>:<電子メールの受信用セキュアポート>**

次に例を示します。

```
add-email-certificates.bat exch14.net:466 exch14.net:996
```

4. ECサーバーを再起動します。

方法2

1. ECが停止していることを確認します。
2. CMDを開きます。
3. 次のコマンドを実行し、証明書をインポートします。

```
<ECフォルダー>\java\windows\x86_64\bin\keytool.exe -import -alias <証明書のエイリアス>  
-file <ルートCA証明書のパス> -keystore <ECフォルダー>\java\windows\x86_  
64\lib\security\cacerts
```

カスタマー証明書のインストール

インストールプロセスの最後で、自己署名の一時証明書を使ってTomcatサーバーの設定を行います。

スタンドアロンのWebアプリケーションネットワーク構成を使用する場合は、以下の手順を実行しなくても、ECのインストール中に生成される自己署名の証明書を使用できます。ただし、次の手順に従って、サーバー証明書をキーストアにインポートすることをお勧めします。

リバースプロキシネットワーク構成を使用している場合、次の手順に従って、ルートCA証明書とサーバー証明書をECサーバーのキーストアにインポートしてください。

Tomcatで使用する証明書をインストールするには、次の手順を実行します。

1. ECが停止していることを確認します。
2. CMDを開きます。
3. 次のコマンドを実行し、一時証明書をキーストアから削除します。

```
<ECフォルダー>\java\windows\x86_64\bin\keytool.exe -delete -alias tomcat -keystore  
<ECフォルダー>\servers\server-0\ec-keystore.jks
```

4. 次のいずれかのコマンドを実行します。

- キーストアをECキーストアにインポートするには、次の手順を実行します。

```
<ECフォルダー>\java\windows\x86_64\bin\keytool.exe -importkeystore -srckeystore <  
キーストアパス> -destkeystore <ECフォルダー>\servers\server-0\ec-keystore.jks -  
srcstoretype <キーストアタイプ>
```

- 証明書をECキーストアにインポートするには、次の手順を実行します。

```
<ECフォルダー>\java\windows\x86_64\bin\keytool.exe -import -alias <証明書のエイリア  
ス> -file <証明書のパス> -keystore <ECフォルダー>\servers\server-0\ec-keystore.jks
```

注: リバースプロキシ証明書の場合、このコマンドをルートCAとサーバー証明書の両方で実行してください。

デフォルトの安全な認証を無効化 (オプション)

次の手順は、認証時のhttpsへのリダイレクトを無効にする場合にのみ実行してください。

注: セキュリティ上の理由から、無効化はお勧めしません。

1. ECが停止していることを確認します。
2. CMDを開きます。
3. **C:\HP\EC\diamond-deploy\disable-secure-authentication.bat**を実行します。
4. ECを開始します。

第5章

Deployment Managerでの構成の更新

構成の更新は、Deployment Managerの [Deployment Type] タブで行います。

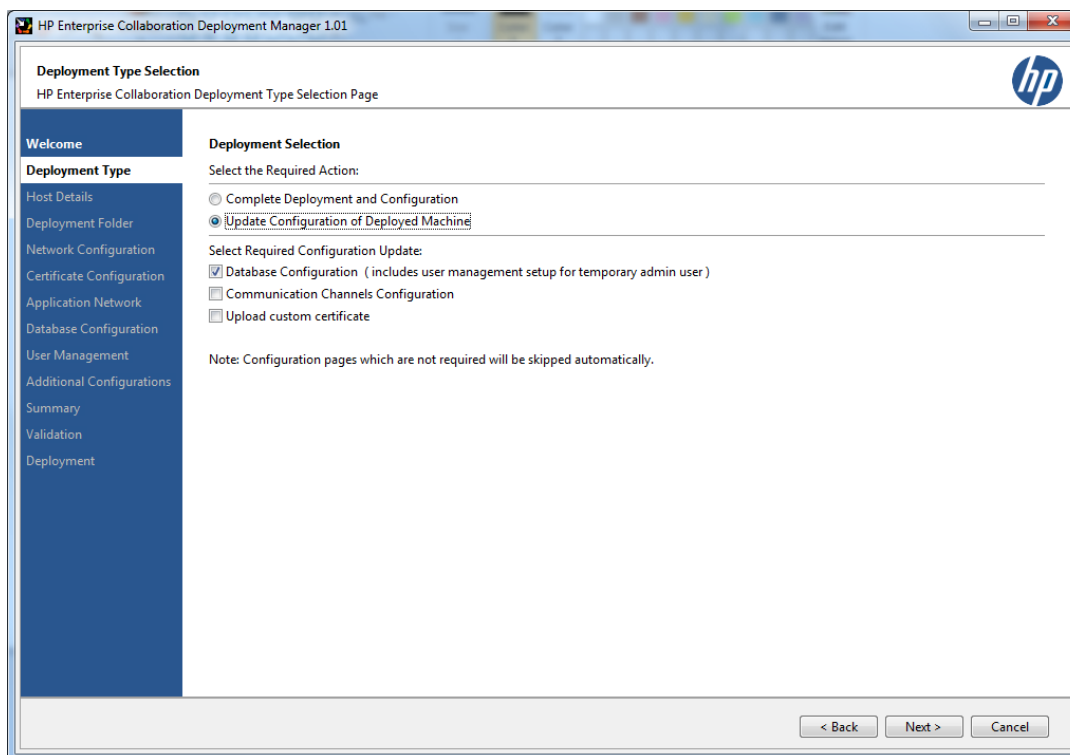
1. [EC-Deployment Manager] フォルダにあるEC.exeをダブルクリックします。
2. Enterprise Collaboration Deployment Manager Wizardが起動します。

[Welcome] ページで [I accept the terms of the license agreement] を選択します。[Next] をクリックします。

3. [Deployment Selection] ページが開きます。

[Update Configuration of Deployed Machine] を選択します。

4. 次の構成の構成を選択できます。



次の構成オプションが表示されます。

- **[Database Configuration]:**この構成を選択すると、更新ウィザードが起動して次のページの内容を変更できます。
 - [EC Deployment Host Details]
 - [Deployment Folder Configuration]

- [MSSQL Database Server Configuration]
- [User Management Configuration]
- [Summary]
- [Validation]
- **[Communication Channels Configuration]**:このオプションが適用されるのは、Enterprise CollaborationとOffice Communicatorを組み合わせて使用する場合のみです。Office Communicatorの設定が完了した後に実行してください(詳細については「[Office Communicator ServerおよびMS Lync Serverとの統合の設定](#)」(29ページ)を参照してください)。
- **[Upload Custom Certificate]**: インストールの最後にカスタマイズしたセキュリティ証明書をアップロードする場合、このオプションを選択します。詳細については、手順8を参照してください。

上記の構成オプションは、すべて選択することが可能です。

5. 構成の更新タイプを選択し、**[Next]**をクリックします。
6. 上記で**[Database Configuration]**を選択した場合、構成ウィザードでは手順4のページが開き、必要に応じて内容を変更できます。

[Communication Channels Configuration]を選択した場合は、[EC Deployment Host Details]、[Deployment Folder Configuration]、[Communication Channels Configuration]の各ページが開きます。[EC Deployment Host Details]と[Deployment Folder Configuration]はインストール中に表示されるページであり、必要に応じて変更できます。

次に、[Communication Channels Configuration] ページを示します。

HP Enterprise Collaboration Deployment Manager 1.0

HP Enterprise Collaboration: Communication Channels Configuration

HP Enterprise Collaboration Product Page

hp

Welcome

Deployment Type

Host Details

Deployment Folder

Network Configuration

Application Network

Database Configuration

User Management

Additional Configurations

Summary

Validation

Deployment

Communication Channels Configuration

OCS Server FQDN:

OCS Server Port:

OCS Application Name:

OCS Application Port:

OCS Application GRUU:

OCS Application SIP URI:

OCS Agent FQDN:

Skip Communication Channels configuration

Note:
OCS Application GRUU: is the trusted application parameter called GRUU in Approvisioner.

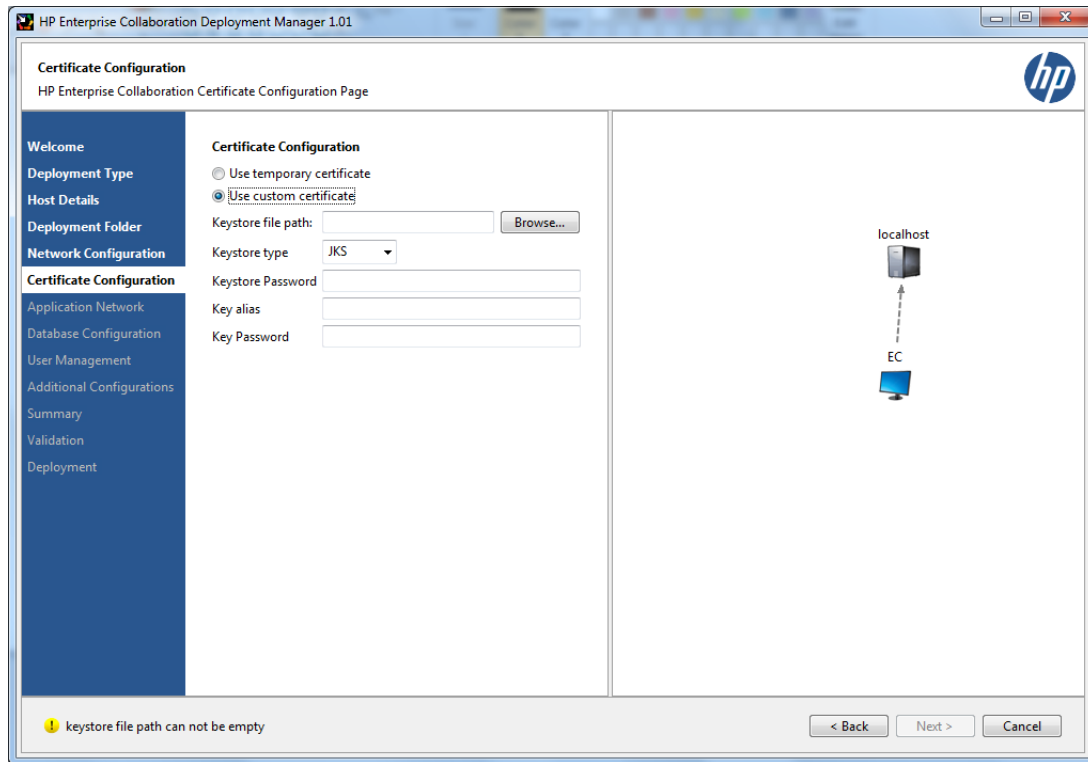
! Insert OCS Server FQDN

< Back Next > Cancel

7. [Communication Channels Configuration] ページでは、次の内容を入力します。

- **[OCS Server FQDN]:**「Office Communicator ServerおよびMS Lync Serverとの統合の設定」(29ページ)プロセスで入力した**OCSプールFqdn**を入力します。
- **[OCS Server Port]:** デフォルト値は5061です。このポート番号は、システム管理者に確認してください。
- **[OCS Application Name]:** デフォルトの名前は**EE**です。「Office Communicator ServerおよびMS Lync Serverとの統合の設定」(29ページ)プロセスで入力した**表示名**を入力します。
- **[OCS Application Port]:** デフォルト値は6000です。「Office Communicator ServerおよびMS Lync Serverとの統合の設定」(29ページ)プロセスで入力した**リスニングポート番号**を入力します。
- **[OCS Application GRUU]:** 「Office Communicator ServerおよびMS Lync Serverとの統合の設定」(29ページ)プロセスで取得した文字列を入力します。
- **[OCS Application SIP URI]:** デフォルト値は**sip:EE@**です。「Office Communicator ServerおよびMS Lync Serverとの統合の設定」(29ページ)プロセスで入力した**連絡先URI**を入力します。
- **[OCS Agent FQDN]:** EEサーバーのFQDNを入力します。

8. [Upload Custom Certificate] を選択した場合、[Use temporary certificate] または [Use custom certificate] を選択してください。
9. [Use custom certificate] を選択する場合は、キーストアの詳細情報を入力します。



サポートされるキーストアは、**JKS**と**PKC**です。

証明書は、入力したキーのエイリアスに基づいてインポートされます。

第6章

アダプターの設定

1. アダプターの.warファイルをwww.hp.com/go/livenetworkからダウンロードします。
2. アダプターの.warファイルを<ECインストールフォルダー>/servers/server-0/webappsに保存します。warファイルの名前は、アダプター名と同じにします。

アダプターをリモートでデプロイする場合は、Tomcat Managerアプリケーションを使用して、次の手順に従います。

<http://tomcat.apache.org/tomcat-7.0-doc/manager-howto.html>

注: ネットワーク速度が低下しないように、アダプターのwarファイルはターゲットサーバーの一時ディレクトリにコピーしてください。デプロイメントの完了後、一時ディレクトリから次のディレクトリにファイルを移動します。

<ECのインストールフォルダー>/servers/server-0/webapps

3. JMXを使用して基本アダプターURLを追加するには、次の手順を実行します。
 - a. <ECアプリケーションURL>/diamond/jmx-console (http://my_host:8080/diamond/jmx-consoleなど)にアクセスします。
 - b. [Diamond] > [Diamond adapter config jmx service] を選択します。
 - c. addAdapterUrlメソッド (下の図を参照) で、次のパラメーターを追加します。
 - adapterName: アダプターの.warファイルと同じ名前にします。たとえば、ファイル名がsm.warの場合、smと入力します。
 - adapterUrl: ローカルデプロイメントの場合、アダプターURLは{local}/adapter_nameとなります。

addAdapterUrl
Add the adapter URL

Name	Type	Value	Description
adapterName	java.lang.String	<input type="text"/>	adapter Name
adapterUrl	java.lang.String	<input type="text"/>	adapter Url

- d. [Invoke] をクリックします。

4. アダプターでLWSSOを使用する場合、アダプターの`war`の中のLWSSO構成ファイルで定義されている`initString`と、ECのインストール時に[Lightweight Single Sign On Configuration] ページで指定した`initString`の値が一致していることを確認します。

第7章

EC構成の1.0から1.1へのアップグレード

ここでは、Enterprise Collaborationをバージョン1.0からバージョン1.1にアップグレードする方法について説明します。

Enterprise Collaborationの旧バージョンがインストールされていて、EC 1.1環境のデータをそのまま使用する必要がある場合は、アップグレードの前に次の手順を実行してください。

注: EC 1.1は、ECの旧バージョンと同じマシンにインストールする必要があります。

1. external-ldap.propertiesファイルとldap証明書ファイル(存在する場合)を、旧バージョンの環境から一時ディレクトリにバックアップします。
2. C:\HP\EC\servers\server-0\webappsのアダプターをすべて一時ディレクトリにバックアップします。
3. データベーススキーマをバックアップします。
4. EC (1.00または1.01)をアンインストールします。これにより、ECサービスとすべてのショートカットが削除されます。

次に、Enterprise Collaboration 1.1をインストールします。

1. 「Enterprise Collaborationのインストール」の手順に従って、[Connect to Existing Schema] オプションを選択し、EC 1.1をインストールします(「MSSQLデータベース管理者の構成」(20ページ)を参照してください)。
2. インストール中、旧バージョンの環境とすべて同じ構成を行ってください(初期化文字列、電子メール、OCSなど)。

注: ここでは、以前に使用した一時管理者とは異なるユーザーを使用する必要があり、ユーザーリポジトリ内に存在するユーザーは使用できません。

3. インストールが完了したら、external-ldap.propertiesファイルをC:\tempディレクトリからC:\HP\EC\confにコピーします(既存ファイルを上書き)。
4. バックアップしたldap証明書(存在する場合)をdiamond-deployに移動し、次のコマンドを実行します。

```
set-ldap-certificate.bat certificate-file-name
```

5. bsf.propertiesを次のように更新します。

```
authentication.provider=EXTERNAL
```

```
personalization.provider=SHARED
```

```
users.provider=EXTERNAL
```

```
groups.provider=EXTERNAL
```

```
roles.provider=SHARED
```

```
roles.relations.provider=SHARED
```

6. バックアップアダプターを一時ディレクトリからC:\HP\EC\servers\server-0\webappsに移動します。
7. ECサーバーを起動します。
8. 既存のすべての会話のインデックスを再生成するために、次の手順でElastic Searchをリセットします。
 - a. `http://diamond_host:<HTTPポート>/diamond/jmx-console`にアクセスします。
 - b. 管理者ユーザーでログインします (バージョン1.1のインストール中、[User Management Configuration] ページで一時的な管理ユーザーが作成されます)。
 - c. [Diamond] > [Diamond search JMX service] を選択します。
 - d. `resetExperienceLastIndexRunTime`メソッドを起動します。

注: アップグレードが完了するとデータベース内に役割の定義がすべて格納されるので、BSFユーザー管理の入力は不要です。

第8章

デスクトップクライアントのインストール

デスクトップクライアントアプリケーションは、ECの会話が変更された場合に変更内容に関する通知を表示するツールです。Enterprise Collaborationで現在進行している会話について、参加者に関連情報を表示します。

ここでは、システムにデスクトップクライアントをインストールする方法と、インストールウィザードで実行される手順の詳細について説明します。

Enterprise CollaborationデスクトップクライアントをEnterprise Collaborationからインストールするには、次の手順を実行します。

1. ECウィンドウの右上隅にあるユーザー名をクリックします。

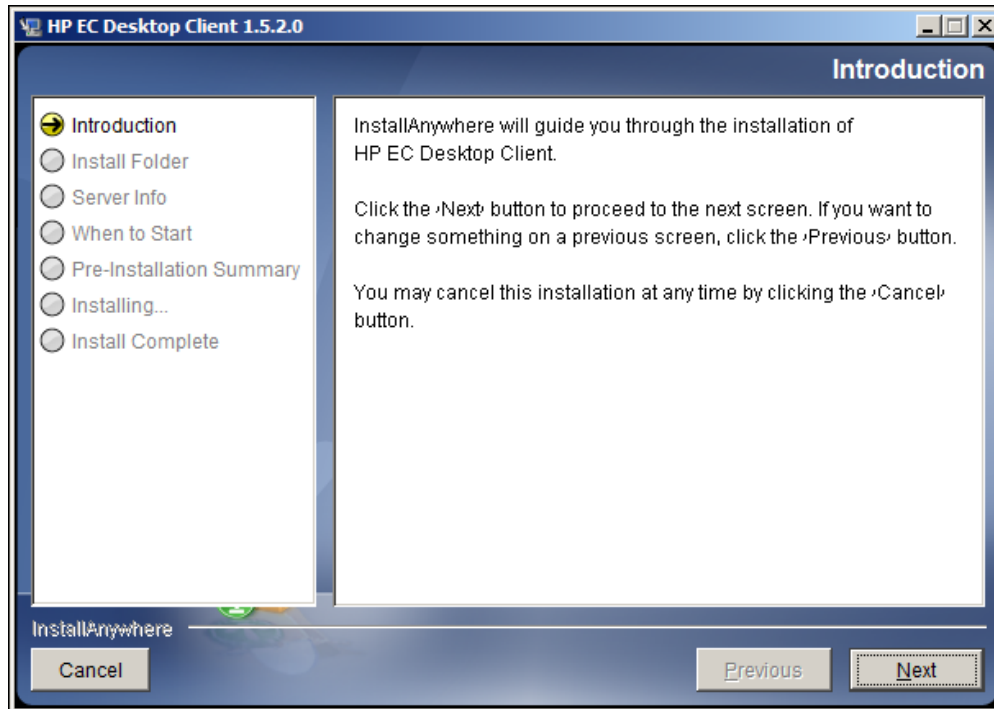


2. [ユーザープロフィール] ウィンドウが開きます。

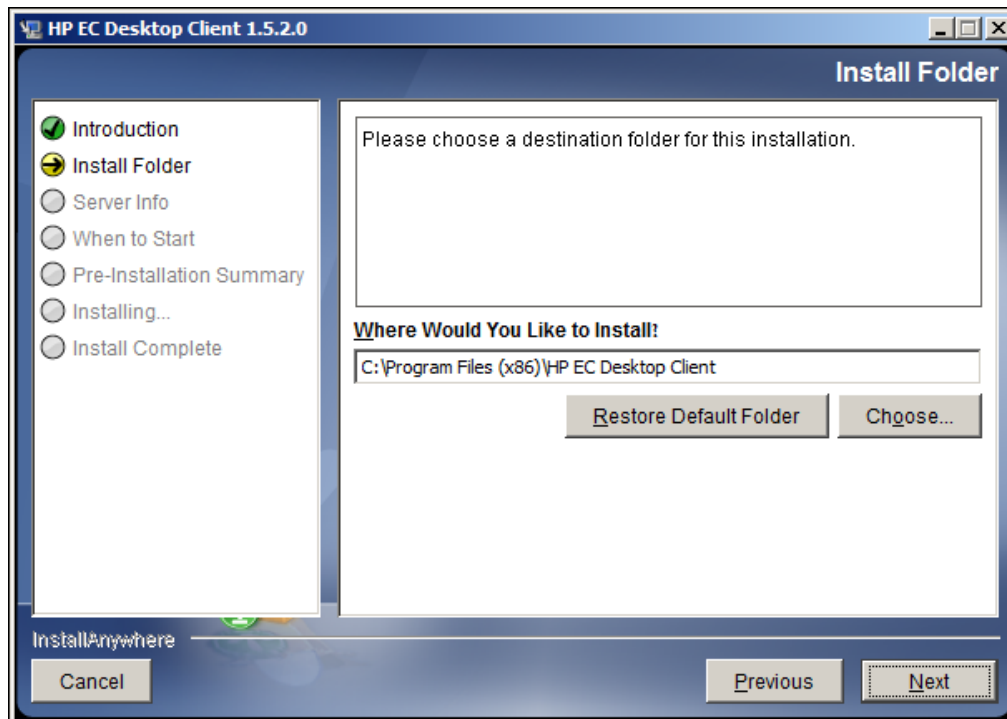


3. ウィンドウの下にある [デスクトップクライアントのダウンロード] リンクをクリックします。
4. [ファイルを開く] 警告 ウィンドウが開くので、[実行] をクリックします。

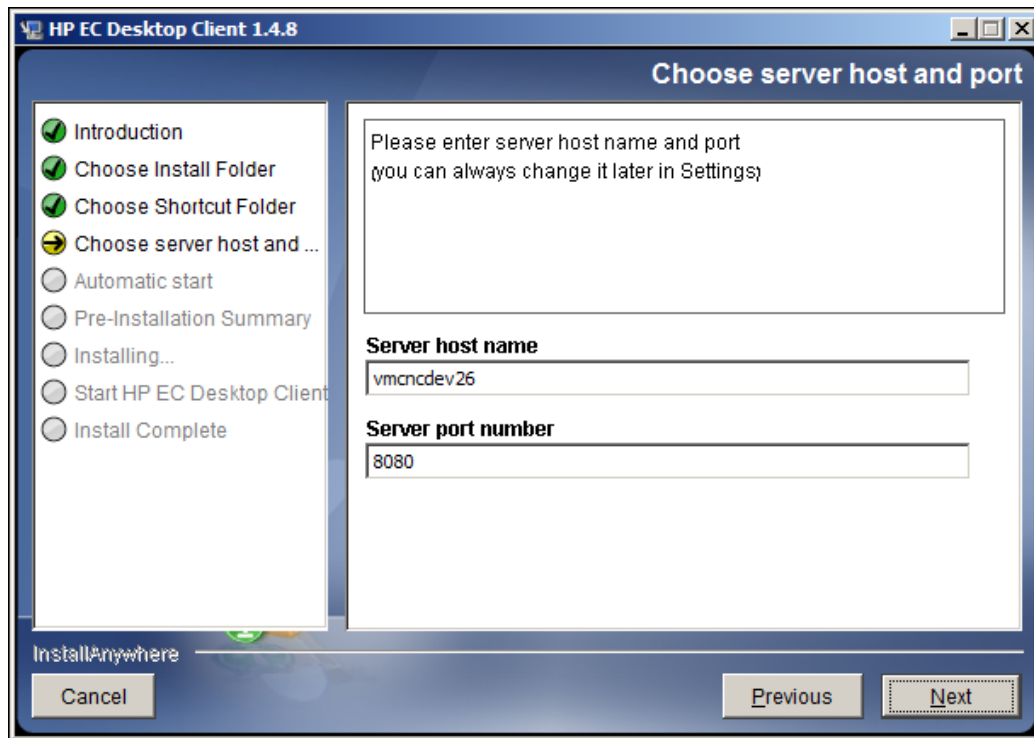
5. [保存] または [開く] を選択し、デスクトップクライアントのzipファイルをダウンロードして解凍します。
6. **hpec_dc.exe**を実行します。
7. HP ECデスクトップクライアントのインストールが開始します。



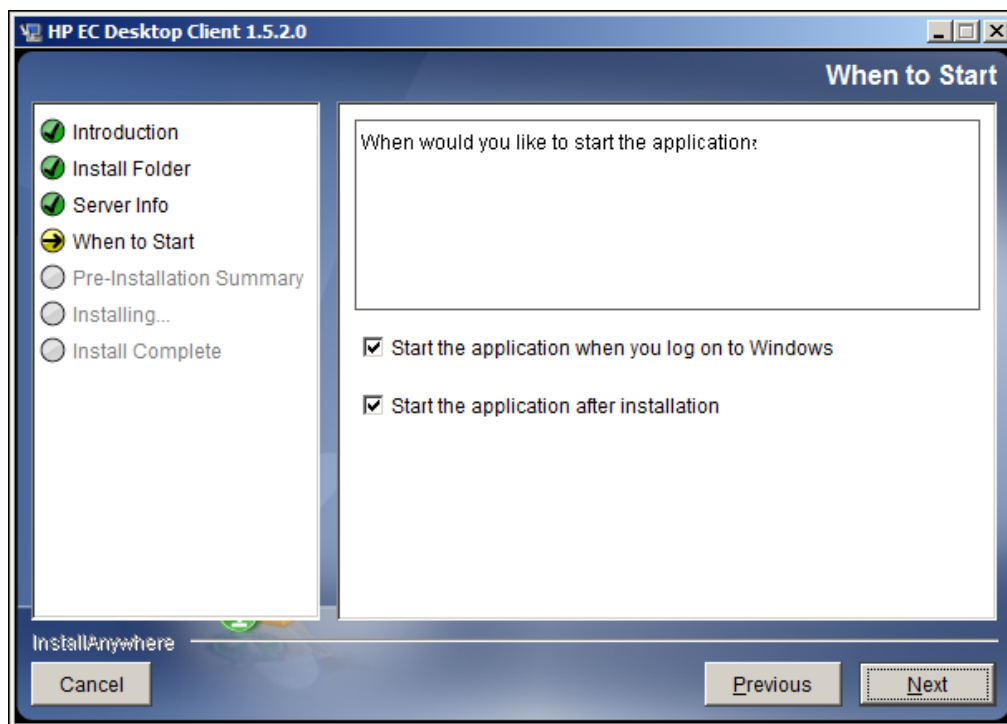
8. [Introduction] ダイアログボックスが開くので、[Next] をクリックします。



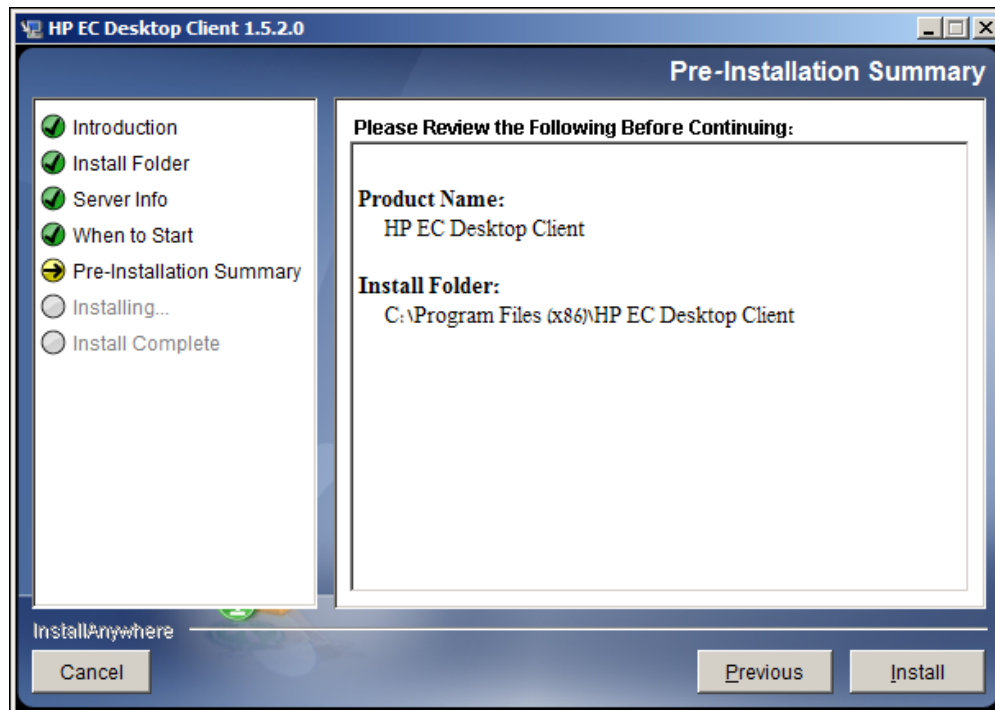
9. **[Choose Install Folder]** ダイアログボックスで、**[Choose]** をクリックしてインストールフォルダを選択してから **[Next]** をクリックします。



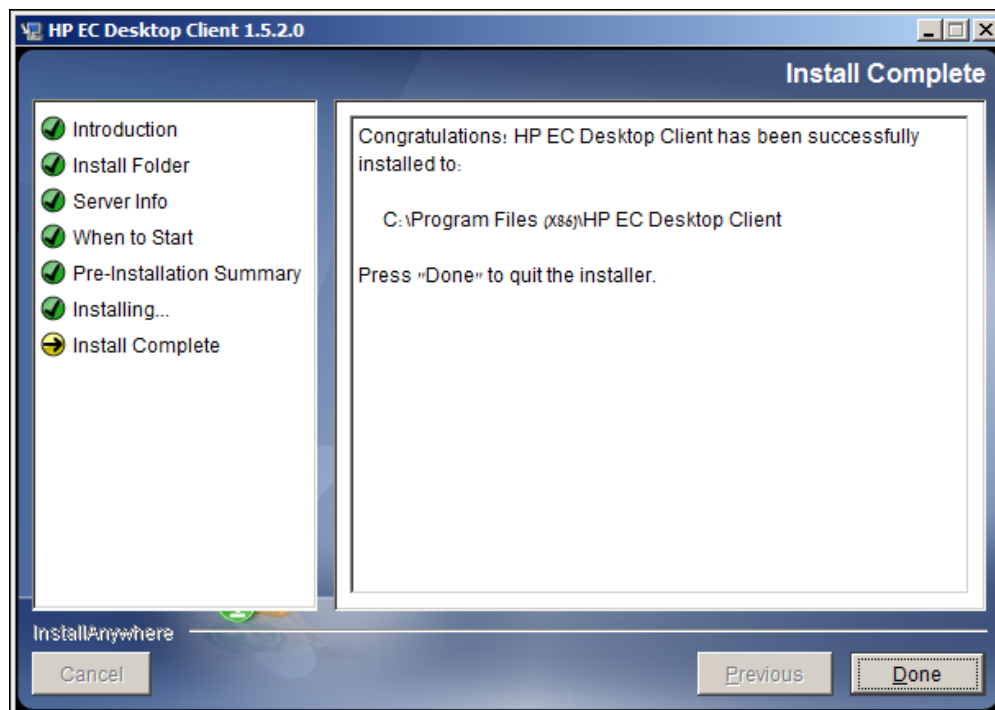
10. **[Choose server host and port]** ダイアログボックスが開いたら、EC Serverのホスト名とポート番号を入力し、**[Next]** をクリックします。



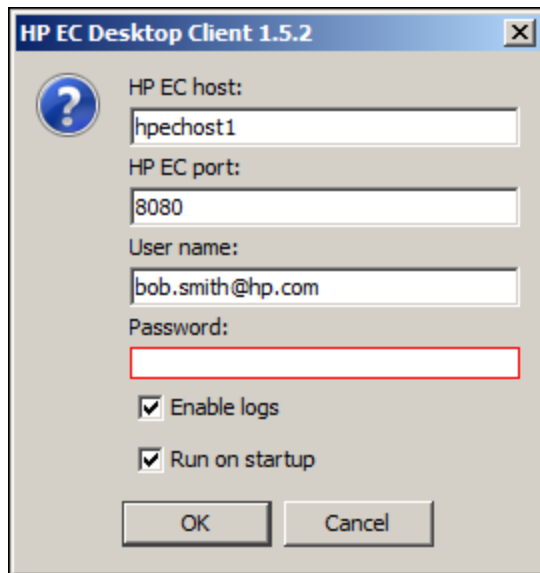
11. [When to Start] ダイアログボックスで、[Start the application when you log on to Windows] を選択します。これにより、Windowsへのログイン時にECデスクトップクライアントが自動的に開始されます。[Start the application after installation] を選択します。これにより、インストールが完了するとすぐにECデスクトップクライアントが起動します。



12. インストールの詳細情報がサマリーで表示されます。内容を確認し、[Install] をクリックします。



13. [Done] をクリックします。[HP EC Desktop Client Settings] ウィンドウが開きます。

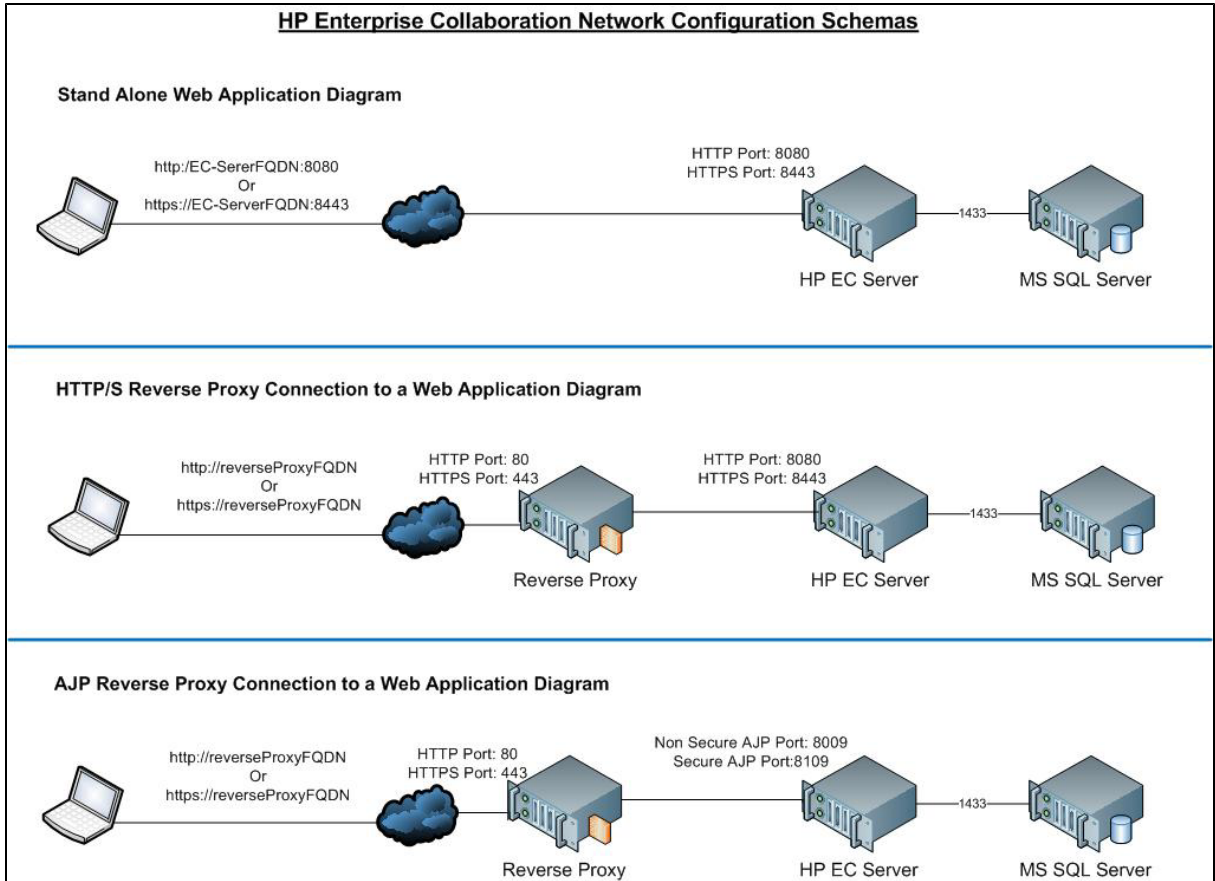


14. [Password] フィールドにユーザーパスワードを入力し、[OK] をクリックします。
15. デスクトップクライアントが起動した後、最小化されてステータスバーに表示されます。
16. [When to Start] ダイアログボックスで **[Start the application after installation]** を選択しなかった場合、[スタート] > [すべてのプログラム] > **[HP EC Desktop Client]** を選択するとデスクトップクライアントをいつでも起動できます。

ECデスクトップクライアントの使用方法の詳細については、『Enterprise Collaborationコンセプトガイド』を参照してください。

付録A: HP Enterprise Collaborationでのネットワーク構成スキーマ

次の図は、HP Enterprise Collaborationで使用するネットワーク構成スキーマを示します。



付録B: external-ldap.propertiesファイルの更新

external-ldap.propertiesファイルを変更する作業には、ユーザーリポジトリに必要なLDAPプロパティに関する知識が必要になります。LDAP構成についてあまり知識がない方は、Apache Directory Studio LDAPブラウザーなどのツールを活用することにより、ユーザーリポジトリで必要になるLDAPプロパティを検出できます。Apache Directory Studio LDAPブラウザーでLDAPにログインする方法については、「[Apache Directory Studio LDAPブラウザーによるLDAPへのログイン](#)」(74ページ)を参照してください。

基本的なLDAPプロパティ

次の表は、ECからLDAPにログインする際、**external-ldap.properties**で構成が必要な基本的なLDAPプロパティを示します。

属性	説明
ldapHost	LDAPホスト名
ldapPort	LDAPポート番号
enableSSL	TrueまたはFalse - LDAPへの接続にSSLを使用するかどうか
useAdministrator	TrueまたはFalse - LDAPへの接続にこのユーザーを使用するかどうか
ldapAdministrator	LDAPユーザーDN (useAdministrator=Trueの場合に定義)
ldapAdministratorPassword	LDAPユーザーのパスワード (useAdministrator=Trueの場合に定義) 注: external-ldap.properties内ではLDAPユーザーのパスワードは暗号化されません。

ユーザープロバイダーの構成

ユーザー組織で使用するLDAPプロパティに基づいて、**external-ldap.properties**ファイルを次の属性で更新します。

属性	説明
usersBase	ユーザー検索で使用するLDAP基本識別名 (DN)。LDAP階層内でこのDNを持つユーザーのみが検索結果として返されます。
usersScope	ユーザー検索でのLDAP検索範囲。usersBaseの場所での検索対象を定義します。SCOPE_BASE検索領域には、userBaseがポイントする単一のエントリーが含まれます。SCOPE_ONE検索領域には、userBaseとその直下の子のみが含まれます。SCOPE_SUB検索領域には、userBaseとサブツリー全体が含まれます。
usersFilter	ユーザー検索に適用するLDAPフィルター。

ユーザーオブジェクトクラスの構成

次のプロパティは、LDAPベンダーの定義や、ユーザーオブジェクトを表すカスタム実装固有のオブジェクトの定義で使われます。

ユーザー構成プロパティを、組織のLDAPサーバー構成プロパティにマッピングするには、組織のLDAPプロパティに基づいて、**external-ldap.properties** ファイルを次の属性で更新します。

属性	説明
usersObjectClass	ユーザーのオブジェクトを表すLDAPオブジェクトクラス。
usersUniqueIDAttribute	ユーザーを一意に識別するIDを表すLDAP属性名。
usersLoginNameAttribute	ユーザーのログイン名を表すLDAP属性名。

次の属性はオプションです。

属性	説明
usersDisplayNameAttribute	ユーザーの表示名を表すLDAP属性名。
usersFirstNameAttribute	ユーザーの名を表すLDAP属性名。
usersLastNameAttribute	ユーザーの姓を表すLDAP属性名。
usersEmailAttribute	ユーザーの電子メールを表すLDAP属性名。
usersSipAttribute	ユーザーのSIPを表すLDAP属性名。
usersPreferredLanguageAttribute	ユーザーの優先言語を表すLDAP属性名。
usersPreferredLocationAttribute	ユーザーの地域を表すLDAP属性名。
usersTimeZoneAttribute	ユーザーのタイムゾーンを表すLDAP属性名。
usersDateFormatAttribute	ユーザーの日付形式を表すLDAP属性名。
usersNumberFormatAttribute	ユーザーの数値形式を表すLDAP属性名。
usersWorkWeekAttribute	ユーザーの稼働日を表すLDAP属性名。
usersTenantIDAttribute	ユーザーのテナントIDを表すLDAP属性名。
usersPasswordAttribute	ユーザーのパスワードを表すLDAP属性名。

グループ検索

次のプロパティは、LDAPグループで実装されている検索機能を定義します。通常グループ用のプロパティとルートグループ用のプロパティの2種類があります。

ルートグループの検索条件を設定することにより、グループの表示数を絞り込むことができます。ルートとルート以外のグループのいずれにも、同じ検索条件を適用できます。この構成が適しているのは、グループ全体の数が少ない場合です。

グループ構成プロパティをLDAPサーバー構成プロパティにマッピングするには、ユーザー組織のLDAPに基づいて、**external-ldap.properties** ファイルを次の属性で更新します。

属性	説明
groupsBase	グループ検索に使用するLDAP基本識別名 (DN)。LDAP階層内でこのDNを持つグループのみが検索結果として返されます。
groupsScope	グループ検索の対象となるLDAPスコープ。 <ul style="list-style-type: none">SCOPE_BASE検索領域には、groupsBaseにポイントした単一のエントリが含まれます。SCOPE_ONE検索領域には、groupsBaseとその直下の子が含まれます。SCOPE_SUB検索領域には、groupsBaseとサブツリー全体が含まれます。
groupsFilter	グループ検索に適用するLDAPフィルター。有効な値

属性	説明
	は、rootGroupsBase、rootGroupsScope、rootGroupsFilterのいずれかです。
rootGroupsBase	グループ検索に使用するLDAP基本識別名 (DN)。LDAP階層内でこのDNを持つグループのみが検索結果として返されます。
rootGroupsScope	グループ検索でのLDAP検索範囲。groupBaseの場所での検索対象を指定します。 <ul style="list-style-type: none"> SCOPE_BASE検索領域には、rootGroupsBaseにポイントした単一のエントリーが含まれます。 SCOPE_ONE検索領域には、rootGroupsBaseとその直下の子が含まれます。 SCOPE_SUB検索領域には、rootGroupsBaseとサブツリー全体が含まれます。
rootGroupsFilter	グループ検索に適用するLDAPフィルター。

グループオブジェクトクラス (LDAPベンダー固有)

次のプロパティは、LDAPベンダーの定義や、静的グループを表すカスタム実装固有のオブジェクトの定義で使用します。複数のオブジェクトクラスをカンマ区切りで指定することが可能です。この場合、設定する属性名をカンマ区切りで定義します。

グループ構成プロパティをLDAPサーバー構成プロパティにマッピングするには、組織のLDAPプロパティに基づいて、**external-ldap.properties** ファイルを次の属性で更新します。

属性	説明
groupsObjectClass	グループオブジェクトを表すLDAPオブジェクトクラス。
groupsMembersAttribute	グループメンバーを表すLDAP属性名。この属性には複数の値を指定でき、静的グループメンバーの完全識別名 (DN) を含みます。

次の属性はオプションです。

属性	説明
groupNameAttribute	グループを一意に識別する名前を示すLDAP属性名。ほとんどのデフォルトのLDAP実装環境では、一般的にこの属性はgroupsDisplayNameAttributeと同じ値に設定されます。
groupsDisplayNameAttribute	グループの表示名を示すLDAP属性名。ほとんどのデフォルトのLDAP実装環境では、一般的にこの属性はgroupNameAttributeと同じ値に設定されます。
groupsDescriptionAttribute	グループの説明を示すLDAP属性名。この属性には、グループの説明が含まれます。
enableDynamicGroups	動的グループを有効にするブール属性。この属性の値がtrueの場合、動的グループが検索されます。非常にサイズの大きい

属性	説明
	動的グループのメンバーを列挙する場合、検索に時間がかかることがあるので注意してください。
dynamicGroupsClass	動的グループオブジェクトを表すLDAPオブジェクトクラス。
dynamicGroupsMemberAttribute	動的グループメンバーを表すLDAP属性名。この属性には、LDAPの検索URLが含まれます。このLDAP検索URLが返す値は、動的グループのメンバーとみなされます。
dynamicGroupsNameAttribute	動的グループを一意に識別する名前を表すLDAP属性名。ほとんどのデフォルトのLDAP実装環境では、一般的にこの属性はdynamicGroupsDisplayNameAttributeと同じ値に設定されます。
dynamicGroupsDisplayNameAttribute	動的グループの表示名を表すLDAP属性名。ほとんどのデフォルトのLDAP実装環境では、一般的にこの属性はdynamicGroupsNameAttributeと同じ値に設定されます。
dynamicGroupsDescriptionAttribute	動的グループの説明を表すLDAP属性名。この属性には、グループの説明が含まれます。

グループ階層

グループ階層属性は、HP Enterprise CollaborationとLDAPサーバーのグループ階層情報との関連を定義します。

属性	説明
enableNestedGroups	グループのネスティングのサポートを有効にします。ネスティングのサポートを無効にすると、グループのサブグループは検索対象から除外されます。
maximalAllowedGroupsHierarchyDepth	グループ階層で許可される深さの最大値。このレベルより下のグループは検索対象から除外されます。

詳細構成

詳細構成の属性は、LDAP接続の調整に使用します。

属性	説明
ldapVersion	LDAPプロトコルのバージョン。次の値を指定できます。 <ul style="list-style-type: none"> 3 (デフォルト) 2 (旧バージョンのLDAP)
baseDistinguishNameDelimiter	基本DNの区切り記号。ユーザーやグループ、ユーザー検索で基本DNを複数指定する場合に使用する区切り記号です。基本DNに含まれている記号は使用できません。基本DNでこの記

属性	説明
	号を使用している場合、デフォルト値を別の記号に変更してください。
scopeDelimiter	スコープの区切り記号。ユーザーやグループ検索でスコープを複数指定する場合に使用する区切り記号です。スコープ名で使用されている記号は使用できません。スコープ名でこの記号を使用している場合、デフォルト値を別の記号に変更してください。
attributeValuesDelimiter	ユーザーやグループの属性名を複数指定する場合に使用する区切り記号です。属性で使用されている記号は使用できないので注意してください。属性名でこの記号を使用している場合、デフォルト値を別の記号に変更してください。

Apache Directory Studio LDAPブラウザーによるLDAPへのログイン

ここでは、Apache Directory Studio LDAPブラウザーを使用してLDAPにログインする方法について説明します。

LDAPサーバーに接続するには、次の手順を実行します。

1. Apache Directory Studio LDAPブラウザーを次のサイトからダウンロードおよびインストールします。
<http://directory.apache.org/studio/>
2. LDAPブラウザーを開き、アプリケーションウィンドウの左下にある [Connections] タブの [New Connection] ボタンを選択します。
3. LDAPホスト名 (ldapHost) とポート番号 (ldapPort) を入力します。
4. 暗号化レベル (enableSSL) を選択します。
5. [Check Network Parameters] ボタンをクリックします。
6. [Next] ボタンをクリックします。
7. 認証方法として、次のいずれかを選択します。
 - [No Authentication]: useAdministrator=false
 - [Simple Authentication]: useAdministrator=true
8. [Finish] ボタンをクリックします (これにより、自動的に接続がテストされます)。