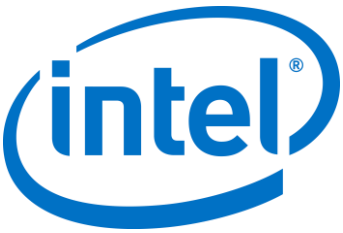
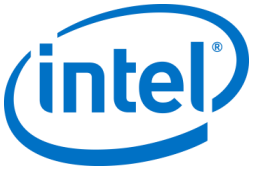


Intel Unite® ソリューション

エンタープライズ導入ガイド

2017 年 5 月



法務情報および免責事項、著作権

本資料に記載されたすべての情報は、予告なく変更されることがあります。インテル® 製品の最新の仕様およびロードマップをご希望の場合は、インテルの担当社員までご連絡ください。

インテル® テクノロジーの機能と利点はシステム構成によって異なり、対応するハードウェアやソフトウェア、またはサービスの有効化が必要となる場合があります。実際の性能はシステム構成によって異なります。絶対的なセキュリティーを提供できるコンピューター・システムはありません。詳細については、各システムメーカーまたは販売店にお問い合わせいただくか、www.intel.co.jp を参照してください。

ここに記載されているインテル製品に関する侵害行為または法的分析に関連して、本書を使用または使用を促すことはできません。インテルに対し、ここで開示された内容を含む特許クレームについて非独占的かつロイヤルティー・フリーの実施権を許諾することに同意したものとみなされます。

本資料は、（明示されているか否かにかかわらず、また禁反言によるとよらずにかかわらず）いかなる知的財産権のライセンスを許諾するためのものではありません。

インテル® 製品には、エラッタと呼ばれる設計上の不具合が含まれている可能性があり、公表されている仕様とは異なる動作をする場合があります。現在確認済みのエラッタについては、インテルまでお問い合わせください。

インテルは、明示たると黙示たるとを問わず、商品性、特定の目的に対する適合性、法律違反のないこと、履行の過程、商取引上の取り扱いもしくは利用の慣例の黙示の保証を含むが、これらに限定しないすべての保証を否認します。

インテルは、本資料で参照している第三者のベンチマーク・データまたは Web サイトについて管理や監査を行っていません。本資料で参照している Web サイトを参照し、本資料で参照しているデータが正確かどうかを確認してください。

Intel、インテル、Intel ロゴ、Intel Unite、Intel Core、Intel vPro は、アメリカ合衆国および / またはその他の国における Intel Corporation またはその子会社の商標です。

この文書はローカライズされることにより、一部の画像の表示が異なることがあります

*その他の社名、製品名などは、一般に各社の表示、商標または登録商標です

目次

1 はじめに

Intel Unite® ソフトウェアは、コラボレーションを簡単にする、安全なオンライン会議スペースです。会議出席者全員を素早く簡単につなぐように設計されています。Intel Unite® ソリューションは、現在入手できるシンプルで直ちにコラボレーションが可能なソリューションであり、将来にわたって追加機能に対応し、イノベーションを実現する基盤となります。

本書は、Intel Unite® ソフトウェアをエンタープライズ・モードでインストールする場合に参照するものであり、機能の詳細やトラブルシューティングについて説明しています。

1.1 対象

このドキュメントは、企業環境内で作業する IT スタッフのほか、Intel Unite® ソリューションを企業環境に導入しようとしている読者を対象としています。

1.2 Intel Unite® ソリューションの用語と定義

エンタープライズ・サーバー (サーバー) – PIN の割り当てと決定を行う PIN サービスが実行される Web サーバーです。クライアント向けのダウンロード・ページ、および設定のための管理ポータルを提供します。

クライアント – ハブに接続するときに使用されるデバイス (Windows*、macOS*、iOS*、Android* または Chromebook*) です。

ハブ – Intel Unite® アプリケーションを実行している、会議室内のディスプレイに接続されたインテル® vPro™ テクノロジー搭載ミニ・フォーム・ファクター PC です。

FQDN – 完全修飾ドメイン名 (Fully Qualified Domain Name) を意味します。

プラグイン – Intel Unite® ソリューションの機能を拡張するための、ハブにインストールされたソフトウェア・コンポーネントです。

IIS – Microsoft* が提供する Web サーバーである、インターネット インフォメーション サービス (Internet Information Services) を意味します。

1.3 Intel Unite® ソリューションの新機能

ソリューションに何が追加されたかを分かりやすく示すため、次の表に 1.0 以降のバージョンで追加された機能をまとめています。

v 2.0	v 3.0	v 3.0 MR	v 3.1
拡張ディスプレイ	ハードウェア・アクセラレーションによる Windows* 用オーディオ / ビデオ・ストリーミング (1080 @20-30 fps)	iOS* によるプレゼンテーションのサポート	管理者ポータルのユーザー体験の改善、設定の選択を支援するダイアログボックスの追加を含む表示の変更
Windows® 10 対応	保護されたゲストアクセス用プラグイン		管理者ポータル：会議のスケジュール
ゲストユーザー用サインインプラグイン	スケジュールされた会議 (1 つの会議室)		管理者ポータル：モデレーター・モード
Skype* for Business 用プラグイン	会議のロック		管理者ポータル：静的 PIN
	iOS* による表示のサポート		管理者ポータル：PIN の予約
			管理者ポータル：PIN の透明度
			管理者ポータル：リモートビューの無効化
			Chrome* OS 対応
			Android* 対応

2 Intel Unite® ソリューションの要件

2.1 エンタープライズ・サーバーの要件

- Microsoft* Windows Server* 2008 以降
- SSL を有効にした Microsoft* インターネット インフォメーション サービス
    - 社内または信頼できるパブリックルートの、SHA2 ベース Web サーバー証明書が必要です。
- Microsoft* インターネット インフォメーション サービスで設定された SMTP 電子メールサーバー
- Microsoft* SQL Server* 2008 R2 以降
- Microsoft* .NET* 4.5 以降
- 4 GB RAM
- 32 GB の空き領域

  注：IIS Web サーバーと Microsoft* SQL データベース・サーバーは、それぞれ別の機器にインストールできます。

2.2 ハブの要件

- Microsoft* Windows* 7 SP1、8.1 または 10 (32 ビットおよび 64 ビット)
    - 推奨される最新のパッチレベル
- Microsoft* .NET* 4.5 以降
- サポートされる SKU[1](第 4 世代以降のインテル® Core™ vPro™ プロセッサーを搭載したミニ PC)
- 有線またはワイヤレス・ネットワーク接続
- 4 GB RAM
- 32 GB の空き領域

2.3 クライアントの要件

- Microsoft* Windows* 7 SP1、8.1 または 10 (32 ビットおよび 64 ビット)
    - 推奨される最新のパッチレベル
- Microsoft* .NET* 4.5 以降
- OS X* 10.10.5 以降
- iOS* 9.3 以降
- 有線またはワイヤレス・ネットワーク接続

[1] サポートされる SKU については、OEM またはインテルの担当者にお問い合わせください。

2.4 IT 関連の注意事項およびネットワークの要件

ハブおよびクライアントのインストールは、IT 部門が確立したソフトウェア頒布プロセスを使用して管理する必要があります。
信頼性を確保するために、ハブの接続には有線ネットワーク接続を使用することを強くお勧めします。有線接続をすることで、特に混雑した領域で無線帯域幅が飽和状態になることがなくなります。
他の注意事項として、Intel Unite® ソフトウェアに着信接続の受け入れを許可する必要がある点が挙げられます。これには、ハブにインストールされているファイアウォールに例外を追加する必要がある場合があります。アプリケーションの例外を作成する具体的な手順については、ファイアウォールのベンダーにお問い合わせください。

実稼動環境では、完全修飾ドメイン名 (FQDN) を使用し、エンタープライズ・サーバーを示す DNS サービス レコードを設定することを強くお勧めします。これによりハブおよびクライアントがエンタープライズ・サーバーを簡単に見つけることができるようになります。
セキュリティ・アップグレードでは、アプリケーションは SHA-2 以上の証明書のみを受け付けます。そのため、Web サーバー上の証明書をアップグレードする必要がある場合があります。IT セキュリティチームと連携してセットアップ中に SHA-2 証明書を入手する必要があります。

2.4.1 モバイル・クライアント・デバイス

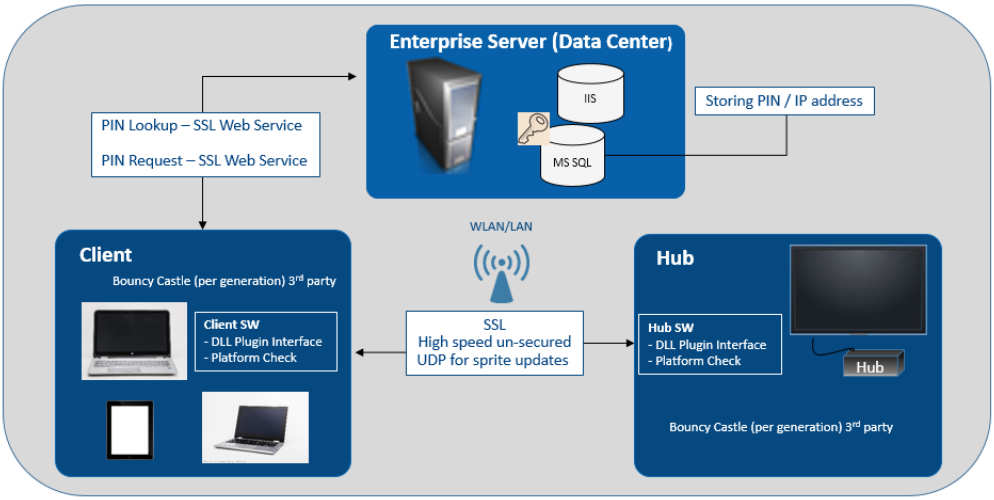
Intel Unite® クライアント OS の一部としてモバイル・クライアント・デバイスを導入する場合は、以下の事項にご注意ください。
Intel Unite® ソリューションに接続するには、iOS* や Android* デバイスを含むクライアント・デバイスをすべて企業ネットワークに接続するか、適切に構成された VPN を使用する必要があります。企業ネットワークに接続せず、個人のキャリアを使用して接続するタブレットや電話を使用する場合 (通常は個人使用目的)、Intel Unite® アプリのセッションに接続できない場合があります。これは、企業ファイアウォールでこの接続が許可されていない可能性があるためです。

IT 管理者向け情報：

- Intel Unite® アプリのユーザーが個人のモバイルデバイスを使用している場合、Intel Unite® への接続には企業ネットワークを使用するか、接続を許可する方法を作成してください。
- デバイスを適切に管理し、ネットワークを安全に保つために必要なツールがあることを確認してください。
- セキュリティー・リスクとなり得るデバイスを管理するための適切な戦略を構築してください。
- 個人デバイスや仕事を目的としたモバイルデバイスに関して、モバイルデバイス管理ポリシーを適用してください。
- セキュリティーは、保護するデータの機密レベルに応じて、最適なレベルのセキュリティーを提供できるようにカスタマイズします。カスタマイズ・レベルは、企業が重要と判断するデータや、保護するためにどれだけドリルダウンするかによって異なります。

3 導入の概要

Intel Unite® ソリューションは、エンタープライズ・サーバー、ハブ、そしてクライアントの 3 つのコンポーネントで構成されています。
エンタープライズ・サーバーは、コンポーネントの中で最初に設定する必要があります。ハブおよびクライアント・アプリケーションが起動されると、接続情報を交換し、PIN の割り当てを受けるために、エンタープライズ・サーバーが使用されるからです。
ハブは、通常は会議室のディスプレイまたはプロジェクターに接続された、インテル® Core™ vPro™ プロセッサーを搭載したミニ PC です。
クライアントは、ハブに表示された手順に従って、クライアント・ソフトウェアをダウンロードし、表示された PIN を入力することでハブに接続します。接続が確立すると、クライアントはコンテンツのプレゼンテーションや表示、注釈付け、そして同じハブに接続された他のクライアントとファイルを共有でき、ハブにインストールされたプラグインとも通信できます。
次の図は、インストールされたコンポーネントの概要を示しています。



3.1 導入のためのリソース

インストールを完了するためには、次の権限が必要です。

- データベースの管理者権限
- エンタープライズ・サーバーの管理者権限
- ハブの管理者権限

次の権限も必要な場合があります。

- SHA-2 証明書を発行する IT セキュリティー管理者
- ファイアウォール・ポリシーの IT セキュリティー管理者権限
- ハブおよびクライアントがエンタープライズ・サーバーを探すために使用する DNS サービスレコードを作成する、IT 管理者権限 (強く推奨)

4 エンタープライズ・サーバーのインストール

4.1 エンタープライズ・サーバーの概要

エンタープライズ・サーバーのインストーラーには、データベース、PIN サーバー、管理者 Web ポータル、およびクライアント・ダウンロード・ページが含まれています。

エンタープライズ・サーバーには、次の 4 つのコンポーネントがあります。

1) Microsoft* SQL データベース：Intel Unite® ソリューション・インフラストラクチャーのステータス情報がすべて保持されます。
2) Web サービス：データベースと、ハブおよびクライアントとの通信を行う標準メッセージング・サービスです。
3) 管理者ポータル Web サイトでは、ハブとクライアントの管理、統計の生成、および監視と警告を行います。
4) クライアント・ダウンロードのランディング Web ページには、クライアント用 Intel Unite® ソフトウェアが用意されています。

また、ハブとクライアントは、エンタープライズ・サーバーの位置をネットワーク・インフラストラクチャー上で確認する際に、ServerConfig.xml ファイルか DNS サービスレコードのいずれかを利用することを理解しておくことが重要です。

クライアントとハブにゼロタッチ構成を使用できるため、DNS サービスレコードを使用することをお勧めします。「DNS サービスレコードを作成する」のセクションを参照してください。DNS サービスレコードを入手できない場合は、ServerConfig.xml ファイルでエンタープライズ・サーバーを設定できます。ServerConfig.xml ファイルの例については、付録 B を参照してください。

4.2 エンタープライズ・サーバーのプレインストール

- サーバーが、指定されているソフトウェアとハードウェアの最低条件を満たしていることを確認します。
- バージョン 8.0 以降の IIS がサーバーにインストールされていることを確認します。IIS が有効でなければサーバーのインストーラーは動作しないため、インストールできません。IIS の有効化やセットアップのヘルプについては、「IIS を有効にする」セクションを参照してください。
- IIS マネージャー で SMTP 電子メールサーバーを設定します。詳細は、「

- 電子メールサーバーの設定」セクションを参照してください。
- ASP.NET 4.5 がインストールされ有効になっていることを確認します。
- SSL が IIS で有効になっていることを確認します (https サイトが動作するはずです)。**注：**信頼できる有効なルートの SHA-2 証明書をインストールするために、IT 部門と連携する必要がある場合があります。
- Windows* 認証または SQL 認証により MS SQL へのアクセス権があることを確認します。「Microsoft* SQL Server* のインストール」のセクションを参照してください。
- エンタープライズ・サーバーの自動ルックアップを有効にするには、DNS サービスレコードを追加します。「DNS サービスレコードを作成する」のセクションを参照してください。

4.2.1 ソフトウェア・アップグレード

ソフトウェア・アップグレードを実行する場合、以下を確認してください。

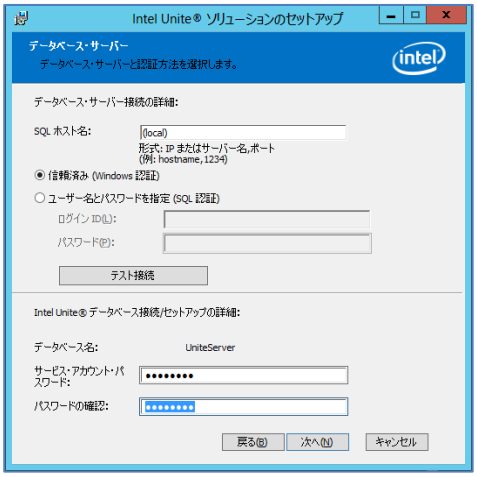
- 変更は元に戻せないため、必ずデータベースをバックアップしてください。
- アップグレード実行前に、データベースへの接続をすべて閉じる必要があります (管理者ポータルからログオフ)。
- アップグレードする間、デフォルトでは PIN サーバー上での Intel Unite server.msi 実行時に、ローカル・インストールとリモート・インストールの両方でデータベース・オプションが選択されます。

4.3 エンタープライズ・サーバーのインストール

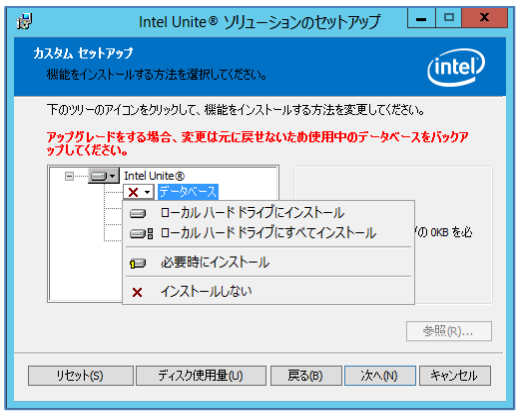
前のセクション「エンタープライズ・サーバーのプレインストール」のすべての手順を確認したら、Intel Unite® ソフトウェアのインストーラーに進みます (このプロセスは、IIS 環境をホストするサーバーで実行する必要があります)。

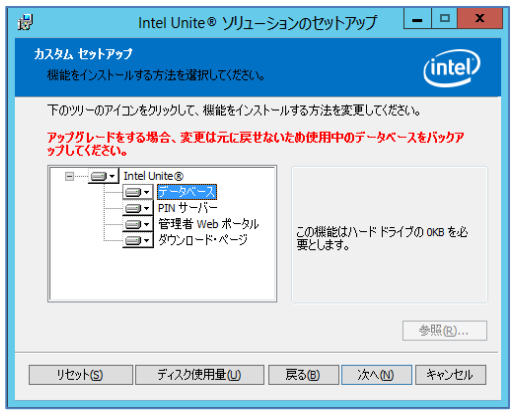
- **Intel Unite Server.mui.msi** ファイルを探してダブルクリックし、ターゲットサーバーにインストールします。
- インストール・ウィザードのオプションで、データベース、Web サービス、クライアント・ダウンロード・ページ、および管理者ポータルの各コンポーネントをインストールするかどうかを指定できます。
- **Intel Unite Server.mui.msi** を起動したら、[**使用許諾契約書に同意します**] ボックスをオンにします。

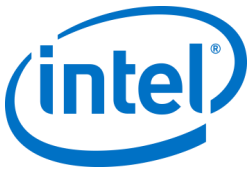
- [**次へ**] をクリックして [データベース・サーバー] ウィンドウに進みます。
- [データベース・サーバー] ウィンドウで、[**データベース・サーバー接続の詳細**] を選択します。使用できるオプションは次のとおりです。
  - [**SQL ホスト名**] ボックスの **(local)** はサーバーのデフォルト値です。この値は、ホスト名を編集して変更することができ、またはデフォルト値のままにすることもできます (同じサーバーに SQL がインストールされている場合は **(local)** のままにします)。
  - サーバーのデフォルト値は [**信頼済み (Windows 認証)**] (すでにログイン済みの場合) ですが、データベースへのアクセス権があり、SQL 認証を選択できる有効な資格情報を持っている場合は [**ユーザー名とパスワードを指定 (SQL 認証)**] を選択します。後者を選択する場合は、[**テスト接続**] をクリックしてデータベース接続をテストしてください。
  - [**データベース接続/セットアップの詳細**] セクションでは、UniteServer と呼ばれる新しいデータベースへのアクセスに使用される **UniteServiceUser** のパスワードを作成する必要があります。次の [**パスワードの確認**] ボックスにパスワードを入力します。
  - パスワードは 8 文字以上で、大文字、小文字、数字、記号をそれぞれ 1 文字以上使用する必要があります。



- [**次へ**] をクリックして、機能の選択を行う [**カスタム セットアップ**] ウィンドウに進みます。データベース機能を展開し、[**ローカル ハード ドライブにインストール**] または [**ローカル ハード ドライブにすべてインストール**] のいずれかを選択します。これにより、前の手順で指定した SQL Server* 内にデータベースが作成されます。



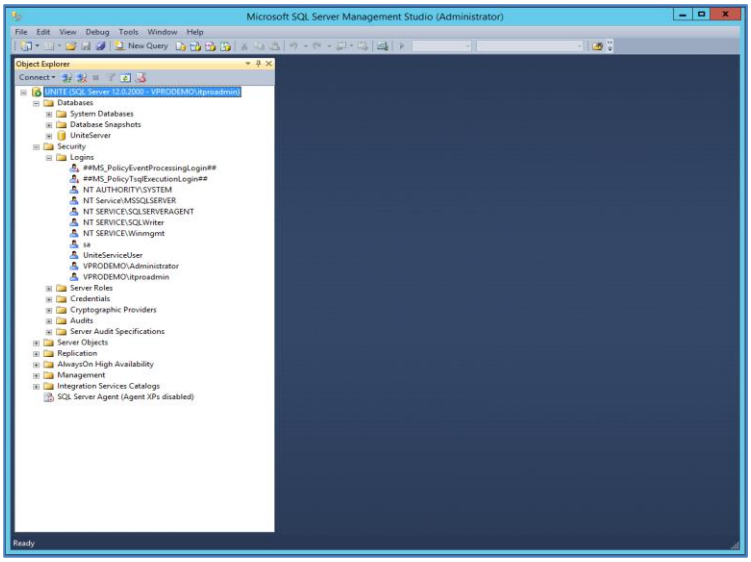




- [**次へ**] をクリックして機能の選択内容を確認し、[**インストール**] をクリックしてインストールを開始します。
- [**完了**] をクリックして、セットアップを終了します。
- これでエンタープライズ・サーバーがインストールされました。次のセクションに進んでハブをインストールしてください。

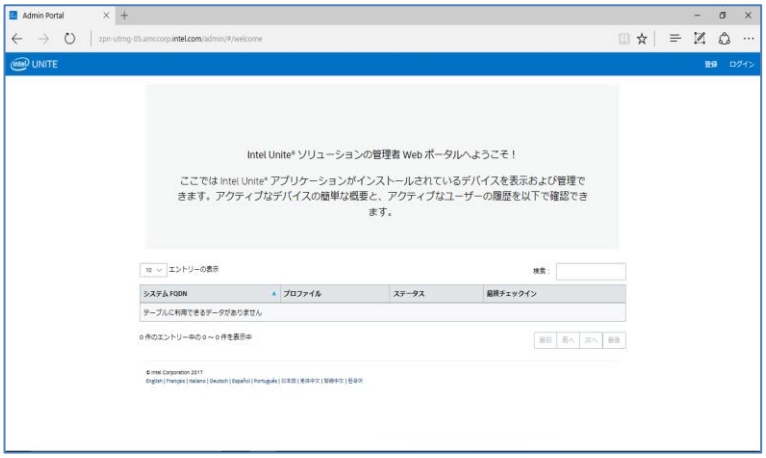
オプション：

- UniteServer データベースが、サーバー上の SQL Management Studio を使用して作成されていることを確認する場合、SQL Management Studio を開き、SQL Server* に接続します。左側のペインで [Databases (データベース)] を展開し、UniteServer データベースが作成されていることを確認してください。



- 下記のリンクから、管理者ポータル (データベースおよび PIN サーバーと一緒に、サーバーにインストールされている場合) にアクセスしてインストールが成功したことを確認します。
  https://<サーバー名>/admin

  アカウントにログインするか、デフォルトの管理者アカウントを使用できます (新しくソフトウェアをインストールした場合)。
  ユーザー：admin@server.com
  パスワード：Admin@1

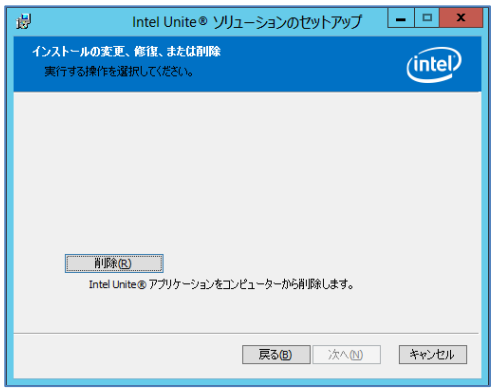


注 ：管理者ポータルへのアクセス時にエラーが発生した場合、「トラブルシューティング」セクションを参照してください。

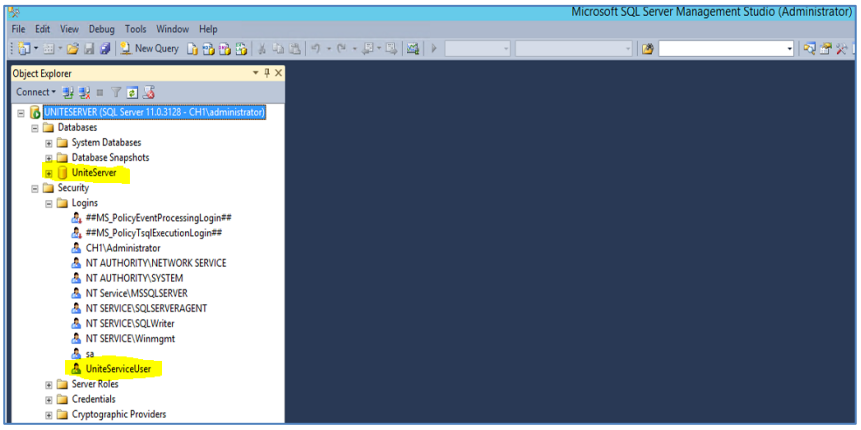
4.4 Intel Unite® アプリケーションのアンインストール

アプリケーションをアンインストールする必要がある場合は、前に作成した UniteServer データベースと UniteServiceUser ログインも削除して、アプリケーション内の競合を回避する必要があります。削除する前に、**必ずデータベースのバックアップを作成してください。**

1. インストーラー **Intel Unite Server.mui** を実行します。
2. [**削除**] をクリックし、[**次へ**] をクリックして進みます。



3. *Microsoft SQL Server Management Studio* に移動し、手動で **UniteServer** SQL データベースと **UniteServiceUser** アカウントを削除します。以下の画像で強調表示された領域を参照します。



5 ハブのインストール

5.1 ハブのプレインストール

エンタープライズ・サーバーにチェックインして通信するには、ハブ・ファイアウォールで Intel Unite® アプリケーションを除外する必要があります。これは、ハブがエンタープライズ・サーバーを探してチェックインできる必要があるためです。

ハブ・インストーラーを実行するとサーバー接続の詳細が表示され、DNS サービスレコードから取得した情報によって手動ルックアップ (インストール・プロセスの [**サーバーの指定**]) をバイパスするオプションが表示されます。ハブ・インストーラーを実行すると、インストーラーにより ServerConfig.xml が編集されます。

インストールの実行時に [**サーバーの自動検索**] または [**サーバーの指定**] のどちらを使用するかについては、PIN のルックアップに選択した方法に応じて決まるため、知っておく必要があります。

DNS サービスレコードが存在することが確実な場合、[**サーバーの自動検索**] を選択できます。不明な場合は、[**サーバーの指定**] オプション (手動ルックアップ) を使用します。このとき、エンタープライズ・サーバーのホスト名が必要です。

ServerConfig.xml を公開キー (次の「公開キー」セクションを参照) を使用して編集した場合は、クライアントおよびハブ・インストーラーに再度キーを入力する必要はありません。

注：サーバーが ServerConfig.xml で定義されている場合は、そのサーバーが DNS サービスレコードよりも優先されます。

5.1.1 公開キー

公開キーはオプションで、ハブまたはクライアントがエンタープライズ・サーバーに通信する方法を指定します。空白のままにしたり指定しない場合、ハブとクライアントはルートが信頼できるかどうかを検証します。アプリケーションが証明書を受け入れない場合は、ユーザーに表示されます。

公開キーは、ハブとクライアントのインストールを実行する際に使用されます。ハブとクライアントのインストーラーを実行する場合に、このキーが必要になります。公開キーを取得するには、https://サーバー名/unite/ccservice.asmx にアクセスしてください。

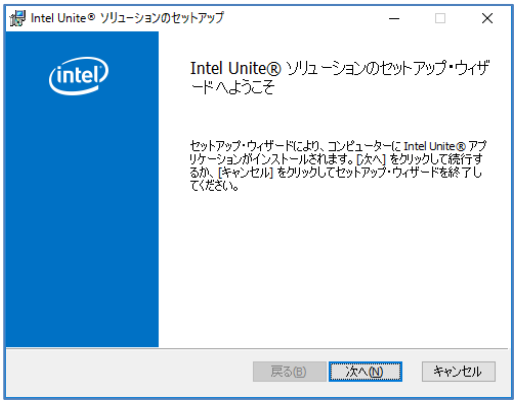
URL バーで鍵型のアイコンをクリックして、証明書情報を表示します。[詳細] に移動して [すべて表示] をクリックし、[公開キー] フィールドまでスクロールし、公開キーをクリックして表示します。必要に応じてその値をコピーし、serverconfig ファイルに貼り付けます。

ServerConfig ファイルに貼り付けた後、文字列からスペースを削除してください。ServerConfig.xml を、公開キーを使用して編集した場合は、クライアントおよびハブ・インストーラーに再度キーを入力する必要はありません。ServerConfig.xml の例については、付録 B を参照してください。

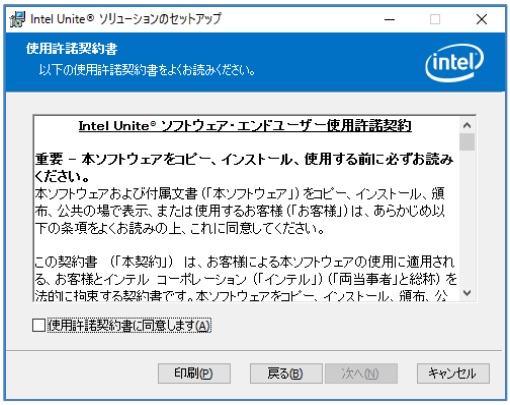
5.2 ハブのインストール

- インストーラーのフォルダーの場所を探して、ハブのインストーラーである **Intel Unite Hub.mui.msi** を実行します。

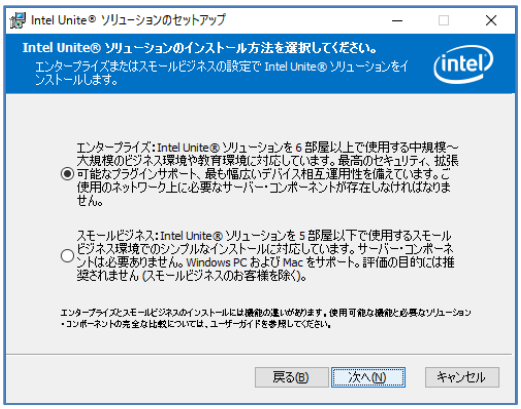
- **[次へ]** をクリックして進めます。



- **[使用許諾契約書に同意します]** チェックボックスを選択したら、**[次へ]** をクリックします。

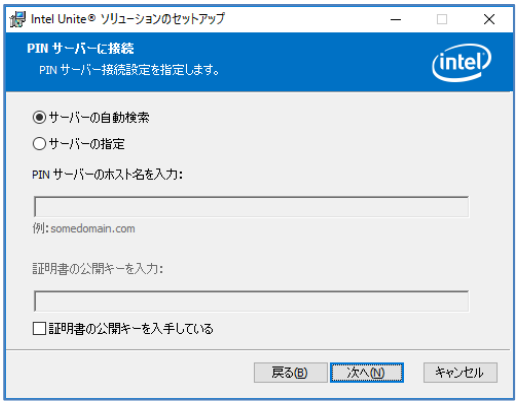


- **[エンタープライズ]** を選択して、**[次へ]** をクリックします。

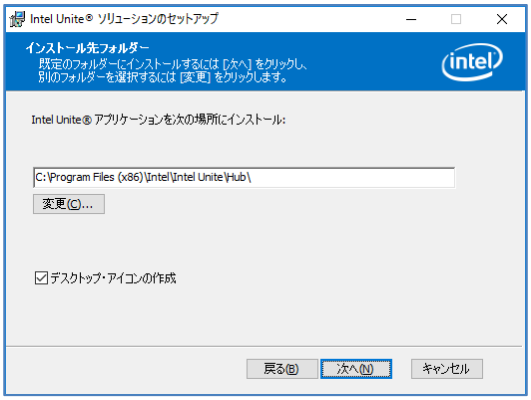


- このウィンドウで、PIN サーバーの接続設定を指定する必要があります。次の選択肢より選択します。
  - [**サーバーの自動検索**]：推奨される選択肢です (デフォルト)。
  - [**サーバーの指定**]：この手順では、エンタープライズ・サーバーのホスト名が分かっている必要があります。
    - **PIN サーバーのホスト名を入力します。**
    - [**証明書の公開キーを入手している**] をオンにしている場合、[**証明書の公開キー**] を入力します。

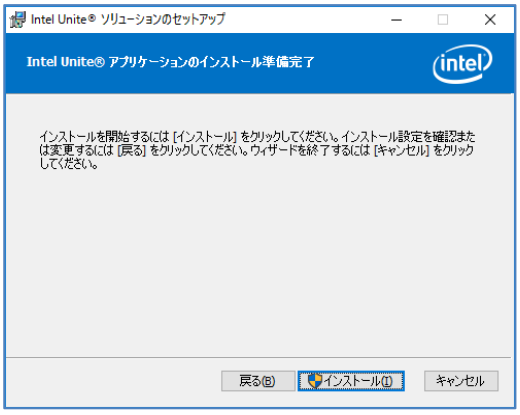
  いずれかを選択して [**次へ**] をクリックします。



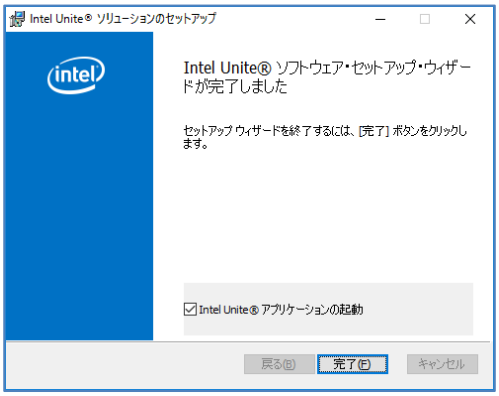
- [**インストール先フォルダー**] ウィンドウが開き、ハブがインストールされるデフォルトのフォルダーが表示されます。インストール先フォルダーは、必要に応じて変更できますが、変更する必要がなければデフォルトの場所のままにします。この手順でデスクトップ・アイコンを作成することもできます。[**次へ**] をクリックして進めます。



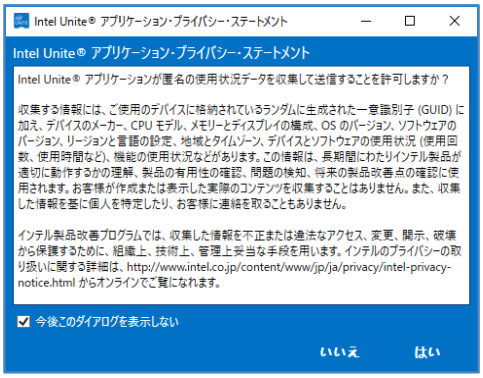
- この手順で、戻って設定を確認するか、[**インストール**] をクリックして進みます。



- インストールが終了すると、[**Intel Unite® ソフトウェア・セットアップ・ウィザードが完了しました**] ウィンドウが表示されます。[**完了**] をクリックして、インストール・プロセスを終了します。

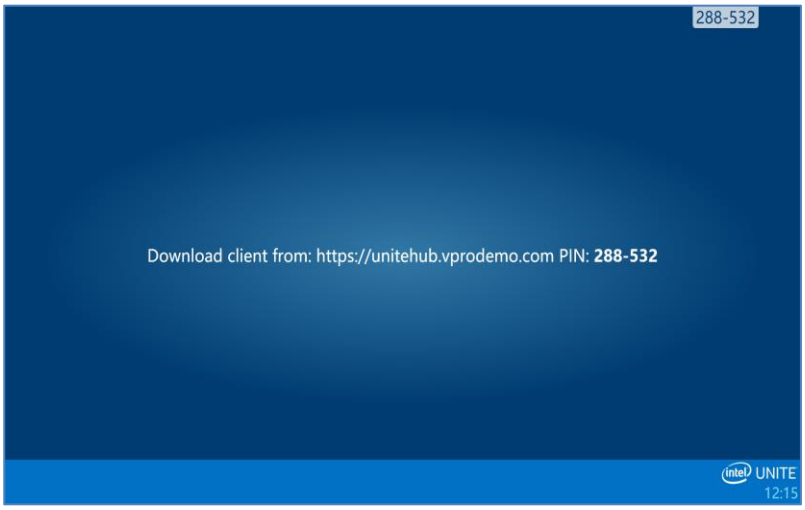


  - 初めてアプリケーションを起動する場合は、**Intel Unite® アプリケーション・プライバシー・ステートメント**が表示されます。



  - Intel Unite® アプリケーション・プライバシー・ステートメントは、匿名の使用状況データを収集する目的で使用されます。インテルでは、常に製品の向上に力を入れており、今後もよりよい製品を提供するためにデータを収集したいと考えています。[**はい**] または [**いいえ**] を選択します。このダイアログボックスを再度表示したくない場合はチェックボックスを選択してください。

- これで、画面またはモニターに PIN が表示されるようになりました。これは、クライアントがハブに接続する際に必要となる PIN です。(PIN が表示されない場合は、「トラブルシューティング」セクションを参照してください。)



5.3 ハブの設定

Intel Unite® ソフトウェアを実行しているハブの設定オプションは、管理者ポータルで変更できます。管理者ポータルには、エンタープライズ・サーバーにチェックインしたすべてのハブに適用されるデフォルトの構成設定が記載されたデフォルトのプロファイルがあります。この設定オプションは、ハブからエンタープライズ・サーバーへの接続が確立された後、ハブに適用されます。設定はハブのチェックイン時に毎回更新されます。ハブに表示する色、画像、PIN サイズ、実装するプラグインなどを含むハブ設定のほとんどが、組織のニーズに合わせてカスタマイズできます。
ハブ設定について、詳しくは「管理者ポータルガイド」セクションを参照してください。

5.4 ハブの推奨プラクティス

エンドユーザーのエクスペリエンスを最大限に高めるには、常に使用できるようにハブを設定し、システム警告やポップアップが画面上に表示されないようにする必要があります。次のような推奨プラクティスがあります。

- Intel Unite® アプリケーションを実行するドメインまたはユーザーに Windows* が自動的にログインするようにします。
- スクリーンセーバーを無効にします。
- システムがスタンバイ状態にならないように設定します。
- システムがログアウトしないように設定します。
- ディスプレイの電源がオフにならないように設定します。
- システム警告が表示されないようにします。

5.5 ハブのセキュリティー

ハブの管理者は、それぞれのハブでセキュリティーの推奨プラクティスが実行されていることを確認してください。自動的にログインしたローカルユーザーが、管理者権限を持つことがないようにしてください。

5.6 プラグイン

Intel Unite® アプリケーションでは、プラグインを使用することができます。プラグインは、アプリケーションの機能や能力を拡張するソフトウェア要素で、ユーザー・エクスペリエンスのモダリティーを実装します。各ハブに固有のプラグインがあります。
Intel Unite® アプリケーションでは、次のプラグインが使用できます。

保護されたゲストアクセス用プラグイン：このプラグインを使用すると、コンピューターは同じエンタープライズ・ネットワーク上になくても、エンタープライズ・サーバーの PIN 検証なしでハブに接続できます。ハブは、Intel Unite® クライアントが接続できるアドホック / ホスト・ネットワーク (アクセスポイント) を作成します。

Skype* for Business 用プラグイン：このプラグインは、オンライン Skype* 会議から参加者を Intel Unite® アプリのセッションに追加するためのソリューションです。このプラグインは、Intel Unite® ソフトウェアのハブ上で実行され、各インスタンスに固有のメールアカウントを管理します。

テレメトリー用プラグイン：このプラグインにより、エンタープライズ・サーバーでハブのデータを受け入れて表示できます (このプラグインがハブにインストールされている場合)。最低条件は、エンタープライズ・サーバー v3.0 (ビルド # 3.0.38.44) です。

プラグインの書き込みに使用する SDK もあります。

ソフトウェア開発キット (SDK)：アプリケーション・インターフェイス・ガイドにより、ソフトウェア開発者または Intel Unite® アプリケーションの追加機能を開発するその他のユーザーをサポートします。

注：インストール方法と各プラグイン・コンポーネントの詳細については、特定のプラグインのガイドを参照してください。

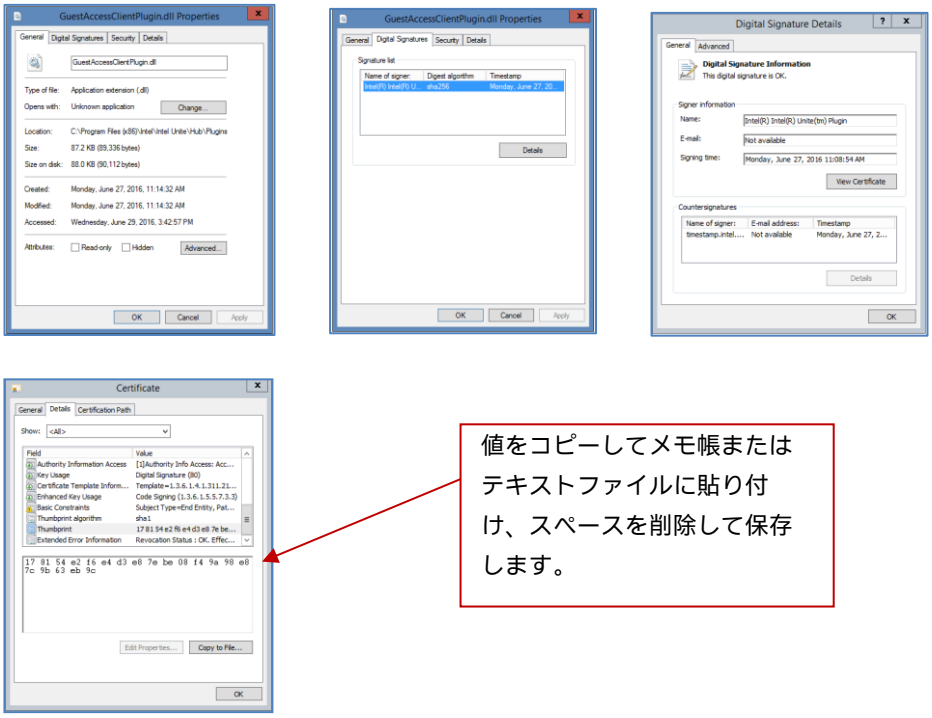
5.6.1 プラグインのインストールに関する注意

各プラグインは、デフォルトでインストール・ディレクトリー内のプラグイン・ディレクトリー [Program Files(x86) \Intel\Intel Unite\Hub\Plugins\PluginName (Plugin.dll)] にインストールされています。プラグインは、アプリケーションの開始時に列挙されます。新しいプラグインを追加した場合、アプリケーションを再起動する必要があります。
プラグインをインストールする前に、Intel Unite® ソリューションのターゲットバージョンとの互換性を確認します [要件はプラグインによって異なるため、個別のプラグインガイドを参照してください]。
使用するプラグインごとに、管理者 Web ポータルでプラグイン証明書ハッシュの値を取得および追加することも必要です。
注：テスト環境ではデフォルトのキー値を使用できますが、実稼働環境では使用しないことをお勧めします。

5.6.2 プラグイン証明書ハッシュの値

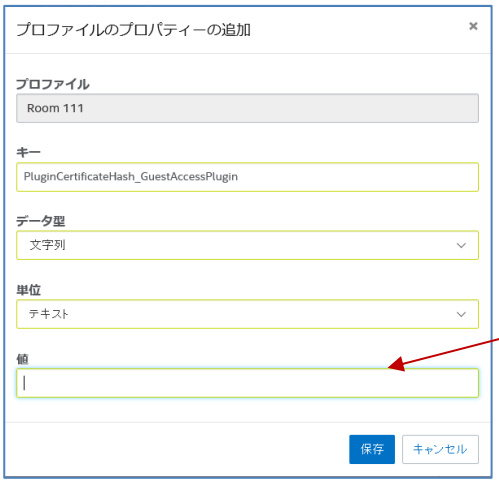
次の手順に従って、プラグイン証明書ハッシュキーの値を確認します。

- プラグインフォルダーでプラグインを探し、***Plugin.dll** (GuestAccessClientPlugin.dll など) を右クリックし、[**プロパティ**] を選択します。
- プラグインの [**プロパティ**] ウィンドウが開いたら、[**デジタル署名**] タブを探し、クリックして開きます。
- [**Intel Unite® プラグイン**] を選択し、[**詳細**] をクリックします。
- [**デジタル署名の詳細**] ウィンドウで、[**証明書の表示**] をクリックします。
- [**証明書**] ウィンドウで [**詳細**] タブを選択し、[**拇印**] が表示されるまで下にスクロールします。
- [**拇印**] を選択し、値が表示されたらメモ帳またはテキストファイルに貼り付け、スペースを削除し、保存します。
- このキー値は、プラグインのプロファイル作成時に使用されます。このキー値は、プロファイル作成後に作成および入力できます。 詳しくは次のセクションを参照してください。



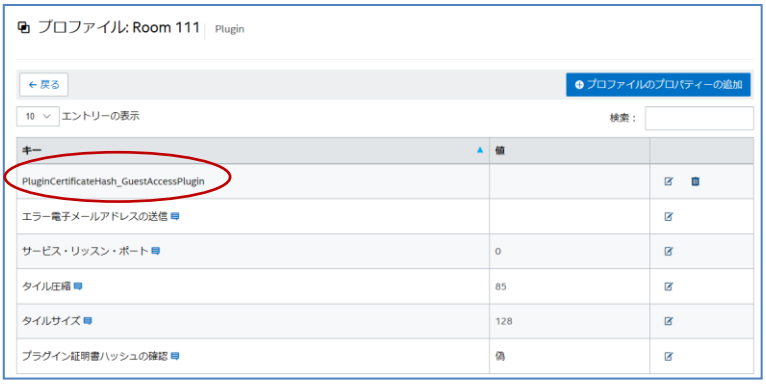
5.6.3 管理者 Web ポータルのプラグインに証明書ハッシュを追加する

管理者 Web ポータルに移動し、[**グループ**] でプラグインを有効にするプロファイルを選択します。
[プロファイル] ウィンドウで、[**プロファイル・プロパティーの追加**] をクリックし、次のとおり入力します。

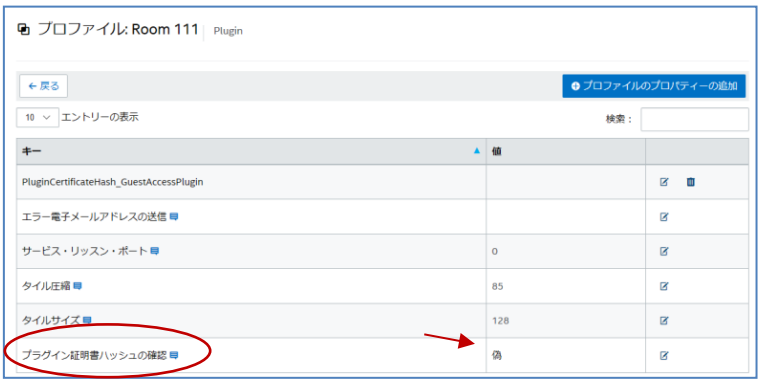


- **キー**： PluginCertificateHash_XXX
  - XXX はハッシュを追加するプラグインの名前です。例えば、識別用の GuestAccessPlugin では、ハッシュに対応するプラグイン名を使用することをお勧めします。
- **データ型：**文字列
- **ユニット：**テキスト
- **値：**「*プラグイン証明書ハッシュの値*」セクションでメモ帳またはテキストファイルに保存した拇印値を使用します。キー値は、キーの作成後に入力することもできます。

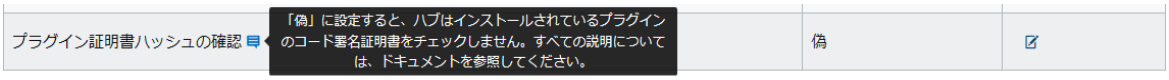
[**保存**] をクリックします。この値は、後で [**編集**] リンクを選択して更新できます。
[プロファイル] ウィンドウに新しいキーが表示されます。



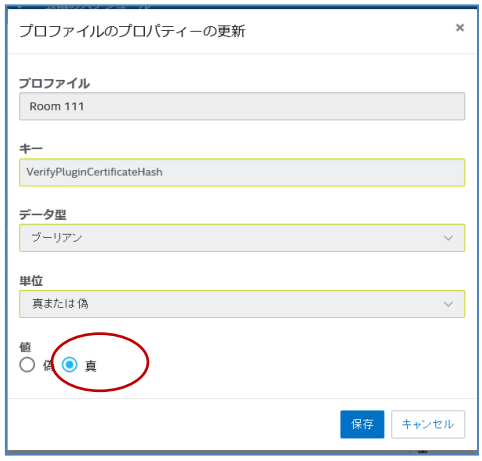
[**プラグイン証明書ハッシュの確認**] キーを真に設定し、有効にする必要があります。デフォルト値は偽です。



真から偽 (またはその逆) に切り替えることで、プラグインを有効または無効にできます。キー値はプラグインの有効性を確保するものであることに注意してください。



[編集] リンクをクリックし、値を [**真**] に変更して [**保存**] をクリックします。



プラグイン設定が有効になりました。

6 クライアントのインストール

6.1 クライアントのプレインストール

クライアントは、エンタープライズ・サーバーを探してチェックインできる必要があります。エンタープライズ・サーバーにチェックインして通信するには、クライアント・ファイアウォールで Intel Unite® のアプリケーションを除外する必要があります。
クライアント・インストーラーを実行すると、サーバー接続の詳細の入力を求めるプロンプトが表示され、DNS サービスレコードから取得した情報によって手動ルックアップ (インストール・プロセスの [**サーバーの指定**]) をバイパスするオプションが表示されます。インストーラーを実行すると、インストーラーにより ServerConfig.xml が編集されます。

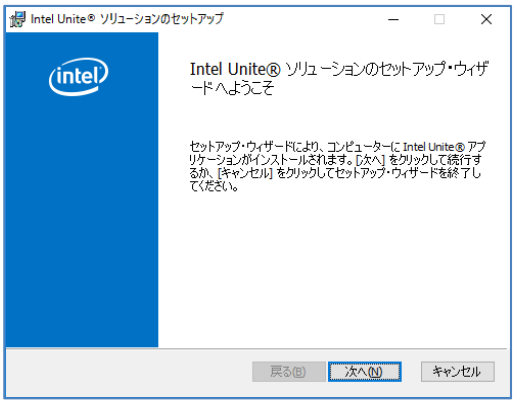
インストールの実行時に [**サーバーの自動検索**] または [**サーバーの指定**] のどちらを使用するかは、PIN のルックアップに選択した方法に応じて決まるため、知っておく必要があります。
DNS サービスレコードがあることが分かっている場合は、[**サーバーの自動検索**] を選択できます。タイプミスを防ぐため、自動ルックアップを使用することをお勧めします。存在するかどうかが不明な場合は、[**サーバーの指定**] オプション (手動ルックアップ) を使用します。この場合はエンタープライズ・サーバーのホスト名が分かっている必要があります。

注：サーバーが ServerConfig.xml で定義されている場合は、そのサーバーが DNS サービスレコードよりも優先されます。

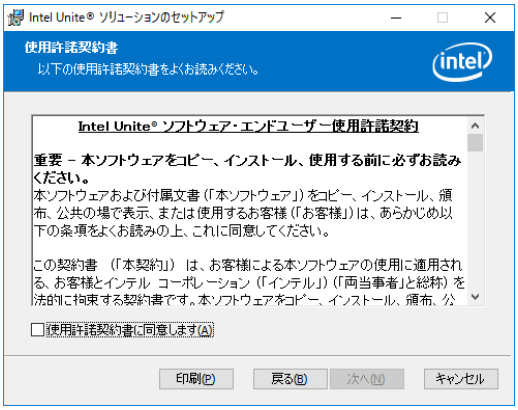
モバイル・クライアント・デバイス：iOS* や Android* デバイスを含むクライアント・デバイスをすべて企業ネットワークに接続するか、適切に構成された VPN を使用する必要があります。企業ネットワークに接続せず、個人のキャリアを使用して接続するタブレットや電話を使用する場合 (通常は個人使用目的)、Intel Unite® アプリのセッションに接続できない場合があります。これは、企業ファイアウォールでこの接続が許可されていない可能性があるためです。詳細については、モバイル・クライアント・デバイスを参照してください。

6.2 Windows* クライアントのインストール

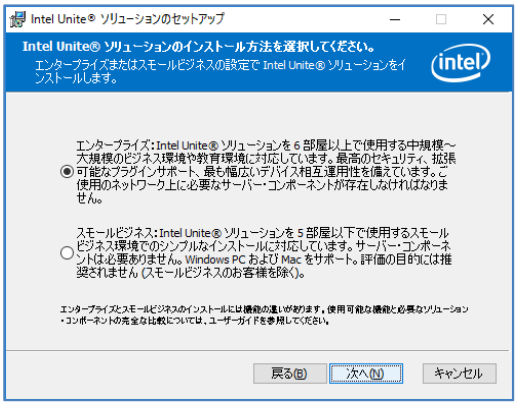
- インストーラーのフォルダーの場所を探して、クライアントのインストーラーである **Intel Unite Client.mui.msi** を実行します。[**次へ**] をクリックして進めます。



- [**使用許諾契約書に同意します**] チェックボックスを選択し、[**次へ**] をクリックします。



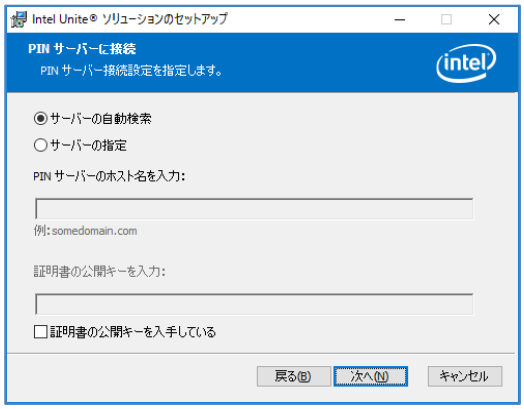
- [**エンタープライズ**] を選択して、[**次へ**] をクリックします。



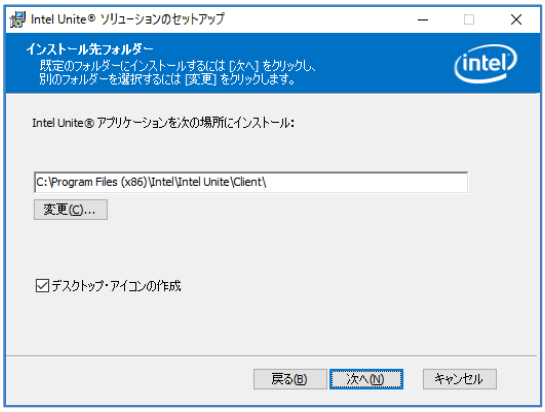
- このウィンドウで、PIN サーバーの接続設定を指定する必要があります。次の選択肢より選択します。
  - [**サーバーの自動検索**]：これが最も便利な選択肢です (デフォルト)。
  - [**サーバーの指定**]：この手順では、エンタープライズ・サーバーのホスト名が分かっている必要があります。
    - [**証明書の公開キーを入力**]：このオプションは [**サーバーの指定**] を選択した場合に有効になります。

- 証明書の公開キーを持っており、この方法を選択した場合に**証明書の公開キー**を入力します。

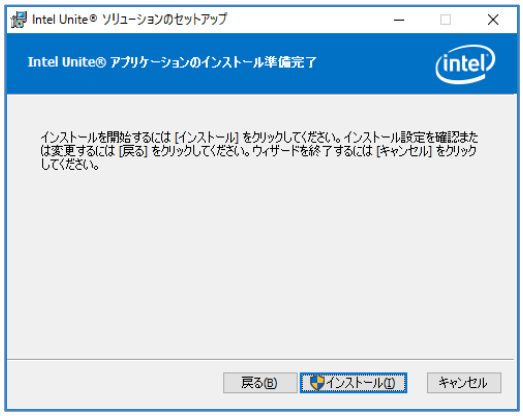
- いずれかを選択し、[**次へ**] をクリックして進みます。



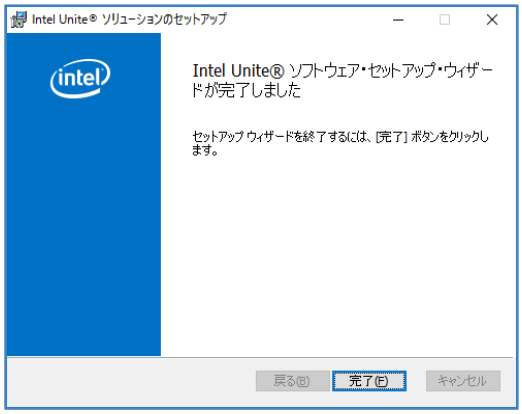
- [**インストール先フォルダー**] ウィンドウが開き、Intel Unite® アプリケーションがクライアントにインストールされるデフォルトのフォルダーが表示されます。インストール先フォルダーは、必要に応じて変更できますが、変更する必要がなければデフォルトの場所のままにします。



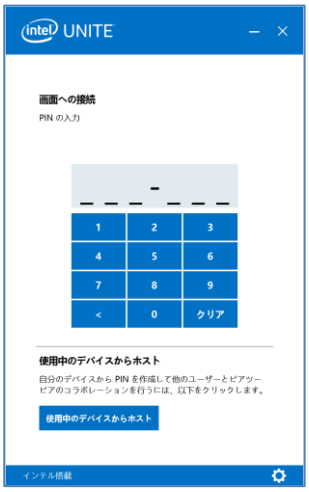
- 戻って設定を確認するか、[**インストール**] をクリックして進みます。



- インストールが終了すると、[**Intel Unite® ソフトウェア・セットアップ・ウィザードが完了しました**] ウィンドウが表示されるので、[**完了**] をクリックします。



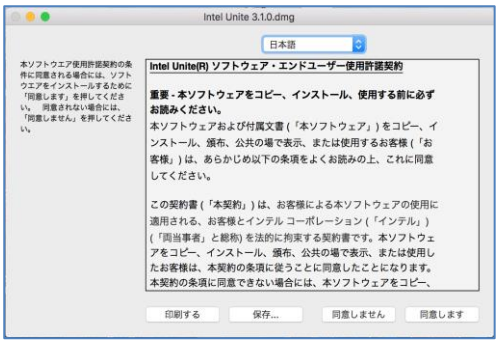
- 次の [**画面への接続**] ウィンドウが表示されます。



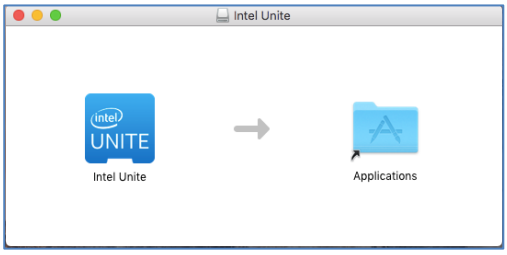
- ハブに接続するには、モニターまたは画面に表示された PIN を入力します。デフォルトでは、PIN は、5 分ごとに変更されます。
- 機能とユーザー情報について、詳しくは「**Intel Unite® ソリューション・ユーザー・ガイド**」を参照してください。

6.3 macOS* クライアントのインストール

- **Intel Unite macOS X,X.dmg** ファイルを探し、Mac* クライアントでソフトウェアをダウンロードします。ファイルをダブルクリックしてアプリケーションを展開します。
- [**エンドユーザー使用許諾契約書**] への同意を求めるプロンプトが表示されます。[**同意する**] をクリックして進めます。



- 展開したら、アプリケーション・フォルダーにドラッグ & ドロップします。



- アプリケーション・フォルダーに移動してアプリケーションを見つけたら、クリックして実行します。
- [**PIN の入力と画面への接続**] 画面が開きます。モニターまたは画面に表示された PIN を入力すると、ハブに接続して共有を開始します。

- 機能とユーザー情報について、詳しくは「**Intel Unite® ソリューション・ユーザー・ガイド**」を参照してください。

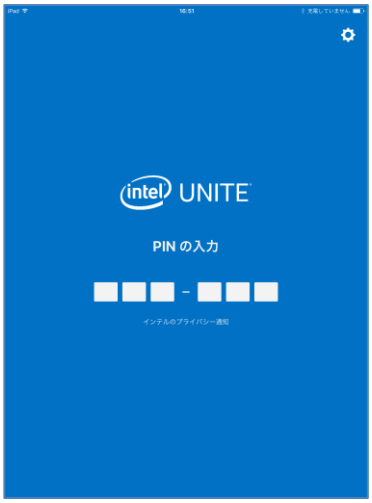
注：アプリケーションは DNS 自動検出 (DNS サービスレコード) を使用してエンタープライズ・サーバーを検索します。デフォルトのエンタープライズ・サーバーは、ユーザーの ~/Library/Preferences フォルダーにある com.intel.Intel-Unite.plist の設定を変更することで指定できます (defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD)。詳細については、このガイドの「*macOS* 用 Intel Unite®* ソリューション」セクションを参照してください。
アプリケーションが接続するエンタープライズ・サーバーを変更することも可能です。[**画面への接続**] の右下隅にあるギアのアイコンをクリックして [**設定**] にアクセスします。
次の 2 つのタブがあります。

[**一般**] ：名前、電子メールアドレス、ユーザーのアバターを入力できます。クライアント・マシンがエンタープライズ・サーバーに接続する場合に、自動で接続する (デフォルト) か、定義されたパスをサーバーに入力して接続するかを選択できます。
[**詳細設定**] : [**デバッグを有効にする**] か、[**信頼済み証明書**] のみ許可するかを選択できます。

6.4 iOS* クライアントのインストール

アプリは、初期の 2010 iPad* を除くすべての iPad* と互換性があります。

- iOS* クライアント (iPad* デバイスなど) で、Apple* App Store* に移動し、クライアント用の Intel Unite® ソフトウェアをダウンロードします。
- アプリのダウンロードが完了したら、アプリを開きます。
- 右上隅にあるギアのアイコンをクリックして [**設定**] にアクセスし、必要な情報を入力します。



- [**設定**] で [スクリーン名] とサーバー情報を入力します。
- サーバー検索では [**自動**] を選択できます。特定のサーバーにアクセスする場合は、[**手動**] をクリックして接続先のサーバーを入力します。
- [**保存**] をクリックします。
- モニターまたは画面に表示された PIN を入力すると、ハブに接続して共有を開始できます。
- 機能とユーザー情報について、詳しくは「**Intel Unite® ソリューション・ユーザー・ガイド**」を参照してください。

6.5 Android* クライアントのインストール

- Android* デバイスで、Google* アプリストアに移動し、クライアント用の Intel Unite® ソフトウェアをダウンロードします。
- アプリのダウンロードが完了したら、アプリを開きます。
- 右上隅にあるギアのアイコンをクリックして [**設定**] にアクセスし、必要な情報を入力します。

- [**設定**] で [スクリーン名] とサーバー情報を入力します。
- サーバー検索では [**自動**] を選択できます。特定のサーバーにアクセスする場合は、[**手動**] をクリックして接続先のサーバーを入力します。
- [**設定の保存**] をクリックします。

- モニターまたは画面に表示された PIN を入力すると、ハブに接続して共有を開始できます。
- 機能とユーザー情報について、詳しくは「**Intel Unite® ソリューション・ユーザー・ガイド**」を参照してください。

6.6 Chrome* OS クライアントのインストール

- Chromebook* デバイスで、Google* アプリストアに移動し、クライアント用の Intel Unite® ソフトウェアをダウンロードします。
- アプリのダウンロードが完了したら、アプリを開きます。
- 右上隅にあるギアのアイコンをクリックして [**設定**] にアクセスし、必要な情報を入力します。

- [**設定**] で [**スクリーン名**]、[**電子メール**]、サーバー情報を入力します。サーバー検索では [**自動**] を選択できます。特定のサーバーにアクセスする場合は、[**手動**] をクリックして接続先のサーバーを入力します。
- [**設定の保存**] をクリックします。

モニターまたは画面に表示された PIN を入力すると、ハブに接続して共有を開始できます。
機能とユーザー情報について、詳しくは「**Intel Unite® ソリューション・ユーザー・ガイド**」を参照してください。

6.7 クライアントの設定

クライアントの構成設定は、管理者ポータルから変更できます。管理者ポータルには、サーバーにチェックインしたすべてのクライアントに適用されるデフォルトの構成設定が記載されたデフォルトのプロファイルがあります。この設定オプションは、クライアントからエンタープライズ・サーバーへの接続が確立された後、クライアントに適用されます。設定は、クライアントがチェックインするたびに更新されます。
設定オプションの詳細については、プロファイルの設定を参照してください。

7 詳細インストール

7.1 スクリプト・インストーラー

このセクションでは、メニューやウィンドウを表示せずにサイレントモードでインストーラーを実行するための情報を示します。この方法では、コマンドラインでプロパティー・パラメーターがインストーラーに渡されます。

サイレント・インストーラーを実行するには、コマンドプロンプトを開いて、次のコマンドラインを使用します。

msiexec /i "クライアント MSI へのパス" PARAMETER=VALUE PARAMETER=VALUE … /qn /l* "ログへのパス"

- /i フラグはインストール用の指定された MSI です。「クライアント MSI へのパス」は、呼び出しているインストーラーのファイル名を指定します。
- 「PARAMETER=VALUE PARAMETER=VALUE …」は、以下の表に示すパラメーターのリストです。
- /qn フラグを指定すると、インストーラーがサイレントモードで実行されます。
- /l* フラグは、指定したログファイルにアウトプットを記録します。

注：msiexec /? コマンドを実行すると **msiexec** のすべてのオプションが表示されます。

各インストーラーに渡すことのできるプロパティー・パラメーターの全リストを以下に示します。

サーバーのインストール・パラメーター	説明
DBHOSTNAME = 「local」、「{IP}」、または「{サーバー},{ポート}」 (デフォルトは local)	Microsoft* SQL Server* のホスト名です。これが、インストーラーによって UniteServer データベースが作成され、データベースのサービスアカウントが追加される場所になります。データベースを使用中のマシンにインストールする場合は、このパラメーターを入力する必要はありません。デフォルトでローカルに設定されるためです。
DBLOGONTYPE = 「WinAccount」または「SqlAccount」 ・デフォルトは WinAccount	Microsoft* SQL Server にアクセスするためのログオンタイプを指定します。オプションは Windows 認証または SQL 認証です。
DBUSER = 「{SQL ユーザー名}」 DBPASSWORD = 「{SQL パスワード}」	ログオンタイプが SqlAccount の場合は、ユーザー名とパスワードを指定します。 注：このアカウントは、データベースを追加し、データベースのサービスアカウントを作成する権限を持っている必要があります。
DBLOGONPASSWORD = “{サービスアカウントのパスワード}”	このパスワードは、サービスアカウントが UniteServer データベースへ接続する際に使用されます。
DBLOGONPASSWORDCONF = “{サービスアカウントのパスワード}”	この変数は、DBLOGONPASSWORD で指定されている値と同じである必要があります。
サーバー機能の選択パラメーター	**説明**

ADDLOCAL = 「ALL」	オプションは 2 つのみです。ALL =データベースおよび PIN サーバー、管理者ポータル、およびダウンロード・ページをインストールします。 (この変数を指定しない場合) = PIN サーバー、管理者ポータル、およびダウンロード・ページをインストールします。
クライアントおよびハブのインストール・パラメーター	**説明**
PINSERVERLOOKUPTYPE = 「Lookup」または「Manual」 デフォルトは Lookup	アプリケーションによる PIN サーバーの検出方法を指定します。「Lookup」では DNS サービスレコードを使用し、「Manual」では PINSERVER のパラメーターを入力する必要があります。
PINSERVER = 「{ホスト名}」	接続先のサーバーのホスト名です。
CERTKEYCHECKED = 「1」または「0」 デフォルトは 0	このパラメーターはオプションです。 0 = 証明書キーのハッシュを確認しない 1= 証明書キーのハッシュを確認する。CERTKEY も指定する必要があります。
CERTKEY = 「{認証キー}」	このパラメーターはオプションです。 PIN サーバーの証明書の公開キーを入力します。
SHORTCUTS	オプションです。「1」に設定すると、デスクトップにショートカットのアイコンが表示されます。
INSTALLTYPE = 「Enterprise」と「StandAlone」の 2 つの値を使用できます。	INSTALLTYPE が「Enterprise」の場合、クライアント/ハブはエンタープライズとしてインストールされます。INSTALLTYPE が「StandAlone」の場合、クライアント/ハブはスタンドアロンとしてインストールされます。
SKIP_EXTENDED_DISPLAY = 「1」または「0」 デフォルトは 0	0 = 偽 1 = 真

7.2 レジストリー・キー

インストーラーやアプリケーションを実行すると、レジストリー・キーがレジストリーに書き込まれます。これらのキーの一部の値は、目的とする結果に応じて調整できます。Intel Unite® アプリケーションによって記述されたキーを理解するために、以下のリストを参照してください。

レジストリー・キー (現在のユーザー)	値	デバイス
HKEY_CURRENT_USER\software\Intel\Unite\ ActiveConnection (DWORD)	[0 = 接続しているユーザーなし 1= 接続しているユーザーが存在]	ハブ

HKEY_CURRENT_USER\software\Intel\Unite\ PublicKey (String)	[接続認証の公開キー]	両方
HKEY_CURRENT_USER\software\Intel\Unite\ CurrentPin (string)	[このシステムの現在の PIN]	ハブ
HKEY_CURRENT_USER\software\Intel\Unite\ DoNotShowPrivacyStatement (DWORD)	[0 = 起動時にプライバシー・ステートメントを表示 1 = プライバシー・ステートメントを表示しない]	両方
HKEY_CURRENT_USER\software\Intel\Unite\ HWThumbprint (String)	[ハードウェアのハッシュ]	両方
HKEY_CURRENT_USER\software\Intel\Unite\ ServicePort (DWORD)	[サービスがリッスンしているポート]	ハブ
HKEY_CURRENT_USER\software\Intel\Unite\ ActivePresenter	[1 = プレゼンテーション中のクライアントが存在 0 = プレゼンテーション中のクライアントなし]	ハブ
HKEY_CURRENT_USER\software\Intel\Unite\PinPadWindows (DWORD)	[1 = アプリケーションで PIN を入力する準備ができている 0 = それ以外の場合]	クライアント
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID 参照：ゲスト・アクセス・プラグイン・ガイド	デフォルト値に設定すると、ゲストアクセスでのセキュリティーが低下します。	ハブ
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK 参照：ゲスト・アクセス・プラグイン・ガイド	デフォルト値に設定すると、ゲストアクセスでのセキュリティーが低下します。	ハブ
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download 参照：ゲスト・アクセス・プラグイン・ガイド	デフォルトのダウンロード・リンクは http://192.168.173.1/download です。	ハブ

HKEY_CURRENT_USER\software\Intel\Unite\ShowAvToggle (DWORD) = 1 (A/V モード有効/無効の切り替え)	Win7 Aero* モード。ユーザーが RTF と WebRTC を切り替えることができるようにします。	クライアント
レジストリー・キー (マシン) :	**値**	**デバイス**
HKEY_LOCAL_MACHINE\software\Intel\Unite\ HubUnlockPassword (String)	[ハブ・アプリケーションを終了するためのパスワード]	ハブ
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableCheckCertificateChain (DWORD)	[自己署名入り証明書の場合に設定。1 = エンタープライズの証明書チェーンを確認しない (サーバー証明書)]	両方
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableUsageCollection (DWORD)	[1 = テレメトリデータの収集を無効にする]	両方
HKEY_LOCAL_MACHINE\software\Intel\Unite\WindowedMode (DWORD) (スモール・ビジネス・モードに限り使用可、エンタープライズ・モードでは機能しません)	[1 = ユーザーがハブをウィンドウモード (最小、最大、閉じるボタン) で起動する 0 = それ以外の場合]	ハブ
HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)	[1 = 証明書アルゴリズム・チェックをスキップする 0 = 強制的にエンタープライズ証明書を SHA2 証明書に使用する]	両方
HKEY_LOCAL_MACHINE\software\Intel\Unite\ ShowOnlyInOneMonitor (DWORD)	[このキーは、ウィンドウモードが 1 に設定されている場合にのみ機能します。 1= 複数のモニターが接続されている場合でも、1 つの PIN ウィンドウのみ表示]	ハブ

HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Unite\S4BPlugin Keywords (文字列) = コンマ,区切りの,キーワード,リスト	Skype* for Business 用プラグインに使用されるキー	ハブ
HKEY_LOCAL_MACHINE\software\Intel\Unite\ LogFile (String)	[実行時デバッグメッセージのログを記録するための書き込みアクセス権を持つファイル名へのパス]	両方

8 管理者ポータルガイド

管理者ポータルは、Intel Unite® アプリケーションがインストールされているデバイスを表示および管理できる、Intel Unite® アプリケーションの管理者用 Web ポータルです。これは、インストール時に PIN サービスと Web サーバーとともにエンタープライズ・サーバーにインストールされるコンポーネントの 1 つです。(「エンタープライズ・サーバーのインストール」のセクションを参照してください)。管理者ポータルがデータベースへのアクセス権を持っている場合、データベースと同じサーバー上にある必要はありません。

新機能に加え、管理者ポータルも新しくなりました。ハブおよびクライアント・デバイスの設定を行いやすくするため、ヘルプメニューおよび機能情報が追加されました。

- 管理者ポータルにアクセスするには、ブラウザーからポータルに割り当てられたリンクに移動します。リンクは https://<yourservername>/admin で、<yourservername> は Intel Unite® サーバーに割り当てられた名前です (デフォルトの名前 = UniteServer、https://uniteserver/admin)

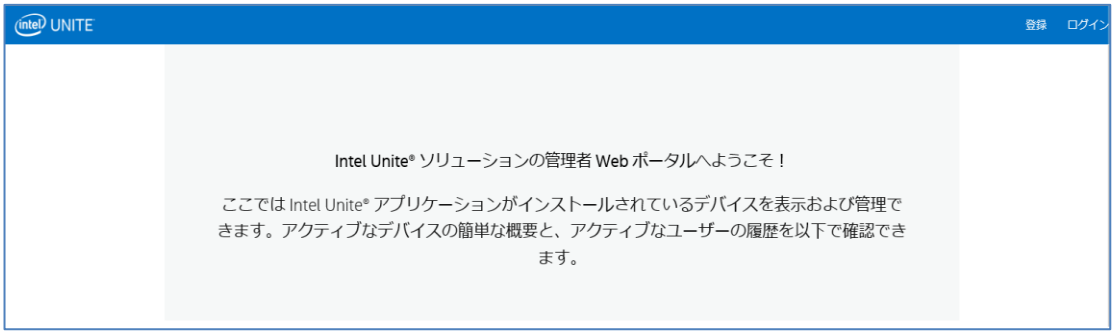
IT 管理者がソフトウェア・インストーラーを実行する場合、デフォルトの管理者アカウントは次のユーザー名とパスワードで作成されます。

- ユーザー：admin@server.com
- パスワード：Admin@1

このアカウントは、管理者ポータルへのフルアクセス権を持ちます。ログインはできますが、アカウントを変更するようシステムから指示されます。すでアカウントを登録している場合、そのログイン情報で管理者ポータルにアクセスしてください。

8.1 管理者 Web ポータルの「ようこそ」ページ

管理者ポータルにアクセスすると、「ようこそ」ページが最初に表示されます。ホームページにアクセスするには、インストール時に作成したデフォルトのアカウントもしくは自分のアカウント情報でログインする必要があります。



8.1.1 アカウントの登録

アカウントを登録するには、管理者ポータルからログアウトしていることを確認します。

- ナビゲーション・バーの右上にある [**登録**] リンクをクリックします。
- 使用する電子メールアドレスとパスワードをフォームに入力して、[**登録**] をクリックします。

- または、管理者ポータルにログインした後、[管理] タブからユーザーを追加または登録できます。

8.1.2 既存アカウントでのログイン

登録済みアカウント、もしくはインストール時に作成したデフォルトのアカウントでログインできます。このデフォルト・アカウントは管理者ポータルへのフルアクセス権を持つため、ポータルへのアクセスを制限するためにも、パスワードを変更することをお勧めします。

8.2 管理者ポータルのホームページ

ホームページには、「ようこそ」のメッセージが表示され、サーバーでチェックインした、すべてのアクティブなシステム (クライアントとハブ) の概要を確認できます。表には、各 [**システム**] の名前、各システムに割り当てられた [**プロファイル**]、[**オン**] または [**オフ**] のステータス、[**最終チェックイン**] の日付と時間が表示されます。

表の各項目は、複数のキーワードで検索ボックスを使用してフィルタリングすることができ、それぞれのキーワードによってすべての列が検索されます。このウィンドウでは、表示エントリー数の <数> をクリックして、表示するエントリーの数を選択できます。表字エントリー数は、10、25、50、100 から選択できます。

8.2.1 ナビゲーション・バー

ナビゲーション・バーから、Web ポータルの別の領域に移動することができます。また、現在ログインしているユーザーが表示され、ログインしているユーザーがいない場合は [**登録**] が表示されます。

Web ポータルには、次のページおよびサブページがあります。

- **デバイス**
- **グループ**
  - デバイスグループ
  - プロファイル
- **管理**
  - サーバーのプロパティー
  - ユーザー
  - 役割

- モデレーター
- 予約済み PIN
- テレメトリー

- **会議のスケジュール**

詳細については、管理者ポータルの本章で、各トピックに該当するセクションを参照してください。

8.2.2 アイコン / リンクの名称

管理者ポータル全体で、次のアイコンやリンクが頻繁に使用されています。

	編集
	詳細を表示
	デバイスの表示
	削除
	特定の値に関する情報を含むダイアログボックス

アイコン上にカーソルを置くと、該当する項目に関する情報を表示できます。

8.3 デバイスページ

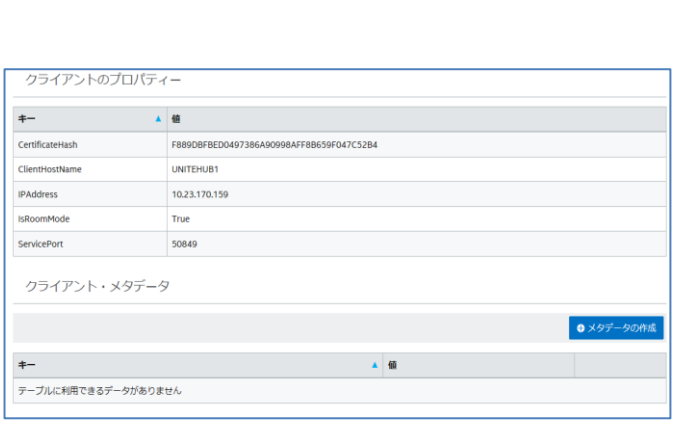
[デバイス] ページには、現在データベースに存在するすべてのデバイスが表示されます。特定のデバイスを選択して、[**表示**]、[**編集**]、[**更新**] または [**削除**] できます。

[**デバイス**] ページには、次の情報が表示されます。

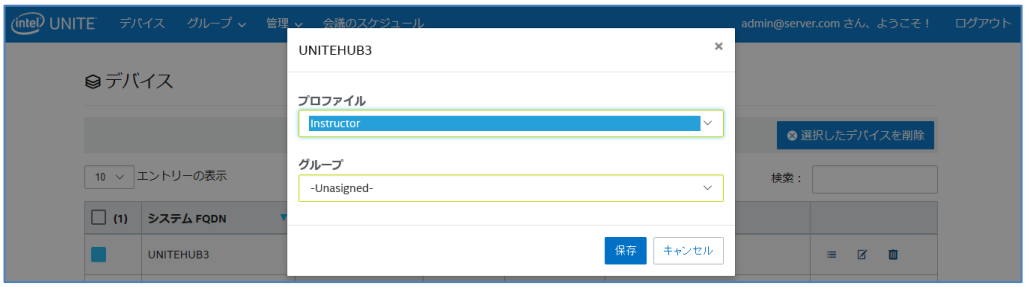
- [**システム FQDN**] はクライアント / ハブの完全修飾ドメイン名
- [**プロファイル**] はデバイスに適用される構成設定を表示
- [**グループ**] はデバイスが割り当てられたグループの名前
- [**ステータス**] はデバイスがアクティブ (オン、緑) か非アクティブ (オフ、グレー) かを表示
- [**最終チェックイン**] はデバイスがサーバーに最後にチェックインした時刻

- **[詳細]**：**[詳細を表示]** リンクをクリックすると、**[クライアントのプロパティー]** ウィンドウが表示され、システム・プロパティーやそのメタデータが表示されます。以下は **[クライアントのプロパティー]** に表示されるキーの一部です。
    - CertificateHash
    - ClientHostName
    - IPAddress
    - IsRoomMode
    - SevicePort

    各キーで使用できる有効な値について、詳しくは「プロファイルの設定」セクションのキー情報と対応する値を参照してください。



[編集] リンク - [編集] リンクをクリックして、デバイス・プロファイルの編集および特定グループへのデバイスの割り当てができます



[削除] リンク - [削除] リンクをクリックすると、管理者ポータルからデバイスが削除されます。デバイスが削除される前に、確認メッセージが表示されます。または、左端の列で 1 つ以上のデバイスを選択し、**[選択したデバイスを削除]** ボタンをクリックします。

8.4 グループページ

[**グループ**] ページのメニューには、[**デバイスグループ**] と [**プロファイル**] の 2 つのオプションがあります。

8.4.1 [グループ] > [デバイスグループ]

[デバイスグループ] は、デバイスを監視目的、機能性および利便性のためにまとめるのに使用できます。同じまたは異なるプロファイルを持つデバイスを 1 つのグループに割り当てることができます。このページでは、グループと、各グループの項目の作成、表示、編集、および削除ができます。[**グループの作成**] をクリックし、グループの名前を指定すると、新しいグループを作成できます。

グループを作成した後は以下を実行できます。

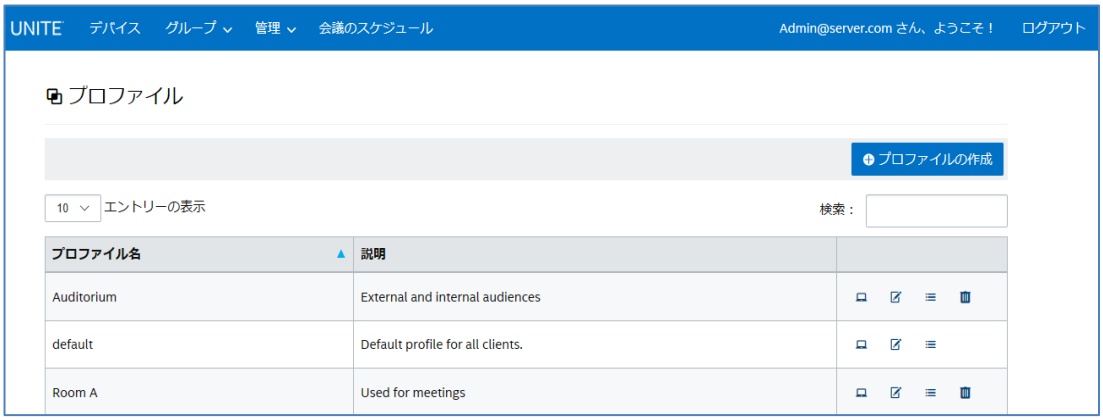
- [**デバイスの表示**] リンクをクリックし、選択したグループに対してデバイスを追加または削除できます。また、右端の列の [**詳細**] リンクをクリックし、そのグループに属する各システムのプロパティーとメタデータを表示できます。

- [**編集**] リンクをクリックし、[**グループ名**] を更新または変更できます。

- 変更した場合、[**保存**] をクリックして変更を保存してください。

8.4.2 [グループ] > [プロファイル]

このページでは、プロファイルの作成、表示、削除、および編集ができます。レイアウトと機能は [**デバイスグループ**] に似ていますが、ここにはプロファイルが含まれています。[**プロファイル**] と [**グループ**] の違いは、[プロファイル] にはデバイスの設定オプションが用意されている点です。デバイスが属することができるプロファイルは 1 つだけですが、複数のデバイスグループに属することができます。



[**プロファイル**] ページには、サーバーで使用できる各プロファイルの [**プロファイル名**] と [**説明**] が表示されます。プロファイルは、エンタープライズ・サーバーにチェックインするすべてのデバイスに適用されます。管理者ポータルにある [**デフォルト**] のプロファイルは削除できません。

[**デバイスの表示**] リンクをクリックすると、選択したプロファイルに割り当てられたシステムが表示されます。
[**編集**] リンクをクリックすると、プロファイル名と説明を更新できます。

特定のプロファイルの [**詳細を表示**] リンクをクリックすると、デフォルトまたは新規作成されたプロファイルのキーおよび値の設定にアクセスできます。それぞれのキー、値、更新またはカスタマイズ用の [**編集**] リンクを示すリストが表示されます。キーと対応する値の詳細については、「*プロファイルの設定*」を参照してください。

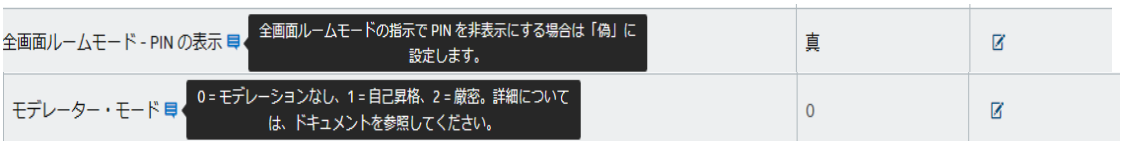
8.4.2.1 デフォルト・プロファイル

[**デフォルト**] プロファイルは、管理者ポータルから削除することはできませんが、別のプロファイルを作成できます。

[**デフォルト**] のキーと値：

キー	値	
ファイル転送を許可する	偽	
オーディオ/ビデオ・ストリーミングのサポート	真	
会議中に PIN を変更する	真	
リモートビューを無効にする	偽	
表示される PIN のサイズ	48	
表示される PIN の透明度	100	
ブロックするファイル拡張子		
最大ファイルサイズ	2147483647	
全画面ルームモード	真	
全画面ルームモード - 背景色		
全画面ルームモード - 背景画像の拡大	偽	
全画面ルームモード - 背景 URL		
全画面ルームモード - 指示	{pin}	
全画面ルームモード - PIN の色		
全画面ルームモード - PIN の表示	真	
全画面ルームモード - 文字の色		
全画面ルームモード - 文字のフォント		
ハブ - キーボードのロック	偽	
ハブ - 時計の表示	真	
モデレーター・モード	0	

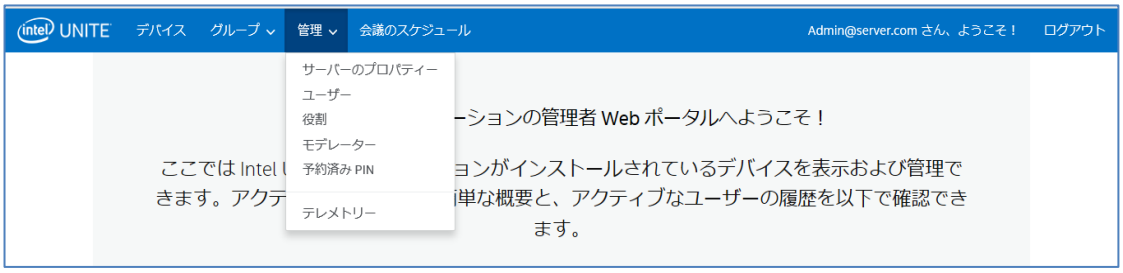
それぞれのキーの横にはダイアログボックスがあり、カーソルをそこに置くと、それぞれのキー値や情報が表示され、キーを編集する前に必要な情報を得ることができます。以下に 2 つの例を示します。



キーおよび対応する値の詳細については、「プロファイルの設定」の表を参照してください。

8.5 管理ページ

[管理] ページは、いくつかのサブページに分かれています。

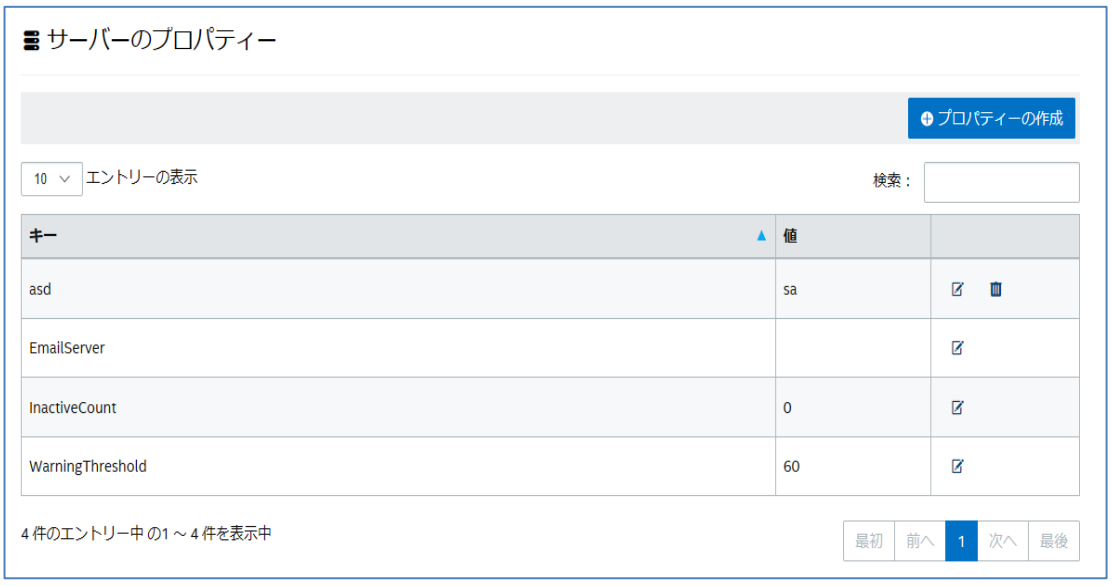


- **[サーバーのプロパティー]**：サーバーキーと値を表示および変更するインターフェイスです。
- **[ユーザー]**：このページでは、アカウントを追加、削除、および手動で編集することができます。
- **[役割]**：新しい役割の作成、既存の役割の更新、役割へのユーザーの割り当て、ユーザー管理権限の編集ができます。
- **[モデレーター]**：機能を役割にグループ化し、ユーザーが会議を制御できるようにします。このセクションでは、簡単にモデレーターを追加または削除できます。
- **[予約済み PIN]**：IT 管理者は、この機能を使用して部屋に PIN を割り当てることができます。PIN は自動生成できます。または、セッションの実施ニーズや部屋の場所に基づき、IT 管理者が手動で設定できます。
- **[テレメトリー]**：テレメトリー・データを表示するには、Intel Unite® ソリューション用のテレメトリー・プラグインをインストールする必要があります。テレメトリー・プラグインを使用すると、IT 管理者は Intel Unite® アプリケーションと、各ハブに接続されているクライアント・デバイスに関する情報を収集できます。

これらのサブページの詳細については、以下のセクションを参照してください。

8.5.1 [管理] > [サーバーのプロパティー]

このページでは、サーバーのキー値のペアを表示、作成、編集、および削除できます。



管理者ポータルでは、次のキーを使用しています。

- **EmailServer**：サーバーが通知を送る宛先の電子メールです。
- **InactiveCount**：Notifications の役割を持つユーザーへ電子メールを送る、Intel Unite® アプリケーションの状態監視ツールが使用します。
- **WarningThreshold**：デバイスが非アクティブと判断されるまでの分数のしきい値です。デフォルトの値は 60 分です。

[**編集**] リンクをクリックすると、キーを更新できます。

8.5.2 [管理] > [ユーザー]

[**ユーザー**] ページには、管理ポータルに登録されている全ユーザーのリスト、そのアカウントがロックされているかどうか、各ユーザーの役割が表示されます。この情報は、[**編集**] リンクをクリックして更新することもできます。

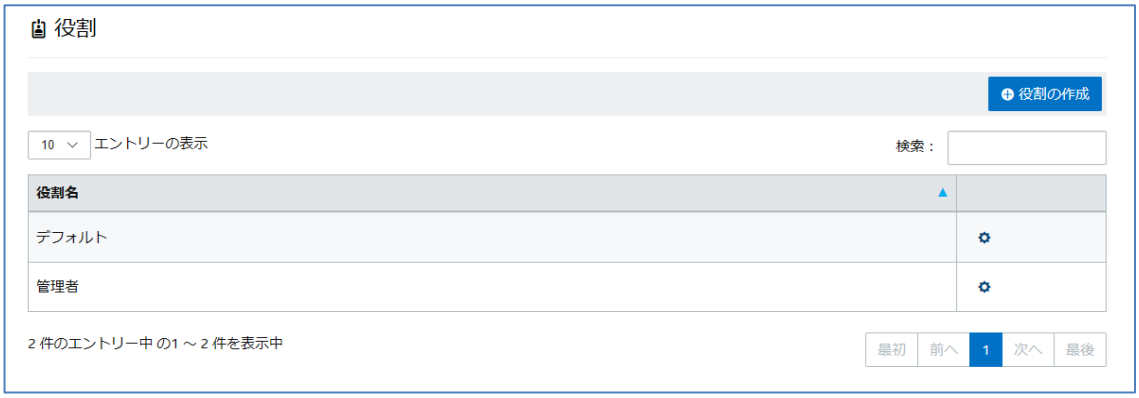
新規ユーザーを追加するには、[**ユーザーの作成**] をクリックし、電子メール、電話番号、パスワードを入力します。ユーザー作成時には、特定の役割を割り当てることができますが、そのままデフォルトの値を維持することもできます。新しいユーザーにアクセス権を割り当てるには、役割を定義し、ユーザーを役割に割り当てます。

同じページ上で役割 ([**デフォルト**] または [**管理者**]) をクリックすると、[**役割**] ページが開きます。[**役割**] の詳細については、このまま次のセクションに進んでください。

デフォルトのアカウントに関する注意事項：デフォルトの admin@server.com アカウントにログインして新しいアカウントを追加した場合、電子メール確認が自動的に送信されることはありません。電子メールアドレスを手動で確認するには、新しいアカウントにログインして、ナビゲーション・バーの右上にある [<ユーザー名> さん、ようこそ！] をクリックします。次に、ページの下部にある [**電子メール確認の送信**] ボタンをクリックします。この手順を実行する前に、web.config xml ファイルでサーバーのメール設定を編集する必要があります。「電子メールサーバーの設定」のセクションを参照してください。

8.5.3 [管理] > [役割]

このページには、現在定義されている [**管理者**] または [**デフォルト**] の役割が表示されます。新しい役割を追加したり、現在の役割を編集したりできます。役割を設定しても、ポータルに対するアクセスは制御されません。ただし、ポータルでの操作は、一連のユーザーに関連付けられている役割に応じて制限されます (ユーザーの作成など) 。



それぞれの役割に割り当てられたアクティビティーとアクセス権を表示するには、右端の列にあるギアのアイコンをクリックして [**アクセス許可**] ウィンドウを開きます。割り当てられたアクティビティーをカスタマイズして、役割のセットに特定の操作を許可することができます。

新しい役割を追加するには、[**役割の作成**] ボタンをクリックして役割名を編集します。その後、[**役割**] ページでギアのアイコンをクリックし、その役割が実行するアクティビティーを選択します。アクセス許可が追加または削除されます。
ユーザーには複数の役割が割り当てられる場合があることに注意してください。

8.5.4 [管理] > [モデレーター]

このページには、モデレーターの役割を割り当てられたユーザーが表示されます。ユーザーにモデレーターを割り当てるには、いくつかの操作を行う必要があります。

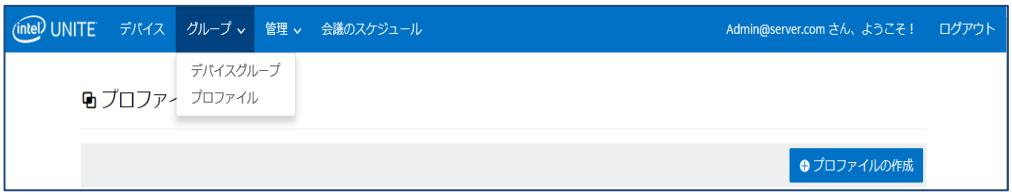
モデレーターを追加する方法は 2 つあります。[**モデレーターの追加**] をクリックし、必要な情報を入力します。または、[**CSV からモデレーターをインポート**] をクリックし、リストに追加する名前と対応する電子メールの CSV ファイルをインポートします。モデレーターの名前を含む CSV ファイルのインポートを選択した場合、フォーマットに気を付けてください。正しいフォーマットは「**名前,電子メール,操作**」です。[**サンプルファイル**] をクリックすると、有効なフォーマットが表示されます。

例： John Smith,jsmith@aaa.com,Add
Sandra Leon,sleon@bbb.com,Delete

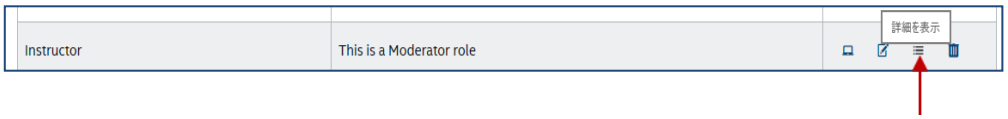
手動でモデレーターの [**名前**] と [**電子メール**] を入力する場合は、[**モデレーターの追加**] をクリックして入力し、[**保存**] をクリックします。

システム上で環境を混在させるため、ハブのプロファイルでモデレーター機能のモードを設定する必要があります。引き続き次の操作を行ってください。

- [**グループ**] ページで [**プロファイル**] を選択し、[**プロファイルの作成**] をクリックします。ウィンドウが開いたら [プロファイル] の名前と説明を入力します。



- 作成したプロファイルをリスト上で見つけ、右端の列に表示されている [詳細を表示] をクリックします。



- [**キー**] 列に表示される [**モデレーター・モード**] キーで、プロファイルに適用するモードの [**値**] を入力します。有効な値は次のとおりです。

モデレーターの説明と値：

0- **非管理**：デフォルトのモードです。会議やセッションにモデレーターはいません。参加者は全員、同等の閲覧およびプレゼンテーションの権利を持ちます。前のバージョンの Intel Unite® ソフトウェア (v3.1 以前) が使用したモードです。

1- **自己昇格**：誰かが自分自身をモデレーターに昇格させるまで、会議やセッションは管理されません。このモードでは、他の参加者にモデレーターを割り当てられるのはモデレーターだけです。モデレーターは、誰がセッション中にプレゼンテーションを行うかについても割り当てることができます。

2- **厳密**：割り当てられたモデレーターのみが会議やセッションを管理します。モデレーターがセッションに参加すると、自動的にこの役割に昇格されます。

注：

a. モデレーターのリストは、管理者ポータルから IT 管理者が管理します。モデレーターは、自分の電子メールアドレスに関連付けられたキーの使用を認証されています。ユーザーがモデレーターに昇格すると、管理者ポータルは URI が記載された電子メールを送信します。この URI をクリックすると、クライアントにモデレーターのトークンがインストールされます。ユーザーがこのプロセスを実行しなければならないのは、各システムにつき 1 回だけです。

b. IT 管理者は、管理者ポータルからユーザーのトークンを削除することで、モデレーターの権利を取り消すことができます。

c. モデレーターに登録用の電子メールを送信する場合、IT 管理者が SMTP リレーを設定しなければ正しく機能しません。

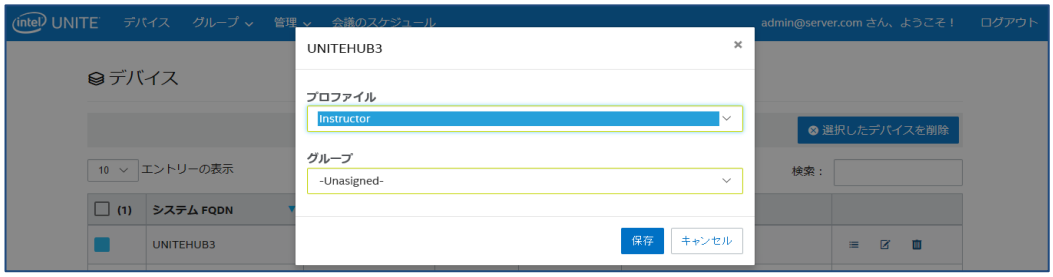
d. SMTP リレーがなく、電子メールで送信する URI を手動で生成する場合、次の操作を行います。

[**管理**] タブに移動し、[**サーバーのプロパティー**] を選択します。[**EmailServer**] の横にある [**編集**] リンクをクリックし、SMTP リレー (例：smtp.example.com:22) を入力します。

認証が必要ない SMTP リレーのみ設定可能です。ユーザーのモデレーター・トークンの取得と手動インストールも可能です。詳細は、「**厳密モードでのトークンの手動インストール**」セクションを参照してください。

- 選択したハブでモデレーターのプロファイルを有効にするには、[**デバイス**] ページに移動し、設定するハブをリストから選択します。次に右端の列に表示される [**編集**] リンクをクリックします。

- ウィンドウが開いたら、[プロファイル] セクションでモデレーター用に作成したプロファイルと、該当する場合は所属するグループを選択し、[**保存**] をクリックします。



モデレーター・リストに入力した後は、選択して (ブルーボックス) [**削除**] をクリックすると削除できます。モデレーターに、会議やセッションにモデレーターとして参加するための URL を送信するには、名前を選択して [**トークンの送信**] をクリックします。

8.5.4.1 厳密モードでのトークンの手動インストール

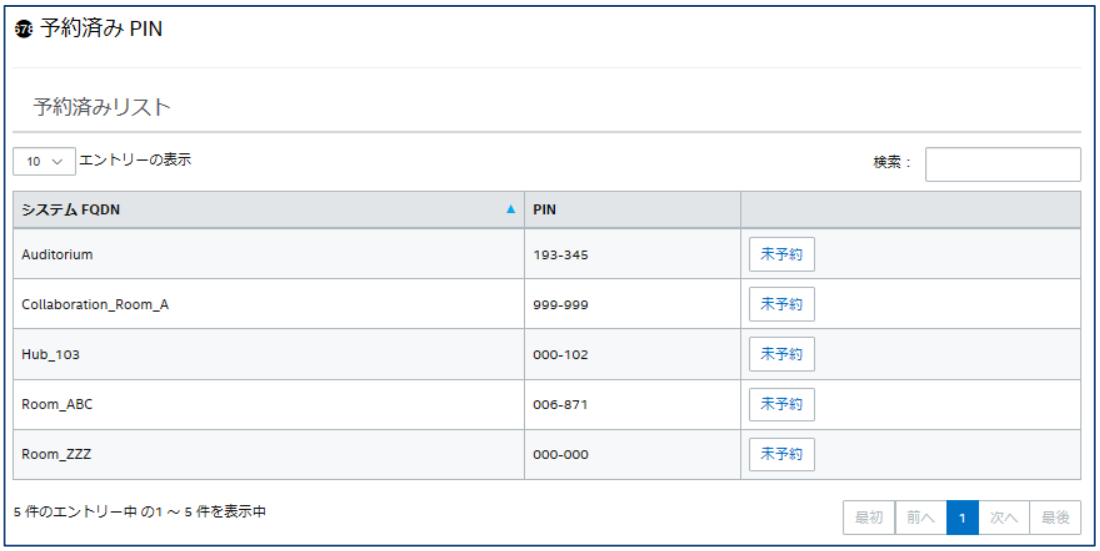
SMTP リレーがない場合、モデレーターとして追加されているユーザー用にモデレーター・トークンを取得し、手動でインストールできます。その場合、Microsoft* SQL Server* Management Studio をインストールする必要があります。
トークンの取得方法：

- モデレーターを追加します
- Microsoft* SQL Server* Management Studio を起動し、エンタープライズ・サーバーのインストール時に使用した管理者資格でデータベース・サーバーに接続します
- [Databases (データベース)]、[UniteServer]、[Tables (テーブル)] の順に展開します
- [dbo.Moderators] を右クリックし、[Select Top 1000 (上位 1000 を選択)] をクリックします
- 表示された結果から、前の操作で追加したものと一致するユーザー名を見つけます
- トークンを右クリックしてクリップボードにコピーします
- メモ帳を開き、URI を作成します。intelunite://localhost/SetModerationToken?Token=<前の操作で取得したトークンをペーストする>
- Intel Unite® の起動
- Windows* デバイスの場合： Internet Explorer* を開き、フル URI をコピー/貼り付けして Enter キーを押します
- Mac* デバイスの場合： Safari* を開き、完全 URI をコピー/貼り付けして Enter キーを押します

8.5.5 [管理] > [予約済み PIN]

このページには 2 つのセクションがあります。システムの [**予約済み**] と [**未予約**] のリストで、会議やセッション中に表示される PIN が静的か否かを示します。IT 管理者は、選択された部屋にシステムを割り当てることができます。ユーザーは、会議やセッションで同じ PIN を入力するか、デフォルト値であるローテーション PIN を使用します。

- [**予約済みリスト**] - IT 管理者がすでに設定している予約リストです。[**未予約**] をクリックすると、割り当てを解除できます。

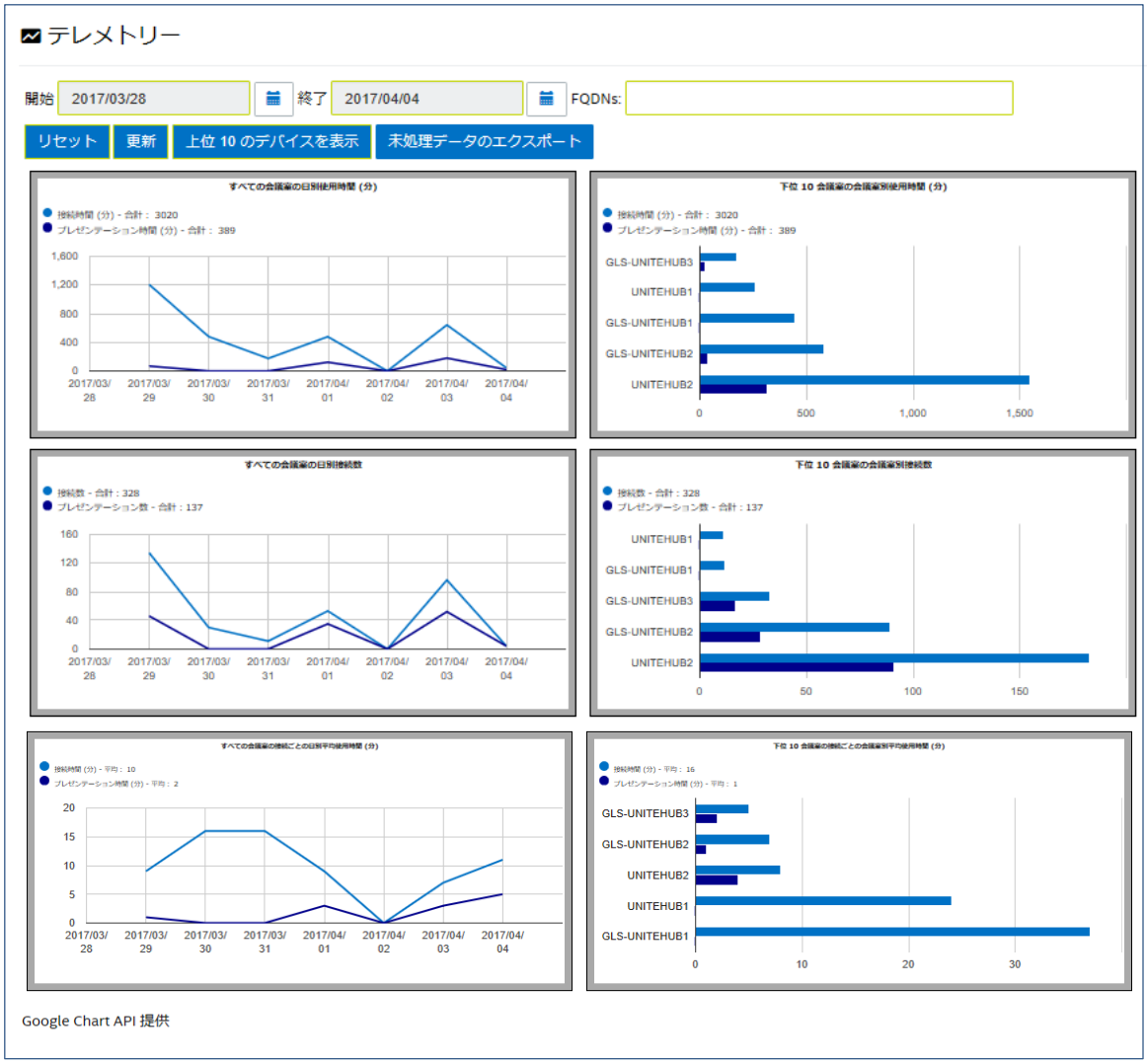


- [**未予約リスト**] - 静的 PIN による予約がないシステムのリストです。PIN は、手動入力、自動生成、CSV ファイルでのインポートができます。

PIN を割り当てたら、[**保存**] をクリックして値を保持します。

8.5.6 [管理] > [テレメトリー]

このページには、管理者ポータルが収集したテレメトリー・データが表示されます。データを表示するには、Intel Unite® ソリューション対応のテレメトリー・プラグインをインストールする必要があります。テレメトリー・プラグインを使用すると、IT 管理者は Intel Unite® アプリケーションと、各ハブに接続されているクライアント・デバイスに関する情報を収集できます。IT 管理者は、各会議室の接続数、日別接続数、接続ごとの平均使用時間などの情報を表示できます。プラグインの展開方法を含む詳細については、「**Intel Unite® テレメトリー・プラグイン・ガイド**」を参照してください。



8.6 会議のスケジュール・ページ

会議のスケジュール・ページは、既存の Microsoft* Office 対応 Intel Unite® プラグインをインストールまたは使用できない参加者のために、会議やセッションの URL を作成する機能です。参加者ならだれでもこのページを表示できます。

[**新しい会議の生成**] ボタンをクリックして URL を作成し、会議またはセッションに参加するユーザーに送信します。

8.7 管理者ポータルのその他の設定オプション

8.7.1 プロファイルの設定

プロファイルを設定するには、[**グループ**] > [**プロファイル**] にアクセスし、管理者ポータルでプロファイルの [**詳細**] をクリックします。これにより、「キー値」のペアの形式で構成設定が表示されます。値を変更して、アプリケーションや会議およびセッション場所の使い勝手をカスタマイズできます。例えば、ハブ・ディスプレイの背景画像、PIN サイズ、フォントの色およびコンテンツなどは、カスタマイズが可能な設定です。
プロファイル内の値をカスタマイズした後にプロファイルの構成設定を適用するには、プロファイルにデバイスを割り当てます。デバイスにプロファイルを適用するには、[**デバイスの表示**] リンクをクリックし、次に [**デバイスリストの更新**] をクリックします。デバイスのリストが表示されたら、デバイスの横にあるチェックボックスをオンにして構成設定を適用します。

次の表に、使用可能な**キー**とその説明、およびキーのデータ型とデフォルト値を示します。

キー	説明	データ型	デフォルト値
ファイル転送を許可する	ハブまたはクライアントのファイル転送機能の有効/無効を切り替えるフラグ	ブーリアン	真
オーディオ/ビデオ・ストリーミングのサポート	Windows* ユーザーが最高の A/V (1080p、20 ~ 30fps) でデスクトップをプレゼンテーションする機能の有効/無効を切り替えるフラグ	ブーリアン	偽

会議中に PIN を変更する	会議またはセッションの PIN をロックします。全ユーザーが接続を切断するまで、PIN は変更されません。 真 = セッション中に PIN を変更できます 偽 = セッション中は PIN がロックされます	ブーリアン	真
リモートビューを無効にする	特定の部屋からのリモートビューを無効化する機能です。設定されている場合、ユーザーがリモートビューを使用してコンテンツを表示しようとすると、使用不可を示すイメージが表示されます 真 = リモートビューを無効にする 偽 = リモートビューを許可する	ブーリアン	偽
表示される PIN のサイズ	ピクセル単位でのサイズ。この値は、画面上の PIN の高さ (ピクセル単位) を表します。大きな値を指定すると、部屋の端からでも PIN を読みやすくなります。	整数	48
表示される PIN の透明度	モニターに表示された PIN のアルファ透明度を制御します 100 = 100% 見えます 1-99 = 周囲の枠と PIN が見え、使用する値により不透明度は変化します 0 = PIN は透明で見えません	整数	100
ブロックするファイル拡張子として表示されるファイルブロック拡張子	ブロックするファイル拡張子のコンマ区切りリスト (exe、bin、msi など)	文字列	空白
ファイルの最大サイズとして表示される最大ファイルサイズ	転送可能なファイルの最大サイズ	整数	2147483647 バイト (有効範囲：0 ~ 2147483647)
全画面ルームモード	ハブの全画面表示を有効/無効にします。 偽：右上隅にのみ PIN が表示されます。 真：右上と全画面表示の背景に PIN が表示されます。	ブーリアン	偽
全画面ルームモード - 背景色	ハブで使用される背景色。HTML の色 (16 進の色) 。 有効な値の例 (RGB 値。形式 #000000) は次のとおりです。	文字列	空白 (黒で表示)

	赤：#FF0000 黄色：#FFFF00 緑：#00FF00 ライトブルー：#00FFFF ダークブルー：#0000FF 黒：#000000 白：#FFFFFF グレー：#808080		
全画面ルームモード - 背景画像の拡大	背景画像が画面全体に拡大されるように設定するフラグ	ブーリアン	偽
全画面ルームモード - 背景 URL	ハブの背景を、指定した URL または画像 (jpg/png) に設定します。この機能を有効にするには、値を「真」に設定します。 例： http://myserver.com/background.jpg	文字列	空白
全画面ルームモード - 指示	ハブに表示するテキスト指示です。代わりに、{PIN} および {ホスト} を使用できます。 クライアントをダウンロードするための URL です。この項目は、全画面ルームモード画面に表示されます。	文字列	{pin}
全画面ルームモード - ピンの色	表示される PIN の色	文字列	空白 (白で表示)
全画面ルームモード - ピンの表示	指示を表示します。この機能を有効にするには、値を「真」に設定します。	ブーリアン	偽
全画面ルームモード - 文字の色	ハブに表示されるテキストの色	文字列	空白 (白で表示)
全画面ルームモード - 文字のフォント	指示のフォント名	文字列	空白
ハブ - キーボードのロック	ハブの Ctrl + Esc、Alt + Tab、チャームバー、Windows キー、および Alt + F4 をロックアウトします。 「真」に設定すると、ハブのロックアウトが有効になります。レジストリー・キー・マシン (レジストリー・キー値) で設定したパスワードで上書きすることができます。	ブーリアン	偽
ハブ - 時計の表示	右下隅にクロックを表示します。	ブーリアン	真

モデレーター・モード	ミーティングやセッションへのモデレーター・モードの割り当て、次の値を使用 0 = モデレーションなし 1 = 自己昇格 2 = 厳密	整数	0
エラー電子メールアドレスの送信	ハブがエラーメッセージを送信する電子メールアドレスを割り当てます	文字列	空白 (白で表示)
サービス・リッスン・ポート	ハブが着信接続をリッスンするポートを割り当てます。	整数	0 (0 = 自動割り当てポート)
タイル圧縮	AV 以外のコンテンツの共有で圧縮率を調整できます。ネットワークを介して送信される、ディスプレイ (タイル) の変更部分に適用される圧縮率 (%) です。 (値を高く設定するほど、より大きな帯域幅が使用されます)	整数	85 (有効範囲：5 ~ 100)
タイルサイズ	AV 以外のコンテンツの共有でタイルサイズを調整できます。画面を分割する際のタイルサイズ。各タイルのサイズ (ピクセル単位) です。	整数	128 (有効範囲：32 ~ 512)
プラグイン証明書ハッシュの確認	プラグインの検証が必要 真 = 証明書ハッシュを検証する 偽 = 証明書ハッシュを検証しない	ブーリアン	真

8.7.2 PIN の更新間隔

デフォルトの PIN の更新間隔は 5 分です。つまり、ハブに表示される PIN は 5 分ごとに変化します。Web サービスサイトの仮想ディレクトリーのルートにある **web.config** ファイルを修正することにより、この値は 1 分単位で 2 ~ 60 分に変更できます。ここには IIS マネージャでアクセスできます。このファイルは、Intel Unite\PinServer ディレクトリーに移動してアクセスすることができます。デフォルトでは、このファイルは C:\Program Files (x86)\Intel\Intel Unite\PinServer にインストールされています。
<add key="**PinExpireTimeInMinutes**" value="5"></add> タグで、値を目的の更新間隔に変更します。

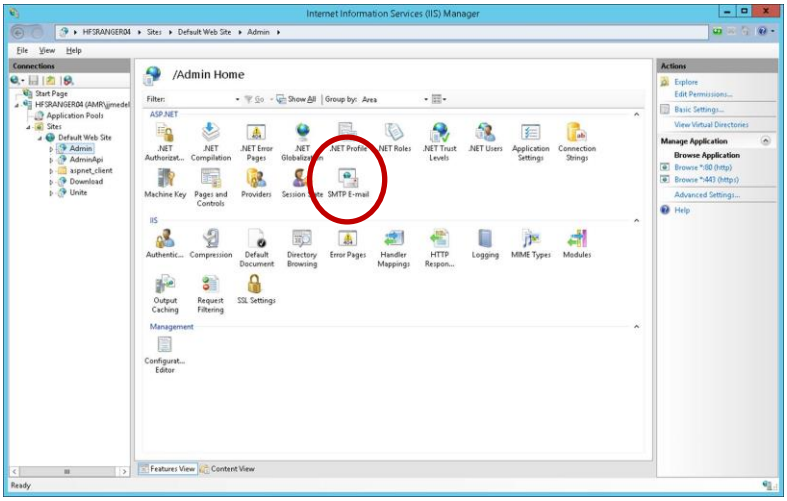
8.7.3 電子メールサーバーの設定

管理者ポータルでは、Intel Unite® アプリケーションをサーバーにインストールしたときに作成される web.config xml ファイル内の SMTP サーバーを定義できます。SMTP サーバーが設定されている場所によっては、**mailSettings** を「ホスト」が SMTP サーバーを示すように web.config xml ファイル内で変更する必要があります。(デフォルトでは、Web.config xml ファイルは C:\Program Files (x86)\Intel\Intel Unite\PinServer にあります。)

SMTP 電子メールサーバーが IIS で設定されていること、エンタープライズ・サーバーのプリインストール時にアプリケーションと適合する正しい設定であることを確認してください。

このファイルの設定は次のとおりです。

```
<mailSettings>
    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />
    </smtp>
</mailSettings>
```



8.7.4 警告と監視

エンタープライズ・サーバーは、警告と監視サービスを提供します。これは選択的なサービスで、管理者ポータルで設定されます。

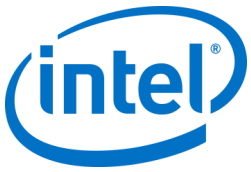
警告に設定されたデバイスは監視され、デバイスが警告のしきい値以内にチェックインしなかった場合、指定されたユーザーに電子メールが送信されます。

非アクティブなデバイスに関する電子メールを受信するように選択するには、管理者ポータルでユーザーに [**Notifications**] の役割が割り当てられていることを確認します。クライアントを監視するように選択するには、**EnableReporting** キーをそのメタデータに追加し、値を [**真**] に設定します。

警告のしきい値は、[**管理**] > [**サーバーのプロパティー**] で設定します。デフォルトは 60 分です。

[**InactiveCount**]：次のチェックですぐに電子メールを受け取る場合は、小さい数値を設定する必要があります。

電子メールアドレス (smtp from) と電子メールサーバー (host) を、/productfiles/release/clocktower.exe.config にある **clocktower.exe.config** ファイルで指定する必要があり



ます。(デフォルトでは、clocktower.exe xml config ファイルは C:\Program Files (x86)\Intel\Intel Unite\ClockTower にあります。)

このファイルの設定は次のとおりです。

```
<mailSettings>
    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />
    </smtp>
</mailSettings>
```

9 OS および PC のセキュリティー・コントロール

9.1.1 最小セキュリティー標準 (MSS)

Intel Unite® アプリケーションを実行しているすべてのデバイスが、組織のデフォルトの MSS 規格を満たしているようにすることをお勧めします。また、パッチ用にエージェントをインストールし、MSS 仕様に従って、ウイルス対策/IPS/IDS ソフトウェアおよび他の必要なコントロールをインストールすることをお勧めします。McAfee スイートのマルウェア対策、IPS、IDS 機能の互換性についてはテスト済みです。

9.1.2 マシンの強化

Windows* のブートローダーのみを起動するために、マシンの Unified Extensible Firmware Interface (UEFI) がロックされている可能性があります (この場合、USB ディスクや DVD から起動しようとしても機能しません)。エグゼキュート・ディスエーブル・ビットを有効にし、インテル® トラステッド・エグゼキューション・テクノロジーを有効にして、設定をパスワードでロックできます。

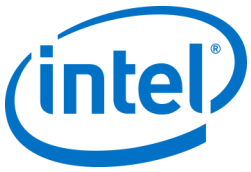
Windows* OS の強化：ベースラインとして、システムは昇格されていないユーザー権限で実行されます。また、不要なプレインストール・ソフトウェアや不要な Windows* コンポーネント (PowerShell*、印刷サービス、ドキュメント・サービス、Windows* 位置情報取得機能、XPS サービス) を含む、未使用のソフトウェアを OS から削除することをお勧めします。

GUI サブシステムのロック：システムでは、キーボードやマウスのない非タッチパネル・スクリーンのみが使用されるため、GUI サブシステムから侵入しにくくなっています。攻撃者からの HID デバイス (USB キーボード/マウス) への接続を防ぐため、**Alt + Tab**、**Ctrl + Shift + Esc**、および**チャームバー**の使用はプログラムでブロックされています。

9.1.3 他のセキュリティー・コントロール

マシンのユーザーアカウントを、Active Directory で特定のマシンアカウントごとにロックすることをお勧めします。多数のユニットを使用して展開する場合、ユーザーアカウントは、特定の建物のフロアごとにロックすることができます。

マシンの所有権：各マシンには、所有者を指定することをお勧めします。マシンが長期間オフラインになった場合、指定された所有者に通知されます。
インテル® vPro™ プラットフォームおよび Intel Unite® ソフトウェア自体が提供するセキュリティー・メカニズム以外に、Microsoft* のマシンの強化に関するガイドラインに従って Microsoft* Windows* OS を強化することをお勧めします。詳細は、以下のリンクの Microsoft Security Compliance Manager (SCM) を参照してください。https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx



注：このリンクの情報には、最もよく知られている方法の強化と関連ドキュメントを含むウィザードベースの強化ツールが含まれています。

10 メンテナンス

組織と IT 管理者は、定期的なメンテナンス・プログラムを決定します。次のメンテナンス・タスクを実行することをお勧めします。

10.1 夜間再起動

ハブは毎日 (夜間を推奨) 再起動することをお勧めします。再起動の前に、キャッシュされた一時ファイルの消去や標準のパッチ手順の開始といったメンテナンス・タスクを実行します。

10.2 パッチ適用方針

可能な場合は前述のように、マシンを夜間に再起動する前に、標準のパッチメカニズムを可能な限り無人モード (GUI プロンプト表示なし) で実行します。

10.3 レポーティング

マシンの稼働時間インジケーターを収集し、組織のニーズに合ったレポートを作成します。

10.4 監視

マシンのハートビートに基づいた状態追跡システムを使用し、必要に応じてバックエンドの稼働時間を分析します。

10.4.1 バックエンドの監視

標準の仮想サーバー監視ツールを使用して警告を生成し、2 次レベルサポートに送信します。

11 macOS* 用 Intel Unite® ソリューション

11.1 背景

macOS* 用 Intel Unite® ソフトウェアは、主要なアプリのパッケージとしてパッケージングされており、IT 固有のプリファレンス値を活用できます。そのために、本アプリは、一般的な Mac* の管理ソフトウェアや技術から、手動インストールや環境設定まで、共通の展開の多くをサポートします。

11.2 一般的な接続のワークフロー

デフォルトでは、本アプリは、接続先として適切なエンタープライズ・サーバーを決定する際に DNS 自動検出 (例えば、DNS SRV レコード) を使用します。全体的なワークフローは次のとおりです。

- (オプション) プリファレンスで定義されたエンタープライズ・サーバー
- 以下のドメインへの自動検出：
  - _uniteservice._tcp
  - _uniteservice._tcp.yourSubDomain.yourDomain.yourTLD
    i. 例：_uniteservice._tcp.corp.acme.com
  - _uniteservice._tcp.yourDomain.yourTLD
    i. 例：_uniteservice._tcp.acme.com
  - HTTP への接続が失敗した場合に、続いて HTTPS への接続を試行
- uniteservice.yourDomain.yourTLD

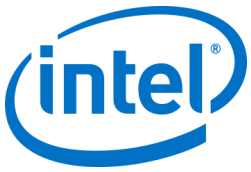
11.3 プリファレンス値

IT 部門は、各ユーザーの ~/Library/Preferences フォルダーにある com.intel.Intel-Unite.plist で次の設定を行うことで、独自のインフラやセキュリティーのニーズを満たすために、Intel Unite® アプリを変更しカスタマイズすることができます。

- **デフォルトのエンタープライズ・サーバーを定義**
  defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD
- **証明書のピン留めのための、エンタープライズ・サーバーの公開キーを定義**
  defaults write com.intel.Intel-Unite EnterpriseServerPublicKey "公開キーの文字列"
- **信頼済みサーバー証明書のみを許可するようにクライアントを強制**
  defaults write com.intel.Intel-Unite ClientOnlyAllowsTrustedCertificates -bool true
- **スタンドアロン・モードで接続するようにクライアントを強制**
  defaults write com.intel.Intel-Unite Standalone -bool true

これらの各設定は、macOS* ターミナル (/Applications/Utilities) を開き、コマンドを入力しリターンキーを押すことで、手動で設定または変更できます。各コマンドのディスカッションおよび詳細は次のとおりです。

- **デフォルトのエンタープライズ・サーバーを定義**



デフォルトのエンタープライズ・サーバーを設定すると、実行している自動検出プロセスを停止します。これは、お使いの Mac* クライアントが唯一独自のネットワーク上に存在する場合に、セキュリティー上の理由やトラブルシューティングのために特定のエンタープライズ・サーバーに Intel Unite® アプリを「ピン留め」するための、便利な設定になります。

- **証明書のピン留めのための、エンタープライズ・サーバーの公開キーを定義**
  エンタープライズ・サーバーにクライアント・アプリケーションを「ピン留め」する場合は、自動検出が使用されているかどうかに関係なく、各クライアントで「公開キーの文字列」を設定することで行えます。この値を取得するには、次の操作を行います。
  - 社内ネットワーク上のいずれかの Mac* で Safari* を開きます。
  - エンタープライズ・サーバーの HTTPS アドレスに移動します。
  - アドレスバーのロックアイコンをクリックします。
  - 証明書シートで [**証明書を表示**] ボタンをクリックします。
  - [**詳細**] の三角ボタンをクリックして展開します。
  - [**公開キー情報**] > [**公開キー**] フィールドが見つかるまで証明書データを下にスクロールします。
  - 「256 bytes:」で始まるデータフィールドをクリックします。
  - データフィールドが展開されます。
  - マウスで選択するか CMD + A で、フィールド内のすべてのデータを選択します。
  - コンテキスト・メニューからデータを [**コピー**] または **CMD + C** で選択して、クリップボードにコピーします。
  - デフォルト・コマンドで、[**公開キーの文字列**] をクリップボードのデータで置き換えます。注：二重引用符でデータを囲む必要があります。

  デフォルトのエンタープライズ・サーバーを定義する場合と同様に、このオプションを設定すると、他のパートナー/場所で他の Intel Unite® ソリューションのインストールへユーザーベースで接続することが困難になります。

- **信頼済みサーバー証明書のみを許可するようにクライアントを強制**
  特定のエンタープライズ・サーバーを定義したり、証明書の公開キーをピン留めしたりする以外に、Intel Unite® アプリが証明書の信頼チェーンで完全に許可されているサーバー/証明書のみへ接続するように命じることもできます。この場合、エンタープライズ・サーバー証明書がキーチェーンで Apple* が定義した公開ルートサーバーをフォローバックしているか、独自のルートサーバー証明書と各クライアントで必要な任意の中間証明書をインストールしていることを確認する必要があります。

- **スタンドアロン・モードで接続するようにクライアントを強制**
  このモードを設定すると、エンタープライズ・サーバーのない環境で PIN を生成しているハブの、UDP 自動検出を実行するための接続ワークフローが変更されます。この状態では、インテル® Core™ vPro™ プロセッサーを搭載したシステムはプライマリホストとして動作し、エンタープライズ・サーバーのインフラをインストールする IT 部門を持たない中小ビジネス環境にとって便利です。このモードは、UDP パケットがブロックされていない、同じサブネット上の各システムでのみ動作します。

11.4 一般的な配布方法

自動検出を使用している場合、配布は、アプリケーション・フォルダーに Intel Unite® アプリケーションをドラッグするのと同じくらい簡単に行うことができます。より複雑な、または追加のセキュリティー設定を必要とする環境では、アプリのパッケージの配布と組み合わせて特定の設定を行うこともできます。これを行うにはさまざまな方法がありますが、ここでは、より一般的な方法の一部を紹介します。

- バッシュスクリプト
  - バッシュスクリプトでお好みの設定を定義でき、アプリケーション・パッケージと組み合わせてユーザーに配布することができます。
- PackageMaker を介したカスタム・インストール・パッケージ
  - preflight または postflight スクリプトを介してお好みの設定を定義することができます。
- Apple Remote Desktop を介したカスタム・インストール
  - Apple Remote Desktop を使用すると、Intel Unite® アプリのパッケージをインストールして、[**UNIX コマンドを送信...**] メニューから任意の環境設定を定義することができます。
- エンタープライズ Mac* 管理ソフトウェアを介したカスタム・インストール
  - 以下を含む最も一般的なエンタープライズ Mac* 管理ソリューションを介して、カスタムのプッシュ型またはプル型のインストールを作成できます。
    - Casper / Bushel
    - Puppet
    - Munki
    - Chef
    - その他

12 トラブルシューティング

12.1 サーバーで Intel Unite® アプリケーションをインストールした後、管理者ポータルにアクセスできません

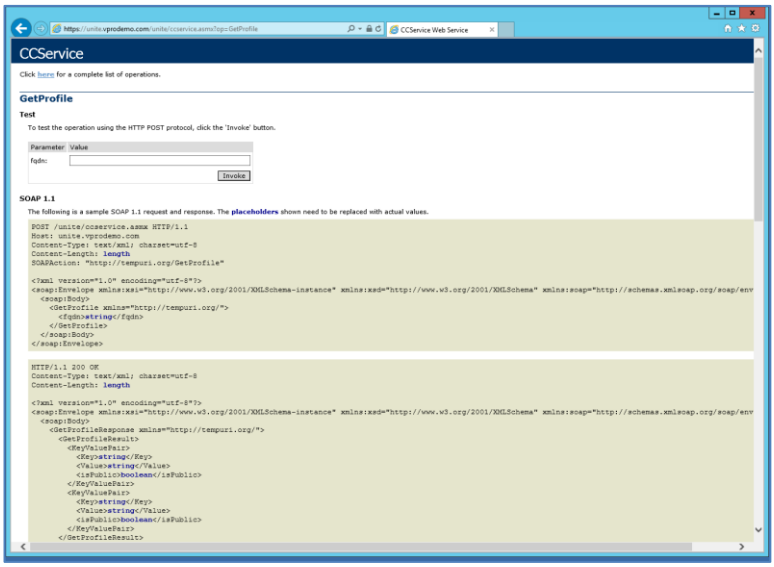
回避策/解決方法：Web サーバーに必要な役割と機能がサーバーに追加されていることを確認してください。

- サーバーマネージャーを使用して、サーバーに役割と機能を追加します。
    - サーバーの役割：Web サーバー
        - 管理ツールを含める
    - .Net* Framework 3.5 機能の追加
    - .Net* Framework 4 機能の追加
        - ASP .NET
            - WCF サービス
            - HTTP アクティブ化
        - Web サーバーの役割：
            - Web サーバー、一般的な HTTP 機能およびデフォルトのドキュメント。

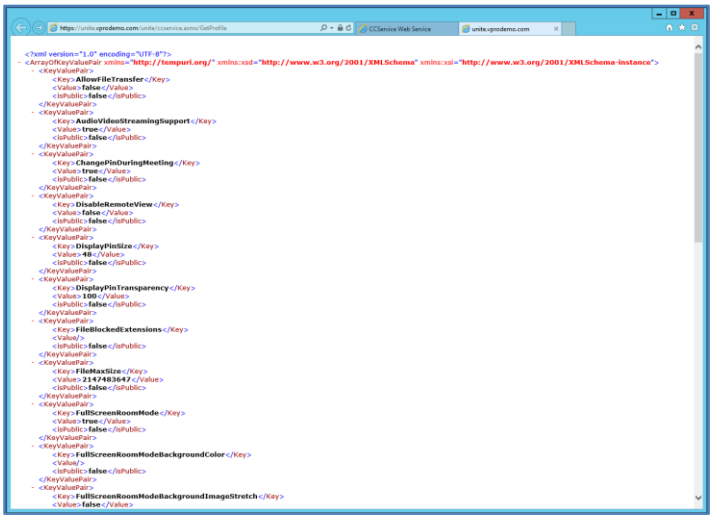
12.2 管理者ポータルにアクセスできない

管理者ポータルにアクセスしたときに Web.config の特定の xml タグに関するエラーページが表示された場合は、ポータルの仮想ディレクトリーのトップレベルにある該当のタグを Web.config から削除します (IIS 管理コンソールからアクセスできます)。

- 次のリンクにアクセスして、Web サービスのインストールが正常に完了したことを確認します。
  https://<サーバー名>/unite/ccservice.asmx
    - [**GetProfile**] を選択します。
    - [**Value (値)**] フィールドに「**test**」と入力して、[Invoke (呼び出す)] を押します。



- 以下に示すように xml ファイルのデフォルト・プロファイルを表示できるか確認します。これは、PIN サービスがデータベースにアクセスでき、正常にデータを取得できることを意味します。



12.3 ハブ・アプリケーション起動時のエラー

ポップアップ・ウィンドウにエラー ID が表示されます。ID に基づいて、エラーの性質を決定できます。

12.3.1 プラットフォーム・チェックがエラー ID333333 で失敗

このエラーは、ハブはプラットフォーム・チェックに合格したものの、コード署名証明書の検証には失敗したことを示します。通常は、OS のルート証明書が更新されておらず、パブリックの Intel Unite® コード署名証明書が検証できないことが要因です。
システムがインターネットに接続されていることを確認し、ブラウザーを開き、
https://www.microsoft.com に移動します (すると、強制的にルート証明書が更新されます)。

12.3.2 プラットフォーム・チェックがエラー ID666666 で失敗

このエラーは、プラットフォームが Intel Unite® アプリケーションと互換性がないことを示します。OEM ベンダーと確認して、サポートされているプラットフォームでアプリケーションを実行してください。

12.4 ハブが PIN サーバーから PIN を取得せず、スクロールダッシュが表示されます

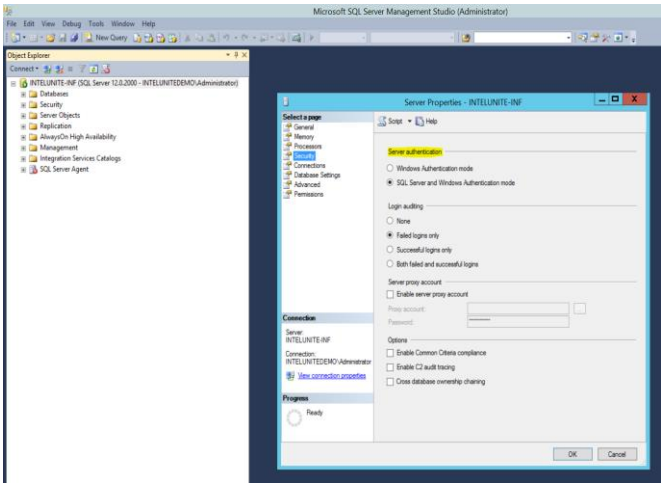
デバッグスイッチを使用して、ハブで Intel Unite® アプリケーションを起動します。つまり、コマンドプロンプトからアプリケーションが保存されているフォルダーに移動し、**IntelUnite.exe** /debug を実行します。実行すると、デバッグウィンドウが開き、接続情報が表示されます。一般的なエラーと回避策の一部が以下に記載されています。デバッグ情報がこれらのエラーのいずれかを示している場合、解決してハブで PIN を取得するための、解決方法/回避策に従ってください。

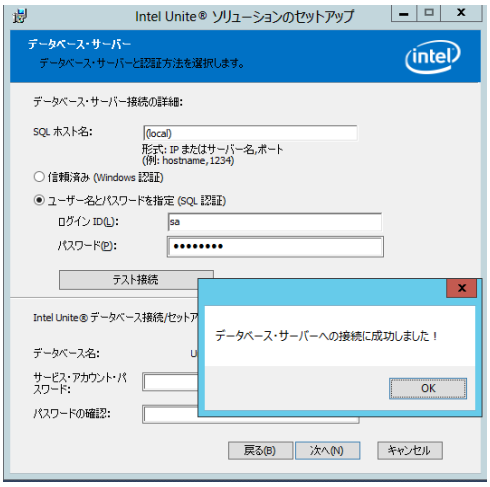
12.4.1 サーバーがリクエストを処理できず、「UniteServiceUser」のユーザーログインに失敗します

これは、SQL ログインで不一致が存在する場合や、ユーザーがエンタープライズ・サーバーを複数回インストールしようとしたためにデータベースのパスワードが破損している場合に発生する場合があります。

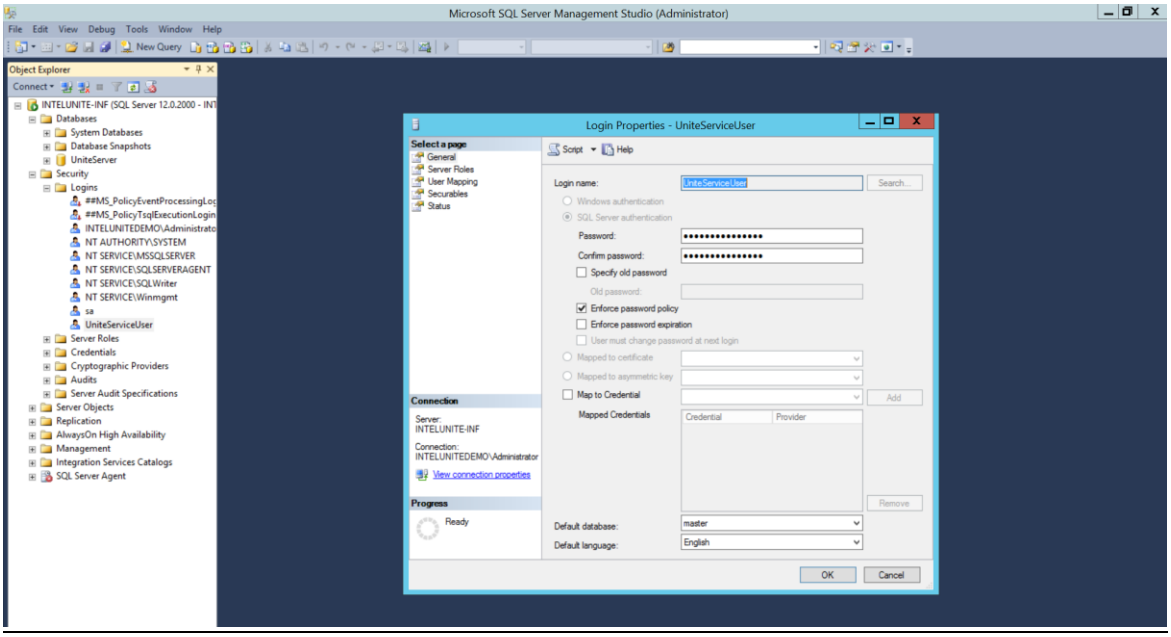
回避策/解決方法：

MS SQL のインストール時に使用する認証モードを確認します。ログイン/認証タイプを変更するには、Microsoft* SQL Management Studio に移動して SQL Server* に接続し、SQL Server* 上で右クリックして [Properties (プロパティ)] を選択します。[Security (セキュリティ)] ページを選択して、サーバーへ Intel Unite® アプリケーションをインストールする際に SQL 認証が選択されている場合、**SQL Server and Windows authentication (SQL Server および Windows 認証)**モードが選択されていることを確認します。





まだエラーが表示される場合は、**UniteServiceUser** のパスワードをリセットします。Microsoft* SQL Management Studio を使用して SQL Server* へ接続するには、**[Security (セキュリティ)]** > **[Logins (ログイン)]** へ移動し、**UniteServiceUser** の上で右クリックして **[Login Properties (ログインのプロパティ)]** ウィンドウを開きます。新しいパスワードを入力し、**[OK]** をクリックして変更を保存します。


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
INTELUNITE-INF (SQL Server 12.0.2000 - INT
Databases
System Databases
Database Snapshots
UniteServer
Security
Logins
##MS_PolicyEventProcessingLog
##MS_PolicyTsqlExecutionLogin
INTELUNITEDEMO\Administrato
NT AUTHORITY\SYSTEM
NT SERVICE\MSSQLSERVER
NT SERVICE\SQLSERVERAGENT
NT SERVICE\SQLWriter
NT SERVICE\Winmgmt
sa
UniteServiceUser
Server Roles
Credentials
Cryptographic Providers
Audits
Server Audit Specifications
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalogs
SQL Server Agent
Login Properties - UniteServiceUser
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Login name:
UniteServiceUser
Search...
Windows authentication
SQL Server authentication
Password:
Confirm password:
Specify old password
Old password:
Enforce password policy
Enforce password expiration
User must change password at next login
Mapped to certificate
Mapped to asymmetric key
Map to Credential
Add
Mapped Credentials
Credential
Provider
Remove
Connection
Server:
INTELUNITE-INF
Connection:
INTELUNITEDEMO\Administrator
View connection properties
Progress
Ready
Default database:
master
Default language:
English
OK
Cancel

12.4.2 サーバーが表示されません。DNS サービスレコードの試行：_uniteservice._tcp

回避策/解決方法：

これは、ハブが DNS レコードを見つけることができない場合に発生する場合があります。デバッグステップとして、コマンド・ライン・ウィンドウを開いて nslookup コマンドを実行します。DNS サービスが実行されているサーバーに対してハブが ping を実行することができ、DNS サービスレコードが Intel Unite® ソリューション向けに作成されていることを確認します。サービスレコードは次の値を持っている必要があります。**Service (サービス)**：_uniteservice、**Protocol (プロトコル)**：_tcp、**Port number (ポート番号)**：443 および **Host offering this service (このサービスを提供しているホスト)**：エンタープライズ・サーバーの FQDN。

12.4.3 SSL/TLS のセキュリティー保護されたチャネルと「uniteserverfqdn」権限で信頼関係を確立できませんでした

最新バージョンの Intel Unite® ソリューションでは、SHA-2 以上の証明書のみを受け付けます。IT 部門と連携し、発行されている信頼済み Web サーバー証明書が SHA-2 証明書であり、証明書パスが有効であることを確認してください。
テスト環境では、SHA-2 証明書を取得するか、環境で暗号化を無効にしてください。

- 暗号化なしで Intel Unite® を使用するには、サイトバインドでセキュアポート 443 の詳細を指定する次の手順をスキップし、MS SQL Server* のインストールに進み、DNS サービスレコードを用意します。また、DNS サービスレコードが作成されたときにサービスがポート 80 で検出されるようにする必要があります。
- 証明書チェックをスキップする別の方法は、ハブとクライアントのマシンアカウントにレジストリーを追加することです。HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)　[1 = 証明書アルゴリズム・チェックをスキップする、0 = それ以外の場合](値が 0 の場合は、強制的にエンタープライズ証明書を SHA2 証明書に使用します)]

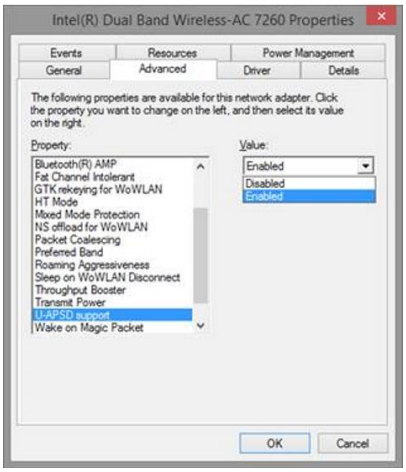
12.5 起動/接続時のクライアント・アプリケーションのクラッシュ

デバッグスイッチを使用してクライアント・アプリケーションを実行し、情報をログファイルに保存します。
(Intel Unite.exe /debug >logfile.txt を実行します)。
ログファイルにメッセージ「例外： - キーが指定された状態で有効ではありません。」がある場合は、アプリケーションを閉じ、ファイル C:\Users\eaviles\AppData\Roaming\Microsoft\Crypto\RSA\[sid]\d046df を削除します。指定された状態で使用するには無効なキーです。

12.6 注意すべき項目：接続時間が通常より長くなったり、画面の更新が断続的に遅くなったりします。

原因：

これは、U-APSD (予定外の自動節電配信) が有効になっているときの、一部のワイヤレス・アクセス・ポイントのバグです。http://www.intel.co.jp/content/www/jp/ja/support/network-and-i-o/wireless-networking/000005615.html を参照してください。
回避策：ワイヤレス・アクセス・ポイントのファームウェアの更新で解決する可能性があります。ただし、ほとんどの企業では、この更新を行うことは容易ではありません。最後の手段として、ワイヤレスドライバーの詳細プロパティーで、クライアントの U-APSD を無効にすることができます。



12.7 注意すべき項目：PIN サーバー上での遅延

回避策/解決方法：エンタープライズ・サーバーは、PIN の割り当てを管理し、PIN を検索して会議室に接続します。セキュリティー機能として、ユーザーがデータベースから PIN とクエリーの PIN を要求することができるレートは、Exponential Backoff アルゴリズムで制限されています。このバックオフメカニズムは、ユーザーの IP アドレスと試行回数に基づいて試行を追跡します。

運用サーバーは、ロードバランサーを使用して、環境内で負荷の管理を助け冗長性を維持します。ロードバランサーは、適切な Web サーバーにトラフィックをリダイレクトします。そのため、Web サーバーは同じ

IP アドレスからすべての要求を受けているように見えることがあるので、バックオフ・アルゴリズムのトリガーとなります。

データベースには、Web サーバーに秒単位で算出された遅延を返すストアド・プロシージャー (*spGetPinBackoffTime*) が含まれます。この機能は無効にでき、その場合ストアド・プロシージャーは常に 0 を返します。これにより、セキュリティー・バックオフ・アルゴリズムは無効になります。

12.8 Mac* クライアントのトラブルシューティング

デバッグメッセージを確認するには、ターミナルから Intel Unite® アプリケーション (/Applications/Utilities) を起動します。
/pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite
アプリケーションが起動し、ターミナル内のすべてのデバッグ情報が表示されます。

12.8.1 エンタープライズ・サーバー接続エラー -1003：指定したホスト名を持つサーバーが見つかりませんでした。

回避策/解決方法：DNS 検索ドメインが正しく定義されていることを確認します。
ユーザーが DNS サーバーを定義して、検索ドメインを指定しない場合、MAC* が自動検出を実行しようと試みたときに、検索対象の DNS ドメインサフィックスがありません。定義された DNS 検索ドメインがない場合、Intel Unite® アプリケーションは、自動検出または *uniteservice* のエントリーが「静的」でも、いずれかにそれらを追加することはできません。そのため、自動検出が *_uniteservice._tcp* 上で動作しない限り、クライアントはエンタープライズ・サーバーを見つけることができません。
最も簡単な解決策は単に DNS 検索ドメインを追加することですが (これは DNS SRV レコードと一致する必要があります)、代わりに *plist* の設定でエンタープライズ・サーバーを定義することもできます。
ターミナルコマンドを使用します。
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

12.8.2 エンタープライズ・サーバーの接続エラー -1001：リクエストがタイムアウトしました

回避策/解決方法：このエラーは、次の 2 つの理由が考えられます。

1. エンタープライズ・サーバーの Web サービスに問題がある可能性があります。
2. Mac* とサーバーの接続にネットワークの問題があります。

これに対処するための最初の手順は、デバッグログで Web サービスを見つけることです。https://サーバー名/Unite/CCService.asmx を検索します。
Safari* にこの URL をコピーして貼り付け、Mac* が Web サービスを得ることができることを確認します。これにより、サーバーへの接続にネットワークの問題があるか、エンタープライズ・サーバー上の Web サービスが実行されているかが確認されます。

12.8.3 エンタープライズ・サーバー接続エラー -1200：SSL エラーが発生し、サーバーへの安全な接続を作成できません。

IT 部門と連携して、Intel Unite® ソリューションで必要な、有効な SHA-2 証明書を取得します。

12.9 Mac OS* 用の Intel Unite® アプリがクライアント・デバイスから削除/アンインストールされ、代わりのバージョンまたは新しいバージョンの Intel Unite® アプリがインストールされましたが、古いインストール・プロパティーが存在します。

Mac* クライアント・デバイス用 の Intel Unite® アプリケーションは OS X* の一般規約に従っています。このため、アプリが削除されてもユーザー設定は削除されません。

回避策/解決方法：

クライアント・デバイスから Intel Unite® アプリケーションをアンインストールします。これらの設定を削除してクリーンな状態に戻すには、次の 2 つの方法があります。

1. ターミナル (/Applications/Utilities) で、次のコマンドを入力します。

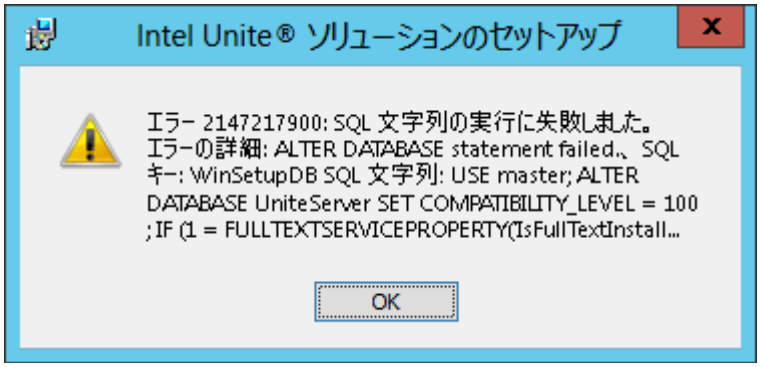
   defaults delete com.intel.Intel-Unite

2. Finder* で、~/Library/Preferences/com.intel.Intel-Unite.plist ファイルを削除し、次の操作を実行します。

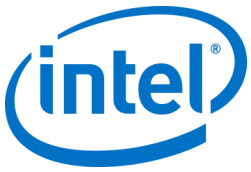
   システムを再起動します。最近では、OS によって Plist ファイルが大量にキャッシュされています。このため、一般的に、これらのファイルを削除して、OS に変更を認識させることはできません。

12.10 エラー 2147217900 ： SQL ストリングの実行に失敗しました。

このエラーは、Intel Unite® サーバーのインストーラーが実行され、Intel Unite® データベースがすでに存在しているにもかかわらず、サーバー名が空白の場合に発生します。



回避策/解決方法：



クラスターにデータベースがすでに存在している場合、インストーラーによりエラーが発生します。このエラーを解消するためには、データベースを削除し、DBAdmin 権限を持っていることを確認してからインストーラーを再度実行します。

12.11 エラーメッセージ： [データベース・エラー]

IT 管理者が管理者コンソールで [トークンの送信] オプションを選択し、[データベース・エラー] のエラーメッセージを受け取った場合、SMTP 設定が間違っている可能性があります。SMTP 電子メールサーバーの設定を検証する必要があります。

12.12 管理者 Web ポータルが正しく表示されない (コンポーネントが表示されない)

Intel Unite® ソフトウェアのアップグレードを実行した後、管理者 Web ポータルの表示が不完全で、テキストボックス、オプション、アイコンなどのコンポーネントが表示されません。これは、IIS の要求フィルターオプションで MIME の種類がブロックされているためです。

回避策/解決方法：

1. IIS マネージャーを開きます。
2. IIS サーバーのプロパティを表示します。
3. [**MIME の種類**] をクリックし、JSON 拡張子を追加します。
    - ファイル名の拡張子：.json
    - MIME の種類：application/json
4. IIS サーバーのプロパティに戻ります。
5. [**ハンドラー マッピング**] をクリックします。
    - スクリプト マップを追加します。
    - 要求パス：*.json
    - 実行可能ファイル：C:\WINDOWS\system32\inetsrv\asp.dll
    - 名前：JSON
6. [**接続**] ペインで、要求フィルター設定を変更する接続、サイト、アプリケーション、またはディレクトリに移動します。
7. [**ホーム**] ペインで、[**要求フィルター**] をダブルクリックします。
8. [ファイル名拡張子の許可] を見つけます。
9. 以下の 4 つの拡張子を追加します：
    - .json
    - .less
    - .woff
    - .woff2

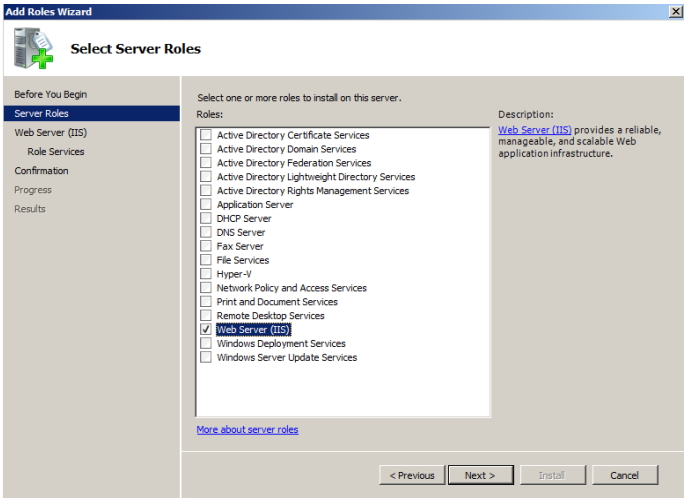
付録 A：エンタープライズ・サーバーの準備

IIS を有効にする

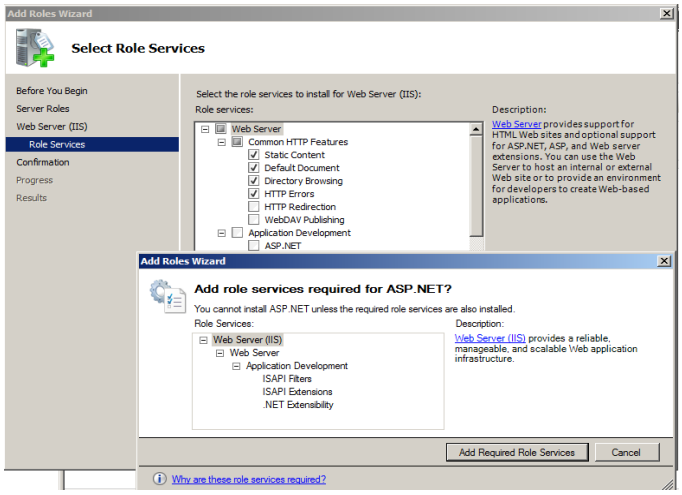
Windows* 2008 用：

Windows Server* 2008 の場合は、.NET* Framework 4.5 の更新プログラムをダウンロードする必要があります (https://www.microsoft.com/en-us/download/details.aspx?id=40779)。

- [**スタート**] をクリックして [**管理ツール**] を選択し、[**サーバー マネージャ**] をクリックします。
- [**役割の概要**] で [**役割の追加**] をクリックします。
- [**役割の追加ウィザード**] を使用して、[**Web サーバー (IIS)**] の役割を追加します (このチェックボックスを選択)。



- [**役割サービスの選択**] ウィンドウが表示されるまで [**次へ**] をクリックします。
- [**アプリケーション開発**] セクションで、ASP.NET が選択されていることを確認し、選択されていない場合は選択します。ASP.NET はデフォルトでは選択されていないことに注意してください。ASP.NET の [**必要な役割サービスを追加**] で、ASP.NET 4.5 も追加します。



- 役割が作成されたら、[**役割**] メニューでパネルの右側にある [**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**] の順に移動して、左側の [**接続**] ペインでサーバーを選択します。

  参照：Windows* Server* ライブラリーのリンク「Windows* Server* 2008 への IIS のインストール」

  注：最新バージョンの Intel® Unite™ では、SHA-2 以上の証明書のみを受け付けます。IT 部門と連携し、発行されている信頼済み Web サーバー証明書が SHA-2 証明書であり、証明書パスが有効であることを確認してください。

  テスト環境では、認証機関と提携して、SHA-2 証明書を取得するか、環境で暗号化を無効にしてください。
  - 暗号化なしで Intel® Unite™ を使用するには、サイトバインドでセキュアポート 443 の詳細を指定する次の手順をスキップし、MS SQL Server* のインストールに進み、DNS サービスレコードを用意します。また、DNS サービスレコードが作成されたときにサービスがポート 80 で検出されるようにする必要があります。
  - または、ハブとクライアントのマシンアカウントにレジストリー・キーを追加して、証明書チェックをスキップできます。
    HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 = 証明書アルゴリズム・チェックをスキップする、0 = それ以外の場合] (値が 0 の場合は、強制的にエンタープライズ証明書を SHA2 証明書に使用します)]

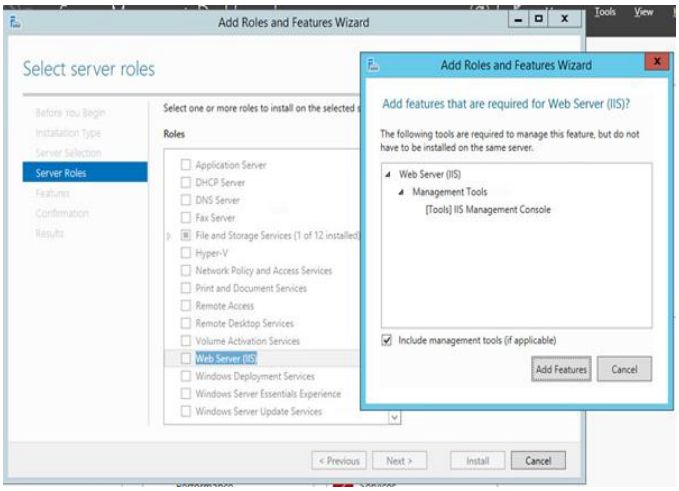
- 証明書を割り当てるには、左側の [**接続**] ペインで [サイト] を拡張して、[**既定の Web サイト**] をクリックします。
- 右側の [**操作**] ペインで、[**バインド**] ([サイトの編集] の下) を選択します。
- [**サイト バインド**] ウィンドウで、[**追加**] をクリックします。
- 次の情報を使用します。

- タイプ：ｈｔｔｐｓ　（注：ｈｔｔｐ　ではありません）
- ＩＰ　アドレス：未使用の　ＩＰ　アドレスすべて
- ポート：４４３
- ホスト名：　（空欄）
- ＳＳＬ　証明書：前の手順でインストールした　ＳＳＬ　証明書を使用します。
- [**ＯＫ**]　をクリックします。

Windows* 2012：

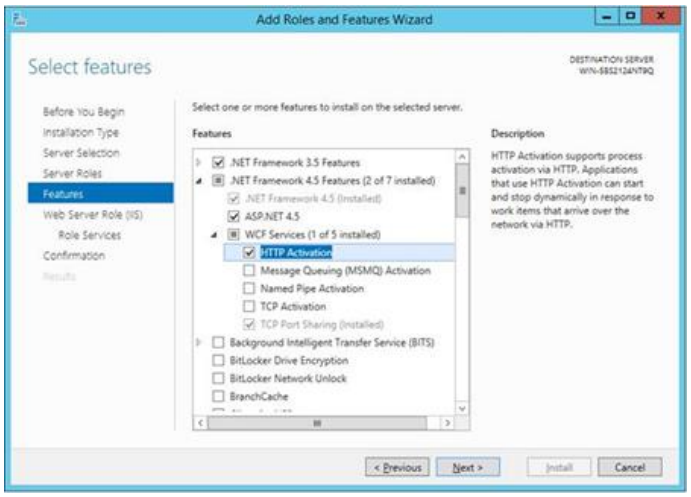
- **Server Manager (サーバー マネージャー)**を開きます。
- [**Manage (管理)**] メニューで、[**Add Roles and Features (役割と機能の追加)**] を選択します。
- [**Role-based or Feature-based Installation (役割ベースまたは機能ベースのインストール)**] を選択します。
- 適切なサーバーを選択します (デフォルトではローカルが選択されています)。
- [**Web Server (IIS) (Web サーバー (IIS))**] を選択し、Web サーバー (IIS) で必要な機能を [**Add Features (機能の追加)**] で追加し、[**Next (次へ)**] をクリックします。

注： Intel Unite® サーバーでインターネット・サーバー証明書を要求する方法の詳細については、Microsoft* の Web リンク https://technet.microsoft.com/en-us/library/cc732906.aspx (英語) に移動し、SSL 証明書ベンダーの手順に従って署名入り証明書を取得してください。



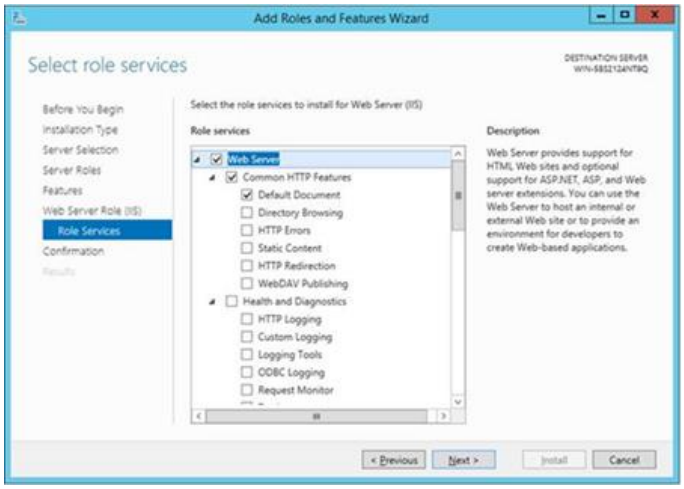
- [Features (機能)] で、IIS に次の機能を追加します (これらはデフォルトのオプションではありません)。
  - .NET* Framework 3.5 の機能
  - ASP.NET 4.5
  - WCF サービス

- [HTTP Activation (HTTP アクティブ化)] (プロンプトが表示されたら、HTTP アクティブ化に必要な機能を追加します) および [**Next (次へ)**] をクリックします。



注：.NET* 3.5 は、インストール中にエラーの原因となる場合があります。対象のコンピューターが Windows Update へのアクセスを持っていない場合、代替ソースのパスを提供します。[**Specify an alternate source path (代替ソースのパスを指定)**] リンクをクリックして、インストール・メディア上の **\sources\sxs** フォルダーへのパスを指定します。
参照：https://technet.microsoft.com/en-us/library/dn482071.aspx

- [Role Services (役割サービス)] ページで、サーバーに [**Web Server Role (IIS) (Web サーバーの役割 (IIS))**] を役割として追加するか、デフォルト値を受け入れます。
- Web サーバーにインストールする次の役割サービスを選択します。
    - HTTP 共通機能
    - 既定のドキュメント



- [**Next (次へ)**] をクリックして続行し、次のウィンドウで [**Install (インストール)**] をクリックして、選択した役割と機能をインストールします。

- 役割が作成されたら、[**Roles (役割)**] メニューでパネルの右側にある [**Web Server Role (IIS) (Web サーバーの役割 (IIS))**]、[**Internet Information Services (IIS) Manager (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)**] の順に移動して、左側の [**Connections (接続)**] ペインでサーバーを選択します。

  注：最新バージョンの Intel Unite® ソリューションでは、SHA-2 以上の証明書のみを受け付けます。IT 部門と連携し、発行されている信頼済み Web サーバー証明書が SHA-2 証明書であり、証明書パスが有効であることを確認してください。

  テスト環境では、暗号化を無効にするか、自己署名の SHA 2 証明書を作成します。
  - 暗号化なしで Intel Unite® を使用するには、サイトバインドでセキュアポート 443 の詳細を指定する次の手順をスキップし、MS SQL Server* のインストールに進み、DNS サービスレコードを用意します。また、DNS サービスレコードが作成されたときにサービスがポート 80 で検出されるようにする必要があります。
  - 管理者として、次の PowerShell コマンドを実行します。
    - New-SelfSignedCertificate –dnsname “yourservername” –CertStoreLocation cert:\LocalMachine\My。ただし、“yourservername” はエンタープライズ・サーバーの FQDN を表します。
  - または、ハブとクライアントのマシンアカウントにレジストリー・キーを追加して、証明書チェックをスキップできます。
    HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)　[1 = 証明書アルゴリズム・チェックをスキップする、0 = それ以外の場合](値が 0 の場合は、強制的にエンタープライズ証明書を SHA2 証明書に使用します)]

- 証明書を割り当てるには、左側の [**Connections (接続)**] ペインで [Sites (サイト)] を拡張して、[**Default Web Site (既定の Web サイト)**] をクリックします。
- 右側の [**Actions (操作)**] ペインで、[**Bindings (バインド)**] ([サイトの編集] の下) を選択します。
- [**Site Bindings (サイト バインド)**] ウィンドウで、[**Add (追加)**] をクリックします。
- 次の情報を使用します。
  - Type：https (注：http ではありません)
  - IP Address：未使用の IP アドレスすべて
  - Port：443
  - Hostname： (空欄)
  - SSL Certificate： (前述の手順でインストールした証明書を選択)
  - [**OK**] をクリックします。
- [**Close (閉じる)**] を選択します。

参照：Windows Server* ライブラリーのリンク「Windows Server* 2012 への IIS のインストール」

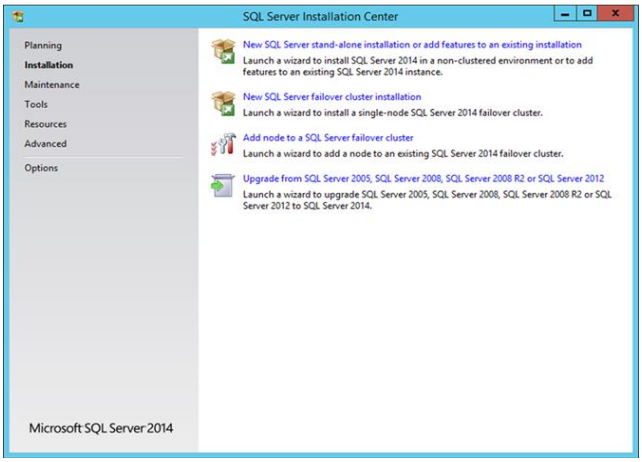
ポート 443 に関する注：Intel Unite® アプリケーションの Web サービスは、ポート 443 を使用してクライアントおよびハブと通信します。前述したように、このポートが有効になっていることを確認してください。

Microsoft* SQL Server* のインストール

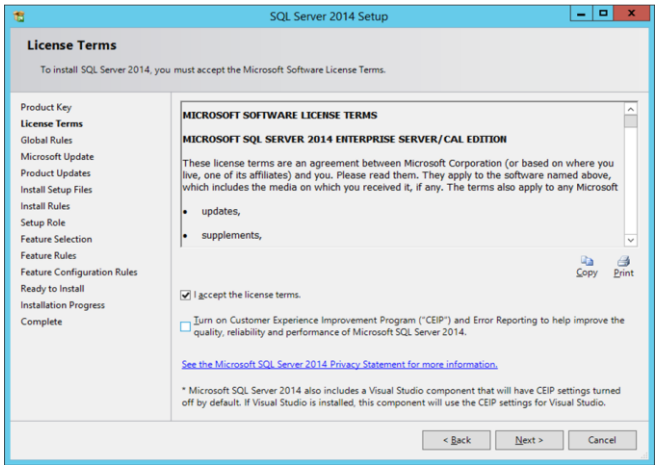
エンタープライズ・サーバーでは　MS　ＳＱＬ　を実行する必要があります。最低条件はバージョン２００８　Ｒ２　以上です。「テスト環境」を実行してアプリケーションに慣れたい場合、新しく専用のＳＱＬ　Ｓｅｒｖｅｒ*　をインストールすることもできますが、これは必須ではありません。Ｉｎｔｅｌ®　Ｕｎｉｔｅ™　アプリケーションは、他のテーブルや既存のデータに干渉することなく、既存のデータベースに独自のデータベース、データテーブル、およびインデックスを作成します。

MS SQL 2014 のインストールについては以下を参照してください。

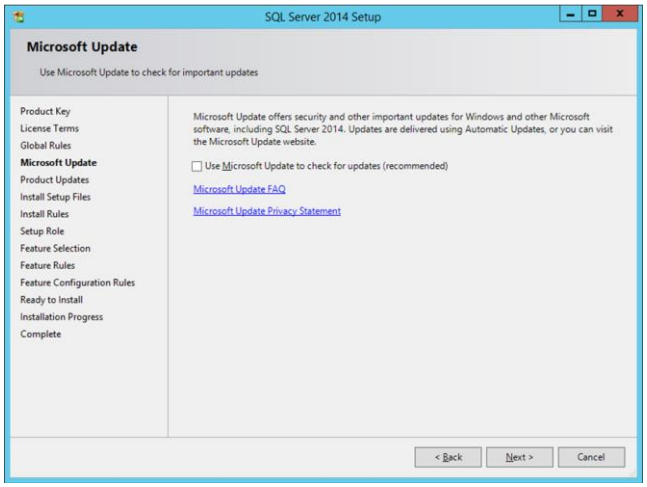
- SQL Server* のセットアップを実行し、SQL Server* インストール センターを開きます。左ペインの [**Installation (インストール)**] をクリックし、[**New SQL Server stand-alone installation or add features to an existing installation (SQL Server の新規スタンドアロン・インストールを実行するか、既存のインストールに機能を追加)**] を選択します。



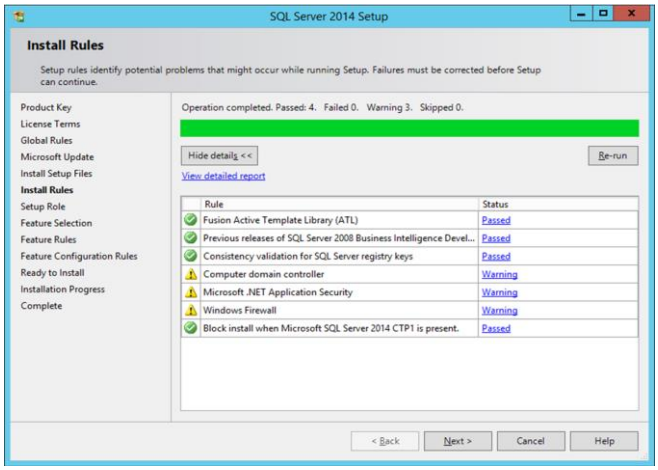
- プロダクトキーを入力して、ライセンス条項に同意し、[**Next (次へ)**] をクリックします。



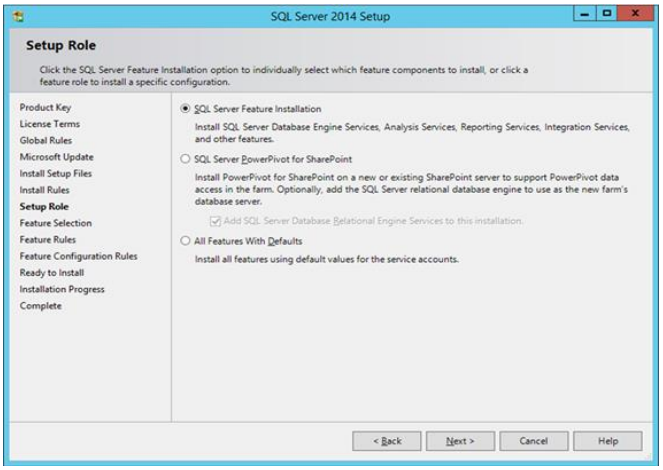
- [**Use Microsoft Update to check for updates (recommended) (Microsoft Update を使用して更新を確認する (推奨))**] を選択して更新を確認して、[**Next (次へ)**] をクリックします。次のウィンドウで、セットアップが製品の更新プログラムを探し、必要な更新プログラムをインストールします。続行するには、[**Next (次へ)**] をクリックします。



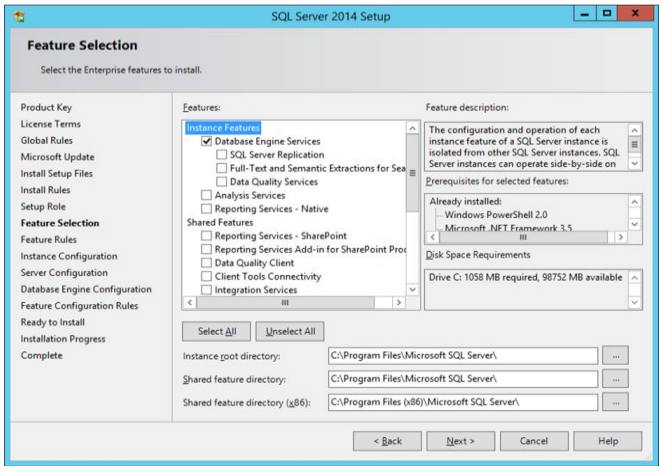
- SQL セットアップが、潜在的な障害と、インストール前に満たす必要がある要件を確認します。[**Next (次へ)**] をクリックして進めます。



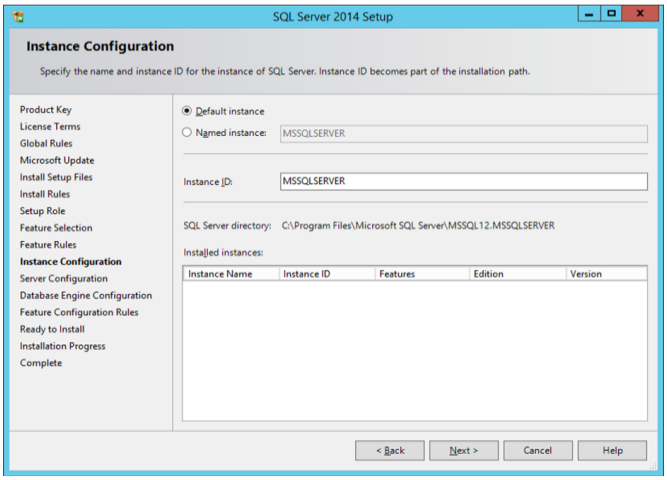
- [**SQL Server Feature Installation (SQL Server 機能のインストール)**] を選択して、[**Next (次へ)**] をクリックします。



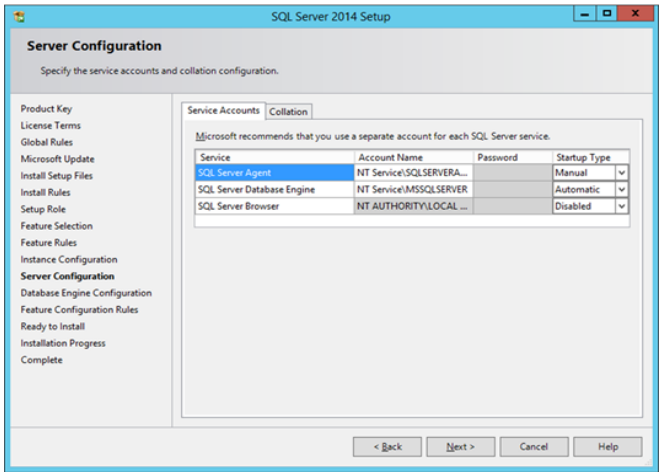
- [**Feature Selection (機能選択)**] で、[**Database Engine Services (データベース・エンジン・サービス)**]、[**Management tools- Complete (管理ツール - 完全)**] を選択し、[**Next (次へ)**] をクリックします。



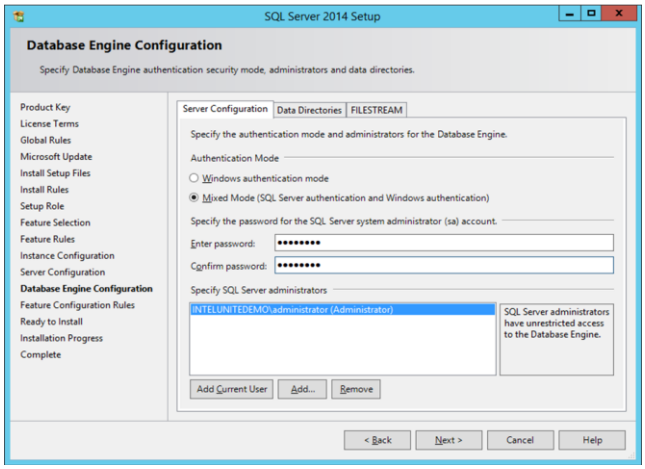
- SQL Server* の名前とインスタンス ID を指定し、[**Next (次へ)**] をクリックします。



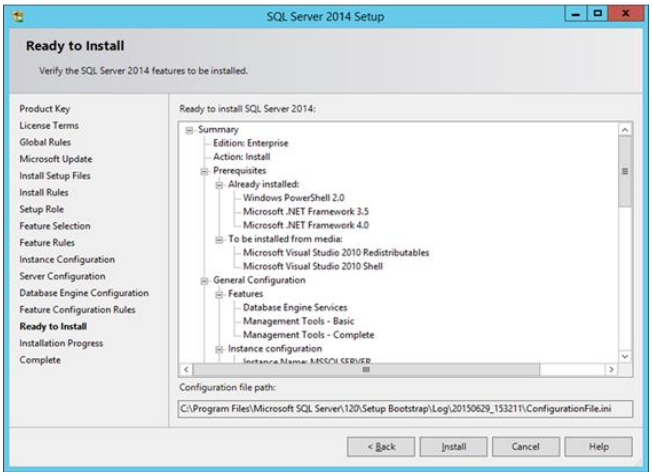
- 各サービスのサービスアカウントを指定し、[**Next (次へ)**] をクリックして続行します。


SQL Server 2014 Setup
Server Configuration
Specify the service accounts and collation configuration.
Product Key
License Terms
Global Rules
Microsoft Update
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Service Accounts
Collation
Microsoft recommends that you use a separate account for each SQL Server service.
Service
Account Name
Password
Startup Type
SQL Server Agent
NT Service\SQLSERVERA...
Manual
SQL Server Database Engine
NT Service\MSSQLSERVER
Automatic
SQL Server Browser
NT AUTHORITY\LOCAL ...
Disabled
< Back
Next >
Cancel
Help

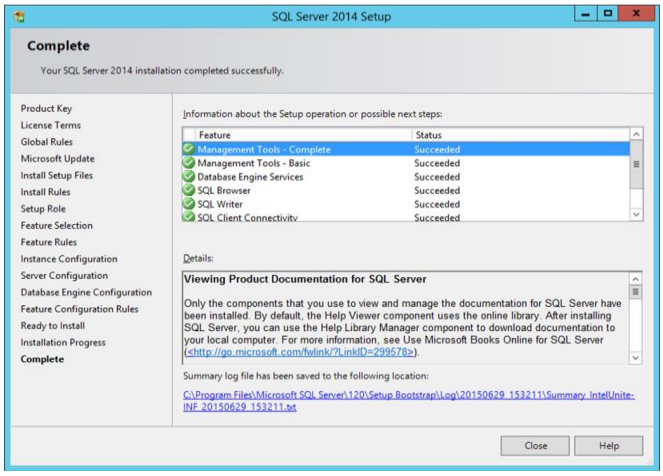
- Mixed Mode (混合モード) 認証 (SQL Server* と Windows* 認証が含まれます) を選択し、SQL Server* の管理者を指定し、[**Next (次へ)**] をクリックします。



- インストールする機能を確認し、[**Install (インストール)**] をクリックします。



- インストールが完了したら、[**Close (閉じる)**] でダイアログボックスを閉じます。



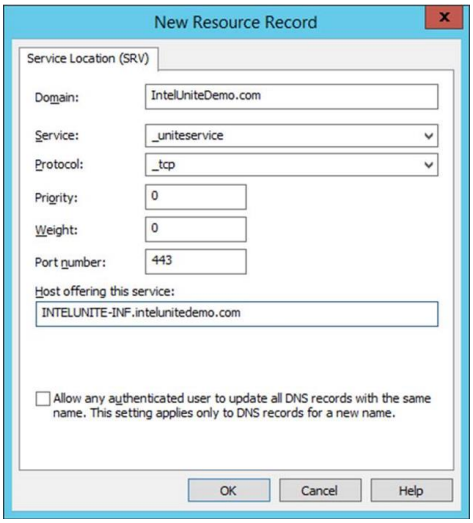
DNS サービスレコードを作成する

ハブやクライアントは、エンタープライズ・サーバーの自動ルックアップ中に、DNS サービスを使用してエンタープライズ・サーバーを検索します。手動ルックアップを使用することもできますが、DNS の使用を強く推奨します。ハブとクライアントのインストール時に手動でエンタープライズ・サーバーのホスト名を入力することを予定している場合、このセクションはスキップしてかまいません。

DNS サービスレコードが使用されている場合、ハブやクライアントは、DNS サービスレコード _uniteservice._tcp.example.com 86400 IN 0 5 443 uniteserver.example.com 内で、_uniteservice._tcp という名前のサービスを探します。

Microsoft* Windows* で DNS サービスレコードを追加するには、次の手順に従います。

- DNS サーバー上で、DNS マネージャーを開きます。
- [Forward Lookup Zones (前方参照ゾーン)] (左ペイン) を展開します。
- ゾーンを右クリックして、[Other New Records... (その他の新しいレコード)] を選択します。
    - [**Select a resource record type (リソース レコードの種類を選択)**] で [**Service Location (SRV) (サービス ロケーション (SRV))**] を選択し、次に [**Create Record (レコードの作成)**] を選択します。
    - [**Service (サービス)**] に「_uniteservice」と入力します。
    - [**Protocol (プロトコル)**] に「_tcp」と入力します。
    - [**Port (ポート)**] に「443」と入力します。
    - [Host offering this service (このサービスを提供しているホスト)] に、エンタープライズ・サーバーのホスト名/IP を入力します。



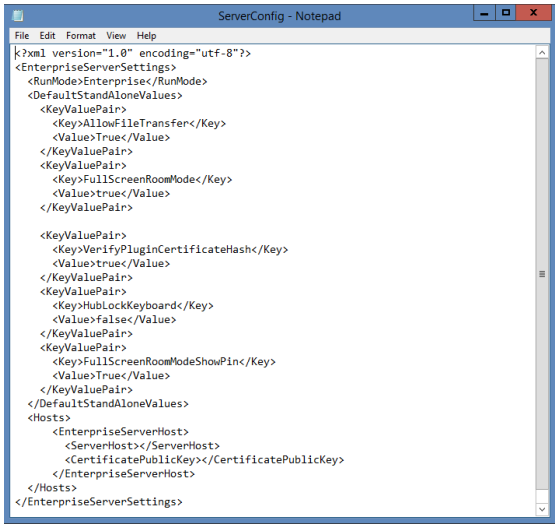
注 : フォワーダーを使用するように DNS サーバーを構成する方法の詳細については、Microsoft* のリンク https://technet.microsoft.com/ja-jp/library/cc754941.aspx にアクセスしてください。

付録 B：ServerConfig.xml の例

ServerConfig.xml ファイルは、ハブと Intel Unite® ソフトウェアのクライアント・コンポーネントのインストール時に作成されます。xml ファイルのデフォルトの場所は、それぞれ C:\Program Files (x86)\Intel\Intel Unite\Hub または C:\Program Files (x86)\Intel\Intel Unite\Client です。

[**Specify Server (サーバーの指定)**] を選択してサーバーのホスト名を入力するとき、またはハブまたはクライアントに Intel Unite® ソフトウェアをインストールする際に **Public Key (公開キー)**を手動で入力するときに、このファイルは編集されます。

インストール後に serverconfig.xml ファイルを編集したい場合は、ファイルが存在するフォルダーに移動し、必要な変更を行います。



サーバーが ServerConfig.xml で定義されている場合は、そのサーバーが DNS サービスレコードよりも優先されます。

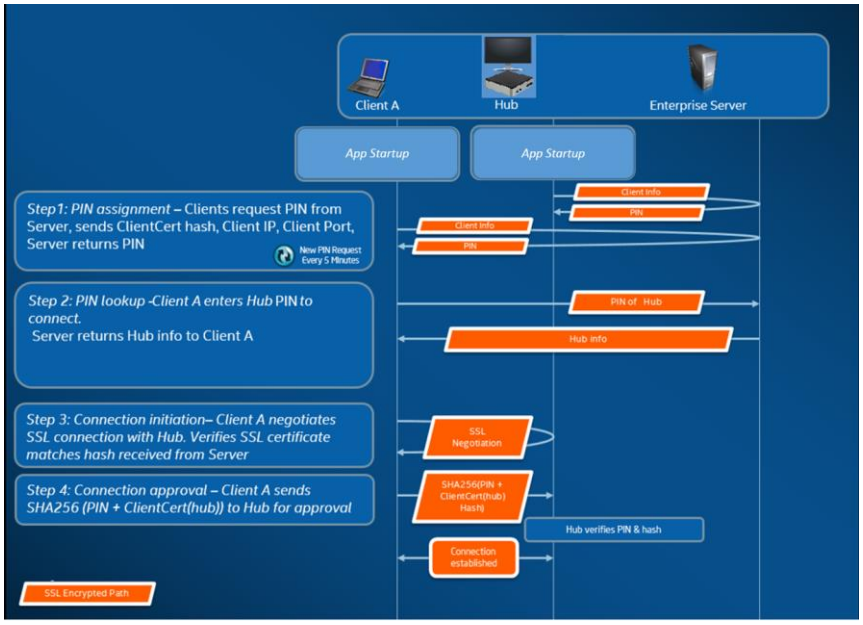
付録 C：Intel Unite® ソリューション - セキュリティーの概要

Intel Unite® ソフトウェア - セキュリティー・フロー

このセクションでは、Intel Unite® アプリケーションのセキュリティー面について説明します。接続のセキュリティー面は、以下の 4 つの手順で説明されます。

1. PIN の割り当て
2. PIN のルックアップ
3. 接続の開始
4. 接続の承認

次の図は、Intel Unite® がインストールされているディスプレイへの接続時に、クライアント (インテル® vPro™ テクノロジー搭載) とハブの各アプリケーションが、エンタープライズ・サーバーから PIN を安全に受け取って解決し、接続を確立する様子を示しています。



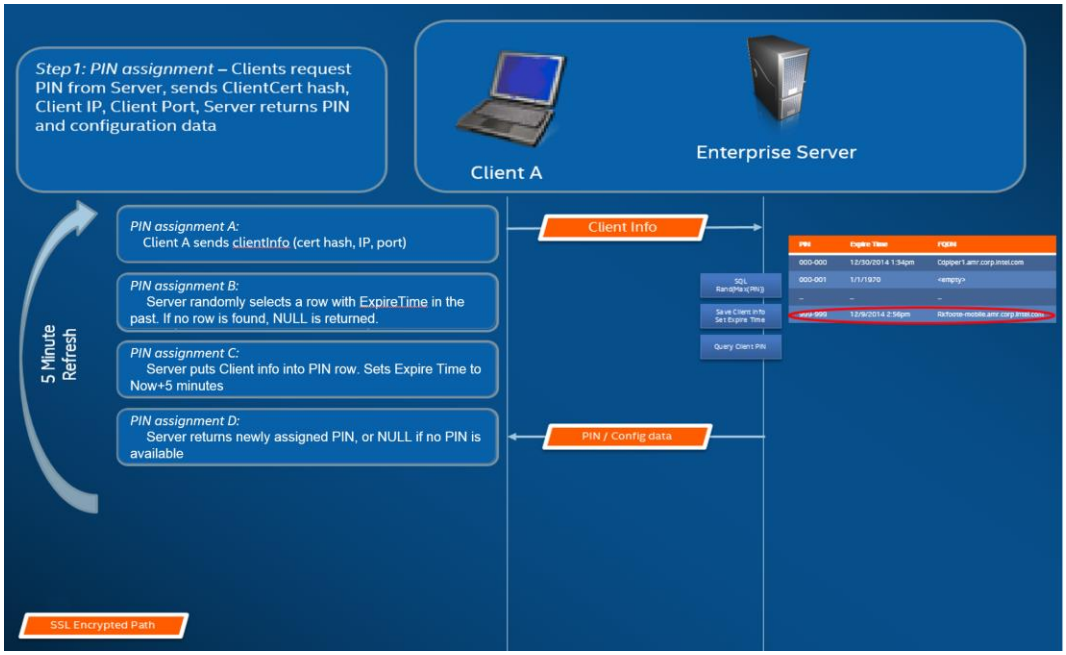
手順 1：PIN の割り当て

次の図は、PIN がどのように割り当てられるかを示しています。このプロセス中に発生するすべてのネットワーク通信は、Web サービスを介して SSL で暗号化されます (TCP 443)。
PIN を受け取ったハブとクライアントは、接続情報と公開キーをサーバーに登録します。公開キーは、接続中に、各コンポーネントが目的のターゲットと通信していることを確認する際に使用されます。

注：クライアント (インテル® vPro™ テクノロジー搭載) とハブに対する PIN の割り当ては、同じフローに従って実行されます。

また、以下の点に注意してください。

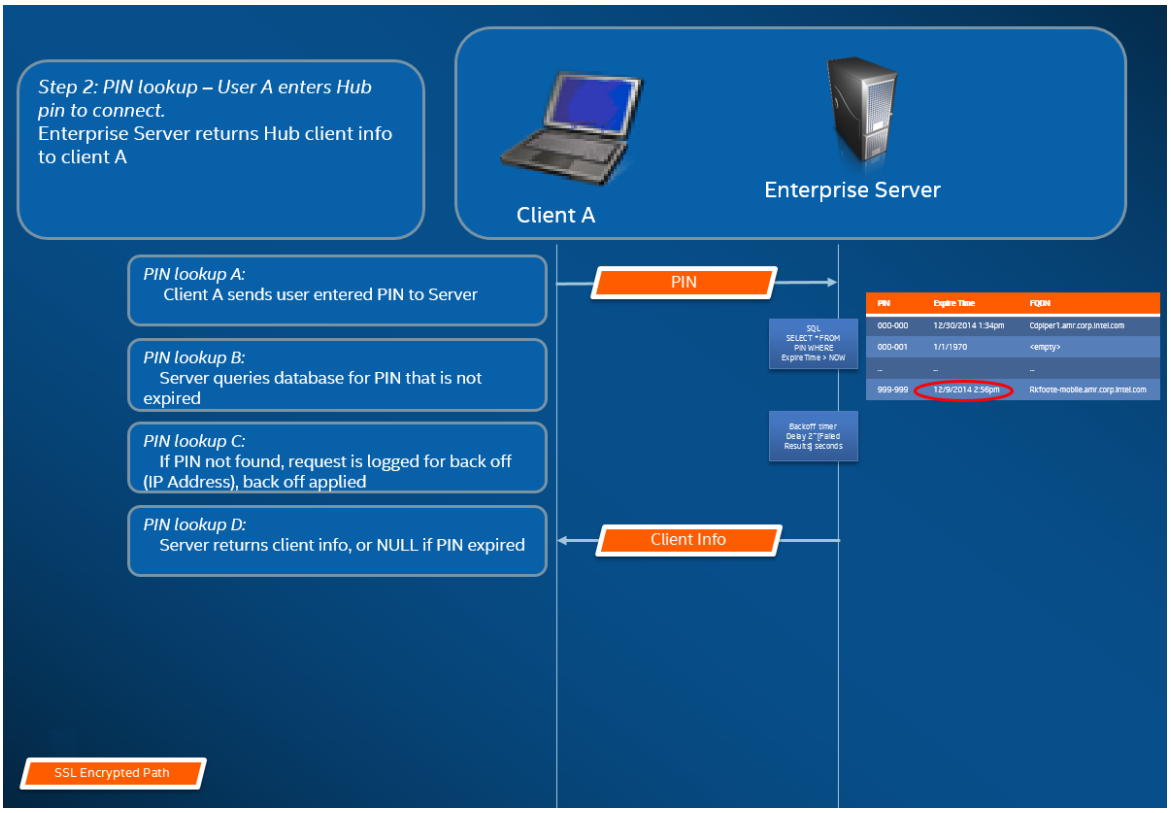
- PIN の更新間隔は設定可能です。
- ハブまたはクライアントが接続情報を送信するとき、ローカルホスト (127.0.0.0/8) と 169.254.0.0/16 の範囲にある IP アドレスは無視されます。
- TCP ポートはクライアントまたはハブごとに設定することも、管理者ポータルからプロファイルを介して適用することもできます。デフォルトでは、オペレーティング・システムによってポートを割り当てます。
- 有効期限が切れた PIN でも、最長 15 秒間アクセスすることができます。
- ユーザーが別のディスプレイに誤って接続するのを避けるために、有効期限が切れた PIN は、期限切れの後 5 分間再割り当てされません。



手順 2：PIN のルックアップ

次の図は、PIN がエンタープライズ・サーバーでどのように解決されるかを示しています。PIN のルックアップ・プロセス中のすべてのネットワーク通信は、Web サービス上で SSL で暗号化されます (TCP 443)。ユーザーがクライアントにターゲットの PIN を入力すると、クライアントは PIN をエンタープライズ・サーバーに送信し、接続情報を取得します。ルックアップが成功すると、エンタープライズ・サーバーはターゲットの有効な接続情報を返します。ターゲットは、ハブまたは Intel Unite® ソフトウェアを実行しているクライアント (インテル® vPro™ テクノロジー搭載) です。
通信情報の他に、ターゲットの公開キーも提供され、クライアント・アプリケーションが正しいターゲットと通信していることを確認できます。

注：ハブとクライアントによる PIN のルックアップは、同じフローで実行されます。

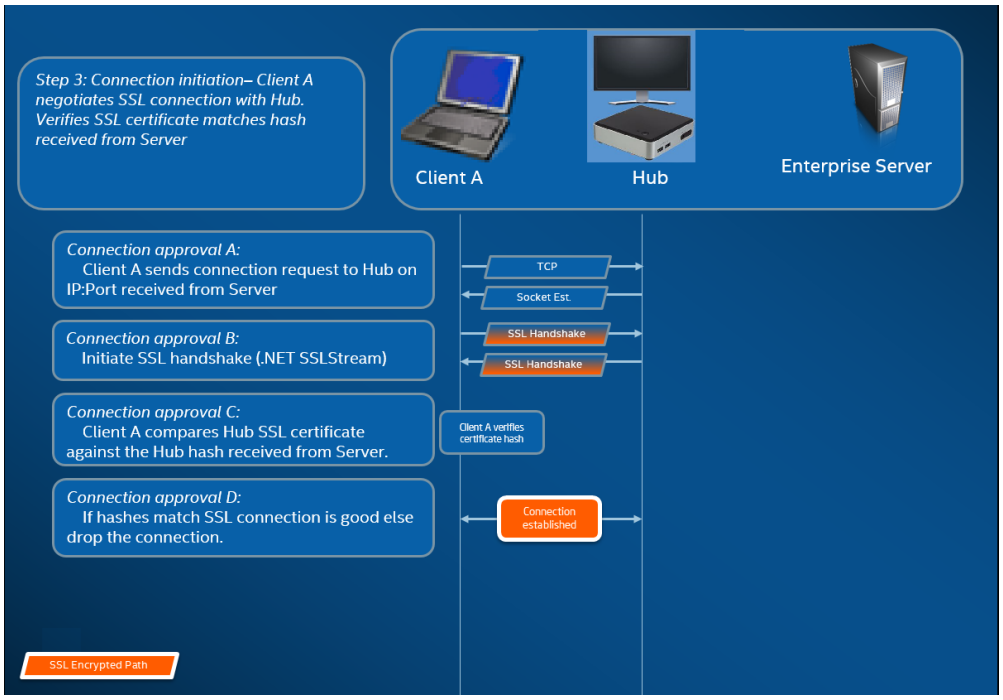


PIN のルックアップのバックオフ

攻撃者がエンタープライズ・サーバーから PIN を取得しようとするのを回避するために、失敗したルックアップ試行はログに記録されます。ユーザーは、10 秒間に 3 回まで失敗できます。3 回を超えると、バックオフメカニズムによって、応答に遅延が発生します (2^x 秒。x は、5 分間にルックアップが失敗した回数)。

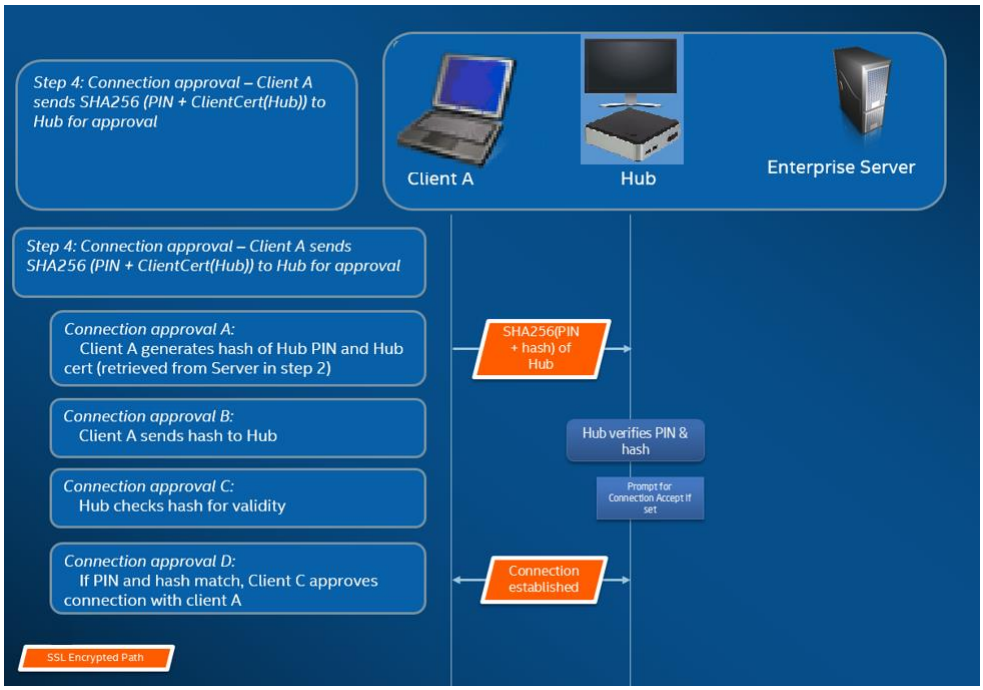
手順 3：接続の開始

次の図は、接続がどのように開始されるかを示しています。クライアントはターゲット (ハブまたは Intel Unite® ソフトウェアを実行しているインテル® vPro™ テクノロジーを搭載したクライアント) との TCP ピアツーピア接続を開始し、SSL ハンドシェイクを開始します。ターゲットから提供された証明書がハッシュ化され、手順 2 でクライアントが受け取ったハッシュと比較されます。このタイプの検証を行うことにより、攻撃や DHCP クライアントの IP アドレスが変更されるといった状況を避けることができます。



手順 4：接続の承認

次の図は、クライアントとターゲットの間で接続がどのように確立されるかを示しています。このターゲットは、ハブまたは Intel Unite® ソフトウェアを実行しているクライアント (インテル® vPro™ テクノロジー搭載) である場合があります。ターゲットが PIN およびクライアント証明書を検証すると、その接続を受け付け、クライアントとターゲットとの間に接続が確立されます。



付録 D：Intel Unite® ソリューション - ロードバランサー

このセクションでは、ロードバランサー/プロキシーが設定されている場合に PIN のバックオフに対処する方法について簡単に説明します。
ロードバランサーを利用している環境では、SQL ストアド・プロシージャー dbo.spGetPinBackoffTime が**常に 0 を返す**ことを確認します。
手順：

- ストアド・プロシージャー dbo.spGetPinBackoffTime を変更します。すべてをコメントアウトし、末尾で「select 0」を使用してもかまいません。
- スクリプトを実行します。

ロードバランサーを利用していない環境では、このストアド・プロシージャーがデフォルトのままであることを確認します。