インテル® エンドポイント・マネジメント・アシスタント（インテル® EMA）

シングル・サーバー・インストール・ガイド

インテル® EMA バージョン：1.4.0

改訂：2021 年 3 月

免責条項

本ソフトウェアおよび関連資料は、インテルの著作権で保護された資料であり、それらの使用はユーザーに提供された明示ライセンス (以下「ライセンス」) に準拠します。ライセンスに別段の定めがない限り、本ソフトウェアまたは関連資料をインテルの事前の書面による許可なしに使用、変更、コピー、発行、配布、公開、送信することは禁止されています。

本ソフトウェアおよび関連資料は、ライセンスに明示的に規定された場合を除き、明示的と黙示的とを問わず一切の保証なく、現状のまま提供されます。

インテルのテクノロジーを使用するには、対応したハードウェア、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。

絶対的なセキュリティーを提供できる製品やコンポーネントはありません。

生じるコストおよび結果は異なる場合があります。

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も許諾するものではありません。

インテルは、明示されているか否かにかかわらず、いかなる保証もいたしません。ここにいう保証には、商品適格性、特定目的への適合性、および非侵害性の黙示の保証、ならびに履行の過程、取引の過程、または取引での使用から生じるあらゆる保証を含みますが、これらに限定されるわけではありません。

本書で説明されている製品とサービスには、エラッタと呼ばれる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® 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。データやシステムの紛失や盗難など、これらの損失の結果生じたいかなる損害に対しても、インテルは責任を負いません。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、http://www.intel.com/technology/vpro を参照してください。

1　はじめに

インテル® エンドポイント・マネジメント・アシスタント (インテル® EMA) は、ファイアウォール外のデバイスも含め、クラウド上のインテル® vPro® プラットフォーム・ベースのデバイスを簡単に管理できるソフトウェア・アプリケーションです。インテル® EMA は、インテル® AMT の設定と使用を容易にするために設計されており、IT 部門が、ワークフローを中断することなく、インテル® vPro® プラットフォームを基盤にしたデバイスを管理できるようにします。結果としてクライアントの管理が簡単になり、IT 組織の管理コストの削減に役立ちます。

インテル® EMA とその管理コンソールは、クラウド上のインテル® AMT デバイスにリモートから安全に接続できるようにすることで、IT 部門に高度で柔軟な管理ソリューションを提供します。主なメリットは次のとおりです。

- インテル® EMA は、インテル® vPro® プラットフォーム上でインテル® AMT を設定および使用し、ハードウェア・レベルのアウトオブバンド管理を実現できます。
- インテル® EMA は、インテル® vPro® プラットフォーム以外のプラットフォームやインテル® AMT が有効化されていないインテル® vPro® プラットフォーム上で OS が実行されている場合、ソフトウェア・ベースのエージェントを使ってシステムを管理できます。
- インテル® EMA は、オンプレミスとクラウドのどちらにもインストールできます。
- インテル® EMA の組込みユーザー・インターフェイスを使用できるほか、API からインテル® EMA の機能を呼び出すこともできます。

この資料は、インテル® EMA サーバーを本稼働環境にインストールして設定する手順と、インストール後にインテル® EMA サーバーを保守管理する手順について説明します。対象読者は、十分な技術的能力を有する、グローバル管理者ロールでインテル® EMA を操作するシステム管理者ユーザーです。

注記 : 学習用に簡略化されたチュートリアル形式のインストール手順は、インテル® EMA クイック・スタート・ガイドに用意されています。

グローバル管理者は、インテル® EMA サーバー全体のインストール、構成、管理と、インテル® EMA サーバー内のテナント使用空間の作成を担当します。その他のインテル® EMA ユーザー (テナント管理者、アカウント・マネージャーなど) は、インテル® EMA サーバーにホストされた各テナントのユーザー、ユーザーグループ、エンドポイント・グループ、管理対象エンドポイント・クライアント・システムのセットアップとメンテナンスを担当します。

注記 : ユーザーロール、テナント、エンドポイント・グループといった主な概念の詳細については、インテル® EMA 管理と使用ガイドを参照してください。同書には、インテル® EMA のテナントとその管理対象エンドポイント・システムのセットアップおよび保守の詳細についても記載されています。

インストールを実行する前に、このガイドをよく読むことをお勧めします。本資料では、インストール要件、コンフィグレーション・パラメーター、インテル® EMA サーバーとそのコンポーネントの詳細なインストール手順について説明します。

1.1　始める前に

セクション 2 で説明するように、インテル® EMA サーバーとそのコンポーネントの実際のインストール作業はかなりシンプルです。それでも、インストール中に入力または選択する内容を事前に把握するため、インストールを開始する前に以下の選択肢について考える時間を取ることをお勧めします。

- セクション 1.3 に記載されている前提条件がすべて満たされていることを確認します。
- セクション 1.4 の「セキュリティーに関する推奨事項」を見直し、インテル® EMA のインストール中、またはインストール後に実行します。
- セクション 1.7 の「スケーリングに関する考慮事項」を参考に、インテル® EMA の実装で使用するのに最適なハードウェアを決定します。
- インテル® EMA サーバーへの接続に使用する完全修飾ドメイン名 (FQDN) や IP アドレスを決定します。
- SQL Server* との接続に Windows* 認証モード (セキュリティー上の理由により推奨) を使用するか、SQL 認証を使用するかを決定します。SQL 認証の場合、インストール前に、ターゲットの資格情報が SQL Server* にセットアップされていることを確認する必要があります。

- IIS を介してインテル® EMA ウェブサイトを 見つける方法と、リクエストの処理方法 (FQDN/ホスト名のみを使用するか、最初に FQDN/ホスト名を使用して次に IP アドレスを使用するか、IP アドレスのみを使用するか) を決定します。追加のホスト名を正しく動作させ、管理するには、DNS サーバーまたはルーターを構成する必要があります。
- インテル® EMA のインストールをドメイン認証モード (Kerberos) で実行するか、デフォルトの通常アカウント (ユーザー名/パスワード) モードで実行するかを決定します。ドメイン認証モードでインストールする場合、Hostname (ホスト名) フィールドにマシンの FQDN を使用することを推奨します。ここで入力した値については、その他のエンドポイントまたはクライアント・ウェブ・ブラウザーから接続できることを確認する必要があります。別の値を使用する場合、IT 部門のプラクティスに従って、インテル® EMA のインストール後にサービス・プリンシパル名 (SPN) を設定してください。
- グローバル管理者ユーザー用に使用する有効なメールアドレスを決定します。

1.2 サポートされるオペレーティング・システム

スタンドアロン・アプリケーションのインテル® EMA エージェントは、以下のオペレーティング・システムにインストールできます。

- Microsoft* Windows* 7 (インテル® AMT 11.8 システムのみ†)
- Microsoft* Windows* 10

インテル® EMA サーバーは、以下のオペレーティング・システムにインストールできます。

- Microsoft* Windows Server* 2012
- Microsoft* Windows Server* 2012 R2
- Microsoft* Windows Server* 2016
- Microsoft* Windows Server* 2019

† Windows* 7 はインテル® AMT 11.8 システムのみでサポートされ、インテル® AMT 16 リリース後はサポートされません。

1.3 インストールの前提条件

インテル® EMA サーバーのセットアップに必要な前提条件は以下のとおりです。

- **コンピューター：**予想されるトラフィックに十分対応できる能力を持つコンピューターまたは仮想マシン。これらの最小仕様を満たさないシステムでは、パフォーマンスの問題が発生する可能性があります。
    - 2 つのインテル® Xeon® プロセッサー、16 スレッド、24GB RAM、1TB (ミラーリング)：この構成で 2 万以上の接続を処理できると考えられます。
- **オペレーティング・システム：**セクション 1.2 の「サポートされるオペレーティング・システム」を参照してください。
    - インテル® EMA は現時点では国際化サポートを提供していません。オペレーティング・システムには、English-US の Windows* 表示言語、English-US システムロケール、English-US 形式 (Windows* 表示言語と同じ) が設定されている必要があります。
- **データベース：**Microsoft* SQL Server* をインストールします。データベースは、インテル® EMA サーバーと同じシステムか、ネットワーク上の別のサーバーで実行できます。使用する SQL Server* で全文検索が有効になっていることを確認してください。デモまたはテスト用である場合は、Advanced 機能付きの Microsoft* SQL Server* Express を使用できますが、本番環境では Microsoft* SQL Server* Enterprise の使用を推奨します。SQL および Active Directory* のインストール、構成、使用に関する高度な実践的知識が必要です (802.1x を使用する場合)。

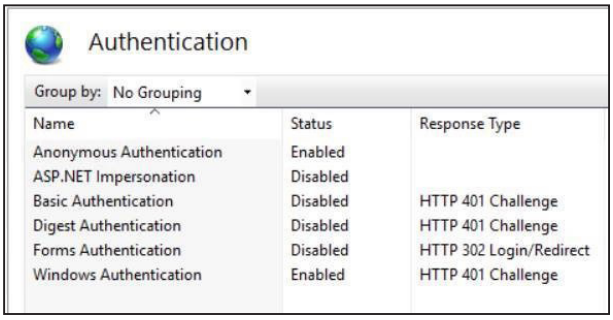
⚠ **重要：**多層セキュリティーを実現するため、Microsoft* SQL Server* Enterprise を使用して透過的なデータ暗号化 (TDE) を有効にすることを推奨します。また、認証モードには Windows* 認証モードを推奨します。

注記：

- Microsoft* SQL Server* 2012、2014、2016、2017、2019 (English-US バージョンのみ) がサポートされています。
- SQL Server* 実行中のマシンのオペレーティング・システムがサポート対象バージョンのオペレーティング・システムで、かつ English-US Windows* 表示言語、English-US システムロケール、English-US 形式 (Windows* 表示言語と同じ) が設定されている必要があります。セクション 1.2 の「サポートされるオペレーティング・システム」を参照してください。
- SQL Server* には必ず十分なリソース (CPU、メモリー、SSD など) を割り当ててください。SQL Server* のリソースを動的に割り当てる場合は、保証された十分な固定リソースが割り当てられることを確認してください。それ以外の場合、**Program Files (x86)\Intel\Platform Manager\EmaLogs** 内のコンポーネント・サーバーのログファイルに、「Unable to get database connection, all connections are busy」などのエラーメッセージが表示される場合があります。
- インテル® EMA は、データベース読み取り回数を減らすために SQL Server* でクエリー通知を使用します。このため、SQL Server* で「Service Broker」を有効にする必要があります。Service Broker が無効になっている場合、**Program Files (x86)\Intel\Platform Manager\EmaLogs** 内のコンポーネント･サーバーのログファイルに警告が表示される場合があります。
- インテル® EMA をインストールする前に、インテル® EMA の SQL 接続文字列で使用される SQL アカウントの権限を確認します。sysadmin 権限 (IIS のデフォルト・アプリケーション・プール ID の新規アカウントを作成するため) と、任意のデータベースを作成、変更、削除できる dbcreator 以上のアクセス許可が付与されている必要があります。また、このアカウントには、データベース・レベルの db_owner、db_datawriter、db_ datareader ロールが割り当てられていなければなりません。「sysadmin」権限が必要なのは、SQL Server* 用の新規ユーザーを「IIS APPPOOL\\DefaultAppPool\」および「ApplicationPoolIdentity\」に作成する必要があるからです (存在しない場合のみ)。これらのユーザーがあらかじめ存在しているか、インテル® EMA ウェブサイトの IIS アプリケーション・プールでこのアカウントを使用しない場合、インストール中に必要なロールは、インテル® EMA データベースを作成するための「dbcreator」になります。「sysadmin」または「dbcreator」権限が必要になるのはインテル® EMA のインストール中のみです。インテル® EMA データベースのユーザーには、「SUBSCRIBE QUERY NOTIFICATIONS」アクセス許可を付与する必要があります。これらのアクセス許可とロールの変更については、セクション 1.4.18 を参照してください。

- **ウェブサーバー：**インテル® EMA では Microsoft* Internet Information Server (IIS) を使用します。最新の IIS 8、IIS 8.5、IIS 10 バージョンを使用してください。
  - ターゲットの IIS には、IIS URL 書き換えモジュールをインストールします。このモジュールがインストールされている場合、インテル® EMA のウェブサイト設定により、レスポンスヘッダー、HSTS ヘッダー、Same Site = strict の cookie、HTTP → HTTPS の自動リダイレクトから IIS サーバーバージョンが除外されます。このモジュールがインストールされていない場合、これらの設定は適用されません。

注記：IIS がすでにインストールされている場合、「Anonymous (匿名)」および「Windows*」を除くすべての認証方法が無効化されていることを確認してください (これら 2 つの認証方法のみを有効化します)。これは、Windows* 認証モードのみに当てはまります。



- **インテル® AMT PKI 証明書:**インテル® AMT の管理者コントロール・モード (ACM) プロビジョニングでは、信頼できる機関によって発行され、ターゲットのインテル® AMT エンドポイントのドメイン名に適合する証明書が必要です。証明書ファイルには完全な証明書チェーンが含まれている必要があります。また、サポートされる OID 2.16.840.1.113741.1.2.3 (インテル® AMT 専用の OID) を使用して発行された証明書でなければなりません。
- **Microsoft* .NET Framework バージョン：**インテル® EMA サーバー・ソフトウェアは Microsoft* .NET Framework 4.8 で構築されています。オペレーティング・システムの Microsoft* .NET Framework がバージョン 4.8 以上である必要があります。.NET Framework 4.8 以上がインストールされていない場合、インテル® EMA インストーラーに .NET Framework 4.8 ランタイムのダウンロードとインストールを促すダイアログが表示されます。
- **ファイアウォール：**承認されたポートのみに接続できるようにするため、ファイアウォール・ソフトウェアの使用を推奨します。このタスクは Windows* に組み込まれたファイアウォール・ソフトウェアで実行できます。
- **ネットワーク:**インストール中に、各種コンポーネント間の通信で使用する値 (ホスト名または IP アドレス) を指定する必要があります。ホスト名または FQDN を選択した場合、この値がネットワーク内の DNS サーバーによって解決されることを確認する必要があります。DNS サーバーがない場合、インストール中は固定 IP アドレスを使用してください。ホスト名/IP アドレスが正しくない場合、インテル® EMA が正しく機能しない場合があります。分散サーバー・アーキテクチャーで Active Directory* を使用している場合、すべてのコンピューター (ロードバランサーをホストしているコンピューターを含む) が Active Directory* に登録されていることを確認してください。
- **ネットワーク・ポート：**表 1 に、サーバー・コンポーネント間の各種通信で使用されるサーバー・ネットワーク・ポートを示します。
    - 特定の機能/用途では、Ajax サーバーと管理機能サーバーが Swarm サーバーを使用して TCP 接続を (ローカルまたはリモートで) 確立します。
    - エンドポイントと Swarm サーバーはセキュアな TCP 接続を介して通信します。インテル® AMT (CIRA) と Swarm サーバーもセキュアな TCP 接続経由で通信します。
    - Platform Manager サービスは名前付きパイプを使用して、同じマシン上の別のインテル® EMA コンポーネント・サーバーと通信します。Platform Manager クライアント・アプリケーションは、セキュアな TCP 接続を介して Platform Manager サービスと通信します。

表 1：サーバー・ネットワーク・ポート

プロトコル	ポート	用途
TCP	443	HTTPS ウェブサーバー・ポート。ウェブブラウザーと ウェブサーバーの間で使用されます。
TCP	1433	SQL Server* のリモートアクセス。内部インテル® EMA サーバーと内部 SQL Server* の間で使用され、インテル® EMA サーバーと SQL Server* が同じマシン上にない場合のみ必要です。これは SQL Server* が使用するデフォルトポートです。
TCP	8000	Platform Manager サービスと Platform Manager クライアントの間の通信で使用されるデフォルト TCP ポート。このポートはインストール中に変更できます。
TCP	8080	エージェント、コンソール、インテル® AMT CIRA のポート。クライアントのエンドポイントとインテル® EMA Swarm サーバーの間で使用されます。下の注記を参照してください。
TCP	8084	ウェブ・リダイレクション・ポート。ウェブブラウザーとウェブサーバーの間で使用されます。
TCP	8089	各種のインテル® EMA コンポーネント・サーバーとインテル® EMA Swarm サーバーの間の通信で使用されます。このポート番号はデフォルトであり、Server Settings (サーバー設定) ページで変更できます。40 ページの「付録 - コンポーネント・サーバーの設定変更」を参照してください。

TCP	8092	Ajax コンポーネント・サーバーが内部のコンポーネント間通信をリッスンするポート。このポート番号はデフォルトであり、Server Settings (サーバー設定) ページで変更できます。40 ページの「付録 - コンポーネント・サーバーの設定変更」を参照してください。
TCP	8093	Swarm コンポーネント・サーバーが内部のコンポーネント間通信をリッスンするポート。このポート番号はデフォルトであり、Server Settings (サーバー設定) ページで変更できます。40 ページの「付録 - コンポーネント・サーバーの設定変更」を参照してください。
TCP	8094	管理機能コンポーネント・サーバーが内部のコンポーネント間通信をリッスンするポート。このポート番号はデフォルトであり、Server Settings (サーバー設定) ページで変更できます。40 ページの「付録 - コンポーネント・サーバーの設定変更」を参照してください。

1.4 セキュリティーに関する推奨事項

このセクションでは、インテル® EMA を使用するにあたって考慮する必要のある、セキュリティーに関する推奨事項を詳しく説明します。以下の推奨事項を実装する方法については、業界のベスト・プラクティスの情報源や IT 組織のポリシーを参照してください。

1.4.1 重要なデータのバックアップ

インテル® EMA のコンポーネント・サーバーは、インテル® EMA インストール時に作成される複数の証明書に依拠しています。

インストーラーによって自己署名付きの MeshRoot ルート証明書が作成されます。この証明書を使用して、証明書ストアの Local Computer (ローカル・コンピューター) \Personal (個人) に格納される 1 つまたは複数の MeshSettingsCertificates が作成されます。これらの MeshSettingsCertificate 証明書は、データベースに保存されるサーバー設定を暗号化/復号化するために使用されます。

MeshRoot 証明書を使用して、インテル® EMA コンポーネント・サーバー (Ajax サーバー、Swarm サーバー、管理機能サーバー、ウェブサーバー) 間の TCP-TLS 通信に使用される相互 TLS 証明書 (EmaMtlsXXX) が作成されます。これらは証明書ストアの Local Computer (ローカル・コンピューター) \Personal (個人) に格納されます。

これらの証明書が失われた場合、インテル® EMA を再び動作させるには、インテル® EMA サーバーを完全に再インストールするしかありません。

そのため、インテル® EMA サーバー (分散環境では各サーバー) をインストールした後、以下の手順を実施することを強くお勧めします。

- **インテル® EMA データベース**をバックアップします (セットアップ直後のみでなく、定期的に実施してください)。
- サーバーマシンの証明書ストアの Local Computer (ローカル・コンピューター) \Personal (個人) にある **MeshSettingsCertificate** をバックアップします。この証明書は、データベースに保存されるサーバー設定を暗号化/復号化するために使用されます。

1.4.2 鍵コンフィグレーション・ファイルのアクセス制御リスト (ACL) の変更

インテル® EMA サーバーをインストールした後、ACL を変更して次のファイルまたはフォルダーへのアクセスを制限する必要があります。

- [インテル® EMA ウェブサイトのルートフォルダー (例：C:\inetpub\wwwroot)] \ web.config
- [インテル® EMA サーバーのインストール・フォルダー (例：C:\Program Files (x86)\Intel\Platform Manager)] \ Platform Manager Server \ settings.txt
- [インテル® EMA サーバーのインストール・フォルダー (例：C:\Program Files (x86)\Intel\Platform Manager)] \ Runtime \ MeshSettings \ connections.config
- [インテル® EMA サーバーのインストール・フォルダー (例：C:\Program Files (x86)\Intel\Platform Manager)] \ Runtime \ MeshSettings \ app.config
- [インテル® EMA サーバーのインストール・フォルダー (例：C:\Program Files (x86)\Intel\Platform Manager)] \ EMALogs

1.4.3 SQL Server* Enterprise での透過的なデータ暗号化 (TDE) の有効化

多層セキュリティーを実現するため、SQL Server* Enterprise を使用して透過的なデータ暗号化 (TDE) を有効にすることを推奨します。

1.4.4 すべての証明書および鍵の安全な保管

インテル® EMA をインストールすると、複数の証明書および暗号鍵が生成されます。インテル® EMA によって生成された証明書および暗号鍵は 20 年後に期限が切れます。

証明書はインテル® EMA サーバーのデータベースとサーバーマシンの証明書ストアに保存されます。これらの証明書は安全に保管してください。証明書が危殆化した場合、インテル® EMA がそれを置き換えて管理対象のエンドポイントにプッシュすることはできません。そうなった場合、インテル® EMA サーバーをアンインストールし、新しい証明書を使用して再インストールし、すべてのユーザーとエンドポイント・グループを再作成し、さらに、すべてのエンドポイントを再登録する必要があります。

ほとんどの暗号鍵はインテル® EMA のサーバー設定に保存されており、インテル® EMA サーバーのデータベースに暗号化されて格納されています。

1.4.5 インテル® EMA REST API および JavaScript* ライブラリーのサンプルファイル

サンプルファイルは、フォルダー [インテル® EMA のインストール・パッケージ・フォルダー] \Samples にあります。インストール時、これらのファイルはインテル® EMA ウェブサイト上に自動的にホスティングされます。これらのサンプルファイルは、API の使用方法を分かりやすく示すため、最小限のコードを使用して実装されています。そのため、クロスサイト・スクリプティングのようなセキュリティー上の懸念に対して対策を取ったセキュアなコーディング手法は使用していません。

⚠ **重要：**上記のサンプルは**決して**本番環境にホスティングしないでください。

開発目的でテスト環境にホスティングするには、Samples フォルダーをインテル® EMA ウェブサイトのルートフォルダー (C:\inetpub\wwwroot\ など) にコピーします。

1.4.6 安全でない暗号スイートの無効化

暗号スイートにより、SSL/TLS セッションで使用される鍵交換、認証、暗号化、アルゴリズムが決定されます。

安全でない暗号スイートを無効化して、TLS 接続に脆弱な暗号化アルゴリズムおよびプロトコルが使用されないようにすることを強く推奨します。

多くのバージョンの Microsoft* Windows Server* において、安全でない暗号スイートがデフォルトで設定されている可能性があります。安全でない暗号スイートによって生じる警告または脅威を以下にまとめます。

- 64 ビット・ブロック暗号化 3DES が SWEEET32 攻撃にさらされる可能性
- 破られた暗号 RC4 は、RFC 7465 で廃止済み
- SSLv3 の CBC モード暗号 (CVE-2014-3566) – パディングオラクル攻撃
- メッセージの整合性検証に MD5 を使用する暗号スイート
- SHA1 の脆弱な証明書署名
- 鍵交換 (DH 1024) は証明書鍵より強度が低い

これらの脅威と警告を回避する 1 つの方法は、こちらのウェブサイト (https://www.nartac.com/Products/IISCrypto) から IIScrypto をダウンロードすることです。この製品は、セキュアチャネル (schannel) と暗号設定を変更するのに役立ちます。

IIScrypto プログラムを実行し、Multi-Protocol Unified Hello、PCT 1.0、SSL2.0、MD5、Triple DES より上のすべての暗号の選択を解除します。これにより、上述の警告 (SHA1 警告を除く) がすべてクリアされます。

1.4.7 強力な暗号化プロトコル

PCT 1.0、SSL 2.0、SSL 3.0、TLS 1.0、TLS 1.1 などの脆弱な暗号化プロトコルを無効化し、TLS 1.2 などの強力な暗号化プロトコルを有効にすることを強く推奨します。さらに、Diffie-Hellman Ephemeral (DHE) プロトコルを使用することをお勧めします。

注記 : お使いの環境に 11.8.77.3664 以前のバージョンのインテル® AMT が動作するエンドポイントが含まれる場合、これらのエンドポイントとの正常な通信を確保するためには TLS 1.1 は有効にしたままにする必要があります。

1.4.8 IIS – 一時的なウェブ TLS 証明書の差し替え

ウェブ TLS 証明書は、ウェブブラウザーとウェブサーバー + Ajax サーバー間の HTTPS 通信に使用されます。インストール中、一時的な自己署名付きウェブ TLS 証明書が作成されます。この証明書はいつでも差し替え可能です。有効な信頼できる認証局によって発行された有効な HTTPS 証明書を使用することをお勧めします。

注記 :

- Platform Manager を IIS サーバーと同じシステムで実行している場合、この TLS 証明書は Platform Manager の TLS 証明書としても使用できます。セクション 4.1 を参照してください。
- インテル® EMA では、自己署名付きウェブサイト TLS 証明書 (およびインテル® EMA 設定証明書) に対し、デフォルトの IIS DefaultAppPool アカウントに秘密鍵への読み取りアクセスを付与します。IIS のデフォルト・アプリケーション・プールが実行されるアカウントを変更した場合、アクセス制御も合わせて変更する必要があります。

一時的なウェブ TLS 証明書を差し替える手順は以下のとおりです。

1. 証明書ストアの Local Computer (ローカル・コンピューター) \Personal (個人) に新しい証明書をインストールします。
2. ウェブサーバー (IIS サーバー) で IIS マネージャーを実行します。
3. Server Certificates (サーバー証明書) に証明書を配置します。
4. Default Web Site (デフォルト・ウェブサイト) ダイアログボックスの Bindings (バインド) セクションを編集して、新しい証明書を設定します。

1.4.9 IIS – IIS ユーザーアカウントの変更

デフォルトでは、インテル® EMA は IIS のデフォルト・アプリケーション・プール (app pool) を使用してインテル® EMA ウェブサイトを実行します。このデフォルト・アプリケーション・プールでは、デフォルトで ApplicationPoolIdentity アカウントが使用されます。Windows* 認証モードで実行される分散インストールでは、インテル® EMA コンポーネント・サーバーがリモートの SQL Server* にアクセスする必要があるため、インテル® EMA ウェブサイトが実行されるアカウントを、リモートの SQL Server* にアクセス可能なアカウントに変更する必要がある場合があります。

その場合、次の手順に従います。

1. SQL 接続で Windows* 認証が使用されている場合、新しい IIS ユーザーアカウントが SQL Server* アカウントのアクセス許可要件およびロール要件を満たしていることを確認します。10 ページのセクション 1.4.18「SQL Server* ユーザーのアクセス許可の変更（必要な場合）」を参照してください。
2. インテル® EMA 用の新しい IIS アプリケーション・プールを追加します。
    1. IIS マネージャーを使用して、新しいアプリケーション・プールを作成します。
    2. **.NET CLR Version v4.0.XXX（.NET CLR バージョン v4.0.XXX）**と、Integrated（統合）パイプライン・モードを選択し、**Start app pool immediately（アプリケーション・プールを直ちに開始する）**チェックボックスをオンにします。
3. 新しいアプリケーション・プールにアカウントを割り当てます。
    1. IIS マネージャーを使用して、新しいアプリケーション・プールのアカウントを変更します。
    2. **Custom Account（カスタムアカウント）**を選択し、必要な Windows* アカウントを指定します。
4. そのアカウントにインテル® EMA のアセット（ファイルやフォルダー、証明書の秘密鍵）へのアクセス権を付与します。
    1. そのアカウントがすでにローカルマシンの管理者グループに割り当てられている場合、この手順は省略します。
    2. **[システムドライブ]\Program Files (x86)\Intel\Platform Manager\EMALogs** への読み取りおよび書き込みアクセス権を付与します。
    3. 以下へのフル・コントロール権を付与します。
        - **[システムドライブ]\C:\inetpub\wwwroot**：すべてのサブフォルダーとファイルにも付与します。
        - **[システムドライブ]\C:\inetpub\wwwroot\web.config**
        - **[システムドライブ]\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\app.config**
        - **[システムドライブ]\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config**
        - **[システムドライブ]\ProgramData\Intel\EMA\USBR**
    4. Windows* の certlm ツールを使用して証明書ストアの Local Computer（ローカル・コンピューター）\Personal（個人）\Certificates（証明書）を開き、証明書を右クリックして All Tasks（すべてのタスク）\Manage Private Keys（秘密キーの管理）を選択し、以下の証明書に「読み取り」アクセス許可を付与します。
        - 一時的なウェブ TLS 証明書。Issued To（発行先）は、インテル® EMA ウェブサイトの FQDN または IP です。Issued By（発行元）は「MeshRoot-XXXX」です。
        - 設定証明書。Issued To（発行先）は「MeshSettingsCertificates-XXX」です。Issued By（発行元）は「MeshRoot-XXXX」です。
        - ウェブサーバー用のコンポーネント間 TLS 証明書。Issued To（発行先）は「EmaMtlsWeb-XXX」です。Issued By（発行元）は「MeshRoot-XXXX」です。
5. IIS マネージャーを使用して、インテル® EMA が使用するアプリケーション・プールを上記で作成した新しいプールに変更します。次に、ウェブサイト全体を再起動します。確認のため、ブラウザーでインテル® EMA ウェブサイトにアクセスし、Windows* のタスク・マネージャーで **w3wp.exe** プロセスが指定したアカウントで実行されていることを確認します。

1.4.10 IIS – TLS（Transport Layer Security）プロトコルの有効化

インターネットを介してやり取りされる情報の秘匿性を守るために設計された業界標準のプロトコルである TLS（Transport Layer Security）プロトコルを有効化することを強くお勧めします。

TLS プロトコルを有効化すると、クライアント/サーバー・アプリケーションが以下のセキュリティー・リスクを検出できるようになります。

- メッセージの改ざん
- メッセージの傍受
- メッセージの偽造

HSTS（HTTP Strict Transport Security）は、オプトインのセキュリティー強化ポリシーです。TLS（Transport Layer Security）プロトコルが使用された場合のみ接続を許可するには、HSTS を有効にする必要があります。

1.4.11 IIS – MachineKey の検証方法

ASP.NET で使用される web.config の MachineKey 要素は、アプリケーションが暗号化とハッシュに使用するアルゴリズムおよび鍵を指定します。MachineKey の検証方法として SHA-2 ファミリーの方法の 1 つ（例えば、HMACSHA256）が設定されていることを確認してください。

1.4.12 IIS – 未指定の IIS 拡張の実行の制限

ISAPI 拡張または CGI の IIS 機能がインストールされている場合、指定していない ISAPI モジュールまたは CGI モジュールの実行が許可されていないことを確認します。

1.4.13 IIS – 動的 IP アドレスの制限

Dynamic IP Address Restrictions（動的 IP アドレス制限）は、DDoS や総当たり攻撃への緩和策として使用できる IIS の設定です。シングル・サーバー・インストールの場合、IIS マネージャーを使用して Deny IP Address based on the number of concurrent requests（同時要求の数に基づいて IP アドレスを拒否する）チェックボックスと Deny IP Address based on the number of requests over a period of time（一定期間の要求数に基づいて IP アドレスを拒否する）チェックボックスをオンにし、環境を保護するために必要な値を設定します。

詳細については、以下のリンクを参照してください。

https://docs.microsoft.com/en-us/iis/manage/configuring-security/using-dynamic-ip-restrictions

1.4.14 IIS – すべてのサイトにホストヘッダーを設定

IIS で同一の IP アドレスおよびポートに複数のウェブサイトがホストされる場合、すべてのサイトにホストヘッダーを設定します。

1.4.15 IIS – 更新された web.config ファイルの見直し

インテル® EMA サーバーをインストールすると、**web.config** ファイルに以下のヘッダーが追加され、既存の web.config ファイルの名前が **web.config.original.<日付>** に変更されます。インストール完了後、新しい web.config ファイルを見直して、必要に応じて変更します。

HTTP ヘッダーの詳細については、以下のリンクを参照してください。

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

インストール中に **web.config** ファイルに自動的に追加されるヘッダーは以下のとおりです。

表 2：web.config に追加されるヘッダー

ヘッダー	値
X-Content-Type-Options	`nosniff`
X-XSS-Protection	`1; mode=block`
X-Frame-Options	`SAMEORIGIN`
Referrer-Policy	`strict-origin`
Expect-CT	`max-age=86400, enforce`
Feature-Policy	`payment 'none'; microphone 'none'; geolocation 'none';`
strict-transport-security **注記：**IIS リライタールールによって追加	`max-age=31536000; includeSubDomains;`

Content Security Policy (CSP) **注記：**プラグインによって追加	`default-src 'self' blob:;script-src 'self' 'unsafe-inline' 'nonce-<autogen_value> ' 'sha256-<multiple values> ';object-src 'none';style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;img-src 'self' data:;font-src 'self' data: https://fonts.gstatic.com;base-uri 'none';worker-src 'self' blob:`

CORS ヘッダーは追加されますが、デフォルトではコメントアウトされています。有効にするには、web.config ファイルを編集してコメントタグを削除し、ドメイン情報を追加します。

```
<!--
<add name="Access-Control-Allow-Origin" value="https://<YOURDOMAINHERE>" />
<add name="Access-Control-Allow-Headers" value="Content-Type" />
<add name="Access-Control-Allow-Methods" value="GET,POST,PUT,DELETE,OPTIONS"
/>
-->
```

最後に、ウェブ検索エンジンによるインテル® EMA サーバーのインストール・インスタンスの検出を無効化する **X-Robots-Tag** ヘッダーが追加されます。

注記：インテル® EMA は、デフォルトの IIS DefaultAppPool アカウントに web.config ファイルへの読み取りアクセス権を付与します。IIS のデフォルト・アプリケーション・プールが実行されるアカウントを変更した場合、アクセス制御も合わせて変更する必要があります。

1.4.16 バイナリー署名のチェック

すべてのインテル® EMA バイナリーは、整合性メカニズムとして署名されています。これらのファイルの署名をチェックして確認することをお勧めします。さらに、信頼できるソース（www.intel.com など）から入手したインストール・パッケージのみを使用することをお勧めします。

1.4.17 Platform Manager のサービス・ユーザー・アカウントの変更

この操作は、インテル® EMA サーバーをインストールした後に実施します。デフォルトでは、インテル® EMA Platform Manager サービスはシステムユーザーで動作します。セキュリティーを強化するため、このサービスをローカルまたはドメインユーザーで実行するように変更することをお勧めします。

それには、**Windows* の Services（サービス）**で **Intel Platform Manager** を見つけ、サービスを実行するユーザーアカウントを変更します。そのローカルまたはドメインユーザーのアカウントには、インテル® EMA サーバーマシンの管理者権限と C:\Program Files (x86)\Intel\Platform Manager（インテル® EMA がインストールされているフォルダー）への読み取りおよび書き込みアクセス権が付与されている必要があります。

さらに、新しい Platform Manager サービスアカウントについて、インテル® EMA インストール・フォルダー内のファイル **settings.txt** に読み取り/書き込みアクセス許可があることを確認します。

1.4.18 SQL Server* ユーザーのアクセス許可の変更（必要な場合）

インストール完了後、インテル® EMA によって使用される SQL アカウントは、ストアド・プロシージャーを実行し、データベース・コマンドを実行する必要があります。そのため、その SQL アカウントにはインテル® EMA データベースへの db_owner、db_datawriter、および db_datareader アクセス許可が必要です。これらのアクセス許可は、インテル® EMA をインストールするとデフォルトで付与されます。db_owner アクセス許可を付与しない場合、この SQL アカウントがインテル® EMA のすべてのストアド・プロシージャーを実行できるよう、実行アクセス許可を付与する必要があります。

また、インテル® EMA データベースのユーザーには、「SUBSCRIBE QUERY NOTIFICATIONS」アクセス許可を付与する必要があります。

1.4.19 ユーザーの作成と管理

インテル® EMA の既存のユーザーアカウントを定期的にチェックし、使用されなくなったアカウントを確実に削除することを強くお勧めします。ユーザーアカウントの作成、変更、削除の詳細については、インテル® EMA 管理と使用ガイドを参照してください。

1.4.20 TLS がインストールされた SQL Server* の使用

SQL Server* とインテル® EMA 間で送信されるデータを暗号化するために TLS がインストールされた SQL Server* インスタンスを使用することを強くお勧めします。詳細については、以下のリンクを参照してください。

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15

1.5 インストールされるインテル® EMA コンポーネント

インストールの完了後、ほとんどのソフトウェア・コンポーネントは **C:\Program Files (x86)\Intel\Platform Manager** フォルダーにインストールされています。主要なコンポーネントは以下のとおりです。

- インテル® EMA Platform Manager サービス：
  - 自動起動の Windows* サービスとしてインストールされ、表示名は **Intel® EMA Platform Manager**、サービス名は **PlatformManager** になります
  - インテル® EMA ウェブサイトのコンテンツを IIS サーバーに展開します
  - マシン上のインテル® EMA コンポーネント・サーバーを監視し、実行されていない場合は自動起動します
  - 分散サーバー・アーキテクチャーでは、それぞれのインテル® EMA サーバーマシンに専用の Platform Manager サービスが構成されます
- インテル® EMA Platform Manager クライアント・アプリケーション：
  - Windows* デスクトップ・アプリケーションとしてインストールされます
  - ユーザーとやり取りするためのグラフィカル・ユーザー・インターフェイス (GUI) を提供します
  - インテル® EMA 内部サーバーイベントのチェックと簡単なサーバー制御に使用されます
  - ローカル/リモートマシン上の Platform Manager サービスと通信します
- インテル® EMA ウェブサイト：
  - エンドユーザー向けの一次 GUI
  - インストール後に、Platform Manager サービスによって IIS サーバー上に展開されます
  - 分散環境では複数のインスタンスを使用できます
  - 詳細については、インテル® EMA 管理と使用ガイドを参照してください
- インテル® EMA REST API：
  - インストール後に、Platform Manager サービスによって IIS サーバー上に展開されます
  - サードパーティー・ソフトウェア開発を有効にすることで、エンドユーザー向けに別のインテル® EMA GUI を作成できるようにします
  - 詳細については、インテル® EMA API ガイドを参照してください
- インテル® EMA JavaScript* ライブラリー：
  - インストール後に、Platform Manager サービスによって IIS サーバー上に展開されます
  - REST API では設計上サポートされない一部の機能を提供します

    - サードパーティー・ソフトウェア開発を有効にすることで、エンドユーザー向けに別のインテル® EMA GUI を作成できるようにします
    - 詳細については、インテル® EMA JavaScript* ライブラリー・ガイドを参照してください
- インテル® EMA Ajax サーバー：
    - Platform Manager サービスによって起動されます
    - JavaScript* ライブラリーのリクエストを処理します
    - 分散環境では複数のインスタンスを使用できます
    - スケジュール設定タスク機能の詳細については、インテル® EMA 管理と使用ガイドを参照してください
- インテル® EMA Swarm サーバー：
    - Platform Manager サービスによって起動されます
    - エンドポイント（デバイス）からの TCP 接続を受け入れて、エンドポイント間の通信を処理します
    - 分散環境では複数のインスタンスを使用できます
- インテル® EMA 管理機能サーバー：
    - Platform Manager サービスによって起動されます
    - エンドポイントに対するインテル® AMT のプロビジョニング/プロビジョニング解除リクエストを管理します
    - Swarm サーバーと通信して、エンドポイントにプロビジョニング/プロビジョニング解除リクエストを送信します
    - 分散環境でもインスタンスは 1 つのみです
- インテル® EMA エージェント：
    - エージェント・ソフトウェアはサーバーマシンにはインストールされません
    - エージェント・インストーラーはインテル® EMA ソフトウェア・パッケージに含まれています
    - インテル® EMA サーバーがエンドポイントを管理するには、そのエンドポイントにエージェントがインストールされている必要があります
    - エージェント・インストーラーのダウンロードおよび管理方法については、インテル® EMA 管理と使用ガイドを参照してください

1.6 重要なファイルおよびディレクトリーの場所

<インストーラー・ディレクトリー>/ EMALog-Intel®EMAInstaller.txt	インストール・ログ
C:\Program Files (x86)\Intel\Platform Manager\ Platform Manager Server\settings.txt	Platform Manager の設定（ポート番号とパスワードを含む）が格納されています。
C:\Program Files (x86)\Intel\Platform Manager\ Runtime\MeshSettings\app.config and connections. config	データベース接続文字列が格納されています。
C:\Program Files (x86)\Intel\Platform Manager\ EMALogs • EMALog-XXX.txt • TraceLog-XXX.txt	各サーバー・コンポーネントのログ。これらは、Platform Manager のイベントログで表示されるログメッセージと同じです。

C:\Program Files\Intel\Ema Agent	64 ビットのインテル® EMA エージェント・ファイルがインストールされる場所。32 ビットのエージェントについては、Program Files (x86) を参照してください。
C:\inetpub\wwwroot	IIS ウェブサイトの場所。

1.7 スケーリングに関する考慮事項

インテル® EMA サーバーの実装を計画するとき、管理対象のエンドポイントの増加に伴い、サーバー・ハードウェアの構成によってインテル® EMA インスタンスの全体的パフォーマンスが左右されることを念頭に置いておく必要があります。次の表に、インテル® EMA サーバーのインストールのために適切なサーバー・ハードウェア構成を決定するのに役立つ可能性のあるテスト結果を示します。この表は、各行のサーバー・ハードウェア構成 (4 CPU、16 GB メモリーなど) において、列見出しのしきい値 (CPU の利用率 80% など) を達成するために要求される管理対象エンドポイントの数を示しています。

注記 : さまざまな環境要因により、パフォーマンスは実装ごとに大きく異なる可能性があります。以下のテスト結果情報は実装前の意思決定を支援するためのみに提供するもので、実際のパフォーマンスを主張するものではありません。

以下のテスト結果によれば、4 CPU、16 GB RAM の 1 台のインテル® EMA サーバーで、約 82,000 台の管理対象エンドポイントを十分にサポート可能と期待されます (以下の「メモリー使用率 10%」の列)。ただし、以下のどの列においても、CIRA を使用する場合はエンドポイントの数を半分に減らすことをお勧めします。さらに、以下のデータは管理対象エンドポイント上のインテル® EMA エージェントのアイドル状態に基づいています。エンドポイントでの KVM セッションなどの使用に備え、ある程度の余裕 (例えば 20%) を持たせる必要があります。

以上の検討事項を踏まえると、4 CPU、16 GB RAM の 1 台のインテル® EMA サーバーを CIRA を使用して実装した場合に推奨される管理対象エンドポイントの最大数は約 33,000 台となります (82000/2 * .80 = 32800)。

表 3 : スケーリング検討用データ

	インテル® EMA CPU 使用率 80%	インテル® EMA CPU 使用率 100%	インテル® EMA メモリー使用率 10%	DB CPU 使用率 80%	DB CPU 使用率 100%
2 CPU、8 GB メモリー	166,389	207,969	44,600	155,775	195,145
4 CPU、16 GB メモリー	349,636	436,972	82,180	290,036	363,566
8 CPU、32 GB メモリー	447,525	559,256	130,977	165,275	207,029

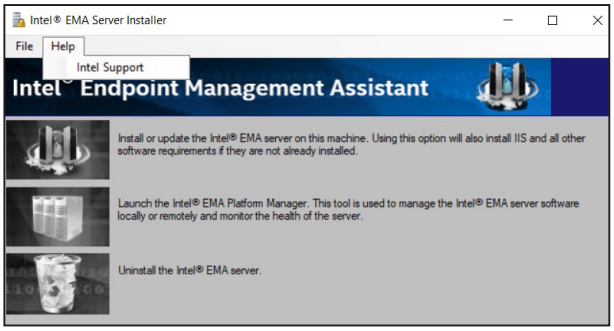
2 インテル® EMA サーバーのインストール/更新

インテル® EMA サーバーをインストールするには、以下の手順に従います。更新については、セクション 2.2 を参照してください。

インストール全般に関する注記：

- インテル® EMA データベースを編集して、手動でユーザーテーブルにユーザーを追加することは避けてください。インテル® EMA のユーザーアカウントはすべて、インテル® EMA のユーザー・インターフェイス (GUI または API) を使用して作成します。
- 同じインテル® EMA データベースを使用する別々のインテル® EMA インスタンスを 2 つインストールすることはサポートされていません。これは、1 つのインテル® EMA インスタンスのサーバー・コンポーネントを複数のマシンにインストールする分散サーバー・アーキテクチャー・インストールとは異なる点に注意してください。
- インテル® EMA の USB リダイレクト (USBR) 機能を使用すると、インテル® AMT を介してリモート・ディスク・イメージ (.iso または .img) を管理対象のエンドポイントにマウントできます。USBR 機能を有効にするため、インストーラーは、すべてのインテル® EMA ウェブサーバー・コンポーネントおよび管理機能サーバー・コンポーネントが実行されているアカウントにアクセス可能なフォルダーを作成します。このフォルダーは、インテル® EMA がアップロードされたイメージファイルを保存するためと、USB リダイレクトによって管理対象のエンドポイントにイメージファイルをマウントする際に保存されたイメージファイルにアクセスするために使用されます。USBR 機能の詳細については、インテル® EMA 管理と使用ガイドの**「USB リダイレクト」**のセクションを参照してください。

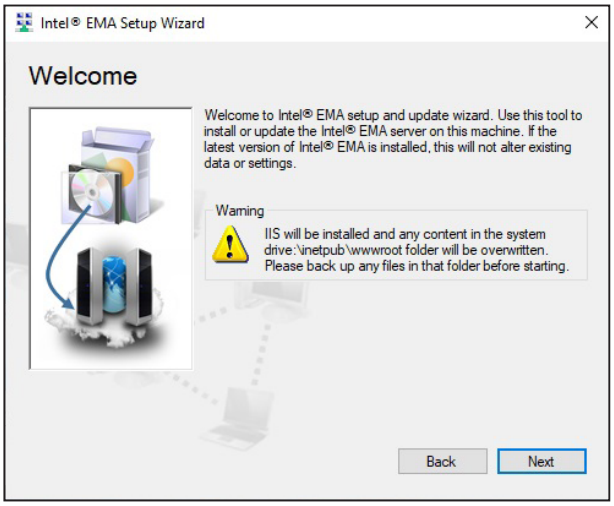
2.1 セットアップ・ウィザードを使用したインストール



インストール ZIP ファイルを解凍したフォルダーを開き、EMAServerInstaller.exe を右クリックして **Run as administrator(管理者として実行)**を選択します。インストーラーが開き、初期チェックに合格すると下部のステータスバーに Ready (準備完了) と表示されます。

左上のアイコンをクリックしてインストール・プロセスを開始します。

注記：不明な点がある場合は、**Help (ヘルプ) > Intel Support (インテルサポート)** をクリックします。

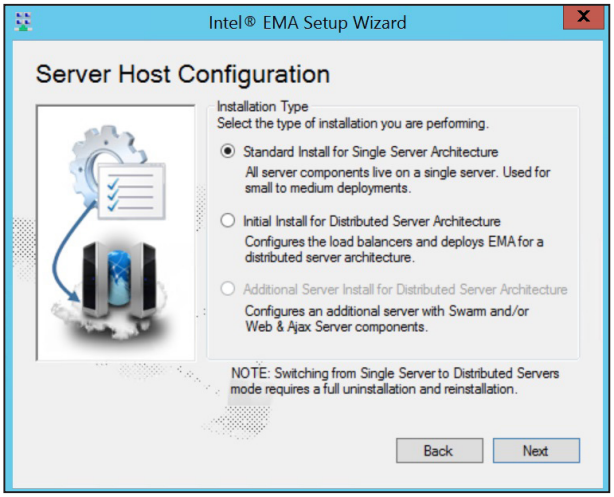


警告!初回インストールでは、インストール・プロセスを続行すると、インテル® EMA セットアップ・ウィザードによって c:\inetpub\wwwroot フォルダー内がすべて削除されます。インストール・プロセスを続行する前に、必要なファイルのバックアップを取ってください。

以前のインテル® EMA バージョンを更新する場合、これは当てはまりませんが、IIS バインドはデフォルト値に設定されます。Welcome(ようこそ)画面で **Next(次へ)** をクリックして、セットアップ・プロセスを続行します。License Agreement(ライセンス契約)が表示されたら、ライセンスに同意して続行します。

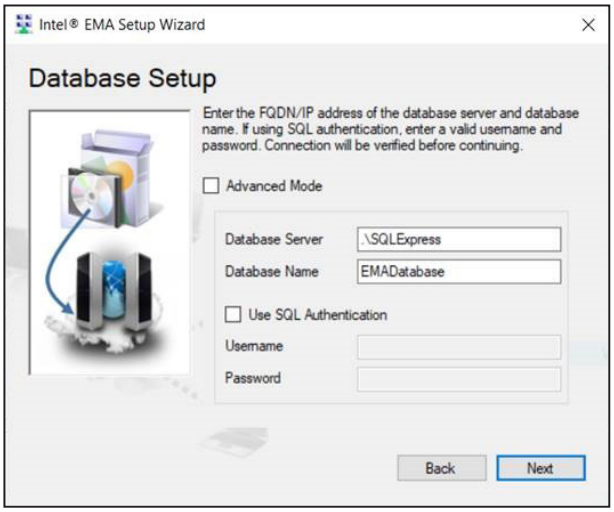
Welcome(ようこそ)画面で **Next(次へ)** をクリックして、セットアップ・プロセスを続行します。

2.1.1 サーバーホストの構成



Standard Install for Single Server Architecture(シングル・サーバー・アーキテクチャーの標準インストール) を選択します。

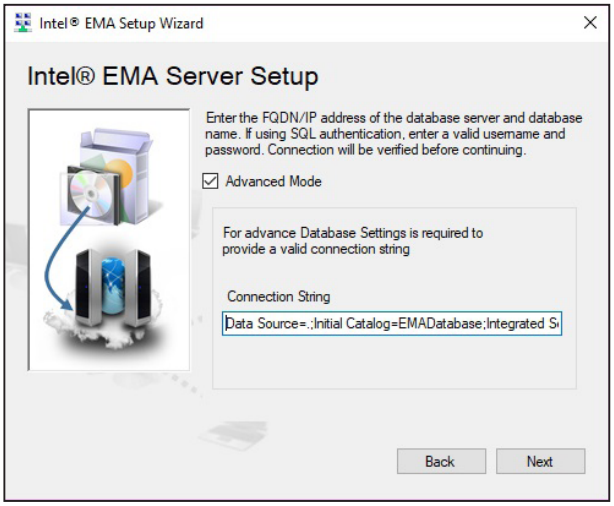
2.1.2 データベースの設定



データベースがホストされているサーバーを指定します。実際の値は、インストールしたデータベース・サーバーによって異なります。詳細については、インストールした SQL Server* を参照してください。

注記：

- インテル® EMA と同じマシンにインストールされた SQL Server* を使用する場合は、localhost を使用できます。
- リモートの SQL Server* を使用する場合、SQL Server* のアカウントに、使用する IIS のデフォルト・アプリケーション・プールの接続が設定されていることを確認してください。
- セキュリティーのため、SQL 認証ではなく Windows* 認証モードを使用することを推奨します。SQL 認証を使用する場合は、はじめにターゲットの資格情報を SQL Server* に設定する必要があります。



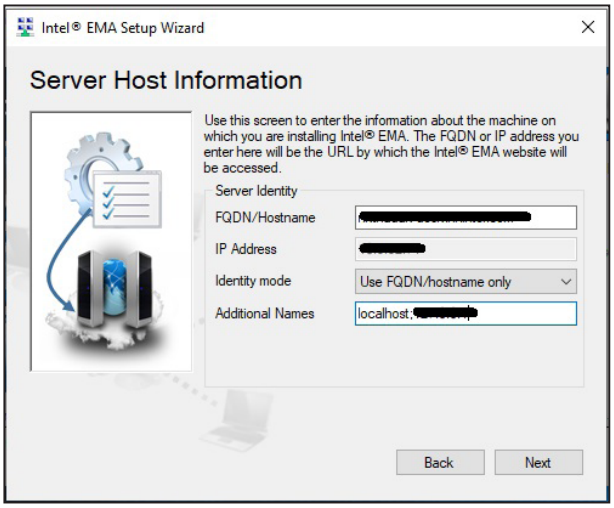
カスタマイズしたデータベース接続文字列を作成する場合は、**Advanced Mode** (アドバンスト・モード) チェックボックスをオンにして、接続文字列を入力します。

基本モードとアドバンスト・モードのどちらでも、インテル® EMA コンポーネント・サーバーが使用する接続文字列が作成されることに注意してください。アドバンスト・モードでは、ユーザーがカスタマイズした接続文字列を作成できます。接続文字列の詳細については、https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax を参照してください。

注記：パラメーター「MultipleActiveResultSets=True」は必須です。

モード (基本またはアドバンスト) に関係なく、接続文字列は暗号化され、**c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config** に保存されます。

2.1.3 サーバーホスト情報



サーバーのウェブサイト TLS 証明書を保有している場合、適合するサーバーのホスト名をここに入力します。

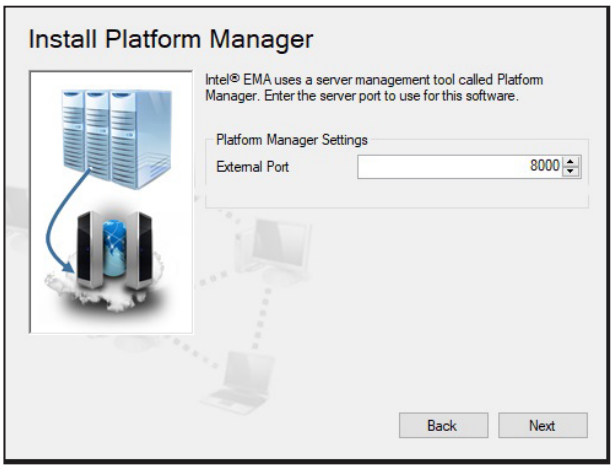
これがメインのインテル® EMA ウェブサイトの HTTPS URL です。この FQDN/ホスト名は、接続先のエンドポイントのエージェント構成ファイルで提供されるので、DNS で正しく解決されることを確認してください。

アイデンティティー・モードの場合：

- **Use FQDN/hostname only (FQDN/ホスト名のみを使用)：**FQDN/ホスト名のみを使用してリクエストを処理します。アドレス指定できる完全な FQDN を入力することを推奨します。
- **Use FQDN/hostname first (FQDN/ホスト名を最初に使用)：**FQDN/ホスト名を使用してリクエストを処理しますが、IP アドレス経由でウェブサイトを探すこともできます。
- **Use IP address (IP アドレスを使用)：**IP アドレスのみでリクエストを処理します。

注記：次のステップで、インテル® EMA をドメイン/Windows* 認証モード (Kerberos) でインストールする場合、Hostname (ホスト名) フィールドにマシンの FQDN を使用することを推奨します。ここで入力した値については、その他のエンドポイントまたはクライアント・ウェブ・ブラウザーから接続できることを確認する必要があります。別の値を使用する場合、IT ベスト・プラクティスに従って、インテル® EMA のインストール後にサービス・プリンシパル名 (SPN) を設定してください。Kerberos を使用する場合、Use IP address (IP アドレスを使用) は選択できません。

2.1.4 Platform Manager の構成



External Port (外部ポート) は、インテル® EMA サーバーで実行されるインテル® EMA Platform Manager サービスが、インテル® EMA Platform Manager クライアント・アプリケーションからの接続を受け入れるために使用されます。指定するポートが基盤ネットワーク上で開いていることを確認してください。

この画面は、更新モードでは編集できません。

2.1.5 ユーザー認証

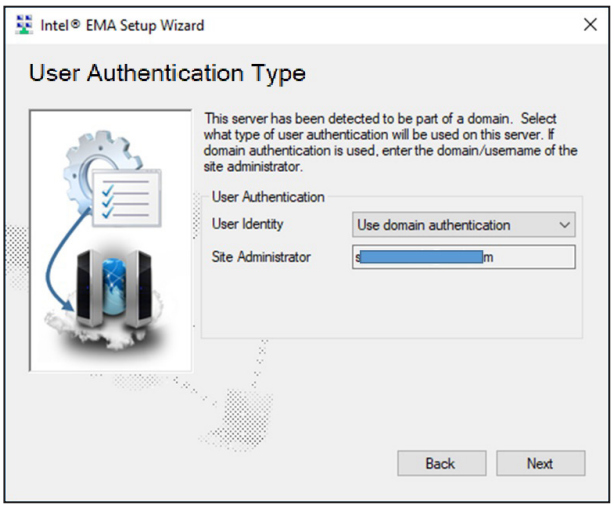
Use normal accounts (通常アカウントを使用) または **Use domain authentication (ドメイン認証を使用)** のどちらかを選択します。

2.1.5.1 通常アカウント

Use normal accounts (通常アカウントを使用) を選択すると、インテル® EMA は内部ユーザー・データベースをそのまま維持します。

これはこのインストール・プロセスのデフォルト設定です。これを選択してインストールしたインスタンスは、ユーザー名/パスワードモードになります。

2.1.5.2 ドメイン認証



使用するサーバーが Active Directory* ドメインに参加している場合、Use domain authentication (ドメイン認証を使用) オプションを選択できます。

現在ログインしているユーザーが、グローバル管理者ロール (左のスクリーンショットでは Site Administrator (サイト管理者) と表示) 付きで自動的に インテル® EMA に追加されます。

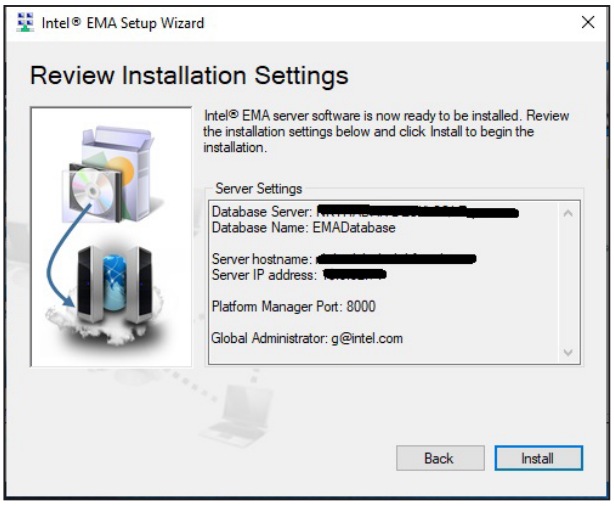
2.1.6 グローバル管理者アカウントのセットアップ

この画面は、セットアップ中にユーザー認証として「Normal accounts (通常アカウント)」を選択した場合にのみ表示されます。ドメインアカウントを使用している場合、インストーラーを実行しているユーザーがグローバル管理者になります。

注記：Name (名前) フィールドは、メールアドレス形式 (name@domain) で入力する必要があります。

Global Administrator (グローバル管理者)：このロールは、ユーザー管理、テナント作成、サーバー管理を実行できます。デバイス管理は実行しません。

2.1.7 まとめ



インストール設定を確認したら、**Install (インストール)** をクリックします。

すべての必要な Windows* コンポーネントがインストールされ、続いてインテル® EMA ソフトウェアがインストールされます。

重要：インストールが完了するまでの間、インストーラーを中止または終了しないでください。インストールのロールバックはサポートされていません。

インストーラーのメインメニュー下部にインストール・ステータスが表示されます。インストール中にインストール・オプションを変更することはできません。

インストール中にログファイルを確認するには、**File (ファイル) > Advanced Mode (アドバンスト・モード)** をクリックします。アドバンスト・モードを終了するには、**File (ファイル) > Advanced Mode (アドバンスト・モード)** をもう一度クリックします。

インストール終了後、インテル® EMA インストーラーと同じフォルダーにあるログファイル **EMALog-Intel®EMAInstaller.txt** を確認できます。

注記：ローカル SQL Server* またはリモート SQL Server* のどちらを使用してインストールした場合も、インストール・ログ・ファイルに以下の警告が表示されます。リモート SQL Server* を使用している場合、このメッセージは無視して問題ありません。ローカル SQL Server* を使用したインストールの場合、IIS のデフォルト・アプリケーション・プールの接続を許可するようにアカウントが設定されていることを確認してください。

```
EVENT: DbWarning, ExecuteNonQuerySafe warning: CREATE LOGIN [IIS
APPPOOL\DefaultAppPool] FROM WINDOWS() - System.Data.SqlClient.SqlException
(0x80131904): User does not have permission to perform this action.
```

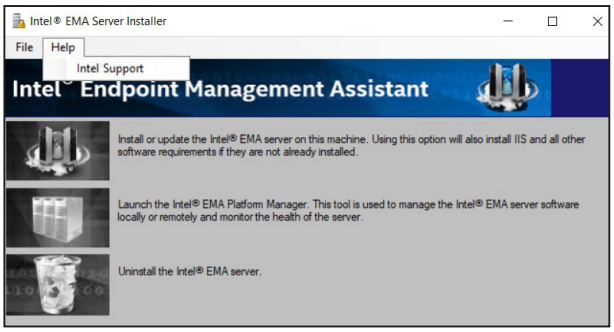
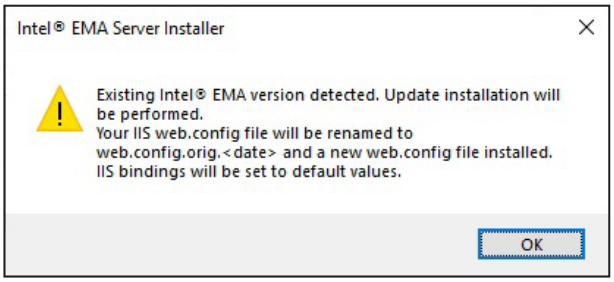
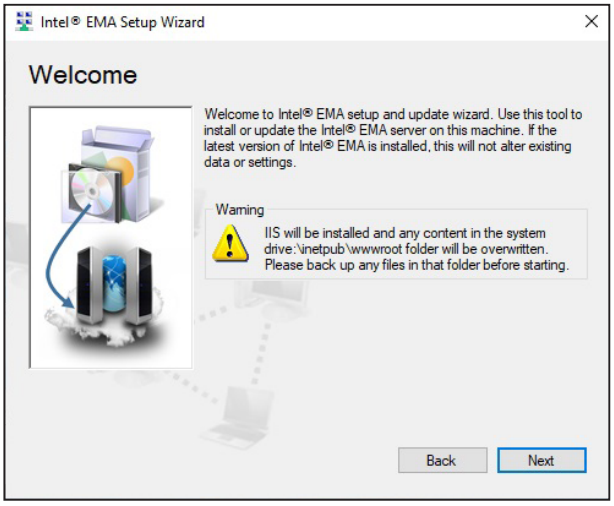
ここまでで、インテル® EMA サーバーの Platform Manager を使用する準備が整いました。Platform Manager の使用についてはセクション 4 で説明します。

2.2 セットアップ・ウィザードを使用した更新インストール

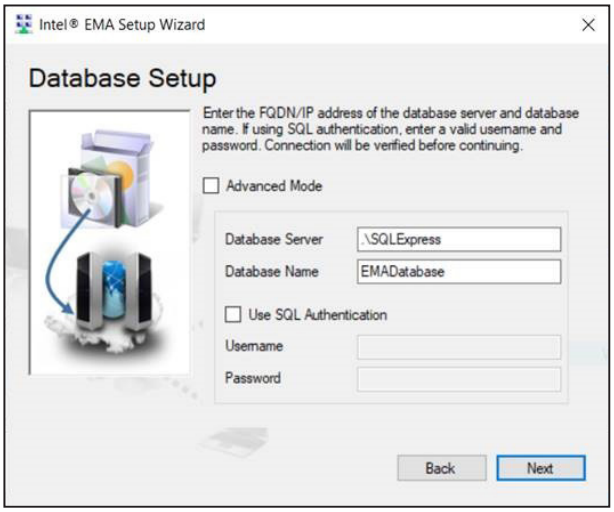
インテル® EMA セットアップ・ウィザードを使用して更新をインストールする手順は次のとおりです。

更新インストールに関する注記：

- 既存バージョンのインテル® EMA を更新する場合、更新のインストール中に、IIS 内のインテル® EMA ウェブサイトのバインドがデフォルト値に設定されます。参照用に更新前のバインドを確認する場合は、インストール後のログファイルから見つけることができます。

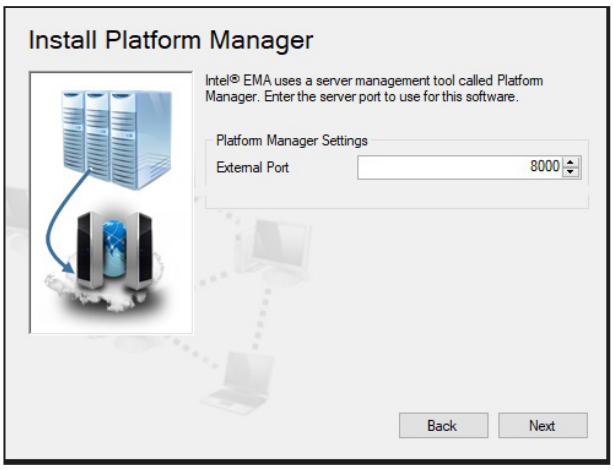
	インストール ZIP ファイルを解凍したフォルダーを開き、EMAServerInstaller.exe を右クリックして **Run as administrator(管理者として実行)**を選択します。インストーラーが開き、初期チェックに合格すると下部のステータスバーに Ready (準備完了) と表示されます。 左上のアイコンをクリックしてインストール・プロセスを開始します。 **注記：**不明な点がある場合は、**Help (ヘルプ) > Intel Support (インテルサポート)** をクリックします。
	更新インストールであることがインストーラーによって検出され、更新ファイルをインストールするために IIS の web.config ファイルの名前が変更されることが通知されます。 **OK** をクリックします。
	Welcome (ようこそ) 画面で **Next (次へ)** をクリックして、セットアップ・プロセスを続行します。 **注記：**IIS のインストールに関する警告は、更新インストールには適用されません。

2.2.1 データベースの設定



注記：更新モードの場合、フィールドはあらかじめ入力されており、変更はできません。

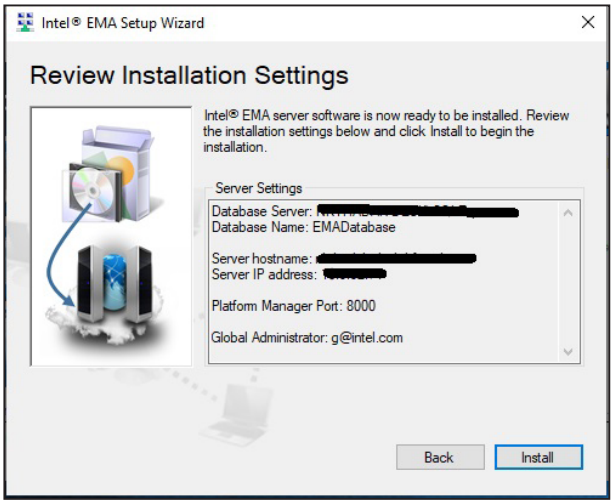
2.2.2 Platform Manager の構成



External Port (外部ポート) は、インテル® EMA サーバーで実行されるインテル® EMA Platform Manager サービスが、インテル® EMA Platform Manager クライアント・アプリケーションからの接続を受け入れるために使用されます。指定するポートが基盤ネットワーク上で開いていることを確認してください。

この画面は、更新モードでは編集できません。

2.2.3 まとめ



インストール設定を確認したら、**Install (インストール)** をクリックします。

すべての必要な Windows* コンポーネントがインストールされ、続いてインテル® EMA ソフトウェアがインストールされます。

重要：インストールが完了するまでの間、インストーラーを中止または終了しないでください。インストールのロールバックはサポートされていません。

インストーラーのメインメニュー下部にインストール・ステータスが表示されます。インストール中にインストール・オプションを変更することはできません。

インストール中にログファイルを確認するには、**File (ファイル) > Advanced Mode (アドバンスト・モード)** をクリックします。アドバンスト・モードを終了するには、**File (ファイル) > Advanced Mode (アドバンスト・モード)** をもう一度クリックします。

インストール終了後、インテル® EMA インストーラーと同じフォルダーにあるログファイル **EMALog-Intel®EMAInstaller.txt** を確認できます。

2.3 コマンドラインを使用したインストール/更新

このセクションでは、コマンドラインからインストールまたは更新する方法を説明します。

コマンド・ライン・インストールには 2 つのモードがあります。Basic Mode (基本モード) と Advanced Mode (アドバンスト・モード) です。すべてのデータベース接続値をコマンドラインで直接提供するには、基本モードを使用します。カスタマイズされたデータベース接続文字列を提供するには、アドバンスト・モードを使用します。

基本モードとアドバンスト・モードのどちらでも、インテル® EMA コンポーネント・サーバーが使用する接続文字列が作成されることに注意してください。アドバンスト・モードでは、ユーザーがカスタマイズした接続文字列を作成できます。接続文字列の詳細については、https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax を参照してください。モード (基本またはアドバンスト) に関係なく、接続文字列は暗号化され、**c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config** に保存されます。

注記：以前のバージョンのインテル® EMA から更新する場合、インストーラーによって接続文字列が自動的に検出されます。

注記：シングルサーバーの標準インストールでは、インテル® EMA インストーラーによって USB リダイレクト (USBR) 機能で使用するためのフォルダーが作成されます。このフォルダーに保存されたイメージファイル (.iso または .img) を使用して管理対象エンドポイントを起動できます。このフォルダーは、SYSTEM、Administrators、および IIS_AppPool\DefaultAppPool のアクセス許可が付与されて作成されます。このアクセス許可を変更した場合、次にインテル® EMA に更新インストールを行うとき、フォルダーのアクセス許可が要件を満たさないことを警告するメッセージがログに記録されます。USBR 機能の詳細については、インテル® EMA 管理と使用ガイドの**「USB リダイレクト」**のセクションを参照してください。

インストール・パッケージを解凍したフォルダー内で、管理者モードでコマンドプロンプトを開きます。

2.3.1 基本モード

以下のコマンド・シンタックス・テンプレートを使用して、山括弧 (<>) で囲まれた値は置き換え、通常のユーザーアカウントを使用してインストールします。ドメイン認証を含むその他のオプションについては、--help オプションを付けて実行ファイル単独で実行してください。

```
EMAServerInstaller.exe FULLINSTALL --host=<サーバーの FQDN> --dbserver=<DB サーバーのアドレス>
--db=<DB 名> --dbuser=<SQL ユーザー> --dbpass=<SQL パスワード> --guser=<グローバル管理者のメール>
--gpass=<グローバル管理者のパスワード> --verbose --console --accepteula
```

注記: 以前のバージョンのインテル® EMA から更新する場合、dbserver、dbadvanced、db、dbuser、dbpass、guser、gpass のパラメーターは入力しないでください。これらは更新には必要ないパラメーターです。指定した場合、インストールは中止され、エラーメッセージが表示されます。更新には、以下のコマンドを使用します。

```
EMAServerInstaller.exe FULLINSTALL --verbose --console --accepteula
```

注記： 以前のバージョンのインテル® EMA から更新する場合、インストーラーによって接続文字列が自動的に検出されます。

サーバーマシンへの接続には、次の構造を使用することもできます。

```
--host=<サーバーマシンの FQDN 名> --ip=<サーバーマシンの IP> [--ipfirst|
--hostfirst]
```

インテル® EMA が最初に IP を使用して接続するようにするには、--ipfirst フラグを使用します。インテル® EMA が最初に FQDN を使用して接続するようにするには、--hostfirst フラグを使用します。

データベース接続には、以下を使用します。

Windows* 認証：--db=<DB 名> and --dbserver=<DB サーバー名>

SQL 認証：--db=<DB 名> and --dbserver=<DB サーバー名>
--dbuser=<ユーザー ID> --dbpass=<パスワード>

「ユーザー名/パスワード」モード (通常アカウントモード) でインストールする場合、コマンドライン構造にグローバル管理者のユーザー名とパスワードを入力する必要があります。これらの必須パラメーターは次のように指定します。

グローバル管理者のセットアップ：--guser=<ユーザー名> --gpass=<ユーザーパスワード>

「ドメイン/Windows* 認証」モードでインストールする場合、--domainauth フラグを指定し、-- guser と --gpass は入力しないでください。

上述の例のシンタックス・テンプレートには --console オプションが使用されているため GUI は読み込まれません。代わりに、インストーラーは画面上に進捗状況を表示し、完了するとコマンドプロンプトに戻ります。

ここまでで、インテル® EMA サーバーの Platform Manager を使用する準備が整いました。Platform Manager の使用についてはセクション 4 で説明します。

2.3.2 アドバンスト・モード

注記： 以前のバージョンのインテル® EMA から更新する場合、インストーラーによって接続文字列が自動的に検出されます。

--dbadvanced パラメーターは、**c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config** に暗号化して保存される、カスタマイズされたデータベース接続文字列を提供するために使用されます。

以下のコマンド・シンタックス・テンプレートを使用して、山括弧 (<>) で囲まれた値は置き換え、通常のユーザーアカウントを使用してインストールします。ドメイン認証を含むその他のオプションについては、--help オプションを付けて実行ファイル単独で実行してください。

```
EMAServerInstaller.exe FULLINSTALL --host=<サーバーの FQDN>> --dbadvanced= "<接続文字列>"
--guser=<グローバル管理者のメール> --gpass=<グローバル管理者のパスワード> --verbose --console
--accepteula
```

接続文字列の詳細については、https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax を参照してください。

注記：パラメーター「MultipleActiveResultSets=True」は必須です。

2.4 アンインストール

アンインストールが完了するまでの間、インストーラーを中止または終了しないでください。

注記：

- アンインストールの前に、インテル® EMA SQL 接続文字列で使用されるアカウントが少なくとも db_creator 権限（任意のデータベースの作成、変更、削除が可能）を持っていることを確認してください。また、このアカウントには、データベース・レベルの db_owner、db_datawriter、db_ datareader ロールが割り当てられていなければなりません。

2.4.1 インストーラー GUI を使用したアンインストール

1. インストーラーのメインメニューの下の方にある **Uninstall the Intel® EMA Server（インテル® EMA サーバーのアンインストール）**を選択します。
2. ダイアログが開いたら、設定証明書を削除するかどうかを決定します。
3. データベースを削除するかどうかを決定します。

   注記：シングル・サーバー・インストールでは、このオプションによりデフォルトの共有 USBR イメージファイル格納フォルダーも削除されます。Server Settings（サーバー設定）ページでカスタムの USBR イメージ格納フォルダーが指定されている場合、そのフォルダーは削除されません。
4. **OK** をクリックし、警告メッセージでも **OK** をクリックします。
5. アンインストールが完了したら、**File（ファイル）> Advanced Mode（アドバンスト・モード）**をクリックしてログをチェックし、正常に完了していることを確認します。

2.4.2 コマンドラインを使用したアンインストール

1. 管理者権限でコマンド・プロンプト・ウィンドウを開きます。
2. インテル® EMA インストーラー・パッケージを展開したディレクトリーに移動します。
3. データベースと設定証明書を削除せずにアンインストールする場合、以下の **UNINSTALL** コマンドを入力して **Enter** を押します。

   ```
   EMAServerInstaller UNINSTALL -c --verbose
   ```
4. アンインストールとともに設定証明書を削除するには、`--deletesettingscert` オプションを追加します。

   ```
   EMAServerInstaller UNINSTALL --deletesettingscert -c --verbose
   ```
5. アンインストールとともにデータベースを削除するには、以下のように `--deletedb` オプションを追加します（設定証明書とデータベースの両方を削除するには、両方のオプションを使用します）。

   ```
   EMAServerInstaller UNINSTALL --deletedb -c --verbose
   ```

   注記：シングル・サーバー・インストールでは、このオプションによりデフォルトの共有 USBR イメージファイル格納フォルダーも削除されます。Server Settings（サーバー設定）ページでカスタムの USBR イメージ格納フォルダーが指定されている場合、そのフォルダーは削除されません。

3　グローバル管理者インターフェイスの使用

インテル® EMA のグローバル管理者ページは、テナント、ユーザー、ユーザーグループを管理するために使用されます。

インテル® EMA にログインする手順は以下のとおりです。

1. ブラウザーを開き、インストール中に指定した FQDN/ホスト名に移動します。
2. ログインページで、グローバル管理者のユーザー名 (メールアドレス) とパスワードを入力します。

注記：ドメイン認証を指定した場合、グローバル管理者向けの Overview (概要) ページが自動的に表示されます。

グローバル管理者向けの **Overview (概要)** ページの右側には Quick links (クイックリンク) があり、よく使う操作へのショートカットが表示されています。また、Getting Started tips (入門ヒント) には、このユーザーロールの簡単なチュートリアルがリンクされています。

ログアウトするには、**Overview (概要)** ページの上部バーにあるユーザー名をクリックし、**Log out (ログアウト)** を選択します。

3.1　グローバル管理者パスワードの変更

この操作は、インストール中に「通常アカウント」認証モードが選択された場合にのみ実行可能です。

上部バーのユーザー名をクリックし、**Change password (パスワードの変更)** を選択します。

3.2　テナントの作成と削除

新しいテナントを作成する手順は次のとおりです。

1. **Overview (概要)** ページ右上の **Quick links (クイックリンク)** にある **Create a tenant (テナントの作成)** をクリックします。あるいは、(左側のナビゲーション・バーにある) **Users (ユーザー)** ページで **Tenants (テナント)** タブを選択し、**New Tenant (新規テナント)** をクリックします。
2. **Tenant Name (テナント名)** と **Description (説明)** を入力して、**Save (保存)** をクリックします。

新しいテナントが作成され、**Manage Tenants & Users (テナントとユーザーの管理)** ページが表示されます。

テナントを削除するには、Manage Tenants & Users (テナントとユーザーの管理) ページで Tenants (テナント) タブを選択し、削除するテナントの省略記号 (...) をクリックし、**Delete Tenant... (テナントの削除)** をクリックします。

3.3　ユーザーとユーザーグループの管理

ユーザーまたはユーザーグループを管理する前に、ターゲットテナントを選択する必要があります。新しいユーザー (新しいグローバル管理者を除く) とユーザーグループは、このターゲットテナントの下に作成されます。

3.3.1　ユーザーグループの追加、変更、削除

新しいユーザーグループを作成する手順は次のとおりです。

1. (左側のナビゲーション・バーにある) **Users (ユーザー)** ページで **User Groups (ユーザーグループ)** タブを選択し、**New Group (新規グループ)** をクリックします。
2. **New Group (新規グループ)** ダイアログで、**Group name (グループ名)**、**Description (説明)** を入力し、**Access Rights (アクセス権)** を指定してから **Save (保存)** をクリックします。

ユーザーグループを削除するには、**Manage Tenants & Users (テナントとユーザーの管理)** ページの **User Groups (ユーザーグループ)** タブを開き、削除するユーザーグループの省略記号 (...) をクリックし、**Delete Group... (グループの削除)** を選択します。

3.3.2 ユーザーの追加、変更、削除

ユーザーを追加する手順は次のとおりです。

1. **Overview（概要）**ページ右上の **Quick links（クイックリンク）**にある **Add or remove users（ユーザーの追加または削除）**をクリックします。あるいは、（左側のナビゲーション・バーにある）**Users（ユーザー）**ページで **Users（ユーザー）**タブを選択します。
2. ユーザーを管理するテナントを選択し、**New User（新規ユーザー）**をクリックします。
3. **New User（新規ユーザー）**ダイアログで、**User name（ユーザー名）**の有効なメールアドレスを入力した後、**Password（パスワード）**を入力（および確認）し、**Description（説明）**を入力します。
4. そのユーザーのロールを選択し、**Save（保存）**をクリックします。

ユーザーを削除するには、**Manage Tenants & Users（テナントとユーザーの管理）**ページの **Users（ユーザー）**タブを開き、削除するユーザーの省略記号（**...**）をクリックし、**Delete...（削除）**を選択します。

注記：

- 最後のグローバル管理者ユーザーは自身のアカウントを削除することも編集することもできません。
- Active Directory* 認証を使うようにインテル® EMA を構成した場合、作成した各ユーザーのユーザー名が Active Directory* ユーザーの userPrincipalName 属性に対応することを確認してください。このモードでは、Password（パスワード）フィールドは表示されません（必要ありません）。

ユーザーを編集するには、**Manage Tenants & Users（テナントとユーザーの管理）**ページの **Users（ユーザー）**タブを開き、削除するユーザーの省略記号（**...**）をクリックし、**Edit...（編集）**を選択します。

自身のユーザーアカウントを編集しているとき、パスワードを変更するために、現在のパスワードを先に入力する必要があります。（自身のロールで管理可能な）別のアカウントを編集する場合は、そのユーザーの現在のパスワードを入力する必要はありません。

「ロックされた」ユーザーに対しては、**Edit（編集）**オプションを使用してユーザーアカウントのロックを解除します。

4　インテル® EMA サーバーの保守

インテル® EMA Platform Manager を使用すると、各インテル® EMA サーバーを監視し、インテル® EMA サーバーマシン上で動作するコンポーネント・サーバー上で各種保守タスクを実行できます。また、新しいインテル® EMA コンポーネント・サーバー・パッケージを展開するために使用することもできます。分散サーバー・アーキテクチャー環境では、1 台のインテル® EMA サーバーマシン上の 1 つの Platform Manager クライアントが、他のインテル® EMA サーバーマシン上のサーバー・コンポーネントに接続し、監視できます。

注記：Platform Manager サービスを実行するユーザーアカウントは必ず変更してください。詳細については、セクション 1.4.17 を参照してください。

4.1　インテル® EMA Platform Manager サービスの設定

Platform Manager を使用する前に、このセクションを見直して、デフォルトの設定を変更する必要があるか決定します。設定可能なすべての値はファイル **C:\Program Files (x86)\Intel\Platform Manager\Platform Manager Server\settings.txt** にあります。

4.1.1　Platform Manager の TLS 証明書

Platform Manager サービスは、サービスとクライアント・アプリケーション間に TCP TLS 接続を提供します。この TLS 接続のデフォルトの証明書は、インテル® EMA インストール時に提供されますが、settings.txt ファイルの「certhash」の値を目的の TLS 証明書サムプリントで更新することで、デフォルトの証明書を信頼できる認証局によって発行された証明書に更新できます。

4.1.2　クライアント認証のための相互 TLS 証明書

Platform Manager サービスは、オプションで、サービスとクライアント・アプリケーション間の接続に相互 TLS の使用を要求できます。そのためには、settings.txt ファイルの「allowedclientcert」の値をクライアント証明書サムプリントで更新します。「allowedclientcert」の行を複数追加することで、複数のクライアント証明書がサポートされます。

この機能を有効にすると、「allowedclientcert」リストに定義された証明書に対応する証明書を提示したクライアントのみが接続を許可されるようになります。

4.2　インテル® EMA Platform Manager クライアント・アプリケーションの使用

Platform Manager サービスの設定が完了すると、Platform Manager クライアント・アプリケーションの使用を開始する準備は整っています。

4.2.1　インテル® EMA Platform Manager の起動

1. インテル® EMA Platform Manager アプリケーションの起動方法は、通常の Windows* デスクトップ・アプリケーションと同じです。
2. **Connect to Platform Manager Server（Platform Manager サーバーに接続）**ダイアログで、インテル® EMA Platform Manager サーバーの識別子（ホスト名/FQDN/IP アドレス）とポートを入力します。インテル® EMA コンポーネント・サーバーと同一のマシン上で作業している場合、localhost:port 値を使用します。
3. **Intel® EMA Web Server Identifier（インテル® EMA ウェブサーバー識別子）**を入力します。これは、インテル® EMA ウェブサイトを開くために使用するホスト名/FQDN/IP アドレスです。
4. サービスを相互 TLS に構成した場合、**Client Authentication Certificate（クライアント認証証明書）**をオンにします。
5. **OK** をクリックします。
6. 確認のメッセージが表示されたら、サーバー証明書を確認して **Accept（承認）**します。

7. **Connection Credentials（接続資格情報）**ダイアログで、グローバル管理者ユーザーのユーザー名とパスワードを入力します。Windows* 認証を使用している場合、**Use Windows Authentication（Windows* 認証を使用）**を選択し、**OK** をクリックします。インテル® EMA サーバーへの接続でエラーが発生した場合、上記の手順で Platform Manager サーバーの正しい識別子を入力したか、インテル® EMA サーバーが動作中であるかを確認します。

   注記：Windows* 認証を使用している場合、Platform Manager を実行中のシステムがドメインに参加しており、お使いのグローバル管理者アカウントがドメインにログインしていることを確認してください。そうでない場合、資格情報の入力が求められます。

8. インテル® EMA Platform Manager ウィンドウが開き、左側のペインにアプリケーション・サーバーが表示されます。**Connect（接続）**のメッセージが表示された場合、Connection Credentials（接続資格情報）ダイアログでグローバル管理者の権限を持つユーザーを入力したことを確認します。

4.2.2 コンポーネント・サーバーのイベントの監視

1. 左側のペインのリストからコンポーネント・サーバーを 1 つ選択します（EMAAjaxServer など）。
2. **Events（イベント）**タブを選択し、そのサーバーのイベントを表示します。イベントのログは、選択されたサーバーマシンの **C:\Program Files (x86)\Intel\Platform Manager\EMALogs\EMALog-[サーバータイプ].txt** にも記録されます。ログファイルには、Events（イベント）タブに表示されるよりも詳細な情報が含まれることに注意してください。
3. 必要な場合、パネル下部の **Trace（トレース）**をクリックし、詳細なデバッグトレースを有効にすることができます（非常に多くのメッセージがログに記録されるようになります）。トレースログは、**C:\Program Files (x86)\Intel\Platform Manager\EMALogs\TraceLog-[サーバータイプ].txt** にも記録されます。

注記：トレースファイルは、選択したコンポーネント・サーバーでトレースが有効化されていない場合は表示されません。

4.2.3 コンポーネント・サーバーの内部トラッキング情報の監視

1. 左側のリストからコンポーネント・サーバーを選択します。
2. Component（コンポーネント）タブを選択し、選択したコンポーネント・サーバーに関する役立つ情報を表示します。以下に示すように、コンポーネント・サーバーごとに追跡される値は異なります。

インテル® EMA Ajax サーバー：

- **AjaxSessions:**インテル® EMA JavaScript* ライブラリーによって発行され、Ajax サーバーによって処理されるアクティブな Ajax リクエストセッションの数
- **HttpSessions：**インテル® EMA JavaScript* ライブラリーによって発行され、Ajax サーバーによって処理される HTTP セッションの数（ウェブ・リダイレクト機能に使用）
- **SwarmSessions：**Ajax サーバーから Swarm サーバーへのアクティブな TCP 接続の数
- **TerminalSessions：**インテル® EMA JavaScript* ライブラリーによって発行され、Ajax サーバーによって処理されるターミナルセッションの数（Serial-Over-LAN 機能とファイル参照機能に使用）。
- **WebSocketSessions：**インテル® EMA JavaScript* ライブラリーによって発行され、Ajax サーバーによって処理されるアクティブな WebSocket セッションの数

インテル® EMA 管理機能サーバー：

- 各行がインテル® AMT プロビジョニングに使用されるスロットです。保留中のインテル® AMT プロビジョニング・リクエストは、利用可能なスロットに入れられます。管理機能サーバーは、すべてのスロットのプロビジョニングを独立して開始します。利用できるスロットがない場合、リクエストはスロットが空くまで待機します。行には、インテル® AMT プロビジョニングの情報が表示されています。

インテル® EMA Swarm サーバー：

- **ConAgents：**Swarm サーバーへのインテル® EMA エージェントのアクティブな TCP 接続の数
- **ConConsoles：**他のインテル® EMA サーバーからのアクティブな TCP 接続の数

- **ConIntelAmt :** Swarm サーバーへのアクティブなインテル® AMT CIRA 接続の数
- **DbFails :** その Swarm サーバーが実行した DB クエリーの失敗数
- **DbQueries :** その Swarm サーバーが実行した DB クエリー数

4.2.4 コンポーネント・サーバーでの基本的なコントロールの実行

コンポーネント・サーバーを一時停止/停止または再開するには、左側のペインのサーバーを右クリックして必要なオプションを選択します。

特定のコンポーネント・サーバーに関して利用可能なコントロール・コマンドを確認するには、サーバーを選択して Console (コンソール) タブに移動し、「help」と入力して **Send (送信)** を選択します。コマンドを以下に列挙します。

すべてのサーバー :

- **testmessage :** インテル® EMA コンポーネントとのコンポーネント間の TCP 接続を介して、テストメッセージを一斉送信します Ajax サーバー、管理機能サーバー、Swarm サーバーの Events (イベント) タブで、[ソースサーバー] から受信した一斉テストメッセージを見ることができます。
- **echo :** 入力した内容を出力します
- **time :** 現在のサーバーマシン時間を出力します。
- **utctime :** 現在のサーバーマシン時間を UTC 時間で出力します。
- **version :** コンポーネントのバージョンを出力します。
- **shutdown :** このサーバーをシャットダウン/一時停止できますが、すぐ後に再起動されます。
- **collect :** .NET ガベージ・コレクションをトリガーします。
- **whoami :** このサーバーランタイムが実行されている現在のアカウントを出力します。
- **logpath :** ログフォルダーのパスを出力します。
- **trace :** トレースのトレースファイルへのログ記録を開始/停止できます。トレースファイルはログパスで指定した場所にあります。

インテル® EMA Ajax サーバー :

- **stats :** Application (アプリケーション) タブに表示されているのと同じ「トラッキングされた値」を出力します。
- **testdb :** インテル® EMA サーバー DB へのテスト接続
- **ajaxcert :** サービス間 TLS Ajax 証明書に関する情報を出力
- **swarmsessions :** 現在の Swarm セッションを出力
- **alertsessions :** 現在のアラートセッションを出力
- **restart :** Ajax サーバーを再起動
- **dbcount :** DB トレースカウントを制御
    - **Start (開始) :** データベース SQL コマンド情報の収集を開始します。Swarm サーバーで実行されます。これには、収集開始時間、収集期間、Swarm サーバーによる総 DB 接続数が含まれます。各 SQL コマンド項目について、実行数、エラー数、総実行時間、SQL コマンドが含まれます。SQL コマンドは、パラメーター化された入力を使用するために設計されていることに注意してください。そのため、値ではなく、ここで名前を挙げたパラメーターのみをログに記録します。
    - **Save and Restart (保存と再開) :** 収集したデータをインテル® EMA サーバーのインストール・フォルダー内の EMALogs フォルダーに保存します。
    - **Cancel (キャンセル) :** データ収集をキャンセルし、何もファイルに保存しません。
- **mcount :** インテル® EMA コンポーネント間の TCP 接続を介して送信された各種タイプの一斉テストメッセージの数を出力します。

- **triggertaskscheduler :** タスク・スケジューラーは通常、定期的に実行するスケジュール済みタスクがないかチェックします。これはチェックを即時にトリガーします。
- **getcompletedtransactions :** 完了したメタデータ・アップロードの情報を出力します。
- **getpendingtransactions :** 保留中のメタデータ・アップロードの情報を出力します。

インテル® EMA 管理機能サーバー :

- **testdb :** インテル® EMA サーバー DB へのテスト接続
- **exec :** 即時に実行すべきインテル® AMT プロビジョニング作業を検出するための管理機能サーバーによるインテル® EMA サーバー DB のチェックをトリガーします。上記の場合以外は、管理機能サーバーは定期的にチェックします。
- **restart :** 管理機能サーバーを再起動します。
- **dbcount :** DB トレースカウントを制御
- **dbcleanup :** オンデマンドのデータベース保守ルーチンを実行します。詳細については、セクション 4.5 を参照してください。
- **slots :** アクティベーション・タスクのスロットを出力します。管理機能サーバーでは現在内部スロットリングが実行されています。最大で 20 のプロビジョニング・タスク (スロット) を同時に実行できます。残りのプロビジョニング・タスクは、インテル® EMA サーバー DB 内でピックアップされるのを待機します。
- **manageabilitycert :** サービス間 TLS 管理性証明書に関する情報を表示します。
- **fileuploadcleanup :** オンデマンドのクリーンアップを実行し、期限切れの USBR 一時ファイルを削除します。

インテル® EMA Swarm サーバー :

- **stats :** 以下を出力します。
    - インテル® EMA エージェントからの受信トラフィックとインテル® EMA エージェントへの送信トラフィック(いずれも単位はバイト)
    - .Net ガベージコレクター : GetTotalMemory の値。この Swarm サーバーが実行したインテル® EMA DB クエリー数、接続数、DB クエリー失敗数。
    - 接続されたインテル® EMA エージェントの数。
    - 受信した一斉メッセージの数、送信した一斉メッセージの数。
    - インテル® EMA サーバーの DB スキーマのバージョン。
- **testdb :** インテル® EMA サーバー DB へのテスト接続
- **swarmcert :** サービス間 TLS Swarm サーバー証明書に関する情報を表示します。
- **servercert :** インテル® EMA Swarm サーバー証明書に関する情報を表示します。
- **resetagentstore :** インテル® EMA DB 内で利用可能なインテル® EMA エージェント・インストーラーに基づいて、メモリー内のエージェント・インストーラー情報を同期します。次に、接続された各インテル® EMA エージェントについて、エージェントのダウンロードとアップロードをチェックします。
- **forcedisconnect :** ターゲット・エンドポイントを当面切断します。エンドポイントは再接続可能です。
- **restart :** Swarm サーバーを再起動します。
- **dbcount :** DB トレースカウントを制御
- **consoles :** 現在接続されているインテル® EMA アプリケーションサーバーのリストを出力します。例えば、「リモートターミナル」セッションを実行している場合、Ajax サーバーと Swarm サーバーの間に 1 つのコンソールセッションがあります。
- **dbschema :** インテル® EMA サーバーの DB スキーマのバージョンを出力します。

- **allownode:** エンドポイントをホワイトリストに追加します。空でない禁止エンドポイント・リストが存在する場合、Swarm サーバーは、インテル® EMA エージェント接続リクエストを受信するとそのリストをチェックします。その受信エージェント/エンドポイントが禁止されている場合、接続を拒否します。

  注記： 現在のインテル® EMA リリースではこの機能は実装されていません。

- **bannode：** エンドポイントを禁止リストに追加します。
- **clearnodeaccess:** メモリー内の禁止リストとホワイトリストをクリアします。リストは Swarm サーバーが再度起動するときに再読み込みされます。
- **nodeaccesslist：** エンドポイントのホワイトリスト/禁止リストを出力します。
- **ipblocklist:** 空でない IP ブロックリストが存在する場合、Swarm サーバーは、インテル® AMT CIRA またはインテル® EMA エージェント接続リクエストを受信するとそのリストをチェックします。この受信 IP アドレスが IP ブロックリスト内で指定されたのと同じサブネットにある場合、接続を拒否します。

  注記： 現在のインテル® EMA リリースではこの機能は実装されていません。

- **swarmid:** この Swarm サーバーの ID とリード Swarm サーバーの ID を出力します。これは、ロードバランサー下で複数の Swarm サーバーが存在する場合に役立ちます。リーダーは通常、最も最近起動した Swarm サーバーで、一番大きな ID を持ちます。
- **agentpingtime:** インテル® EMA エージェントの TCP 接続を維持するための現在の ping 時間を出力します。数値引数を指定した場合、ping 時間をその値（秒単位）に設定します。
- **agentrequireping：** Swarm サーバーによって送信された ping に対してすべてのインテル® EMA エージェントが pong を返す必要があるかを出力します。1 は true、0 は false です。true の場合、Swarm サーバーは pong が受信されなかった場合、そのエージェントの TCP 接続をドロップします。引数（1 または 0）を指定すると値を設定できます。
- **ignoredupagents：** デフォルトでは無効です。インテル® EMA Swarm サーバーがインテル® EMA エージェント接続を受信し、その接続が既存の接続と同じエンドポイント ID を持つ場合、既存の接続を切断および削除して、新しい接続を受け入れます。一方、この機能を有効にすると、何もせずに新しく受信した接続を無視するだけになります。1 または 0 が出力されます。1 は true（有効）、0 は false（無効）です。引数（1 または 0）を指定すると値を設定できます。
- **swarmpeers：** その他のピア Swarm サーバーの ID と IP アドレスを出力します。

4.3 新しいパッケージの展開

パッケージは、コンポーネント・サーバーまたはウェブサイトを含む zip ファイルです。1 つのインテル® EMA リリースに複数のパッケージが含まれます。パッケージは、インテル® EMA リリースの StoredPackages フォルダーにあります。

注記: 古いバージョンのインテル® EMA がインストールされている場合、Platform Manager を使用して、インテル® EMA データベースを操作することなく新しいバージョンをアップロードして展開することができます。ただし、新しいリリースにインテル® EMA データベースに関する変更が含まれている場合は、インテル® EMA インストーラーを使用して更新を実行する必要があります。

特定のコンポーネント・サーバーを更新する手順は次のとおりです。

1. 左側のペインで **Intel® EMA Servers（インテル® EMA サーバー）** を開き、リストからマシン（localhost など）を選択します。
2. **Storage（ストレージ）** タブを選択します。
3. **Upload（アップロード）** をクリックし、マシンに展開する .zip パッケージ（EMASiteCoreReact.zip など）を選択します。古いバージョンは、Component Packages（コンポーネント・パッケージ）リストにある新しいバージョンで置き換えられます。
4. **Deploy（展開）** をクリックし、新しいパッケージを選択したマシンに展開します。

4.4 データベース接続文字列の更新

インストール後に、データベース接続文字列を更新する手順は次のとおりです。

1. インテル® EMA インストーラー・ウィザードを実行します（インストール・フォルダーで **EMAServerInstaller.exe** を右クリックし、**Run as administrator（管理者として実行）**を選択します）。
2. **File（ファイル）**メニューから **Advanced Mode（アドバンスト・モード）**を選択します。**Database（データベース）**メニューを含む追加のメニューが表示されます。
3. **Database（データベース）**メニューで **Update Database（データベースの更新）**を選択します。**Update Database Settings（データベース設定の更新）**ダイアログが表示されます。
4. サーバーまたはデータベース名、または SQL 認証 ユーザーおよびパスワードを更新するには、これらのフィールドに新しい値を入力し、**Update（更新）**をクリックします。新しいカスタマイズされたデータベース接続文字列を入力するには、次のステップへ進みます。
5. **Advanced Mode（アドバンスト・モード）**チェックボックスをオンにします。
6. 新しい **Connection String（接続文字列）**を入力します。接続文字列の詳細については、https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax を参照してください。

   注記：パラメーター「MultipleActiveResultSets=True」は必須です。
7. **Update（更新）**をクリックして接続文字列を更新し、Update Database Settings（データベース設定の更新）ダイアログを閉じます。

注記：

- 新しい接続文字列の設定を反映するには、すべてのインテル® EMA コンポーネント・サーバー（Swarm サーバー、管理機能サーバーなど）を再起動する必要があります。
- それまでの接続文字列ファイル **c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config** のコピーが作成されます。
- 分散サーバー・アーキテクチャー環境では、接続文字列をすべてのインテル® EMA サーバーシステムで更新する必要があります。

4.5 定期的なデータベース保守

インテル® EMA データベースは時間とともに拡大し、いずれはパフォーマンスに影響が生じます。データベース性能を最適に保つには、定期的にテーブル・インデックスをリビルドし、データベースの行ファイルをクリーンアップし、ファイルのログを記録する必要があります。さらに、自動化されたデータベース・クリーンアップ・ユーティリティー DBCLEANUP があります。DBCLEANUP は、定期的に自動実行され、監査ログテーブルなどの特定のテーブルの保守を行って古いエントリーを削除します。DBCLEANUP を自動実行する間隔（Audit Log Cleanup Interval）については、セクション 6.3 を参照してください。

DBCLEANUP コマンドは、Platform Manager を使用して、管理機能サーバーの Console（コンソール）タブで手動で実行することもできます。その場合、次の手順に従います。

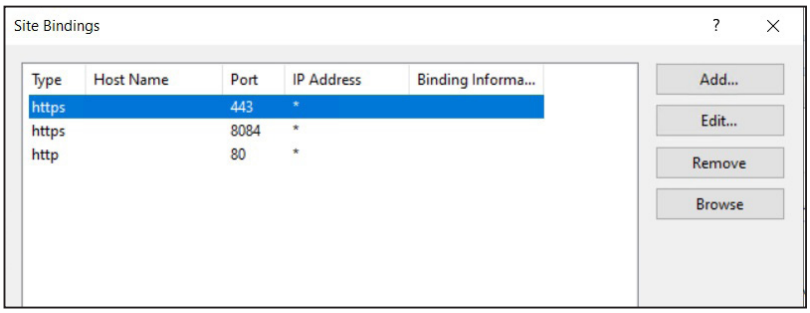
1. Platform Manager を実行します（詳細はセクション 4.2.1 を参照してください）。
2. 左側のナビゲーション・ペインから、**Intel® EMA Servers（インテル® EMA サーバー）> localhost > EMAManageabilityServer** を選択します。
3. **Console（コンソール）**タブを選択します。
4. **Component Console（コンポーネント・コンソール）**ウィンドウで、プロンプトにコマンド `dbcleanup` を入力し、**Enter** を押します。

4.6 インテル® EMA サーバーのバックアップからの復元

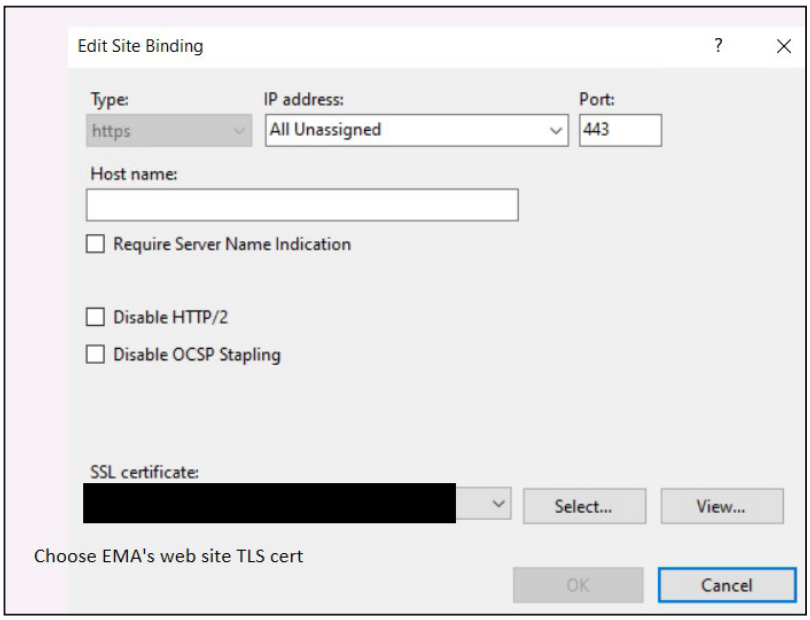
セクション 1.4.1 で、インテル® EMA をインストールした後にインテル® EMA データベースと MeshSettingsCertificate のバックアップを取ることをお勧めしました。このセクションでは、そのバックアップからインテル® EMA サーバーを復元する方法について説明します。

1. クリーンなシステムで開始します。
2. データベースのバックアップを復元します。
3. MeshSettingsCertificate 証明書 (秘密鍵を含む) を証明書ストアの Local Computer (ローカル・コンピューター) \ Personal (個人) の場所に復元します。秘密鍵へのアクセスが、インテル® EMA コンポーネントを実行するアカウントおよびインテル® EMA IIS ウェブサイトを実行するアカウントに対して開放されていることが必要です。
4. 14 ページのセクション 2「インテル® EMA サーバーのインストール/更新」で説明したとおり、インテル® EMA インストーラーを実行し、シングルサーバーのセットアップを選択します。必ず、復元したデータベースを参照してインストールします。インストーラーにより、更新インストールが実行されることが通知されます。これは異常ではありません。
5. IIS マネージャーで、IIS バインドの設定が正しいことを確認します。次のような情報が表示されます。

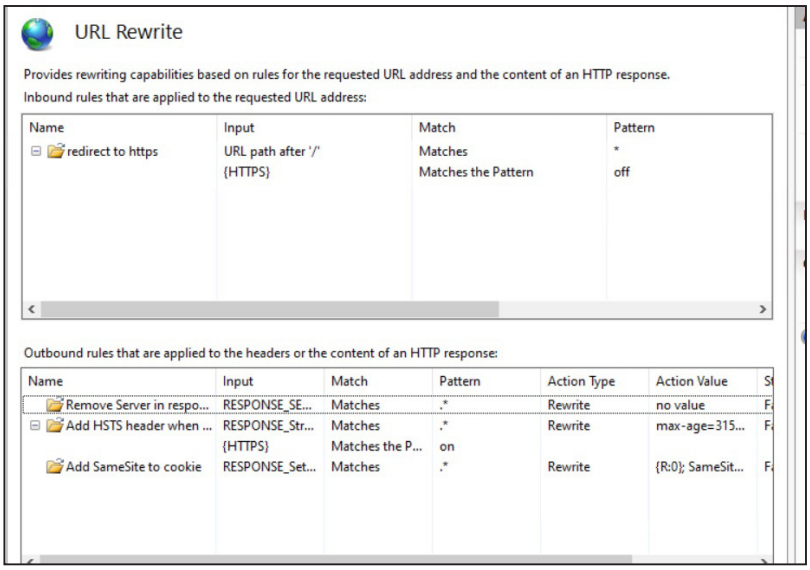
   サイトのバインドは次のようになります。



   ポート 443 と 8084 について、バインドの詳細は以下のようになります (443 または 8084 ポート)。

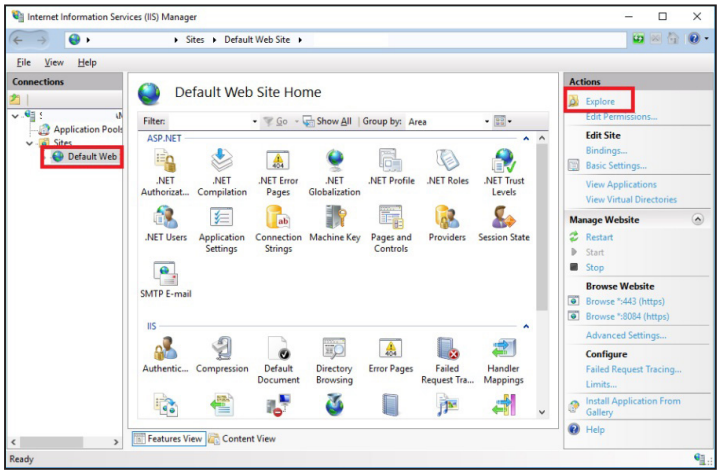
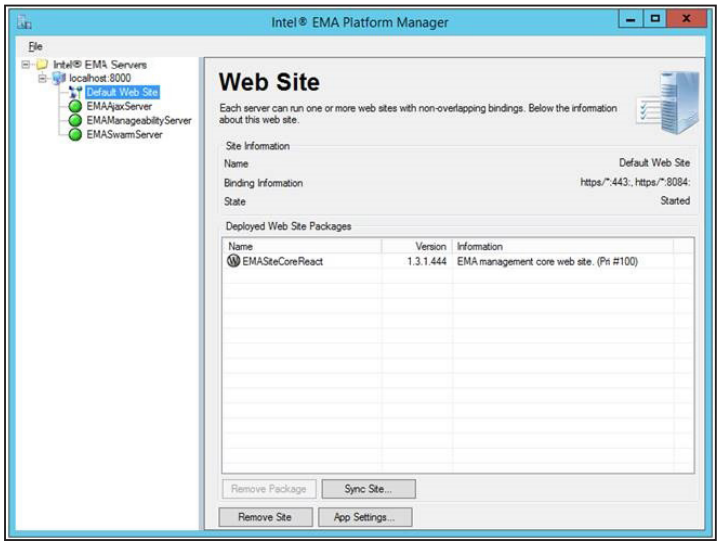


   URL リライトについては、以下のような設定が表示されます。


URL Rewrite
Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.
Inbound rules that are applied to the requested URL address:
Name
Input
Match
Pattern
redirect to https
URL path after '/'
Matches
*
{HTTPS}
Matches the Pattern
off
Outbound rules that are applied to the headers or the content of an HTTP response:
Name
Input
Match
Pattern
Action Type
Action Value
Remove Server in respo...
RESPONSE_SE...
Matches
.*
Rewrite
no value
Add HSTS header when ...
RESPONSE_Str...
Matches
.*
Rewrite
max-age=315...
{HTTPS}
Matches the P...
on
Add SameSite to cookie
RESPONSE_Set...
Matches
.*
Rewrite
{R:0}; SameSit...

5 付録 - インストール後のトラブルシューティング

ログ、トレース、イベントのチェック	インストール・ログ・ファイル **EMALog-Intel®EMAInstaller.txt** は、インテル® EMA インストーラーと同じフォルダー (インストーラーをダウンロードし、実行した場所) にあります。 **注記：**ローカル SQL Server* またはリモート SQL Server* のどちらを使用してインストールした場合も、インストール・ログ・ファイルに以下の警告が表示されます。リモート SQL Server* を使用している場合、このメッセージは無視して問題ありません。ローカル SQL Server* を使用したインストールの場合、IIS のデフォルト・アプリケーション・プールの接続を許可するようにアカウントが設定されていることを確認してください。 `EVENT: DbWarning, ExecuteNonQuerySafe warning: CREATE LOGIN [IIS APPPOOL\DefaultAppPool] FROM WINDOWS() - System.Data.SqlClient.SqlException (0x80131904): User does not have permission to perform this action.` 各インテル® EMA コンポーネント・サーバーのログファイル、トレースファイル、イベントを表示する方法については、本ガイドのセクション 4 を参照してください。
インテル® EMA サーバーのインストール・エラー	**Intel® EMA Platform Manager Package path not set correctly(インテル® EMA Platform Manager パッケージのパスが正しく設定されていません)** インストーラーが既存の Platform Manager 設定ファイル (例：C:\Program Files (x86)\Intel\Platform Manager\Platform Manager Server\settings.txt) は見つけられますが、その設定ファイルにリストされたインテル® EMA パッケージ (例：C:\Program Files (x86)\Intel\Platform Manager\Packages) を見つけることができません。 **対策：** 1. すべてのオプションを選択して、インテル® EMA サーバーをアンインストールします。 2. インテル® EMA Platform Manger がアンインストールされ、インテル® EMA のインストール・フォルダー (C:\Program Files (x86)\Intel\Platform Manager など) にファイルが残ってないことを確認します。 3. インテル® EMA サーバーを再インストールします。
インテル® EMA Platform Manager サービスが開始しない	すべての Windows* サービスと同様に、サービスの開始に長い時間がかかると (デフォルトでは 30 秒)、インテル® EMA Platform Manager サービスはタイムアウトします。低速なマシンでは、インテル® EMA Platform Manager サービスの起動中にこのタイムアウトに達してしまうことがあります。その場合、インテル® EMA は正常に動作しません。 このサービスのステータス、イベント、ログを確認します。 • **Windows* の Services (サービス)** ビューアーで、サービスが正常に起動していることを確認します。 • **Windows* の Event Viewer(イベント ビューアー)** で、Windows Logs (Windows* ログ) \ System (システム) を展開し、Level (レベル) が Error (エラー) で、Source (ソース) が Service Control Manager のエントリーを見つけます。

	• このサービスによって例外が発生した場合、Windows* ドライブの PlatformManagerError.txt (C:\PlatformManagerError.txt など) にログファイルがあります。 **対策：** Windows* のレジストリー設定を変更してタイムアウト値を修正します。方法については、インターネットで「Error 1053 ServicesPipeTimeout」を検索して情報を集めることをお勧めします。
インテル® EMA ウェブサイトへのアクセス時のエラー	ウェブサイトが展開されていることを確認します。上述のパッケージパスの問題により、ウェブサイトが展開されていない場合があります。 **対策：** Windows* の IIS マネージャーを使用してインテル® EMA ウェブサイトのフォルダーを調べます (右上の **Actions (操作)** で **Explorer (エクスプローラー)** をクリックします)。そのフォルダーには多くのサブフォルダーやファイルが表示されるはずです。  もし表示されない場合、Platform Manager で Sync Site (サイトを同期) を実行し、ウェブサイトを再展開します。 

Windows Server* マシンでの Internet Explorer* の使用	Windows Server* (Windows Server* 2014 など) では Internet Explorer* のデフォルトのセキュリティー設定により、インテル® EMA の多くの機能が正常に機能しなくなることがあります。 **対策：** Windows Server* マシンでは、その他のウェブブラウザー (Chrome*、Firefox* など) を使用することをお勧めします。
ターゲットのインテル® EMA ウェブサイト URL はインテル® EMA ウェブサイトの証明書と一致する必要がある	インテル® EMA ウェブサイトにアクセスするために使用される URL がインテル® EMA ウェブサイト証明書の Issued To (発行先) フィールドと一致しない場合、ウェブブラウザーのセキュリティー・フィルタリングによって多くの機能がブロックされます。 **対策：** インテル® EMA の URL が証明書の **Issued To(発行先)**フィールドと一致することを確認してください。
インテル® AMT セットアップ/プロビジョニング中の警告とエラー	ターゲットのインテル® AMT ファームウェアのステータスによっては、警告/エラーが一時的なエラーである場合があります。インテル® EMA 管理機能サーバーは、失敗したセットアップを自動で定期的に再試行します。ただし、一時的なものではない警告/エラーもあり、その場合は対処が必要です。 **注記：**セットアップ/プロビジョニング中に管理機能サーバーによってログに記録される警告/エラーメッセージについては、本ガイドの Platform Manager のセクションを参照してください。 **無視できる一時的な警告/エラー** 警告/エラーのタイプ – OTP_REQUIRED： Message:Host Based Admin Setup (1st try): OTP_REQUIRED Message:Unable to go to admin mode, rolling back out of client mode. 警告/エラーのタイプ – INTERNAL_ERROR due to Unauthorized WSMAN call: Message:Creating DotNetWSManClient object... Warning:Error (2): Intel.Manageability.WSManagement.WSManException: The remote server returned an error: (401) Unauthorized. Message:Host Based Setup (1st try): INTERNAL_ERROR **注記：**上記のエラーが発生した場合でも、サーバーは 3 回目の試行までインストールをリトライします。 **対処が必要な警告/エラー** PKI ドメイン・サフィックスが PKI 証明書と一致しない： 警告/エラーのタイプ – Message:Host Based Admin Setup (3rd try): AUTH_FAILED

	警告/エラーのタイプ – Message:Unable to go to admin mode, rolling back out of client mode. インテル® Management and Security Application Local Manageability Service (LMS) が正しく動作していないことによる INTERNAL_ERROR 警告/エラーのタイプ – Warning:Error (2): Intel.Manageability.WSManagement.WSManException: The underlying connection was closed: The connection was closed unexpectedly. 警告/エラーのタイプ – Message:Host Based Setup (3rd try): INTERNAL_ERROR インテル® AMT FW にリセットが必要なことによる WSManException Warning:Error (2): Intel.Manageability.WSManagement.WSManException: The underlying connection was closed: The connection was closed unexpectedly. ---> System.Net.WebException: The underlying connection was closed: The connection was closed unexpectedly. インテル® Manageability Server がセットアップをリトライした後にこのエラーが解決しない場合、インテル® AMT マシンをシャットダウンし、電源ケーブルを抜き、イーサネット・ケーブルを抜いて、インテル® ME ファームウェアをリセットします。その後、両ケーブルを元どおり接続し、マシンを再起動します。 インテル® AMT FW の証明書ストアが一杯であることによるエラー Error: .[omitted]..... Certificate Store in firmware is full and no more certificates can be added. この場合、このインテル® AMT システムのプロビジョニングを解除することをお勧めします。その後、インテル® EMA の手動プロビジョニングまたは自動プロビジョニングを使用してこのシステムをもう一度セットアップします。
インテル® AMT は動作しないが、その他すべての機能は正常に動作している	このセクションは、インテル® EMA サーバーが **Use hostname only (ホスト名のみを使用)** モードでインストールされており、ターゲット・エンドポイントがインテル® AMT CIRA でプロビジョニングされているシナリオに適用されます。 インテル® AMT が動作しないがその他の機能はすべて正常動作している場合、インテル® EMA サーバーのインストール時に入力されたホスト名/FQDN をインテル® AMT CIRA ファームウェアが解決できていない可能性が高いです。 **対策：** 1. ターゲット・エンドポイントのプロビジョニングを解除します。 2. クリーンなセットアップと、クリーンな (プロビジョニングが解除された) エンドポイントを使用して、CIRA プロビジョニングを実行し、プロビジョニング・イベントを確認します。 a. 確認するには、Platform Manager で、EMAManageabilityServer の **Events (イベント)** タブに移動します。エラーが発生していないことを確認します (数件の警告なら問題ありません)。

	b. ターゲット・エンドポイントで **Intel® Management and Security Status** ツールを開き、**General（全般）**タブを開きます。プロビジョニングが成功した場合、**Configured（設定済み）**と **Remote Control Connection is Enabled（リモート・コントロール接続が有効）**という 2 つのイベントが表示されます。 c. プロビジョニングが成功していた場合、続けて残りの手順を行います。成功していなかった場合、インテル® Manageability Server のイベントおよびログをチェックし、問題を修正します。 3. EMASwarmServer の **Component（コンポーネント）**タブ（Platform Manager 内）で、**ConIntelAmt** の値を確認します。これはアクティブな CIRA 接続の数です。CIRA を使用してエンドポイントを 1 つプロビジョニングし、CIRA がインテル® EMA Swarm サーバーへの接続を確立できた場合、この値は 1 になります。数値が正しくない場合、ターゲット・エンドポイントを再起動し、1 ～ 2 分待ちます。それでも **ConIntelAmt** 値が正しくない場合、続けて残りの手順を行います。 4. この時点で、おそらく、インテル® AMT CIRA ファームウェアはホスト名/FQDN を解決できていません。本当にそうであるか確かめるため、**fixed IP address（固定 IP アドレス）**モードを使用してプロビジョニングを行います。**fixed IP address（固定 IP アドレス）**モードが正常に動作するなら、名前解決の問題が根本原因であることが分かります。その場合は、IT 管理者に相談してください。一時的に **fixed IP address（固定 IP アドレス）**モードを使用するには、以下の手順を行います。 a. Server Settings（サーバー設定）ページで、管理機能サーバーの **ciraserver_ip** 設定を変更します（次のページの「付録 - コンポーネント・サーバーの設定変更」を参照してください）。 b. 設定を保存し、管理機能サーバーを再起動します。 5. ターゲット・エンドポイントのプロビジョニングを解除し、プロビジョニングを再実行します。今回は、上記で指定した IP アドレスが CIRA によって使用されます。
インテル® EMA サーバーのアンインストール時にデータベースのドロップが失敗する	インテル® EMA サーバーをアンインストールするとき、「Unable to drop database.（データベースをドロップできません）」という警告/エラーが表示されることがあります。 **対策：** 1. Microsoft* SQL Server* Management Studio を開いてデータベースに接続し、既存のデータベースをチェックします。インテル® EMA データベースが Single User（シングルユーザー）モードに設定されているかを調べます。 2. ターゲット・データベースを右クリックして **Delete（削除）**を選択します。Delete（削除）オプション・ウィンドウの値はいずれもデフォルトのまま変更しないでください。ターゲット・データベースを削除します。 3. データベースが削除されない場合、データベース・サーバーを右クリックして **Restart（再起動）**を選択します。データベース・サーバーが再起動したら、もう一度ターゲット・データベースの削除を試みます。

6　付録 - コンポーネント・サーバーの設定変更

インテル® EMA サーバーを構成する各種コンポーネント・サーバー (Swarm サーバー、Ajax サーバーなど) の設定は、左側にある縦長のナビゲーション・バーの **Settings (設定)** からアクセスできる **Server Settings (サーバー設定)** タブで変更できます。

以降のサブセクションでは、各コンポーネント・サーバーで利用可能な設定を説明します。

注記：任意の種類のコンポーネント・サーバーについて **serverIps** または **messagePort** 設定を変更した場合、設定変更したコンポーネント・サーバーだけでなくすべてのコンポーネント・サーバーを再起動する必要があります (分散サーバー・アーキテクチャーでは、すべてのサーバーマシンで行う必要があります)。また、上記の 2 つの設定を変更したときに、インテル® EMA ウェブサーバーを再起動するため、インテル® EMA ウェブサイトの IIS アプリケーション・プールをリサイクルする必要があります。それ以外の設定については、変更したコンポーネント・サーバーを再起動するだけで問題ありません。**messagePort** を変更した場合、新しいポートがファイアウォールでブロックされていないことを確認してください。

6.1　Swarm サーバー

設定	説明
Admin Port (管理ポート)	Swarm サーバーの管理 TCP リスナーがバインドされるポートです。他のインテル® EMA サーバープロセスから Swarm サーバーへの通信に使用されます。デフォルトは 8089 です。
Admin Port Local (管理ポートローカル)	管理 TCP リスナーがローカル・ループバックのみにバインドされるかどうかを決定します。値は 0 と 1 です。 0 = 分散サーバー環境 1 = シングルサーバー環境
enableCIRAPowerPolling	CIRA 電力ステートの定期的なポーリングを有効にします。値は True/False です。デフォルトは True です。
Log File Path (ログファイルのパス)	インテル® EMA ログファイルへのパスです。
maxdbconnections	このサーバーへの同時 DB 接続の最大数です。
messagePort	インテル® EMA コンポーネントからの内部トラフィックを受け付けるために、このコンポーネント・サーバー・タイプがリッスンする TCP ポートです。デフォルトは 8093 です。
serverIps	このコンポーネント・サーバー・タイプが実行されているマシン IP アドレスのリストです。例えば、Swarm サーバーがマシン ip1、ip2、ip3 で実行中の場合、serverIps にすべての IP アドレスが含まれます。
Swarm Servers (Swarm サーバー)	アクティブな Swarm サーバーのリストです (形式は IP アドレス : ポート)。
TCP Connection Retry (TCP 接続リトライ)	インテル® EMA サーバー コンポーネント間で通信接続を確立するときのリトライ間の待機時間です。
TCP Connection Idle (TCP 接続アイドル)	通信確立後に、コンポーネント間で送信されるハートビート・メッセージの間隔です。

6.2　Ajax サーバー

設定	説明
Ajax Cookie Auto Refresh Range (Ajax Cookie の自動リフレッシュ範囲)	Ajax Cookie の寿命を延長できる範囲 (単位：分)。
Ajax Cookie Idle Timeout (Ajax Cookie のアイドル・タイムアウト)	Cookie が追加されてから期限切れになるまでの時間 (単位：分)。

設定	説明
Http Header Access Control Allow Headers (Http ヘッダーアクセス制御許可ヘッダー)	Ajax リクエストに対応して設定する追加のヘッダー。
Log File Path (ログファイルのパス)	インテル® EMA ログファイルへのパスです。
maxdbconnections	このサーバーへの同時 DB 接続の最大数です。
messagePort	インテル® EMA コンポーネントからの内部トラフィックを受け付けるために、このコンポーネント・サーバー・タイプがリッスンする TCP ポートです。デフォルトは 8092 です。
serverIps	このコンポーネント・サーバー・タイプが実行されているマシン IP アドレスのリストです。例えば、Ajax サーバーがマシン ip1、ip2、ip3 で実行中の場合、serverIps にすべての IP アドレスが含まれます。
Swarm Servers (Swarm サーバー)	アクティブな Swarm サーバーのリストです (形式は IP アドレス : ポート)。
User Access Failed Max Count (ユーザーアクセス最大失敗数)	ユーザーアカウントがウェブ API によってロックされるまでにパスワードを間違える回数。
Expire Sessions (セッションの期限)	Ajax サーバーがセッションに期限を設けるかどうかを設定します (デフォルトは有効)。

6.3 管理機能サーバー

設定	説明
Audit Log Cleanup Interval (Hours) (監査ログ・クリーンアップ間隔 (単位 : 時間))	インテル® EMA データベース内の監査ログレコードがクリーンアップされる間隔 (単位 : 時間)。
Audit Log Cleanup Interval (Days) (監査ログ・クリーンアップ間隔 (単位 : 日))	インテル® EMA データベース内の監査ログレコードがクリーンアップされる間隔 (単位 : 日)。
CIRA Server IP (CIRA サーバー IP)	CIRA アクセスサーバーの IP アドレス。CIRA アクセスサーバーとは、Swarm サーバー (分散アーキテクチャーの場合、Swarm サーバーのロードバランサー)です。インストール・モードで IP アドレスを使用している場合のみ使用されます。
CIRA Server Host (CIRA サーバーホスト)	CIRA アクセスサーバーのホスト名。CIRA アクセスサーバーとは、Swarm サーバー (分散アーキテクチャーの場合、Swarm サーバーのロードバランサー) です。インストール・モードでホスト名を使用している場合のみ使用されます。これはマルチサーバーのインストールに使用されます。
CIRA Server Port (CIRA サーバーポート)	CIRA アクセスサーバーのポート。CIRA アクセスサーバーとは、Swarm サーバー (分散アーキテクチャーの場合、Swarm サーバーのロードバランサー) です。ロードバランサーによって、(CIRA から) 受信したトラフィックを Swarm サーバーの 8080 ポートにダイレクトに伝えるために使用されます。
File Upload Clean Interval (ファイル・アップロード・クリーン間隔)	再開可能な不完全なファイルを処理するためにファイル・クリーンアップ・プロセスが実行される間隔 (単位 : 時間)。
File Upload Retention Period (ファイル・アップロード保持期間)	再開可能な不完全なファイル・アップロードが自動削除されるまでに保持される期間 (単位 : 日)。
Log File Path (ログファイルのパス)	インテル® EMA ログファイルへのパスです。

設定	説明
maxdbconnections	このサーバーへの同時 DB 接続の最大数です。
Maximum USBR Image Storage Capacity per Tenant **(テナントごとの最大 USBR イメージ保存容量)**	各テナントが USBR イメージの保存に使用できるディスク容量 (単位 : GB)。
Maximum USBR Image storage Capacity Per EMA Instance **(EMA インスタンスごとの最大 USBR イメージ保存容量)**	そのインテル® EMA インスタンスで USBR イメージの保存に使用できる (すべてのテナントを合わせた) 総ディスク容量 (単位 : GB)。
Maximum USBR Slot Count per Tenant **(テナントごとの最大 USBR スロット数)**	各テナントに許可されたアクティブな USBR セッションの数。
Maximum USBR Idle time **(最大 USBR アイドル時間)**	USBR セッションが自動的に終了されるまでにアイドル状態でいられる時間。
messagePort	インテル® EMA コンポーネントからの内部トラフィックを受け付けるために、このコンポーネント・サーバー・タイプがリッスンする TCP ポートです。デフォルトは 8094 です。
serverIps	このコンポーネント・サーバー・タイプが実行されているマシン IP アドレスのリストです。例えば、管理機能サーバーがマシン ip1、ip2、ip3 で実行中の場合、serverIps にすべての IP アドレスが含まれます。
Swarm Servers **(Swarm サーバー)**	アクティブな Swarm サーバーのリストです (形式は IP アドレス : ポート)。
USBR Images Root Directory **(USBR イメージのルート・ディレクトリー)**	アップロードされた起動可能イメージファイル (.iso および .img) が保存される、インテル® EMA サーバー上のルート・ディレクトリー。デフォルト値は **C:\ProgramData\Intel\EMA\USBR** です。 **注記 :** イメージのアップロード後にこのフォルダーが変更された場合、システム管理者は元のフォルダーから変更後のフォルダーに内容を手動でコピーする必要があります。
USBR Redirection Manager Loop Interval **(USBR リダイレクト・マネージャー・ループ間隔)**	アクティブな USBR セッションのステータスのポーリング間隔です。
usbrRedirectionThrottlingRateInMilliseconds	USBR ファイルデータをターゲット・エンドポイントのインテル® AMT ファームウェアに送信する際の遅延時間。データレートが高過ぎる場合、インテル® EMA の特定の内部データフローが適切に動作しないため、データレートをスロットルするために必要になります。 **注記 :** USBR を使用する際は、CIRA ベースのプロビジョニングを強くお勧めします。USBR はレイテンシーの影響を受けやすいため、インテル® EMA は USBR を CIRA でプロビジョニングされたエンドポイントに最適化しています。TLS リレーを使用している場合、グローバル管理者として、Server Settings (サーバー設定) の Manageability Server (管理機能サーバー) セクションの USBR Redirection Throttling Rate (USBR リダイレクト・スロットル・レート) を調整する必要があります。この設定はネットワーク環境ごとに異なります。10 ミリ秒から始め、ネットワーク環境に適合するレートになるまで 10 ずつ増加させることをお勧めします。50 ミリ秒より長くする必要があることはほとんどありません。この設定を大きくすると、特に CIRA エンドポイントにおいて、USBR ブート・パフォーマンスが低下します。TLS リレーのみのインスタンスでのみ使用してください。

設定	説明
	デフォルト値：0、最大値 1000、最小値 0。 推奨値 = 10 から開始して、10 ずつ増やし、ネットワークに適切なレートを見つける。

6.4 ウェブサーバー

設定	説明
Access Token Time to Live (アクセストークン TTL)	API ベアラートークンの有効期間 (単位：秒)。
Ajax Server Host (Ajax サーバーホスト)	Ajax サーバーのホスト名または IP アドレス、あるいは Ajax サーバーのロードバランサー。
Allowed Domains, Enable Allowed Domains (許可ドメイン、有効化許可ドメイン)	Ajax サーバーによって使用されます。有効な場合、ウェブサーバーは受信した Ajax/WebSocket リクエストをチェックして、受け入れるか拒否するかを判断します。 AllowedDomains は、test1.intel.com、test2.intel.com のサンプルを含むコンマ区切りのリストです。 EnableAllowedDomains は 0 (false) か 1 (true) です。
Log File Path (ログファイルのパス)	インテル® EMA ログファイルへのパスです。
maxdbconnections	このサーバーへの同時 DB 接続の最大数です。
Swarm Server Host (Swarm サーバーホスト)	Swarm サーバーのホスト名または IP アドレス、あるいは Swarm サーバーのロードバランサー。
Swarm Server Port (Swarm サーバーポート)	シングル・サーバー・インストールでは 8080。分散サーバー・アーキテクチャーでは、Swarm サーバーのロードバランサーによって開放される Swarm サーバーポート。
Global Catalog Port (グローバルカタログ・ポート)	Active Directory* のグローバルカタログへの接続に使用されるポートです。AD ユーザー名とパスワードが提供されたときに、AD ログインを実行するために使用されます。デフォルトは 3269 (SSL ポート) です。
Max Access Token TTL (最大アクセストークン TTL)	API ベアラートークンのリフレッシュまでの最長時間です。
Frontend Storage Type (フロントエンド・ストレージ・タイプ)	インテル® EMA ウェブサイトのランタイム情報をブラウザー・ローカル・ストレージに保存するか、ブラウザー・セッション・ストレージに保存するかを指定します。ローカルストレージを使用する場合、フロントエンド・ウェブサイトを閉じた後もセッションが残ります (再ログイン不要)。セッションストレージを使用する場合、フロントエンド・ウェブサイトを閉じた後、セッションは失われます。

7 付録 – ドメイン/Windows* 認証のセットアップ

ドメイン/Windows* 認証モードでインストールする場合、インテル® EMA インストーラーによってドメイン/Windows* 認証の基本的な設定がセットアップされます。多種多様なネットワーク・インフラストラクチャー・シナリオがあります。IT 管理者が追加のステップを実施する必要のあるシナリオもあります。

7.1 インストール時に設定されるサーバー接続情報

インテル® EMA インストーラーの実行時、External Identity (外部 ID) セットアップの Hostname (ホスト名) フィールドには、マシンの NetBIOS ホスト名または NetBIOS FQDN を使用することを推奨します。ここで入力した値については、その他のエンドポイントまたはクライアント・ウェブ・ブラウザーから接続できることを確認する必要があります。NetBIOS 名は、Windows* のファイル・エクスプローラーで **This PC (PC)** を右クリックし、**Properties (プロパティー)** を選択します。

別の値を使用する場合 (ロード・バランシングのシナリオなど)、IT 部門のプラクティスに従って、インテル® EMA のインストール後にサービス・プリンシパル名 (SPN) を設定してください。

7.2 IIS ウェブサイトの認証と .NET 承認

ドメイン/Windows* 認証モードでインストールすると、インテル® EMA は、インテル® EMA ウェブサイトの以下のプロパティーを (デフォルトの IIS ウェブサイト・セットアップとは異なった方法で) 設定します。

- IIS セクションの Authentication (認証) で、Anonymous Authentication (匿名認証) も有効にし、**Application Pool Identity (アプリケーション プール ID)** を選択します。
- ASP.NET セクションの .NET Authorization Rules (.NET の承認規則) で、Anonymous Users (匿名ユーザー) へのアクセスを許可する必要があります。

上記のプロパティーが正しく設定されていることをよく確認してください。

7.3 エンドユーザーが使用する Internet Explorer*

ドメイン/Windows* 認証が正常に動作するには、インテル® EMA ウェブサイトが **Local Intranet (ローカル・イントラネット)** ゾーンにあるものとして認識される必要があります。ゾーンを確認するには、インテル® EMA ウェブページを右クリックして **Properties (プロパティー)** を選択します。

ユーザーによっては、Internet Explorer* の **Compatibility View Settings (互換表示設定)** で **Display intranet sites in Compatibility View (イントラネット・サイトを互換表示で表示する)** チェックボックスをオンにしている場合があります。このチェックボックスはオフである必要があります。オンの場合、インテル® EMA ウェブサイトは正常に動作しません。

7.4 オプション – ウェブサイト・コンテンツへのアクセス許可の付与

このアクセス許可をセットアップする方法は、NTFS、URL 承認など複数存在します。IT 管理者はインフラストラクチャー固有のニーズに合わせてセットアップする必要があります。

7.5 オプション – ダブルホップ構造

この操作は、通常のインテル® EMA インストールでは行う必要はありません。ログインした資格情報を別のバックエンド・サーバーに渡すなど、特別なダブルホップ認証をサポートする必要がある場合、いくつか追加設定が必要になります。例えば、サーバーマシンの AD のコンピューター・オブジェクトの **Delegation (委任)** などです。標準の IT プラクティスに従ってください。

7.6 参考資料

- https://blogs.msdn.microsoft.com/chiranth/2014/04/17/setting-up-kerberos-authentication-for-a-website-in-iis/
- https://blogs.msdn.microsoft.com/webtopics/2009/01/19/service-principal-name-spn-checklist-for-kerberos-authentication-with-iis-7-07-5/
- https://support.microsoft.com/en-us/help/326214/how-to-configure-user-and-group-access-on-an-intranet-in-windows-serve
- https://weblogs.asp.net/owscott/iis-using-windows-authentication-with-minimal-permissions-granted-to-disk
- https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/anonymousauthentication
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831722(v=ws.11)

8 付録 – 802.1X 認証に対応したネットワーク・インフラストラクチャーの構成

本セクションの対象読者は、インテル® AMT で 802.1X 認証を有効化しようとするインテル® EMA グローバル管理者です。該当しない場合、本セクションは無視してください。

インテル® EMA は、RADIUS 仕様の Microsoft の実装であるネットワーク・ポリシー・サーバー (NPS) と互換性がある Extensible Authentication Protocol (EAP) をサポートしています。

注記：このセクションでは主に、802.1x を使用するために必要なインテル® EMA サーバーシステムの設定を全体的に説明します。特定のテナント使用空間に対して 802.1x プロファイルを設定する方法については、インテル® EMA 管理と使用ガイドを参照してください。

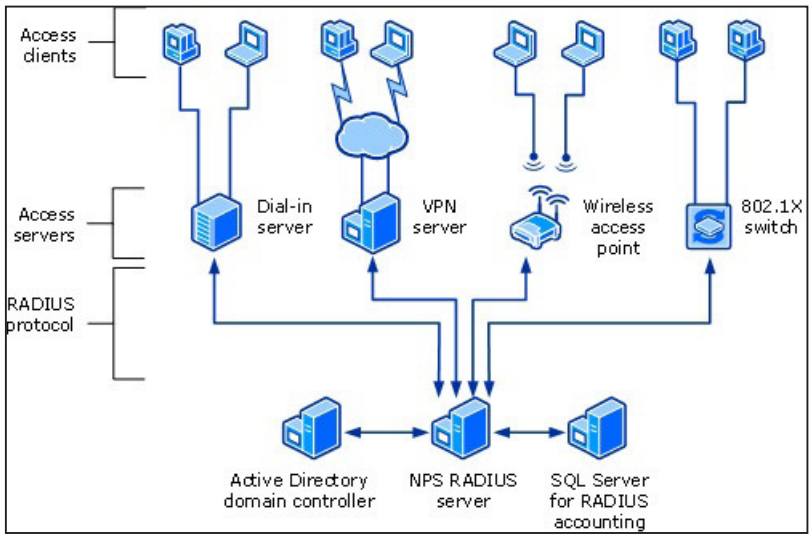
8.1 RADIUS サーバー - NPS

NPS とは、インターネット技術特別調査委員会 (IETF) が RFC 2865 および 2866 で策定した RADIUS 標準の Microsoft による実装です。NPS は RADIUS サーバーとして、多くの種類のネットワーク・アクセス (無線、認証スイッチ、ダイヤルアップおよび仮想プライベート・ネットワーク (VPN) リモートアクセス、ルーター間の接続など) に対して、一元化された接続認証、承認、アカウンティングを実行します。

NPS により、無線、スイッチ、リモートアクセス、VPN 環境などを異種混合で使用できるようになります。NPS は、Windows Server* 2016 で利用可能なリモート・アクセス・サービスとともに使用できます。

以下の図は、多種多様なアクセス・クライアントに対して RADIUS サーバーとして動作する NPS を示しています。

図 1：NPS コンポーネント



NPS を RADIUS サーバーとして構成する場合、Server Manager (サーバー・マネージャー) の NPS コンソールで、Standard Configuration (標準構成) と Advanced Configuration (詳細な構成) のいずれかを使用できます。NPS を RADIUS プロキシーとして構成する場合は、必ず詳細な構成を選択します。

8.2 Microsoft* NPS の構成

8.2.1 依存関係

ユーザー・データベース：接続試行中にユーザーを検索および認証するためのデータベースとすべての必須オブジェクトが必要です。そのための最も一般的なソースは Active Directory* です。本ガイドでは、NPS 上でユーザー認証を構成するためのソースとして Active Directory* を使用する場合を説明します。

PKI インフラストラクチャー：使用した 802.1X EAP プロトコルによって証明書の使用が要求される場合、NPS が RADIUS サプリカント (エンドポイント) から提供された資格情報を正しく検証するには、必要なインフラストラクチャーおよび認証局がドメインに展開済みである必要があります。

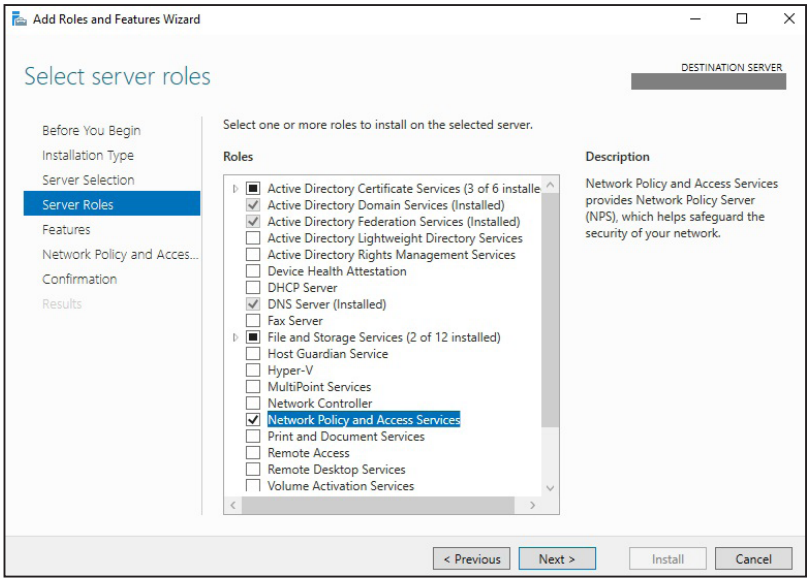
RADIUS クライアント：この構成で RADIUS クライアントとして動作できるのは、RADIUS サーバーとの間で要求および応答を送受信可能な任意のデバイスです。ネットワークへの接続可否を決定するプロセスによって生じる情報を使用可能な任意のデバイスについても同様です。有線接続では、このデバイスは通常、802.1X 認証互換のネットワーク・スイッチです。無線接続では、通常、802.1X 認証互換の (WPA エンタープライズまたはそれに類する) ネットワーク・ルーター・デバイスです。

NPS を正常に展開するには、上記すべての依存関係を、本機能とは別に設定する必要があります。

8.2.2 ステップ 1 – Windows Server* に NPS ロールを追加する

1. Server Manager (サーバー・マネージャー) コンソールで **Add Roles and Features (役割と機能の追加)** ウィザードを開始します。
2. **Next (次へ)** をクリックし、**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。
3. もう一度 **Next (次へ)** をクリックします。
4. サーバーを選択し、**Next (次へ)** をクリックします。
5. Server Roles (サーバーの役割) パネルで **Network and Policy Access Services (ネットワーク・ポリシーとアクセスサービス)** を選択し、**Next (次へ)** をクリックします。

   図 2：サーバーの役割の選択

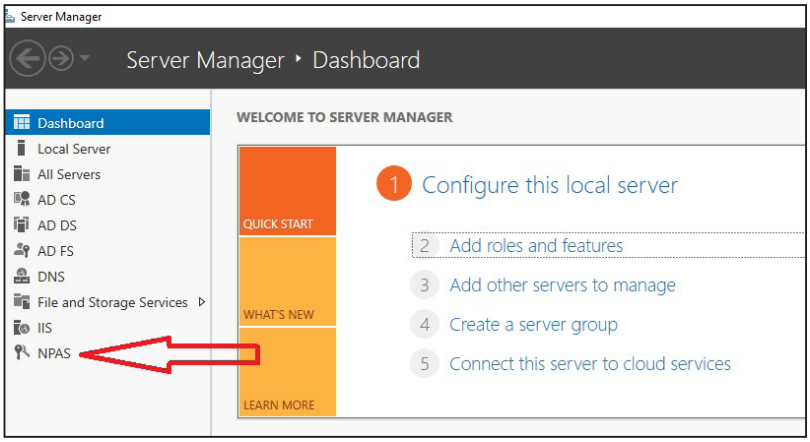
   

   (確認ダイアログが表示された場合、**Include management tools (管理ツールを含める)** チェックボックスをオンにします)

6. Features (機能) パネルで **Next (次へ)** をクリックします。

7. Network and Policy Access Services (ネットワーク・ポリシーとアクセスサービス) パネルで **Next (次へ)** をクリックします。
8. Confirmation (確認) パネルで設定を確認し、**Install (インストール)** をクリックします。再起動が促されたら、画面の案内に従って進めます。
9. 設定が完了したら、ウィザードを閉じます。
10. 前の手順が成功だった場合、Server Manager (サーバー・マネージャー) に NPAS (ネットワーク・ポリシーとアクセスサービス) の役割が表示されます。

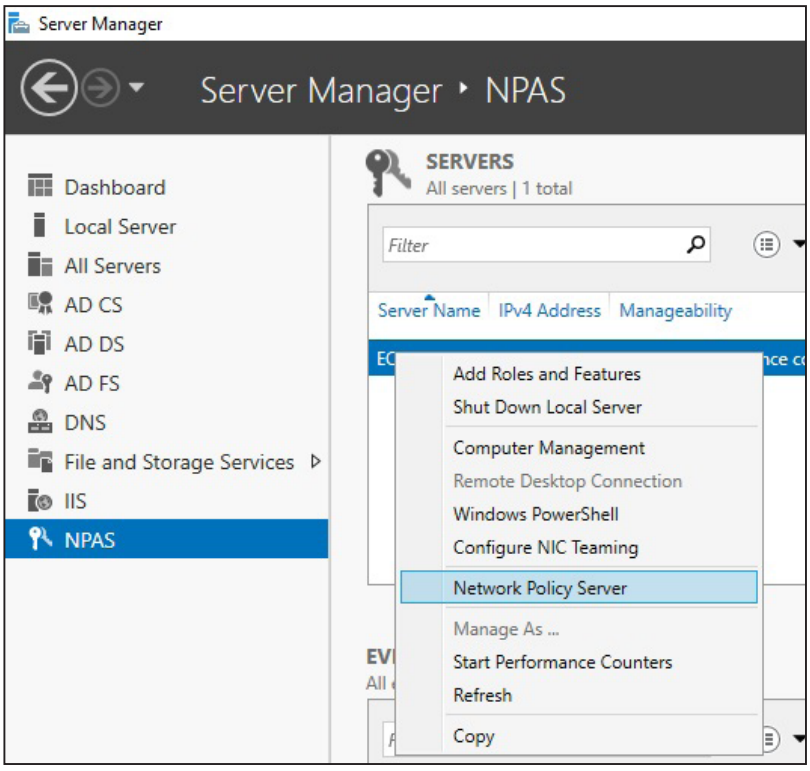
図 3：左側のパネルに NPAS の役割が表示される



8.2.3 ステップ 2 – NPS を RADIUS サーバーとして構成する

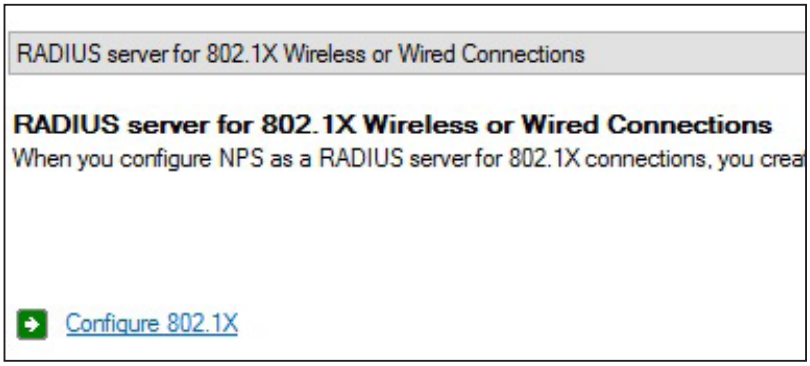
1. Server Manager (サーバー・マネージャー) コンソールで **Network Policy and Access Server (ネットワーク・ポリシーとアクセスサービス)** を選択し、サーバーを右クリックして **Network Policy Server (ネットワーク・ポリシー・サーバー)** を選択します。

図 4：NPS の設定を開く



2. NPS（ネットワーク・ポリシー・サーバー）コンソールの Standard Configuration（標準構成）セクションの **Configuration Scenario（構成シナリオ）**のドロップダウン・リストから **RADIUS Server for 802.1X Wireless or Wired Connections（802.1X ワイヤレス接続またはワイヤード（有線）接続用の RADIUS サーバー）**を選択します。
3. 下部の構成リンクが Configure 802.1X（802.1X を構成する）に変わります。リンクをクリックしてプロセスを続行します。

図 5：変更された構成リンク



4. **Select 802.1X Connections Type（802.1X 接続の種類の選択）**パネルでは、このポリシーを使用して認証されるネットワーク接続の種類（有線/無線）を選択します。Wired（ワイヤード）接続か Wireless（ワイヤレス）接続のいずれかを選択し、ポリシーに名前を付け、**Next（次へ）**をクリックします。
5. **Specify 802.1X Switches（802.1X スイッチの指定）**パネルでは、1 つまたは複数の RADIUS クライアントを設定します。これらのデバイスは、NPS との間で要求と応答をルーティングします。**Add（追加）**をクリックすると、New Radius Client（新しい RADIUS クライアント）が表示されます。該当する情報を入力し、**OK** をクリックします。次に、**Next（次へ）**をクリックします。

   重要：shared secret（共有シークレット）は、NPS と RADIUS クライアントで同じにする必要があります。
6. **Configure an Authentication Method（認証方法の構成）**パネルで、ポリシーで使用するプロトコルと資格情報の種類を選択します。本ガイドの例では、証明書ベースの資格情報を持つ EAP-TLS プロトコルの構成を示しています。
7. **Configure（構成）**ボタンをクリックし、NPS に接続試行があったときに NPS からサプリカント（エンドポイント）に渡される TLS 証明書を選択します。

   重要：この証明書は、エンドポイント・デバイスが信頼する認証局によって発行されたものである必要があります。
8. 完了したら、**OK** をクリックし、**Next（次へ）**をクリックします。
9. **Specify User Groups（ユーザー グループの指定）**パネルで、NPS に接続試行があったときにクライアントの資格情報を検証するために使用するグループをすべて選択します。インテル® EMA では、セキュリティー・グループのリスト指定をサポートしています。インテル® AMT デバイスをセキュリティー・グループに追加することで、802.1X 認証が容易になります。これらのグループをネットワーク・ポリシーに含める必要があります。**Next（次へ）**をクリックして構成を続けます。
10. 必要な場合、トラフィック制御の属性を設定し、**Next（次へ）**をクリックします。
11. 構成を確認して **Finish（完了）**をクリックします。

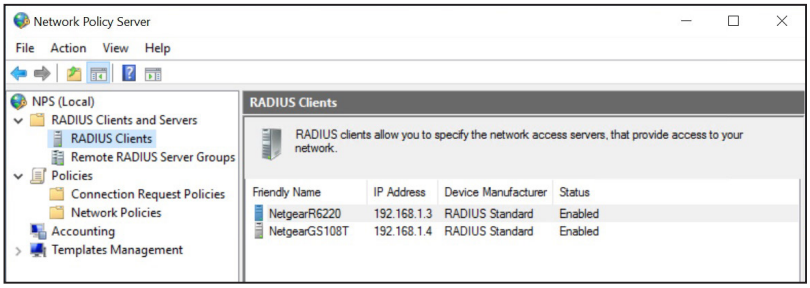
8.2.4 構成後に行う操作

NPS に以下の操作を実行し、必要に応じて RADIUS サーバーを調整します。

8.2.4.1 RADIUS クライアントの作成または編集

1. Network Policy Server（ネットワーク・ポリシー・サーバー）ウィンドウ左側のナビゲーション・ツリーから **RADIUS Clients and Servers（RADIUS クライアントとサーバー）> RADIUS Client（RADIUS クライアント）**を開きます。

図 6：RADIUS クライアントのオプションを開く



2. 新しいクライアントを作成するには、セクション名をクリックして **New（新規）**をクリックします。既存のクライアントを編集するには、クライアントをダブルクリックします。
3. 必要な情報、特に以下の情報を設定します。
    - **Address (IP or DNS)（アドレス (IP または DNS)）：**これは、サーバーにアクセスするクライアント・デバイスのアドレスです。
    - **Shared secret（共有シークレット）：**実際の RADIUS クライアントによって認証に使用されるパスフレーズを作成します。

8.2.4.2 接続要求ポリシーの作成または編集

これらのポリシーは、クライアントからの要求をフィルタリングします。クライアントのプロパティーや使用されたネットワーク・インターフェイスの種類などによって接続を許可または拒否し、オプションで受信した要求に追加の設定を適用します。

1. Network Policy Server（ネットワーク・ポリシー・サーバー）ウィンドウ左側のナビゲーション・ツリーから **Policies（ポリシー）> Connection Request Policies（接続要求ポリシー）**を開きます。
2. 新しいポリシーを作成するには、セクション名をクリックして **New（新規）**をクリックします。既存のポリシーを編集するには、ポリシーをダブルクリックします。
3. 必要な構成を設定します。特に、要求が満たす必要のある Conditions（条件）を設定します。

8.2.4.3 ネットワーク・ポリシーの作成または編集

これらのポリシーは、ネットワークへのアクセスを許可または拒否するために接続に適用されます。802.1X 認証に使用されるプロトコルがこれらのポリシーによって検証されます。

1. Network Policy Server（ネットワーク・ポリシー・サーバー）ウィンドウ左側のナビゲーション・ツリーから **Policies（ポリシー）> Network Policies（ネットワーク・ポリシー）**を開きます。
2. 新しいポリシーを作成するには、セクション名をクリックして **New（新規）**をクリックします。既存のポリシーを編集するには、ポリシーをダブルクリックします。
3. 必要な構成を設定します。特に、要求が満たす必要のある Conditions（条件）と Constraints（制約）を設定します。

図 7：ネットワーク・ポリシーのプロパティーを開く(a)

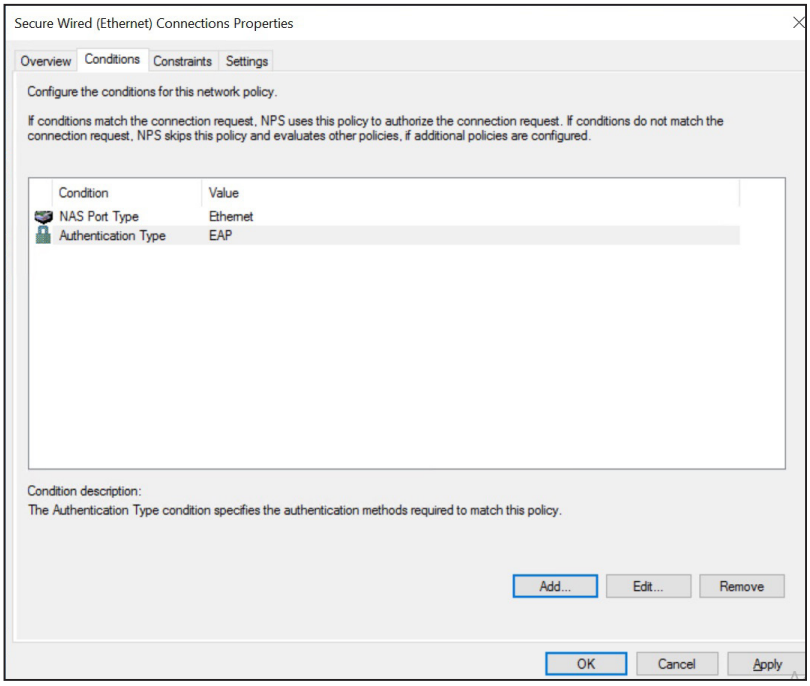
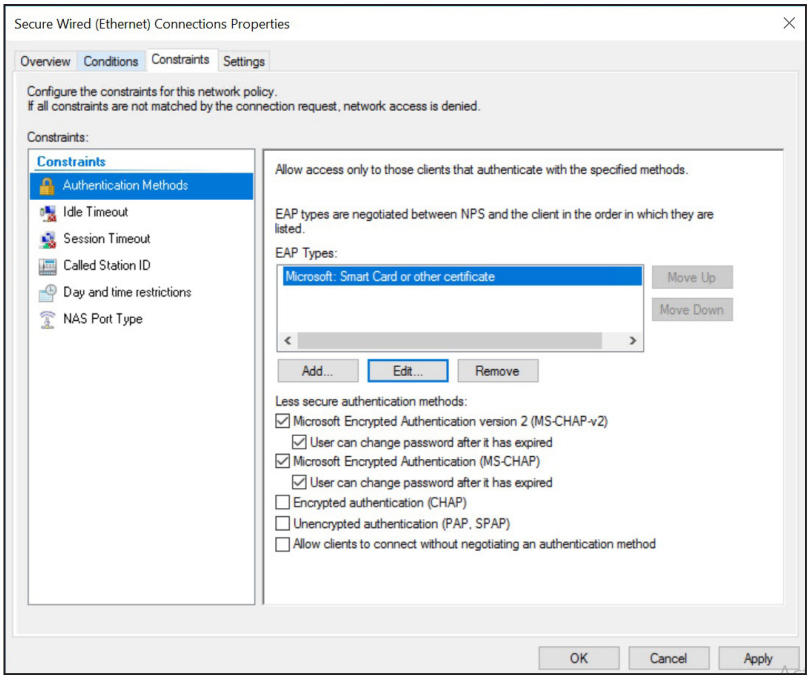


図 8：ネットワーク・ポリシーのプロパティーを開く(b)



8.3 RADIUS クライアントの構成

RADIUS クライアントを構成するには、デバイスのマニュアルを参照し、その指示に従って上述の設定を使用して希望するネットワークを設定します。

無線アクセスポイントの場合、通常、以下の設定が必要です。

- 802.1X を使用して認証するネットワークを選択する
- 認証プロトコルから WPA/WPA2 エンタープライズを選択する

- RADIUS Server (RADIUS サーバー) フィールドに RADIUS サーバー (NPS) の IP アドレスまたはホスト名を入力する
- Shared Secret (共有シークレット) に RADIUS サーバーを構成したときと同じ共有シークレットを入力します。

有線イーサネット・スイッチの場合、通常、以下の設定が必要です。

- RADIUS Server (RADIUS サーバー) の設定項目に RADIUS サーバー (NPS) の IP アドレスまたはホスト名を入力する
- Shared Secret (共有シークレット) に RADIUS サーバーを構成したときと同じ共有シークレットを入力します。
- ポートベース認証の 802.1X の設定を有効にする
- ポート認証の設定で、802.1X を使用して認証するポートを指定する

8.4 エンドポイントのネットワークへの接続

デバイスがネットワークにアクセスするためには、以下のことを確認してください。

- **RADIUS サーバー –** NPS が正しく構成され、有効化されていること。必要なメディア、RADIUS クライアント、および資格情報タイプに対応するアクティブなネットワーク・ポリシーと接続要求ポリシーが設定されていること。
- **RADIUS クライアント –** 該当するすべてのネットワーク・デバイスとアクセスポイントが上記の NPS との間で要求と応答を転送するように構成されていること。
- **サプリカント –** エンドポイント・デバイスは、正しい資格情報タイプを使用して指定されたネットワークに接続するよう構成されている必要があります。このため、インバンド (OS) 接続の場合は、デバイス上の証明書ストアに該当する証明書をインストールする必要があります。アウトオブバンド接続 (インテル® AMT) の場合は、ネットワークの構成に使用された 802.1X 設定に適合するインテル® AMT プロファイルを使用してデバイスをプロビジョニングする必要があります。

8.5 環境セットアップ例

このセクションでは、インテル® EMA で 802.1X 認証プロビジョニングのインテル® AMT デバイスを実装したある環境の構成をすべて紹介します。

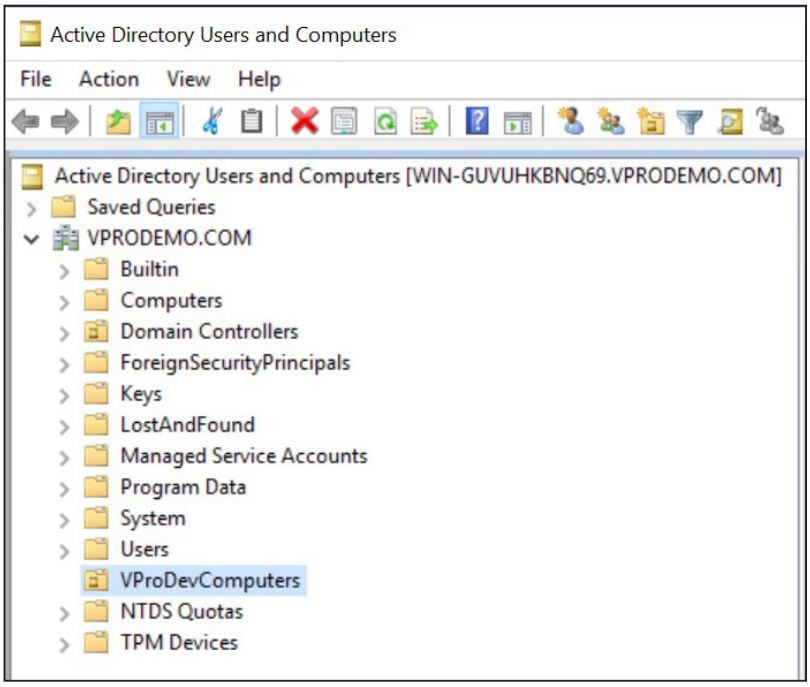
この環境は次の要素から成ります。

- 次のサーバー、サービス、プログラムを備えた Windows Server* 2016 Standard :
  - Active Directory* ドメインサービス
  - Active Directory* 証明書サービス
  - DHCP サーバー
  - DNS サーバー
  - Internet Information Services
  - ネットワーク・ポリシー・サーバー
  - SQL Server* 2016
  - インテル® エンドポイント・マネジメント・アシスタント v1.3.2
  - 静的 IP アドレス : 192.168.1.2
- イーサネット接続用スマートスイッチの Netgear Prosafe GS108T
- 無線接続用の Netgear AC1200 スマート Wi-Fi* ルーター、モデル : R6220
- エンドポイントとして、インテル® vPro® テクノロジー対応、インテル® AMT v11.8.50 を搭載した Dell* Latitude* E7270

8.5.1 Active Directory* ドメインサービス

1. ドメイン **VPRODEMO.COM** に組織単位 (OU) を追加します。この組織単位 **VProDevComputers** には、802.1X 認証に使用されるコンピューター・オブジェクトを格納します。

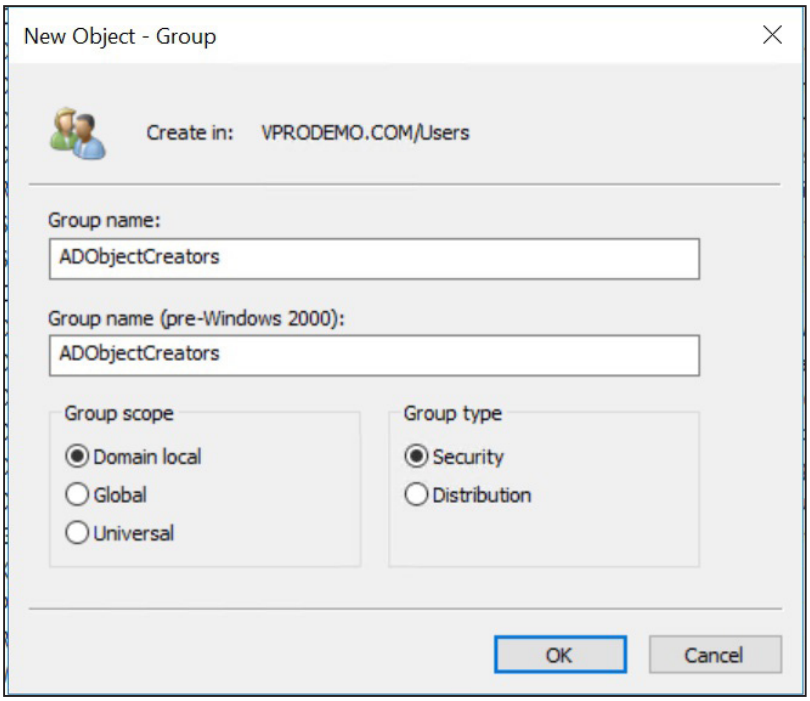
図 9：組織単位 (OU) を追加する



2. インテル® EMA サーバーを実行しているマシンに権限を追加します。

   a. Group scope (グループのスコープ) を Domain Local (ドメインローカル) に設定したセキュリティー・グループを作成します。

   図 10：セキュリティー・グループを作成



   b. 新しく作成したセキュリティー・グループに、ターゲットのコンピューター・オブジェクトを追加します。管理機能サーバーをホストするマシンについてこの作業を行います。

   図 11：新しいセキュリティー・グループにコンピューターを追加

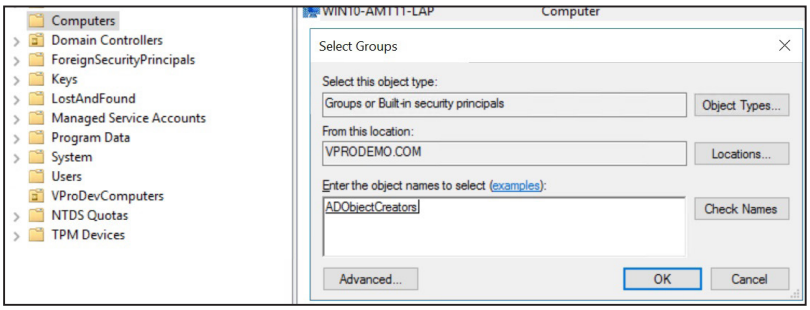
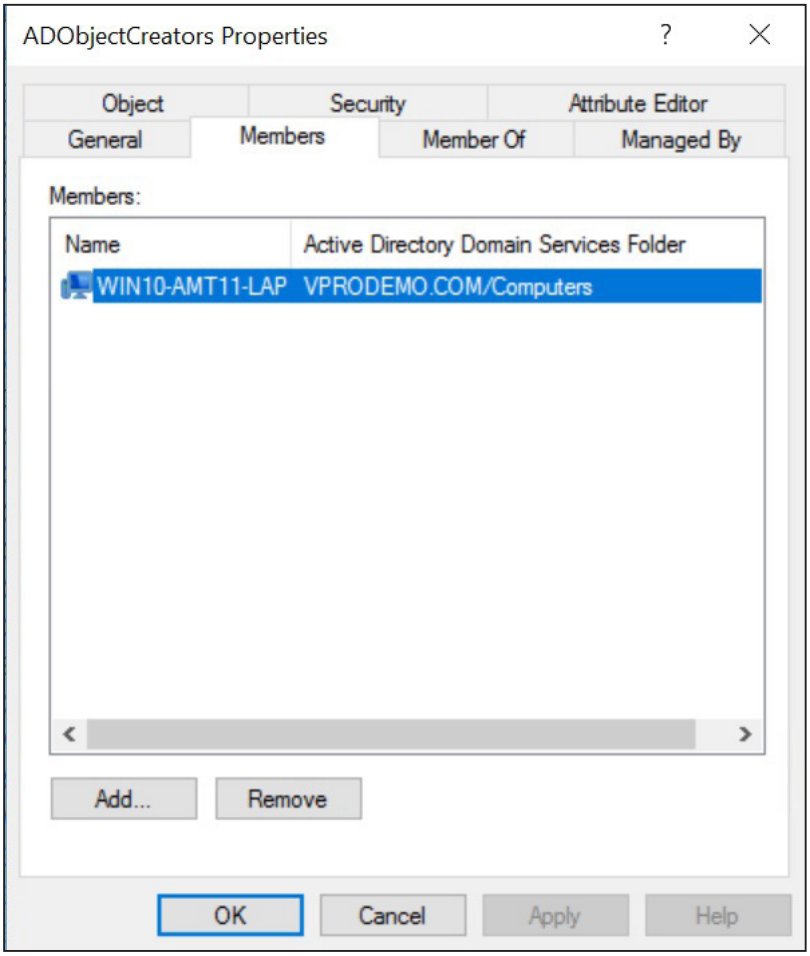


図 12：セキュリティー・グループのメンバーの変更



c. 新しいセキュリティー・グループを、802.1X 認証用の AD コンピューター・オブジェクトが作成される組織単位の Security（セキュリティー）タブに追加します。このセキュリティー・グループには、利用可能なすべてのアクセス許可が付与されていることを確認し、Advanced（詳細設定）を編集して、このグループの権限の適用対象を This object and all descendant objects（このオブジェクトとすべての子オブジェクト）にします。

図 13：OU のセキュリティー・リストを変更

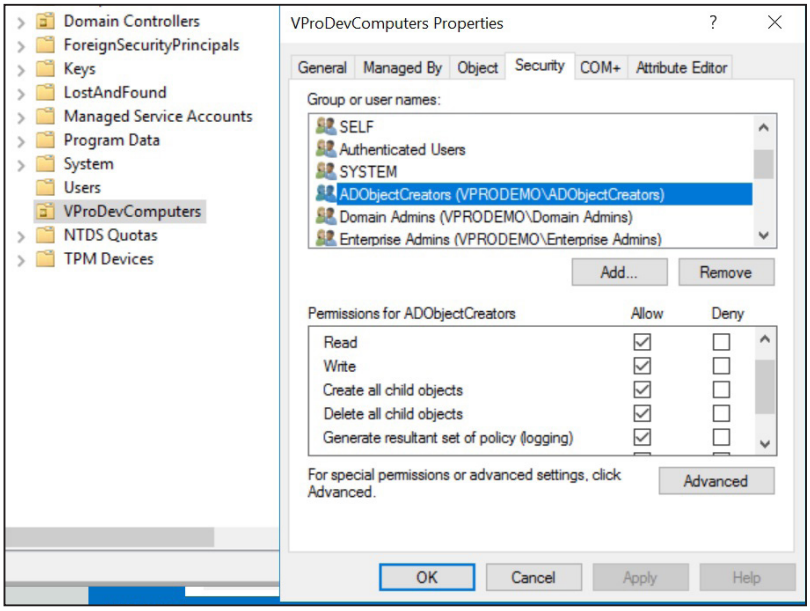
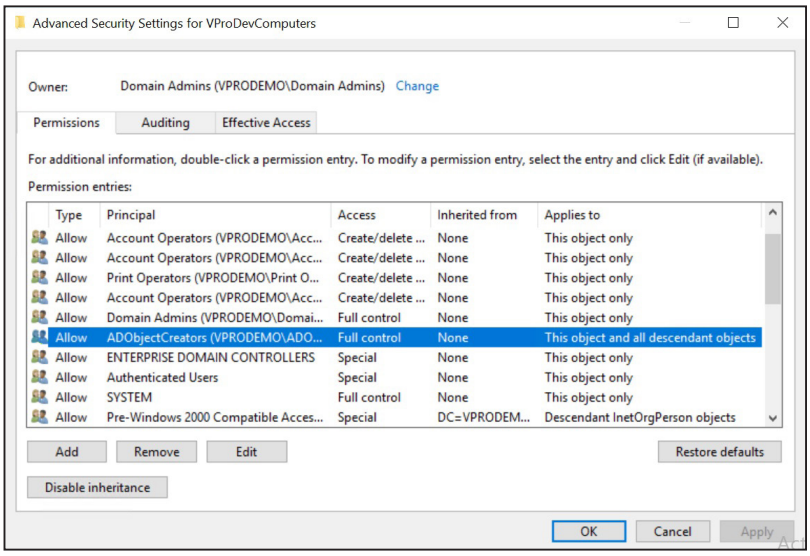


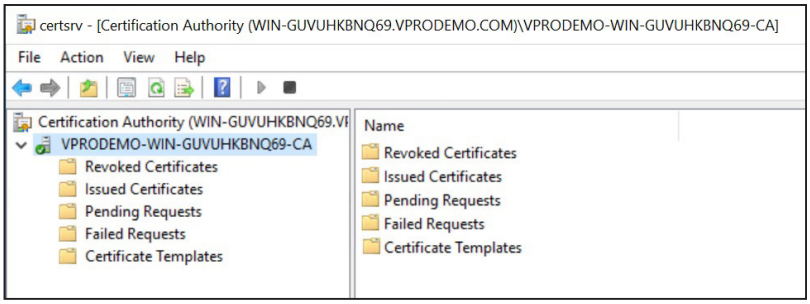
図 14：詳細なセキュリティー設定



8.5.2 Active Directory* 証明書サービス

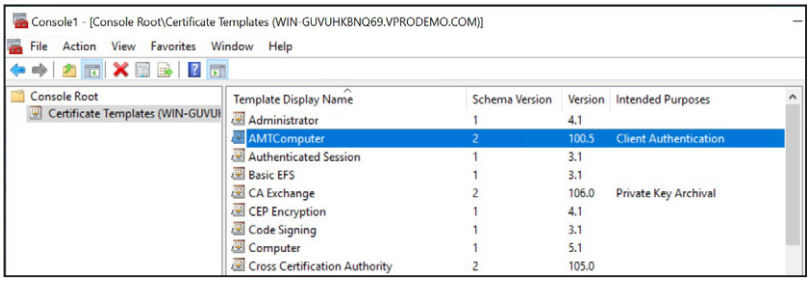
1. 認証局 (エンタープライズ・ルート CA) の VPRODEMO-WIN-GUVUHKBNQ69-CA を選択します。

図 15：認証局のリスト



2. 証明書テンプレート **AMTComputer** を作成します。これは、Workstation Authentication (ワークステーション認証) テンプレートをベースに複製されたテンプレートです。

図 16：証明書テンプレートのリスト



   a. **AMTComputer** を右クリックし、**Properties (プロパティー)** を選択します。

   b. Subject Name (サブジェクト名) タブで **Supply in the request (要求に含まれる)** を選択します。

   c. Request Handling (要求処理) タブで **Allow private key to be exported (秘密キーのエクスポートを許可する)** チェックボックスをオンにします。

   d. Security (セキュリティー) タブで、**Domain Computers** に **Read (読み取り)** と **Enroll (登録)** のアクセス許可を付与します (手動登録の場合、**Everyone** も追加します)。

   e. 認証局でテンプレートを有効にします (**Certificate Template (証明書テンプレート)** を右クリックし、**New (新規) > Certificate Template to Issue (発行する証明書テンプレート)** を選択します)。

8.5.3 ネットワーク・ポリシー・サーバー

1. 以下のように、各ネットワーク・アクセス・ポイントに 1 つずつ、計 2 つの RADIUS クライアントをセットアップします。

表 4：ネットワーク・ポリシー・サーバー RADIUS クライアント

フレンドリー名	IP アドレス	ベンダー	ステータス
NetgearGS108T	192.168.1.4	RADIUS Standard	有効
NetgearR6220	192.168.1.3	RADIUS Standard	有効

図 17：RADIUS クライアント 1

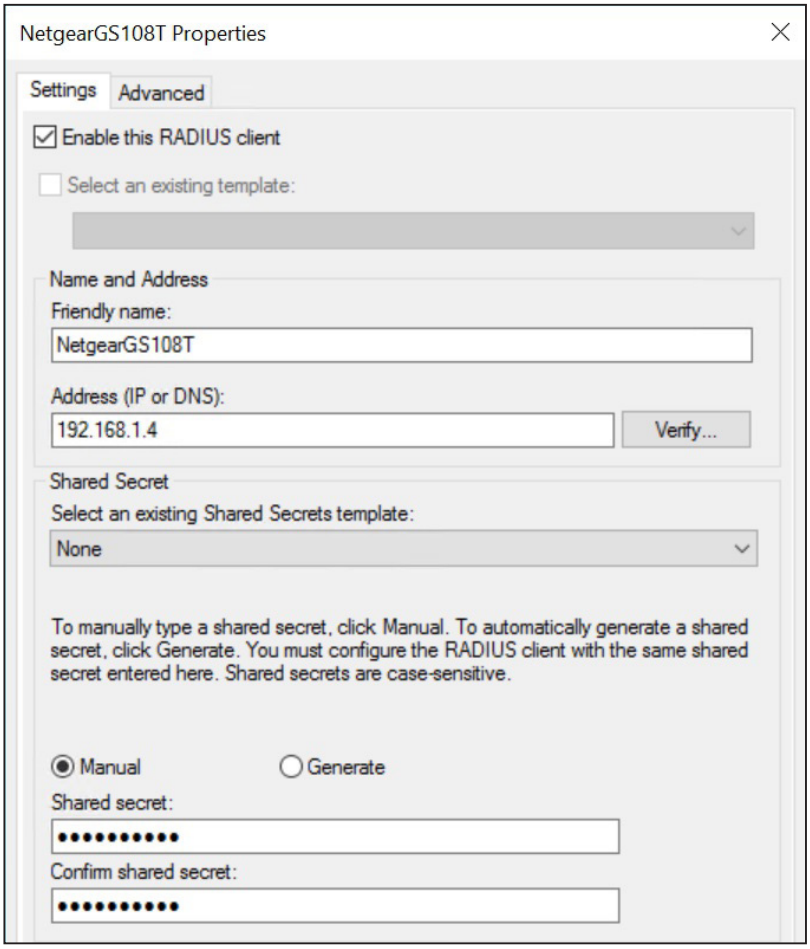
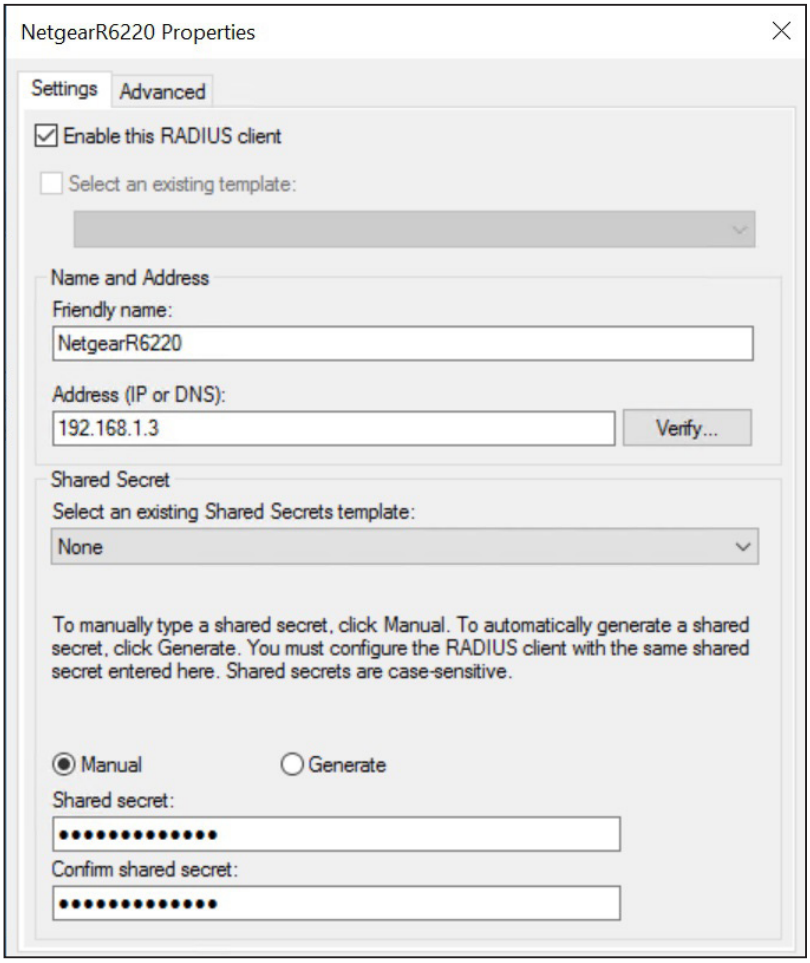
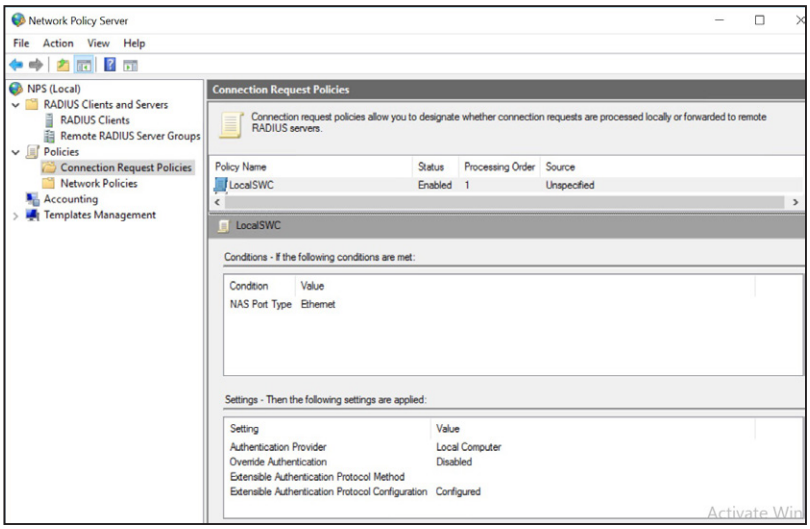


図 18：RADIUS クライアント 2



2. 接続要求ポリシーをセットアップします。

図 19：NPS の Connection Request Policies（接続要求ポリシー）ビュー



3. EAP-TLS プロトコルを使用して接続を評価するために使用するネットワーク・ポリシーをセットアップします。以下のプロパティーを指定します。

    - Conditions (条件) : Authentication Type (認証の種類) = EAP
    - Constraints (制約) : Authentication Methods (認証方法) - EAP Types (EAP の種類) : Microsoft: Smart Card or other certificate (スマートカードまたはその他の証明書)

図 20 : NPS の Network Policies (ネットワーク・ポリシー) ビュー

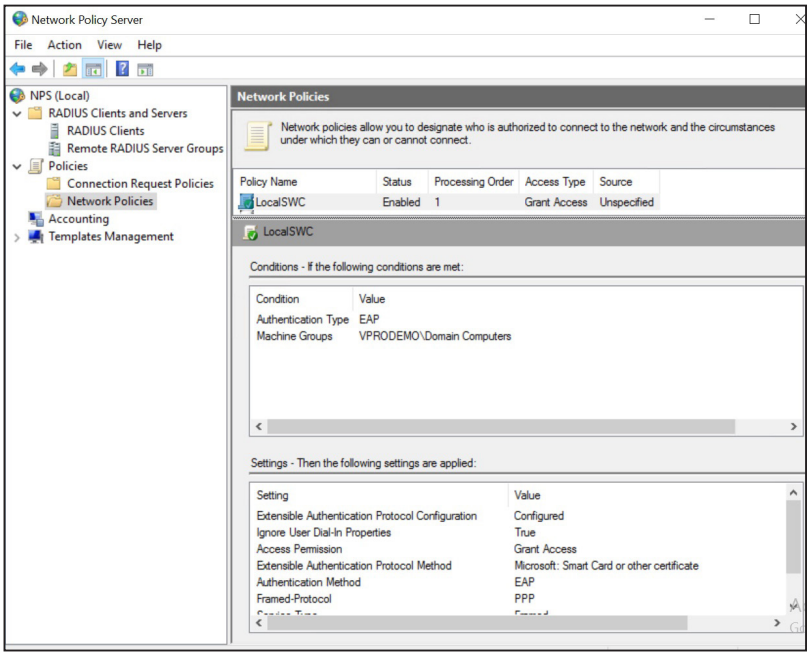
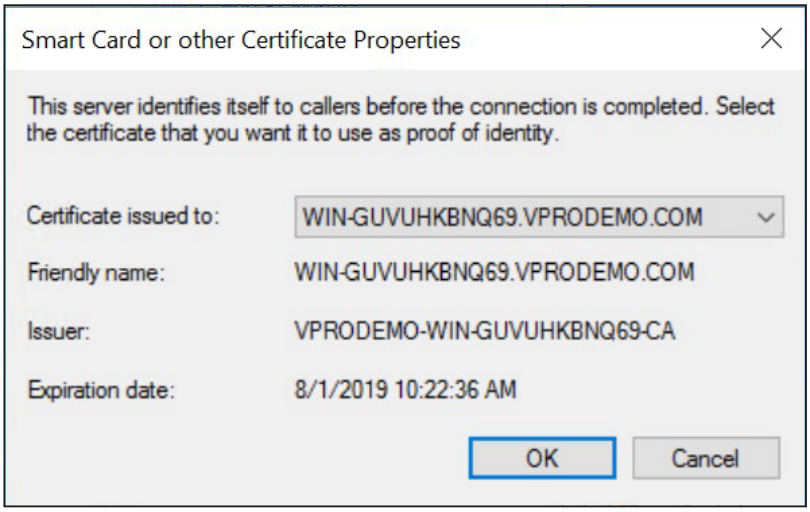


図 21 : EAP Types (EAP の種類) : Microsoft: Smart Card or other certificate properties (スマートカードまたはその他の証明書のプロパティー)



8.5.4 有線接続

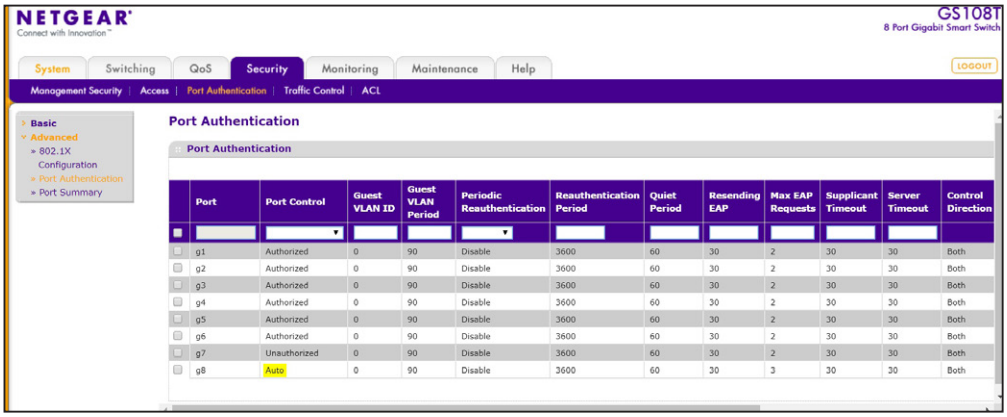
以下の例では、静的 IP アドレス 192.168.1.4 を持つイーサネット・スイッチ Netgear GS108T を使用します。

1. ポート認証：**Security（セキュリティー）> Port Authentication（ポート認証）> Advanced（詳細設定）> Port Authentication（ポート認証）**

   a. **Port Control（ポート制御）**を **Auto（自動）**に設定し、RADIUS サーバーを使用して接続を認証するポートを指定します。

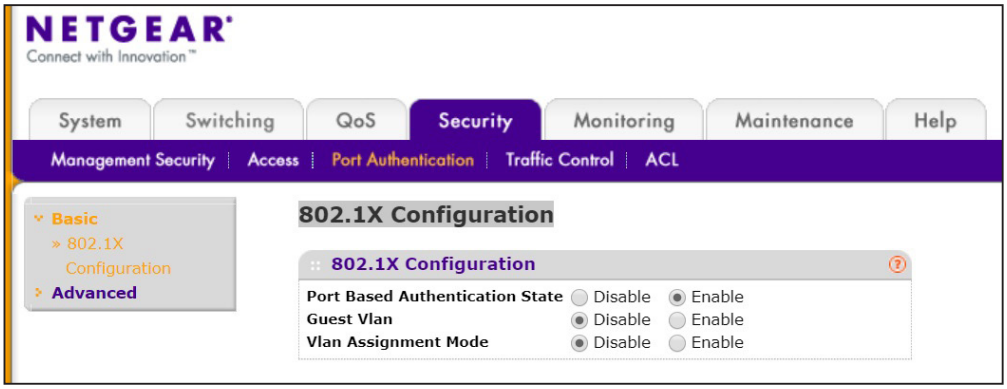
   b. 制限しないポートについては、**Port Control（ポート制御）**を **Authorized（認証済み）**に設定します。

図 22：ポート認証の設定



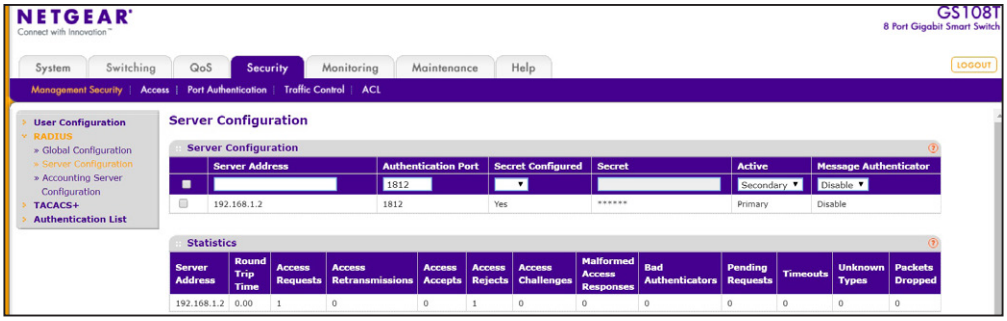
2. 802.1X の設定：**Security（セキュリティー）> Port Authentication（ポート認証）> Basic（基本）> 802.1X Configuration（802.1X の設定）**で、ポートベースの認証で 802.1X を有効化します。

図 23：802.1X の設定



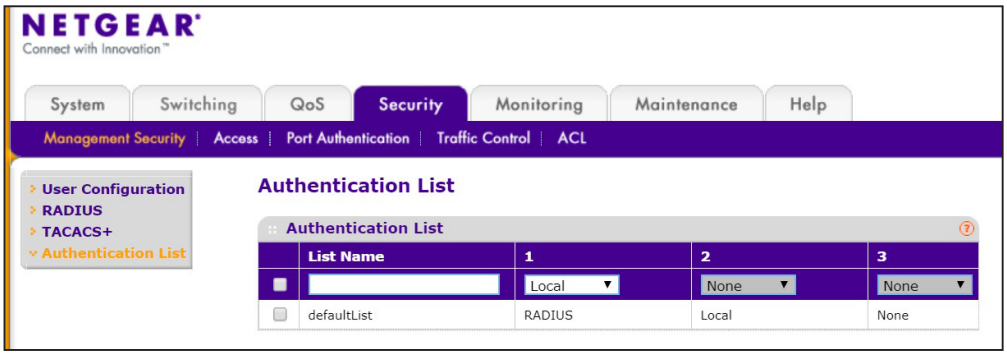
3. RADIUS サーバーの設定：**Security（セキュリティー）> Management Security（管理セキュリティー）> RADIUS Server Configuration（RADIUS サーバーの設定）**で、RADIUS サーバーの設定を追加し、この接続用に作成した NPS RADIUS クライアントに定義された共有シークレットを指定します。

図 24：RADIUS サーバーの設定



4. 認証リスト：**Security（セキュリティー）> Management Security（管理セキュリティー）> Authentication List（認証リスト）**で、現在の defaultList を編集し、RADIUS を 1 番目の認証コードに設定します。

図 25：認証リストの設定



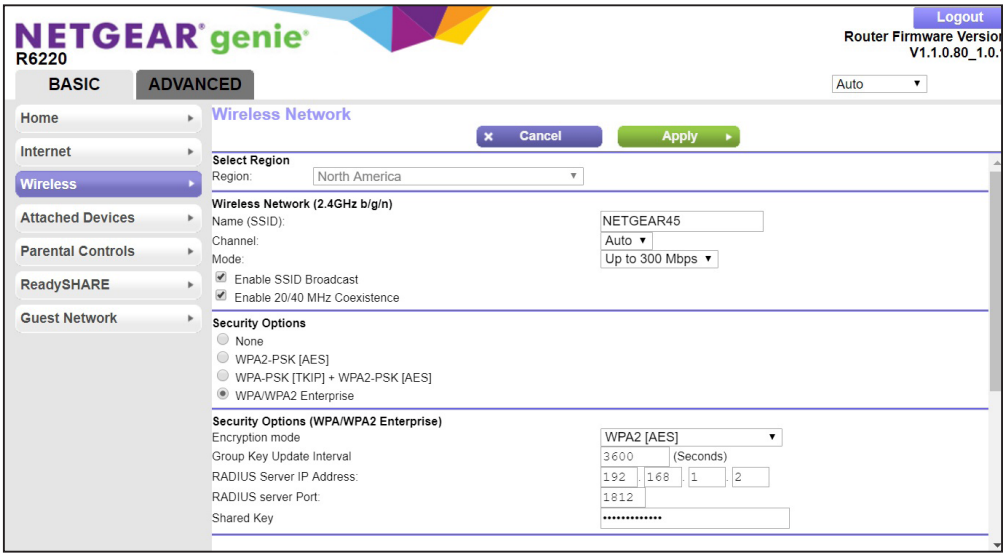
8.5.5 無線接続

静的 IP アドレス 192.168.1.3 を持つ Wi-Fi* アクセスポイント Netgear R6220 を使用します。

制限された無線ネットワーク：**Basic（基本）> Wireless（無線）**で、802.1X 認証の無線ネットワークを 1 つ選択します（この例では 2.4 GHz）。

- Security Options（セキュリティー・オプション）：WPA/WPA2 エンタープライズを設定します。
- Security Options（セキュリティー・オプション）の詳細設定：WPA2 [AES] を設定します（WPA でも動作します）。
- RADIUS サーバーの IP アドレスを指定し、この接続のために作成した NPS RADIUS クライアントに定義された共有シークレットを設定します。

図 26：無線ネットワーク設定



8.6 用語集

AAA：認証（Authentication）、承認（Authorization）、アカウンティング（Accounting）。

CA：認証局（Certification Authority）

NPS：ネットワーク・ポリシー・サーバー（Microsoft による RADIUS 標準の実装）