

WYSE TECHNOLOGY INC.

WDMセキュリティガイドライン

ホワイトペーパー

v1.0

2012/12/10

本文書は、Wyseクラウドクライアントおよびゼロクライアントを安全に管理するためのWyse Device Manager (WDM) の設定について詳しく説明します。また、安全な管理のためのWDMおよびWyseシンクライアント端末の設定に関する一般的なガイドラインと具体的な手順を説明します。

目次

1. はじめに.....	2
2. 適用範囲.....	2
3. 参照資料.....	2
4. WDMアーキテクチャ	3
5. セキュリティガイドラインの概要	4
6. 詳細なセキュリティガイドライン	4
6.1. セキュアモード (HTTPS) の有効化	4
6.2. 非セキュアなコンポーネントおよびサービスの無効化.....	4
6.2.1. FTP リポジトリの無効化.....	4
6.2.2. HTTP リポジトリの無効化.....	5
6.2.3. TFTP サーバー/サービス.....	5
6.3. WDMのデフォルトパスワードおよびデフォルト設定の変更.....	5
6.3.1. SQL データベースパスワード.....	5
6.3.2. ソフトウェアリポジトリ.....	5
6.3.3. 通信に使用されるポート.....	5
6.3.4. ファイアウォール設定.....	6
インストール時.....	6
インストール後.....	6
6.4. デフォルトの端末設定の変更.....	9
6.4.1. Write-Filter.....	9
6.4.2. リモートシャドウイング (VNC)	9
6.4.3. BIOSおよびユーザーのパスワード.....	10
6.4.4. ドメイン参加.....	11
6.4.5. PXE イメージング.....	11
6.5. Wyse 端末での最新のファームウェアおよびソフトウェアの使用	11
6.6. Active Directory の統合および委任.....	12
6.7. ネットワークの設定	12
付録A – 項目のチェックリスト	13
付録B – IISでのセキュリティモード (HTTPS) の有効化	14

WDMセキュリティガイドライン

1. はじめに

本文書は、Wyseクラウドクライアントおよびゼロクライアントを安全に管理するためのWyse Device Manager (WDM) の設定について詳しく説明します。また、安全な管理のためのWDMおよびWyseシンクライアント端末の設定に関する一般的なガイドラインと具体的な手順を説明します。ご使用の端末が承認されたWDMサーバーによってのみ管理されるよう、本文書に記述された設定を有効にすることをお勧めします。

2. 適用範囲

本文書のガイドラインおよび推奨事項はWDMバージョン4.9向けのもですが、現在サポートされているWDMの旧バージョンにも適用できます。一部の設定手順は、WDMがインストールされている特定のオペレーティングシステム (OS) に関連しています。本文書では、WDM 4.9をインストールするOSとしてWindows Server 2008 R2を使用します。サポートされるその他すべてのOSにも同様の設定を適用できます。本文書中の「端末」はクラウドクライアント（「シンクライアント」や「ゼロクライアント」とも呼ばれる）を指します。また、「エージェント」はWDMエージェント（「HAgent」とも呼ばれる）を指します。

一般的な推奨事項：

- Wyseサポートサイトから入手可能な最新のWDMバージョン（適用可能なホットフィックスを含む）、OSおよびファームウェアのバージョンおよびHAgentを使用してください。
- WDMの導入前に本文書を最後までお読みください。デフォルト以外のパスワードの使用などのセキュリティ設定の中には、インストール前またはインストール時に設定した方が簡単なものがあります。また、ポートやパスワードにデフォルト以外の設定を選ぶ場合は、インストール時に[Custom]オプションを使用することをお勧めします。

3. 参照資料

本文書に加えて、次の資料を参照できます。

- 資料
 - WDM
 - WDM Installation Guide
 - WDM Administrators Guide
 - Wyse enhanced SUSE Linux INI Reference Guide
 - Wyse enhanced Ubuntu Linux INI Reference Guide
 - ThinOS INI Reference Guide
 - Windows Embedded Administrators Guide
- WDMのコモンクライテリア認証レポート
 - www.commoncriteriaportal.org/files/epfiles/Wyse_CR.pdf
 - www.commoncriteriaportal.org/files/epfiles/Wyse_ST.pdf
 - www.commoncriteriaportal.org/

- Wyseソフトウェアのダウンロード
 - www.wyse.com > [Support] > [Downloads] をクリックして製品を選択してください
 - <https://appservices.wyse.com/pages/serviceandsupport/support/downloads.asp>

4. WDMアーキテクチャ

WDM Enterpriseは、主要コンポーネントを別々のサーバーにインストールすることで、パフォーマンスと拡張性の向上および帯域幅の最適化を図る分散アーキテクチャを提供しています。すべてのコンポーネントを単一のサーバーにインストールすることも可能です。WDM Workgroupでは、すべてのコンポーネントが単一のサーバーにインストールされます。Workgroup機能とEnterprise機能の比較についての詳細は、<http://www.wyse.com/products/software/management/WDM>を参照してください。

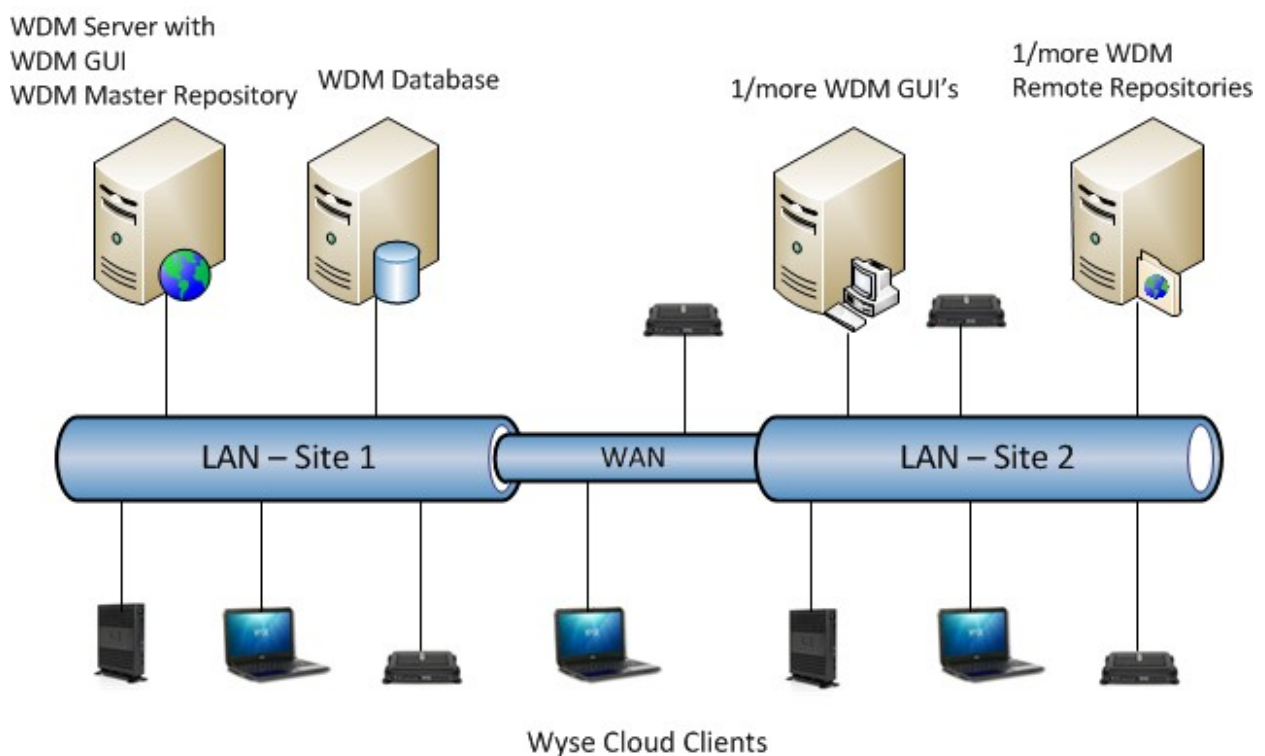


図 1: WDM Enterprise アーキテクチャ

5. セキュリティガイドラインの概要

ご使用のWyse端末を安全に管理するためのセキュリティガイドラインは以下の通りです。

1. セキュアモード (HTTPS) の有効化
2. 非セキュアなコンポーネントおよびサービスの無効化
3. WDMのデフォルトパスワードおよびデフォルト設定の変更
4. デフォルトの端末設定の変更
5. Wyse端末上での最新のファームウェアおよびソフトウェアの使用
6. Active Directoryの統合および委任の使用
7. ネットワークの設定

6. 詳細なセキュリティガイドライン

本セクションでは、WDMのセキュリティ機能と、前セクションに挙げた各項目の詳細な設定手順を説明します。

6.1. セキュアモード (HTTPS) の有効化

WDMはシンクライアント端末管理にあたり、「非セキュア (HTTP)」と「セキュア (HTTPS)」という2つのプロトコルを使用できます。WDMのインストール時のデフォルトは非セキュアモード (HTTP) を使用するようになっていますが、インストール後にHTTPSを有効にすることも可能です。本セクションでは、HTTPSを使用するためのWDM、IIS およびエージェントの設定手順を説明します。

セキュアモード (HTTPS) を設定するための手順

1. HTTPSを使用するようにIISを設定します
詳細な手順は「付録B - IISでのセキュアモード (HTTPS) の有効化」を参照してください。
2. WDMでHTTPSおよびCA認証を有効にします
 - a) [WyseDeviceManager] GUI を開きます
 - b) [Configuration Manager] > [Software Repositories]を選択し、リポジトリをダブルクリックします
 - c) [Secure (HTTPS)]を有効にします
 - d) [CA Validation]を有効にします
3. 証明書を端末にインポートします
ルート証明書/CA認証局のパブリック証明書を端末にインポートする方法については、「WDM Administrators Guide」を参照してください。WTOS、SUSE LinuxおよびUbuntu Linux OSを搭載した端末については、INIファイルを通じて証明書をインポートする別の方法があります。

6.2. 非セキュアなコンポーネントおよびサービスの無効化

安全な管理環境を維持するには、次のサービスおよび機能を無効にする必要があります。

6.2.1. FTPリポジトリの無効化¹

- a) [WyseDeviceManager] GUIを開きます

¹ PCoIP端末 (Pクラス) は、FTPを使ったファームウェアパッケージの配信のみをサポートしています。FTPリポジトリを無効にすると、ファームウェアパッケージの配信によるアップデートができなくなります。

- b) [Configuration Manager] > [Software Repositories] を選択し、リポジトリをダブルクリックします
- c) [Transfer Type] ドロップダウンを[HTTP]に設定します

6.2.2. HTTPリポジトリの無効化

「付録B – IISでのセキュアモード (HTTPS) の有効化」の手順を実行してHTTPSを有効にしてから、次の手順を実行してIISでHTTP通信を無効にします。

- a) [スタート]をクリックし、[プログラムとファイルの検索]テキストボックスに「inetmgr」と入力して[インターネットインフォメーションサービス(IIS)マネージャー]を開きます
- b) [サイト] > [Rapport HTTP Server] > [Rapport HTTP Server] を選択し、右端のペインの[バインド...]をクリックして[サイトバインド]ページを開きます
- c) [サイトバインド]ページで、httpの行をクリックします
- d) [削除]および[閉じる]をクリックします

6.2.3. TFTPサーバー/サービス

WDMサーバーで以下を実行します。

- a) [スタート] > [すべてのプログラム] > [管理ツール] > [サービス]を押します
- b) [WDM TFTP]を見つけます
- c) ダブルクリックして[停止]を選択します
- d) [スタートアップの種類]を[無効]に設定します
- e) [OK]を押します

6.3. WDMのデフォルトパスワードおよびデフォルト設定の変更

WDMのインストール時、インストーラは、WDMで使用する多くのコンポーネントにデフォルトのパスワードと設定を選択します。インストール後にデフォルト以外の値を設定できるものもありますが、インストール時に設定しなければならないものもあります。

WDMインストーラで使用するデフォルト設定は次の通りです。

6.3.1. SQLデータベースパスワード

WDMは、「sa」ユーザーの特権で「rapportdb」というSQL Serverインスタンスを使用します。デフォルト以外のパスワードを指定する方法については、以下の「インストール時」セクションを参照してください。

6.3.2. ソフトウェアリポジトリ

WDM は、FTP、HTTPまたはHTTPSベースのソフトウェアリポジトリ（パスワード（WDMのマスターソフトウェアリポジトリと、1つ以上のリモートソフトウェアリポジトリ））の使用をサポートしています。デフォルト以外のパスワードを設定する方法については、以下の「インストール時」および「インストール後」を参照してください。

6.3.3. 通信に使用されるポート

WDMは、WDMコンポーネントおよびHAgentとの通信にさまざまなポートを使用します。これらのポートのリストは「Installation Guide」を参照してください。次のコンポーネントには、標準以外（デフォルト以外）のポートを使用することをお勧めします。

- WDM SQLデータベース：SQL Serverが使用するデフォルトのTCPポート1433
- WDM HTTPおよびHTTPSポート

6.3.4. ファイアウォール設定

WDMでは、WDMコンポーネントがインストールされたコンピュータのファイアウォール規則から特定のポートを除外する必要があります。使用するサービスおよび機能のみを有効にしてください（例外を追加してください）。

例えば、P20などのPCoIP端末がない場合は、ThreadX Manager Serviceが使用するTCPポート9880および50,000の例外を追加する必要はありません。

本セクションの以降の部分では、WDMのインストール時またはインストール後にデフォルト設定を変更するために使用できる具体的な手順を説明します。

インストール時

a. データベース設定

SQL Serverデータベースでデフォルト以外の設定をする場合は、インストール後よりもインストール時に行う方が簡単です。

○ SQL Serverパスワード

WDMインストーラは、ユーザー「sa」のために組み込みデータベース（インスタンス名：RAPPORTDB）としてMicrosoft SQL Expressを含んでいます。インストールを[Typical]で実行すると、デフォルトパスワードが使用されます。[Custom]インストールでも、このパスワードを選択できます。また[Custom]インストールでは、組み込みデータベースではなく、既存の（WDMの旧バージョンにインストールされた）データベースや別のデータベース（SQL Serverのフルバージョンなど）を使用できます。

○ SQL Server通信ポート

WDMは、SQL Serverデータベースとの通信に、デフォルトのTCPポート1433を使用します。このポートは、[Custom]インストールを選択して設定できます。

b. ソフトウェアリポジトリパスワード

WDMエージェントは、[rapport]というユーザー名を使用して、WDMリポジトリに接続します。[rapport]ユーザーのパスワードはデフォルト以外に変更することをお勧めします。[Typical]でインストールを実行するとデフォルトパスワードが使用されます。[Custom]インストール時にもこのパスワードを選ぶことができます。

c. ファイアウォール設定

WDM 4.9以降、管理者がインストール時にPrerequisitesユーティリティを使用して、デフォルトのファイアウォールポートを設定できるようになりました。デフォルト以外のポートを設定したい場合や、WDMの旧バージョンを使用している場合は、このユーティリティのFirewall Settingsコンポーネントを実行せず、例外ファイアウォールを手動で設定することをお勧めします。

インストール後

● 通信に使用するポート

WDMが使用するポートは、次のように設定できます。

■ IIS

WDMは、端末との通信にインターネットインフォメーションサービス（IIS）のWebサーバーを使用します。WDMがインストールされたサーバーのIIS設定で、次の変更を行う必要があります。

- WebサーバーHTTP（非セキュア）ポート：デフォルトのTCPポート80
- WebサーバーHTTPS（セキュア）ポート：デフォルトのTCPポート443

1. [スタート]をクリックし、[プログラムとファイルの検索]テキストボックスに「inetmgr」と入力してIISマネージャーを開きます
2. [サイト] > [Rapport HTTP Server] > [Rapport HTTP Server]を選択し、右端のペインにある[バインド...]をクリックして[サイトバインド]ページを開きます
3. [サイトバインド]ページで、httpまたはhttpsの行をクリックします
4. [編集]をクリックして、[ポート]に新しい値を指定します
5. [OK]をクリックしてから、[閉じる]をクリックします
6. 設定を有効にするためにIISサーバーを再起動します
 - IISマネージャーの[Rapport HTTP Server]ページに移動します
 - 右側パネルの[Webサイトの管理]で[再起動]をクリックします

注：変更後にWDMの [Preferences]ダイアログを開き、WDMで新しい設定が反映されているかどうか確認してください。

- **ソフトウェアリポジトリパスワード**

1. WDMがインストールされたWindowsサーバーで[コントロール パネル]を開きます
2. [ユーザーアカウント]に移動します
3. ユーザー[rapport]のパスワードを変更します
4. [WyseDeviceManager] GUIを開きます
5. [Configuration Manager] > [Software Repositories] を選択します
6. リポジトリをダブルクリックし、[HTTP]セクションの[Password]テキストボックスと[Verification]テキストボックスに、rapportユーザーの変更後の新しいパスワードを入力します

- **SQL Server通信ポート**

SQLポートを変更する（デフォルトの1433以外にする）には、次の手順を実行します。

- データベースサーバー
 1. [スタート]を押して、[Microsoft SQL Server] > [Configuration Tools]を選択します
 2. [SQL Server Configuration Manager]を開きます
 3. [SQL Server ネットワーク構成] > [RAPPORTDBのプロトコル]を選択します
 4. 右側ペインで[TCP/IP]をダブルクリックします
 5. [IP アドレス]タブで、データベースマシンに対応するIPアドレスの[TCP ポート]値を設定します
 6. WDMマシンを再起動します
- 管理GUIおよびソフトウェアリポジトリを含むWDMコンポーネントを実行するすべてのコンピュータ（分散インストールの場合）
 1. [レジストリーエディター]を開きます（[スタート] > [プログラムとファイルの検索]フィールドに「regedit」と入力）
 2. [Software] > [Wow6432Node] > [Rapport] > [Database] ノ

ードを選択します

3. [DBPort]の値をSQL Serverの設定と同じ値に設定します
4. [WyseDeviceManager] GUIを再起動します

■ **WDM Preferences :**

- [WyseDeviceManager] GUIを開きます
- [Configuration Manager] > [Preferences]を選択します
- [Service Preferences]をダブルクリックし、[Serv/Port Settings]を選択します

6.4. デフォルトの端末設定の変更

シンクライアント端末上で端末設定を安全に管理するには、攻撃の脆弱性を軽減する設定も必要です。本セクションでは、管理の必要があるさまざまな設定の概要を示します。設定方法の一部については特に詳しく説明します。詳細（リモート送信可能なINI設定など）については、各プラットフォームの管理者ガイドを参照してください。内容は以下の通りです。

1. Write-Filter
2. リモートシャドウイング (VNC)
3. BIOSおよびユーザーのパスワード
4. ドメイン参加
5. PXEイメージング

6.4.1. Write-Filter

WyseのWindows Embedded製品には「File Based Write Filter (FBWF)」という保護機構が組み込まれており、デフォルトで有効になっています。Write-Filterが有効になっている場合（システムトレイの緑のボタンがオンの状態）、端末に対して行われた変更は再起動後は保持されず失われます。Write-Filterを有効または無効にできるのは管理者だけです。

Write-Filterを有効にしておくことをお勧めします。WDMは、Windows Embedded端末に対するアップデートの実行時に、Write-Filterをリモートから自動的に有効／無効にします。

6.4.2. リモートシャドウイング (VNC)

Wyse端末（P20を除く）には、WDM管理者がユーザー端末の画面状態をWDM管理GUIから表示できるリモートシャドウイング用のVNCサーバーが組み込まれています。これにより、管理者およびデスクユーザーは、端末ユーザーのいる場所やデスクまで出向くことなく、実質的な技術サポートを提供できるようになります。

VCNクライアントはWDMサーバー上にあります。リモートシャドウ機能はVCNプロトコルを使用します。デフォルトでリモートシャドウセッションが確立されると、WDM管理者はセッションを開始するためにパスワードを入力する必要があり、端末ユーザーに通知が行われます。端末ユーザーはリモートシャドウの要求を拒否することができます。リモートシャドウセッションが確立されると、ユーザーの承認後あるいはタイムアウト後に、システムトレイのアイコンがアクティブセッションでの端末ユーザー情報を提供します。

以下は、リモートシャドウをより安全にするためのオプションです。

- 端末からVNCクライアントを削除する (WESおよびLinux端末の場合)
- VNCクライアントを無効にし、デバッグ時のみ明示的に有効にする
- リモートシャドウイングのため、VNCが使用するデフォルトパスワードを変更する
- デフォルトのVNCクライアント (WDM内) およびVNCサーバー (端末上) を安全性の高いサードパーティ製バージョンに置き換えることで、暗号化とログインを可能にする
- リモートシャドウの要求を受信した時点で、VNCサーバー (端末上) のデフォルト動作を設定する
- 既知のソースまたは承認されたソース (WDMサーバーなど) からの接続のみを受け入れるよう、VNCサーバー (端末上) を設定する

6.4.3. BIOSおよびユーザーのパスワード

Wyse端末は、ローカルユーザーおよびローカル管理者に対してパスワードを使用します。無許可ユーザーが端末を使用したり、特権レベルを引き上げて悪用したりすることがないように、これらの値を変更する必要があります。

個々の端末上でこれらの設定を行うための手順については、プラットフォーム/OSに固有の管理者ガイドを参照してください。また、これらの設定を特定の1台の端末に対し設定し、Wyse USB Firmware Toolを使用してOSまたはファームウェアを吸い上げて(コピー/プルして)から、WDMを通じてすべての端末に適用することもできます。

変更する必要がある設定およびパスワードを以下に示します。

1. BIOS設定

WTOS、Windows Embedded、またはWyse enhanced SUSE Linuxオペレーティングシステムを搭載した端末が該当します。これらのオペレーティングシステムを搭載した製品は、BIOS設定 (ブートデバイス、ブートオーダー設定を含む) を保護するローカルBIOSパスワードを持っています。

レベル	Windows Embedded	Wyse enhanced SUSE Linux	Wyse enhanced Ubuntu Linux (ARMベースの T50)	WTOS (ARMベースの T10 ² を除く)
端末ごと (端末での直接操作)	ブート時に[Del] キーを押してBIOSメニューを表示する	ブート時に[Del] キーを押してBIOSメニューを表示する	ブート時に電源ボタンと[Del] キー ³ を押す	ブート時に電源ボタンと[Del] キー ³ を押す
WDM経由	変更済みのOSとBIOSを、WDMを通じて配信する	変更済みのOS、BIOSおよびINI設定を、WDMを通じて配信する	変更済みのOS、BIOSおよびINI設定を、WDMを通じて配信する	変更済みのOS、BIOSおよびINI設定を、WDMを通じて配信する

表1 : Wyse端末上のBIOSまたはブートメニューのオプション

² ARMベースのWTOSプラットフォーム (T10) には、ローカルブートまたはBIOSオプションがありません。すべての関連する設定は、リモート配信されるINIファイルでのみ設定できます。

³ ブート時に2つのオプションがあります。電源ボタン+[P]キーを押すとブートオーダーを選択でき、電源ボタン+ [Del] キーを押すとBIOSメニューへ入るためのパスワード入力ダイアログが表示されます。

各プラットフォームにはプラットフォーム固有の設定があり、以下が制御可能です。

- BIOSパスワード
 - ブート順序
 - USBメモリからブート
2. ローカルユーザーおよび管理ユーザーのパスワード
これは、WTOSおよびPCoIP端末（P20など）を含むすべてのWyse端末が該当します。

オペレーティングシステム/ プラットフォーム	ローカルユーザー	ローカル管理者
Windows Embedded	User	Administrator
Wyse enhanced SUSE Linux	Thinuser	Admin
Wyse enhanced Ubuntu	Thinuser guest	Admin
Linux	<なし>	Admin ⁴
WTOS	<なし>	<admin パスワードを設定可能>
PCoIP (P20)	<なし>	<admin パスワードを設定可能>

表2：Wyse端末上のユーザーおよび管理者のアカウント

6.4.4. ドメイン参加

Windows Embedded端末は、会社のActive Directory（AD）ドメインに参加することもでき、端末ユーザーがADベースの認証情報を使用してログインするように構成できます。これによりセキュリティの階層が追加され、通常のADベースのツールによるモニタリングが可能になります。

6.4.5. PXEイメージング

x86ベースのプラットフォーム上で実行されているWyse端末のイメージは、PXEプロトコルを使用して吸い上げることができます。WDMには、PXEベースのイメージングを提供するためのTFTPサーバーが組み込まれています。WDMは、PXE以外またはその他の方法によるOS/ファームウェアのアップデート（INIベース）をサポートしています。

PXEイメージングの必要がない場合は、端末からのPXE要求に応答するWDMサーバー上のTFTPサービスを無効にすることもお勧めします。端末上のBIOS設定のブートオーダーでPXEの優先度を低く設定するか、またはPXEサポートを無効にすることをお勧めします。これは通常、端末のキッティング時に変更する必要があります。

6.5. Wyse端末での最新のファームウェアおよびソフトウェアの使用

Wyse製品部門は、端末上で実行されるソフトウェアを定期的にアップデートします。これらのソフトウェアアップデートは、Webサイトの[Support] > [Downloads]セクションで公開されています。アップデートには、以下のカテゴリがあります。

- WDMエージェント（HAgent）
- OSまたはファームウェアのアップデート
- サードパーティコンポーネント（Citrix Receiver、VMware View Clientなど）のソフトウェアアップデート

⁴ WDMが配布するINI設定ファイルを通じて設定できます。

6.6. Active Directoryの統合および委任

WDM（およびそのコンポーネント）がインストールされているコンピュータへのアクセスについては、通常のWindows認証情報を通じて管理することをお勧めします。WDM管理GUIへのアクセスは必要に応じて提供し、WDMコンピュータへのアクセスを許可されたユーザーごとに、WDM管理GUIのための特権を割り当てる必要があります。

WDMは、Active Directoryドメインにすでに参加しているコンピュータにインストールすることができます。追加の管理者については、WDM管理GUIのみをインストールしたコンピュータにアクセスを限定する必要があります。

Active Directoryおよび委任の設定は、以下のように管理できます。

- [WyseDeviceManager] GUIを開きます
- [Configuration Manager] > [User Permissions] ノード（左側ペイン）を選択します
- 右クリックして[新規作成] > [User/Group]を選択します
- ローカルマシンのドメインまたはADドメインからユーザーを追加します
- 端末を管理するための以下のような特権を割り当てます
 - 端末固有：リモートシャドウ、リアルタイム（再起動、シャットダウン）、削除
 - パッケージ（OS／ファームウェア、ソフトウェア、設定）の作成、編集、登録および実装
 - レポートの作成および表示
 - ビューの作成、変更

6.7. ネットワークの設定

本セクションでは、WDMおよびWyse端末が使用しているネットワークが、コンピューティング環境全般の共通セキュリティガイドラインに従っていることを確認するための一般的なガイドラインを説明します。

- DNSおよびDHCPサーバー
Wyse端末は、DNSおよびDHCPベースのディスカバリ方式を使用して、WDMに自動チェックインによる登録を実行します。DNSおよびDHCPサーバーに権限のないユーザーがアクセスすることによって端末が無許可で管理されないよう、これらのサーバーへのアクセスを制限することをお勧めします。自動ディスカバリに必要なDNSおよびDHCPサーバー設定の詳細は「WDM Administrator's Guide」を参照してください。
- PXEトラフィック
Wyse製品でのPXEプロトコルの使用についての詳細は「PXEイメージング」セクション（セクション6.4）を参照してください。ネットワークにおけるPXEトラフィックを制限／ブロックすることをお勧めします。
- パスワードポリシー
一般的なコンピュータシステムで堅牢なパスワードを設定するために利用されているパスワードの複雑性のガイドラインに従ってください。

付録A – 項目のチェックリスト

本セクションでは、本文書で説明されている設定のリストを示します。

1. はじめに.....	2
2. 適用範囲.....	2
3. 参照資料.....	2
4. WDMアーキテクチャ	3
5. セキュリティガイドラインの概要	4
6. 詳細なセキュリティガイドライン	4
6.1. セキュアモード (HTTPS) の有効化	4
6.2. 非セキュアなコンポーネントおよびサービスの無効化.....	4
6.2.1. FTPリポジトリの無効化.....	4
6.2.2. HTTPリポジトリの無効化.....	5
6.2.3. TFTPサーバー/サービス.....	5
6.3. WDMのデフォルトパスワードおよびデフォルト設定の変更.....	5
6.3.1. SQLデータベースパスワード.....	5
6.3.2. ソフトウェアリポジトリ.....	5
6.3.3. 通信に使用されるポート.....	5
6.3.4. ファイアウォール設定.....	6
インストール時.....	6
インストール後.....	6
6.4. デフォルトの端末設定の変更.....	9
6.4.1. Write-Filter.....	9
6.4.2. リモートシャドウイング (VNC)	9
6.4.3. BIOSおよびユーザーのパスワード.....	10
6.4.4. ドメイン参加.....	11
6.4.5. PXEイメージング.....	11
6.5. Wyse端末での最新のファームウェアおよびソフトウェアの使用.....	11
6.6. Active Directoryの統合および委任.....	12
6.7. ネットワークの設定	12
付録A – 項目のチェックリスト	13
付録B – IISでのセキュリティモード (HTTPS) の有効化	14

付録B – IISでのセキュリティモード (HTTPS) の有効化

HTTPSまたはルート証明書を使用したセキュアな通信の設定

SSLを使用したセキュアな通信の設定

IIS 6.0およびIIS 7（および7.5）でSSLを有効にする方法は複数あります。IIS 6.0でSSLを設定するには、以下のガイドラインを使用してください。

Windows Server 2003上のIIS 6.0でのSSLの設定

以下のガイドラインを使用してください。

リンク [IIS 6.0 Resource Kit Tools](#) から **IIS 6.0 Resource Kit Tools** をダウンロードします。

1. IIS 6.0 Resource Kit Toolsをインストールします。
2. コマンド プロンプトに移動し、ディレクトリをバイナリ **selfssl.exe** の場所（「c:\Program Files\IIS Resources\SelfSSL」など）に変更します。
3. 以下のパラメータを指定して、**selfssl**ユーティリティを実行します。
4. **selfssl /N:cn=certificate_name /S:site_id**（例えば、**selfssl /N:cn=MyComputer.Sample.com /S:1**。サイトIDが1の場合、cnはコンピュータのFQDN名とIPアドレスを組み合わせたものになります）
5. 次に、以下のようにして**SSLを設定**します。
 - コマンド プロンプトに移動して、ディレクトリを**adsutil.vbs**ファイルの場所（例えば「c:\Inetpub\AdminScripts」）に変更します。
 - 以下のようにして、コマンドプロンプトから**adsutil.vbs**を実行します。
 - **cscript.exe adsutil.vbs set /w3svc/site_id/SecureBindings ":443**（例えば、サイトIDが1の場合、**cscript.exe adsutil.vbs set /w3svc/1/SecureBindings ":443**）。

Windows Server 2008 R2上のIIS 7でのSSLの設定

以下のガイドラインを使用してください。

リンク [SelfSSL.exe](#) から **SelfSSL7**ユーティリティをダウンロードします。

1. 以下のパラメータを指定して、**SelfSSL7.exe**ユーティリティを呼び出します。
2. **SelfSSL7.exe /Q /N cn=Certificate_Name /I /S Web_Site_Name**。例えば、**SelfSSL7.exe /Q /N cn="TestCert.TestLab.com" /I /S "Default Web Site"**

ルート証明書を使用したセキュアな通信の設定

Windows Server 2008 R2上のIIS 7へのルート証明書のインストール

以下のガイドラインを使用してください。

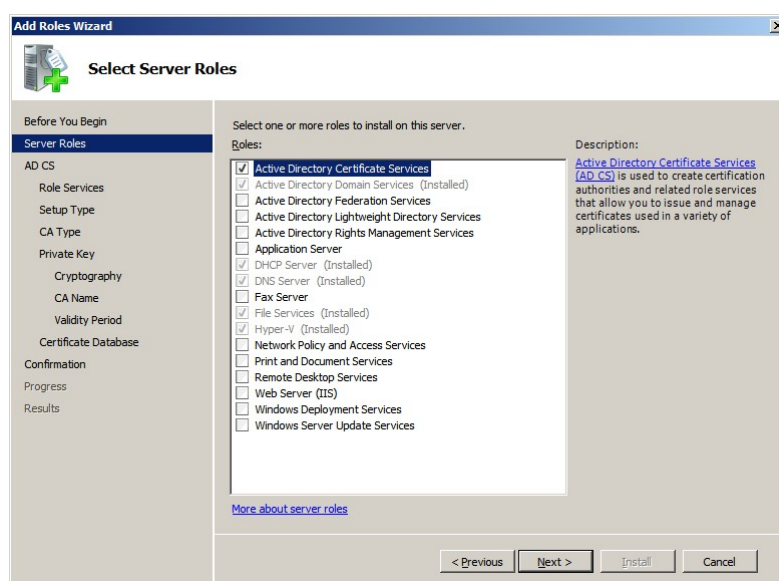
証明書をインストールするには、以下の2つの手順を実行する必要があります。

- ドメインコントローラサーバーに証明書をインストールする
- WDMサーバーに証明書をインストールする

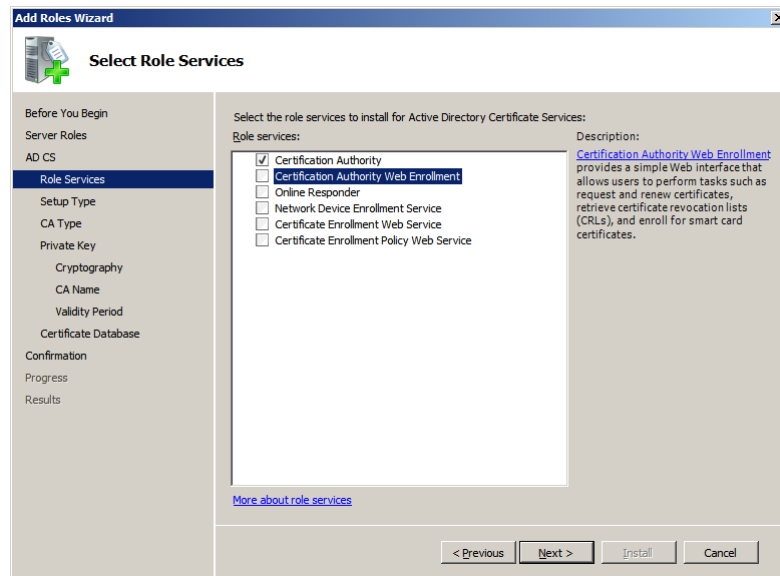
ドメインコントローラサーバーへの証明書のインストール：

以下のガイドラインを使用してください。

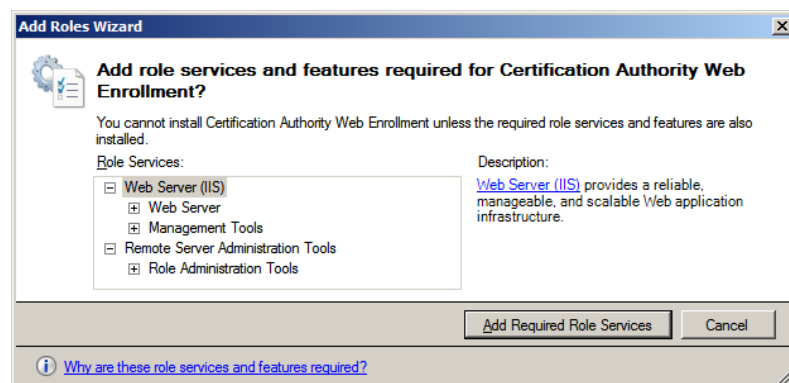
1. [サーバーマネージャー]を起動します。
2. ツリーペインで[役割]を選択し、[役割の追加]を選択します。
3. [役割の追加ウィザード]で、ツリーペインから[サーバーの役割]を選択します。
4. [サーバーの役割]ページで、[役割]リストから[Active Directory証明書サービス]を選択します。



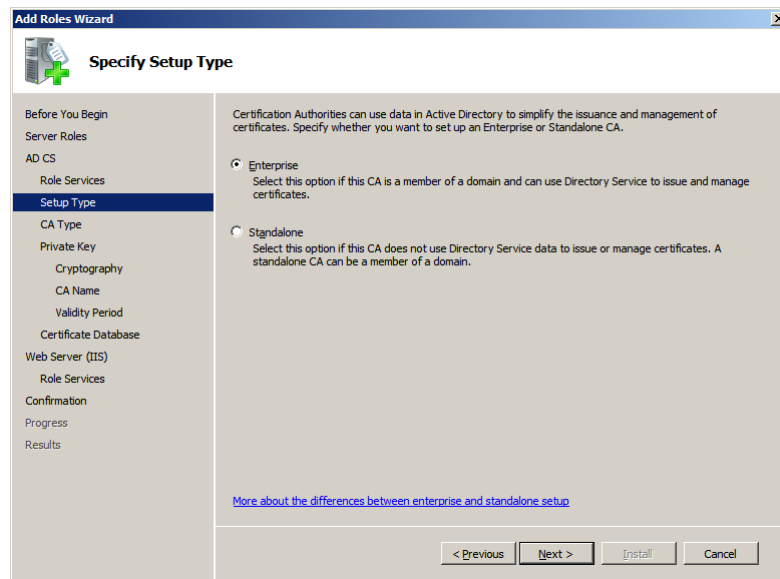
5. [次へ]->[次へ]をクリックします。次に、[役割サービス]リストで[認証機関]および[認証機関Web登録]にチェックを入れます。



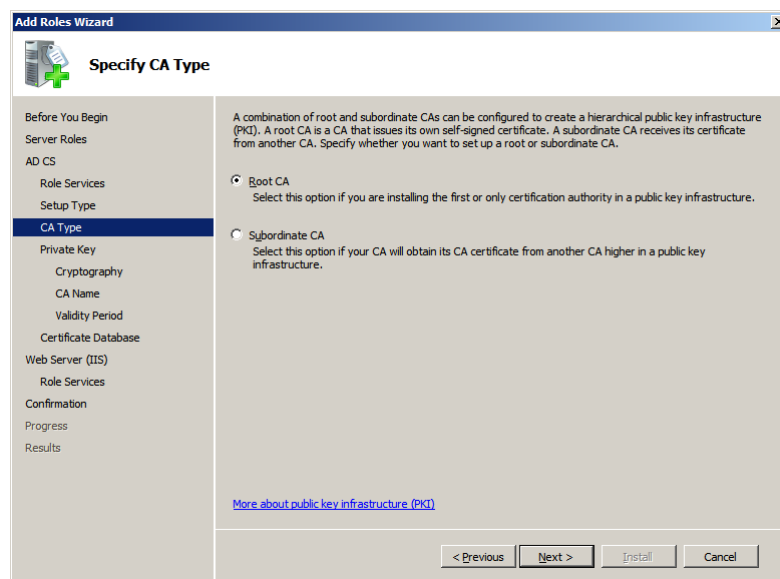
6. IISがサーバーにインストールされていない場合は、[認証機関Web登録]にチェックを入れた後、別ページで[役割の追加ウィザード]が表示されます。



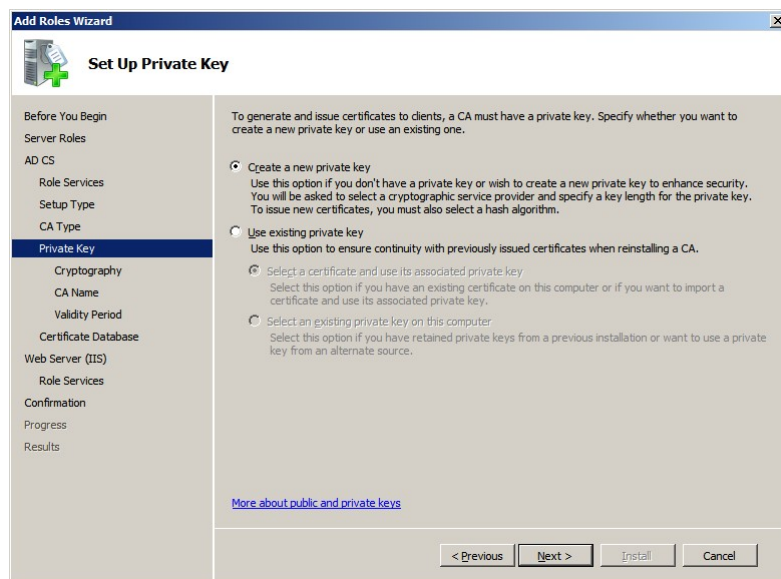
7. 上記ページで、[必要な役割サービスを追加]ボタンをクリックし、[次へ]をクリックして[セットアップの種類の指定]ページを開きます。



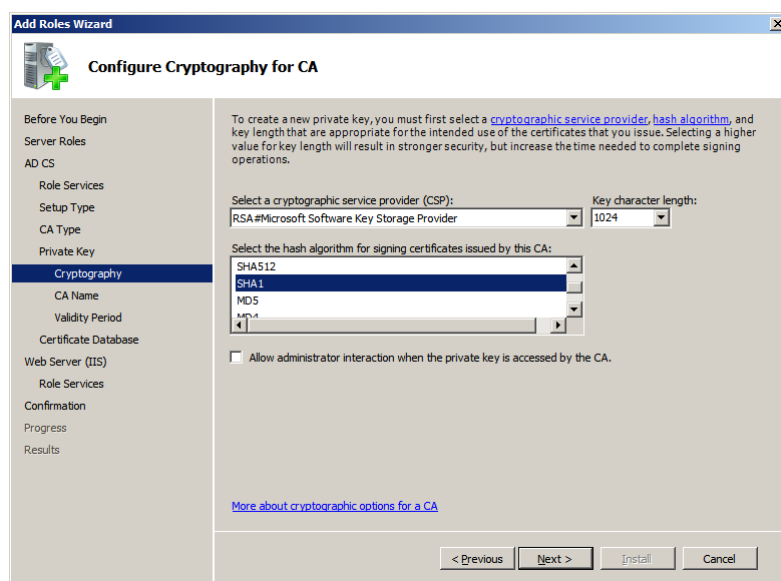
8. 上記ウィンドウで、必要に応じて[エンタープライズ]または[スタンドアロン]を選択し、[次へ]をクリックして[CA の種類の設定]ページを開きます。




9. [CA の種類の設定]ページで、必要に応じて[ルート CA]または[下位CA]を選択し、[次へ]をクリックして[秘密キーの設定]ページを開きます。



10. [秘密キーの設定]ページで、必要に応じて[新しい秘密キーを作成する]または[既存の秘密キーを使用する]を選択し、[次へ]をクリックして[CAの暗号化を構成]ページを開きます。

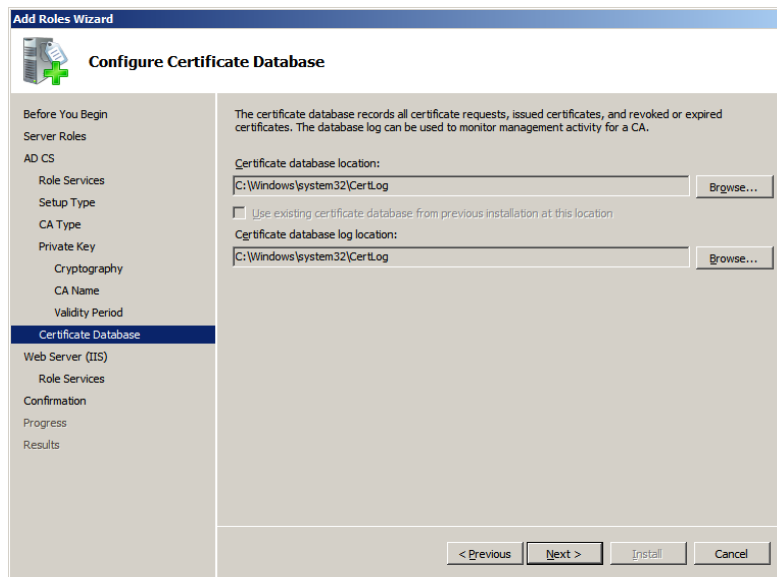


11. [CAの暗号化を構成]ページで、必要に応じて[暗号化サービスプロバイダー（CSP）を選択]フィールドの値を選択し、[キーの長さ]を指定し、[このCAから発行された証明書の署名に使用するハッシュアルゴリズムを選択]フィールドの値を選択し、[CAが秘密キーにアクセスするときに、管理者による操作を許可する]のチェックを選択または選択解除し、[次へ]ボタンをクリックして[CA名を構成]ページを開きます。

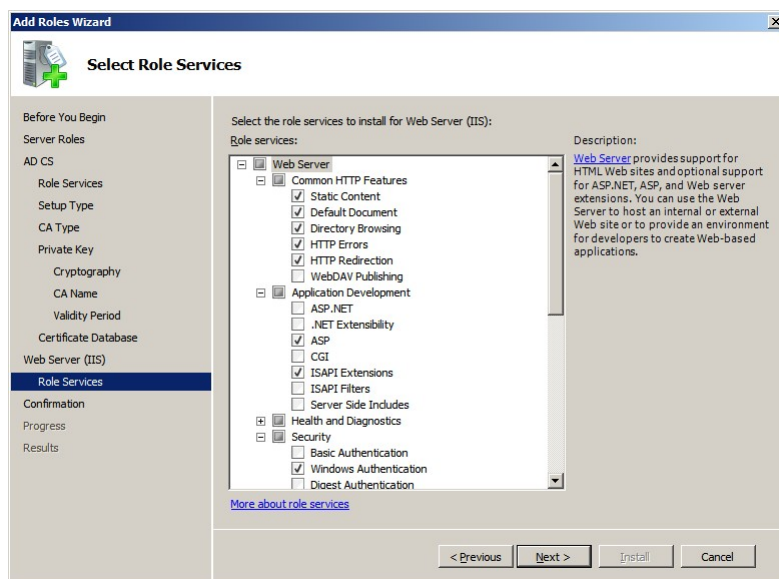
 注：証明書の共通名は、WDMサーバーのコンピュータ名と一致している必要があります。

12. [CA名を構成]ページで[このCAの共通名]および[識別名のサフィックス]フィールドの値を指定し、[次へ]をクリックして[有効期間の設定]ページを開きます。

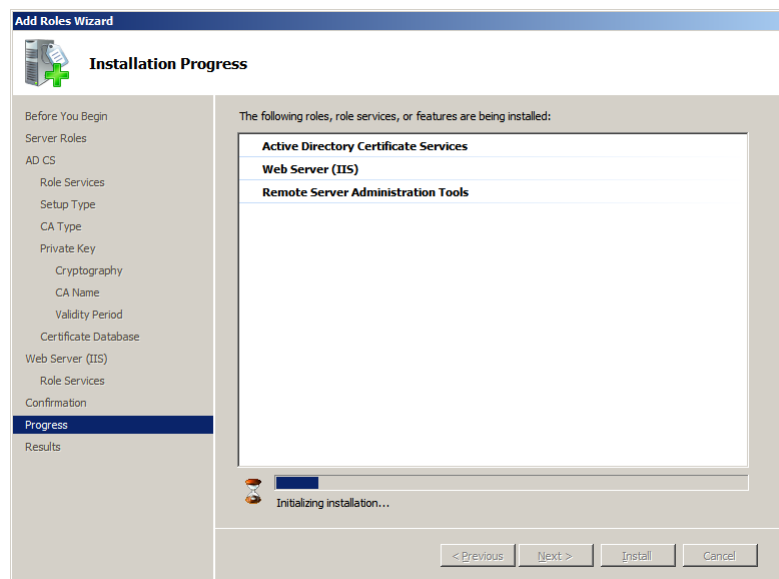
13. [有効期間の設定]ページで、このCAから生成される証明書の有効期間を選択し、[次へ]をクリックして[証明書データベースを構成]ページを開きます。



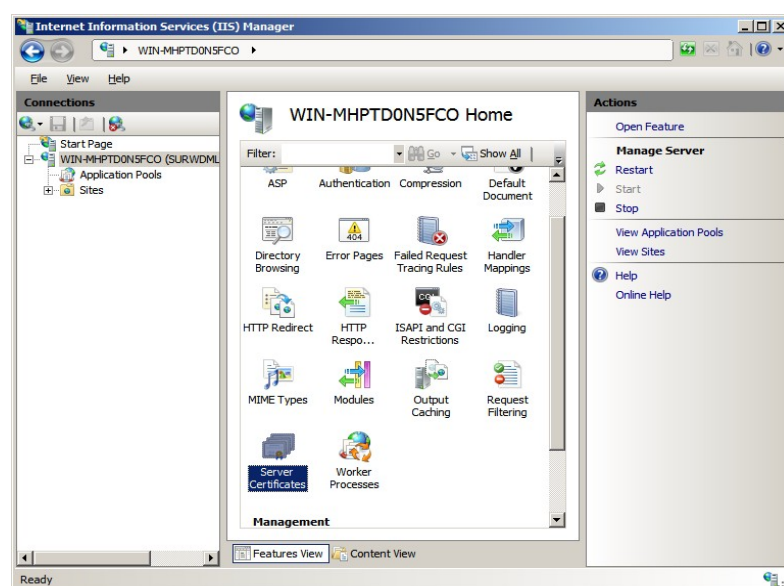
14. [証明書データベースを構成]ページで、[証明書データベースの場所]と[証明書データベースログの場所]を選択し、[次へ]をクリックして[Webサーバー(IIS)]の役割追加ページを開きます。



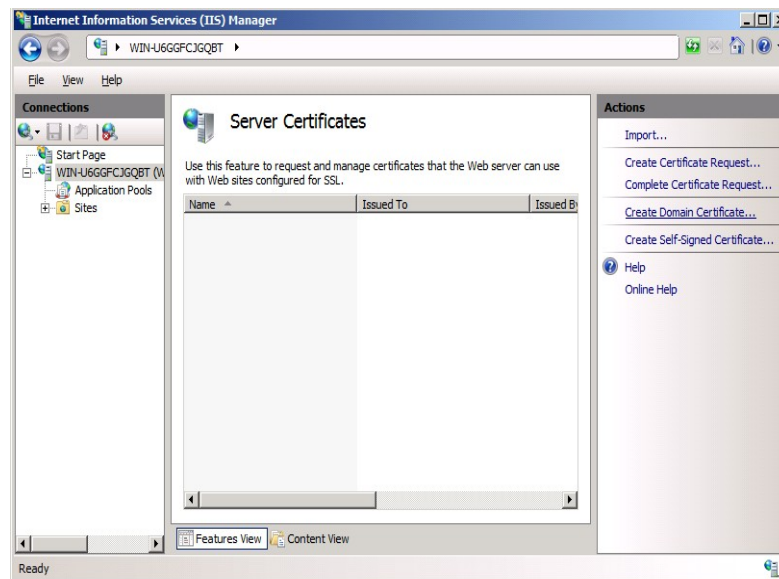
15. デフォルト値を受け入れ、[次へ] > [インストール]をクリックします。
16. これで、Active Directory証明書サービス、Webサーバー (IIS) および認証機関Web登録がインストールされます。



17. 証明書サービス(証明機関)をインストールしたら、ドメインコントローラの[インターネットインフォメーションサービス(IIS)マネージャー]を起動します。
18. [サーバermanage]のツリーペインで[役割]を展開し、[Webサーバー (IIS)]->[インターネットインフォメーションサービス (IIS) マネージャー]をクリックして[インターネットインフォメーション(IIS)マネージャー]ページを開きます。

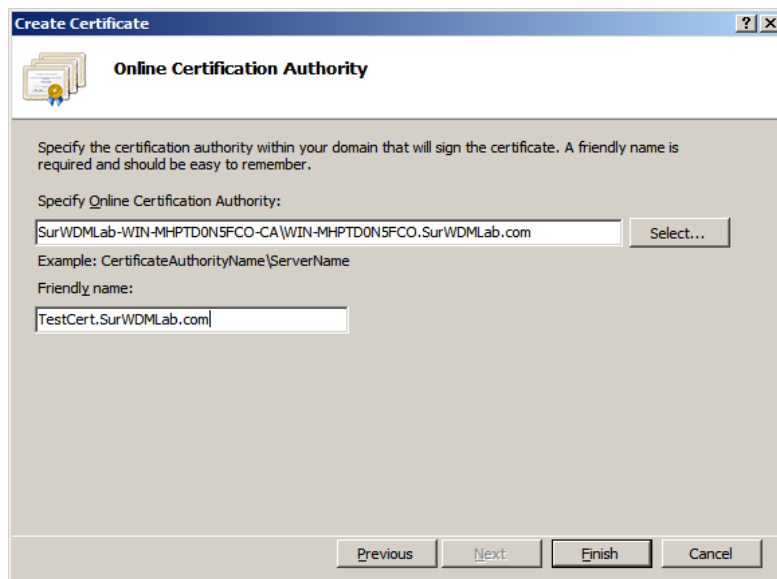


19. ツリーペインでサーバー名ノードを選択し、中央ペインで[サーバー証明書]アイコンをダブルクリックします。



20. [サーバー証明書]ページの右側ペインで、[ドメイン証明書の作成...]をクリックして証明書の作成を開始します。

21. [証明書の作成]ページで必要な情報を入力し、[次へ]をクリックして[オンライン証明機関]ページを開きます。

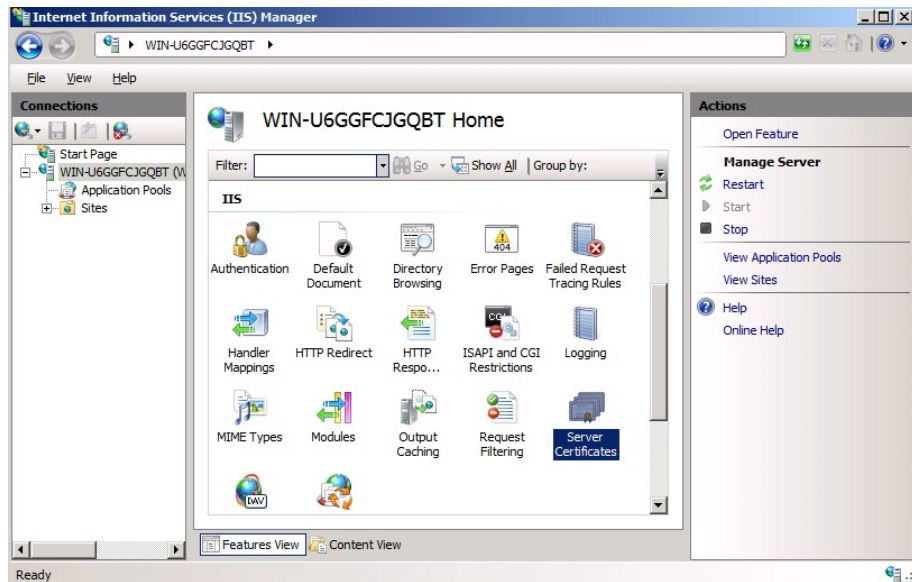


22. [オンライン証明機関]ページで、[選択...]を選択して[オンライン証明機関の指定]を設定し、さらに[フレンドリ名]を指定して[終了]をクリックします。
23. これで、ドメインコントローラサーバーでの証明書のインストールが完了しました。次はWDMサーバーへの証明書のインストールに進みます。

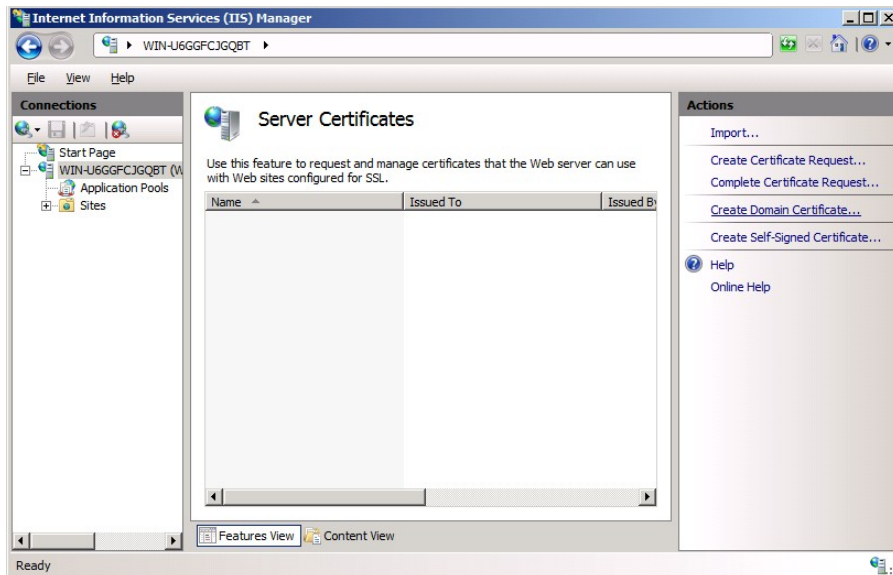
WDMサーバーへの証明書のインストール：

以下のガイドラインを使用してください。

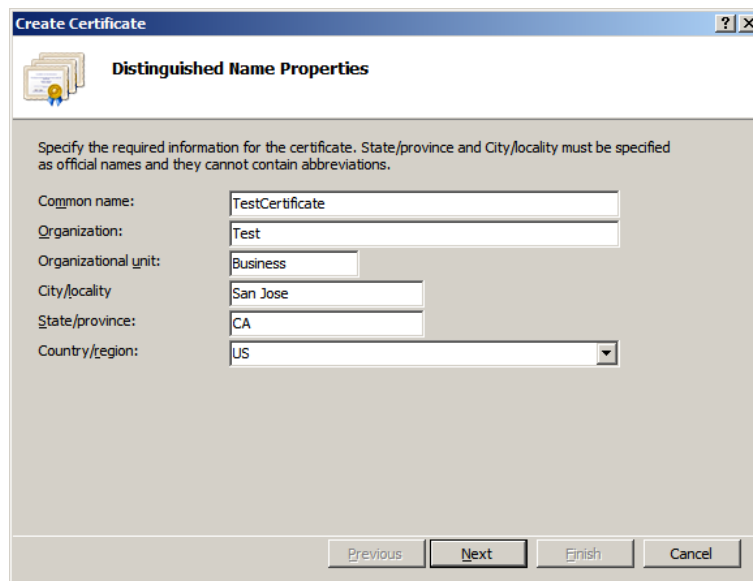
1. タスクバーで[スタート] > [管理ツール] > [インターネットインフォメーションサービス (IIS) マネージャー]をクリックし、[インターネットインフォメーションサービス(IIS)マネージャー]ページを開きます。



2. ツリーペインでサーバー名ノードをクリックし、中央ペインで[サーバー証明書]アイコンをダブルクリックして[サーバー証明書]ページを開きます。



3. [サーバー証明書]ページの右側ペインで[ドメイン証明書の作成...]をクリックし、証明書の作成を開始します。



Create 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: TestCertificate

Organization: Test

Organizational unit: Business

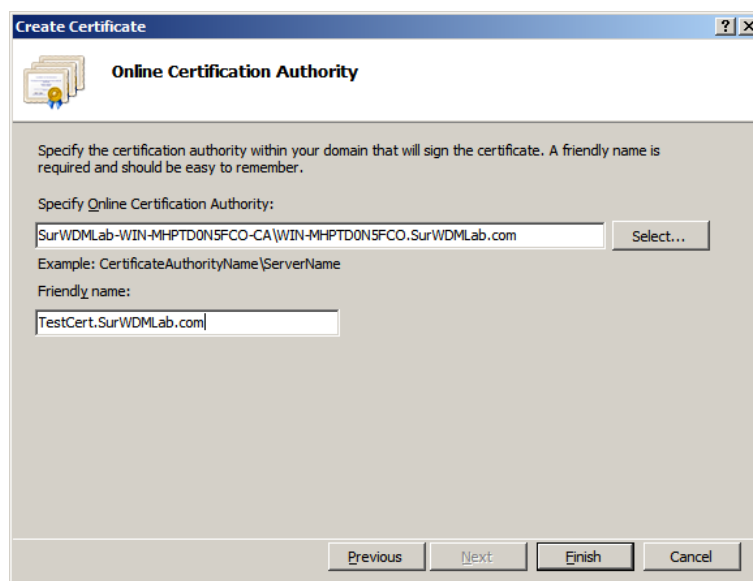
City/locality: San Jose

State/province: CA

Country/region: US

Previous Next Finish Cancel

4. [証明書の作成]ページで必要な情報を入力し、[次へ]をクリックして[オンライン証明機関]ページを開きます。



Create Certificate

Online Certification Authority

Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.

Specify Online Certification Authority:

SurWDLab-WIN-MHPTD0N5FCO-CA\WIN-MHPTD0N5FCO.SurWDLab.com Select...

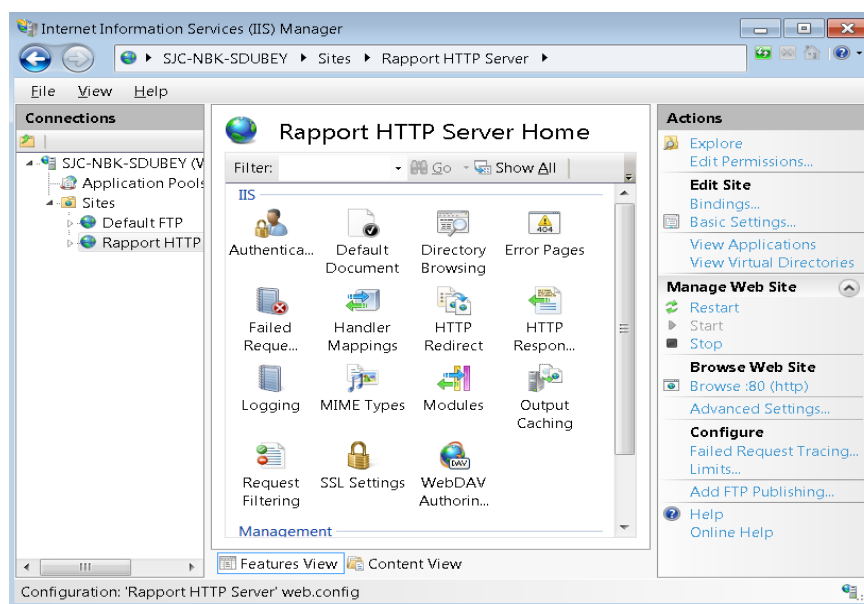
Example: CertificateAuthorityName\ServerName

Friendly name:

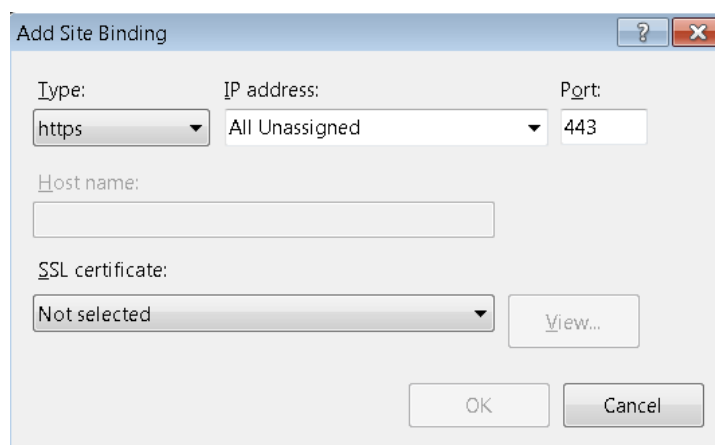
TestCert.SurWDLab.com

Previous Next Finish Cancel

5. [オンライン証明機関]ページで、[選択...]をクリックして[オンライン証明機関の指定]を設定し、さらに[フレンドリ名]を指定して[終了]をクリックします。
6. これで、WDMサーバーへの証明書のインストールが完了しました。
7. 証明書のインストール後に、サーバー名ノード > [サイト] > [Rapport HTTP Server]を選択し、右端ペインの[サイトの編集]セクションの下にある[バインド...]をクリックして[サイトバインド]ダイアログを開きます。



8. [サイトバインド]ダイアログで[追加]をクリックし、[サイトバインドの追加]ダイアログを開きます。



9. [サイトバインドの追加]ダイアログを開いたら、[種類]ドロップダウンからhttpsを選択し、[SSL証明書]ドロップダウンから 作成した証明書を選択し、[OK]ボタンをクリックします。
10. HTTPS通信のみを開始するには、以下のようにします。
サーバー名ノード> [サイト] > [Rapport HTTP Server] を選択し、[SSL設定]をダブルクリックします。



11. [SSL設定]ページで[SSLが必要]チェックボックスを選択し、[適用]をクリックします。