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）

管理と使用ガイド

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。

本資料は、インテル® EMA サーバーのインストールが完了した後に、エンドポイントにインテル® EMA をセットアップおよび構成する方法を説明します。また、時間の経過による組織の拡大と変化に合わせて、インテル® EMA の使用環境 (「テナント」と呼ぶ。以下のセクション 1.2.1 を参照) を保守、変更する方法についても説明します。さらに、インテル® EMA テナント環境で各ユーザーロールが実行できるタスクなど、インテル® EMA を使用するにあたって必要な主な概念と用語を定義します。最後に、管理対象のエンドポイントに対して実行可能な管理アクションを紹介し、それらのアクションを実行するためのステップ・バイ・ステップの手順を説明します。

1.1 使用要件

インテル® EMA を使用してエンドポイントを管理するには、次のコンポーネントが必要になります。

- サポートされるウェブブラウザー：Internet Explorer* 11+、Chrome* 63+ (2017 年 12 月以降)、Firefox* 52+ (2017 年 3 月以降)。
- インテル® アクティブ・マネジメント・テクノロジー (インテル® AMT) に関する知識：インテル® AMT ソリューションに関する全般的な知識が必要です。適切なセットアップ/プロビジョニング・アプローチと、各種コントロール・モードについての知識が求められます。インテル® EMA は、インテル® AMT 11.8 以上のみをサポートしています。

  注記: インテル® AMT の知識が必要になるのは、アウトオブバンド機能を使用する場合のみです (セクション 1.2.6 を参照)。

インテル® AMT の詳細については、次の資料を参照してください。

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm

1.1.1 エージェントの前提条件

インテル® EMA エージェントをセットアップするために必要な前提条件を以下に記載します。

- **オペレーティング・システム:** インテル® EMA エージェントは、Microsoft* Windows* 7 と Windows* 10 (いずれも 32 ビットと 64 ビットの両方) のオペレーティング・システムで正式にサポートされています。
- **注記:** 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。

- **ファイアウォール：**インテル® EMA エージェントをインストールすると、インストールされたエージェントのバイナリープロセスに Windows* ファイアウォールの以下のインバウンド・ルールがセットアップされます。その他のファイアウォールをご利用の場合、インストールされたエージェントのバイナリープロセスに対して、以下のインバウンド・ルールが設定されていることを確認してください。
    - ピアツーピア・トラフィック：ローカルポート 16990 の UDP、ローカルおよびリモートアドレスの任意の IP、エッジ・トラバーサルはブロックされます。
    - ピアツーピア・トラフィック：ローカルポート 16990 の TCP、ローカルおよびリモートアドレスの任意の IP、エッジ・トラバーサルはブロックされます。
    - ローカル・ループバック管理トラフィック：ローカルポート 16991 の TCP、ローカルおよびリモートアドレスの 127.0.0.1、エッジ・トラバーサルはブロックされます。
- **インテル® アクティブ・マネジメント・テクノロジー（インテル® AMT）：**インテル® EMA は、インテル® AMT 11.8 以上のみをサポートしています。アウトオブバンドのエンドポイント管理にのみ必要です。後述のセクション 1.2.6 を参照してください。
  以下の表は、エンドポイントで USBR over CIRA を使用するためのインテル® AMT バージョンの必要最低要件を示しています。

インテル® AMT バージョン	**ビルド番号**
インテル® AMT 11.8	すべて
インテル® AMT 12	12.0.70.1607 以降
インテル® AMT 14	14.0.45.1341 以降
インテル® AMT 15	すべて

  USBR の詳細については、セクション 1.2.8 を参照してください。

1.2 主な概念

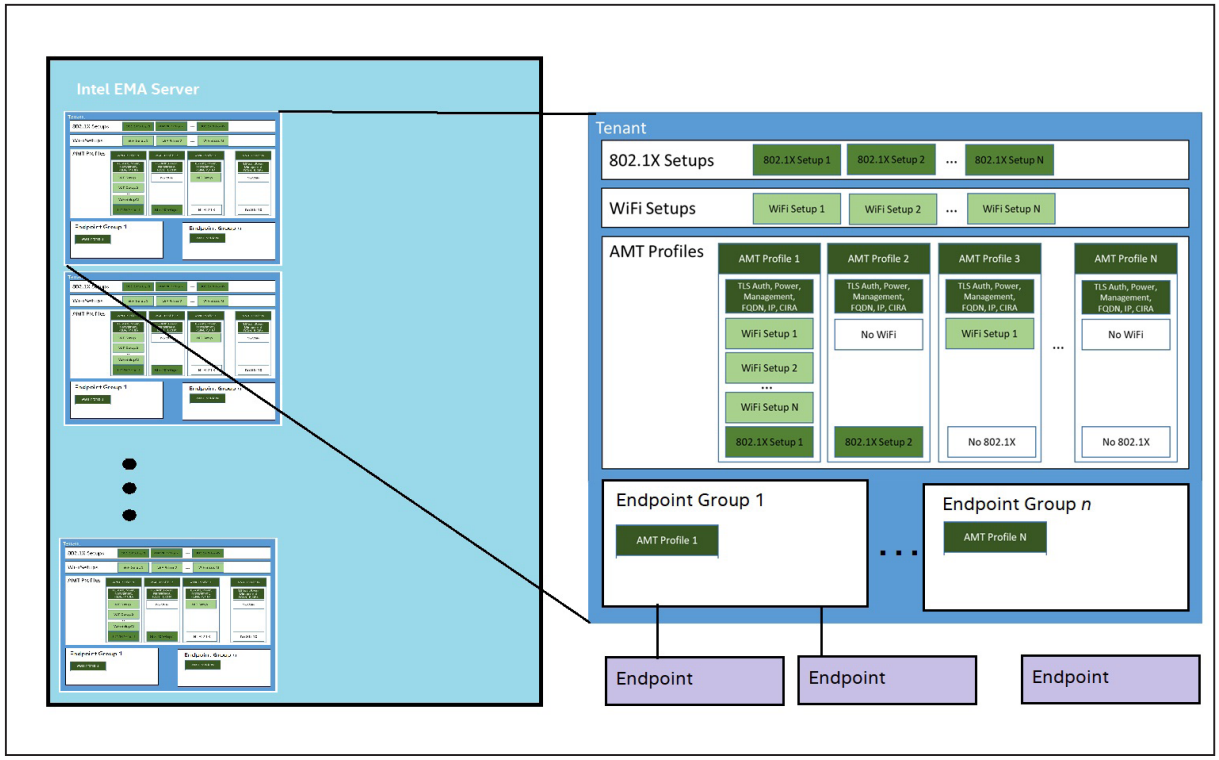
以下のセクションでは、インテル® EMA ソリューションで使用される主なツール、コンポーネント、ロール、プロセスについて説明します。

1.2.1 テナント

テナントとは、インテル® EMA サーバー内の各使用スペースであり、それぞれが 1 つのビジネス・エンティティーを表します。例えば、テナントは 1 企業、1 組織、または企業内の 1 事業所所在地などの場合があります。単一のインテル® EMA サーバーで複数のテナントをサポートできます。テナント内のユーザー、エンドポイント・グループ、エンドポイントは、テナントごとに独立しています。

以下の図は、インテル® EMA サーバーとそのテナントとの関係を示しています。エンドポイント・グループ、プロファイル、エンドポイントなどのその他の概念について、以降のセクションで説明します。

図 1：インテル® EMA サーバーとテナント



1.2.2 ユーザーロール

1 人のユーザーに設定できるロールは 1 つのみです。逆に、1 つのロールを複数のユーザーによって実行できます。使用できるロールは次のとおりです。

- **Global Administrator（グローバル管理者）：**このロールはユーザー管理、テナント管理、サーバー管理を実行します。グローバル管理者はエンドポイント管理は実行せず、どのエンドポイント・グループにも属しません（属すことができません）。グローバル管理者がコントロールする範囲は、1 つのインテル® EMA サーバー・インストール・インスタンス内のすべてのテナントにわたります。
- **Tenant Administrator（テナント管理者）：**特定のテナントに固有のロールです。そのテナント内のすべての操作（ユーザー管理、エンドポイント管理、インテル® AMT の検出）を実行できます。そのため、テナント管理者は、そのテナント内のどのユーザーグループにも属しません（属すことができません）。テナント管理者ユーザーは、グローバル管理者ユーザーを管理できません。
- **Account Manager（アカウント・マネージャー）：**特定のテナントに固有のロールです。ユーザー管理のみを実行できます。ただし、アカウント・マネージャーは、上位のロール（テナント管理者やグローバル管理者など）を持つユーザーを管理できません。アカウント・マネージャーはエンドポイント管理を実行できません。そのため、どのユーザーグループにも属すことができません。
- **Endpoint Group Creator（エンドポイント・グループ作成者）：**特定のテナントに固有のロールです。エンドポイント管理、エンドポイント・グループの新規作成、インテル® AMT プロファイルの管理を実行できます。エンドポイント・グループ作成者は、複数のユーザーグループに属することができ、自らが属するすべてのグループを管理できます。エンドポイント・グループ作成者はユーザー管理を実行できません。ただし、そのテナントに含まれるすべてのユーザーグループ、すべてのエンドポイント・グループ作成者、すべてのエンドポイント・グループ・ユーザーのリストを表示できます（つまり、そのテナント内でユーザーロール階層が同位以下のユーザーロールを表示できます。アカウント・マネージャー、テナント管理者、グローバル管理者を表示することはできません）。
- **Endpoint Group User（エンドポイント・グループ・ユーザー）：**特定のテナントに固有のロールで、エンドポイント管理のみ実行できます。エンドポイント・グループ・ユーザーは、複数のユーザーグループに属することができますが、ユーザー管理は実行できず、自身のユーザー情報のみ表示できます。

1.2.3 エンドポイント・グループ

エンドポイント・グループは、共通した構成と権限を持つエンドポイントの集合です。各エンドポイントが参加できるエンドポイント・グループは 1 つだけですが、別のエンドポイント・グループに変更することは可能です。エンドポイント・グループを作成するとき、次の共通する設定を指定する必要があります。

1. ポリシーセット : ポリシーセットは、そのエンドポイント・グループに属するエンドポイント上で実行できるアクションの種類をコントロールします。詳細については、セクション 3.4.1 を参照してください。
2. インテル® AMT の自動セットアップ : そのエンドポイント・グループに参加するすべてのエンドポイントについて、インテル® EMA がこの共通のインテル® AMT 構成のセットアップを試みます。

エンドポイントをインテル® EMA サーバーに接続するように構成/設定する必要がある場合、対象のエンドポイント・グループのポリシーファイルを含むインテル® EMA エージェント・インストーラーをダウンロードして実行する必要があります。これにより、エンドポイントはインテル® EMA サーバーに接続し、ポリシーファイルに指定されたエンドポイント・グループに参加します。

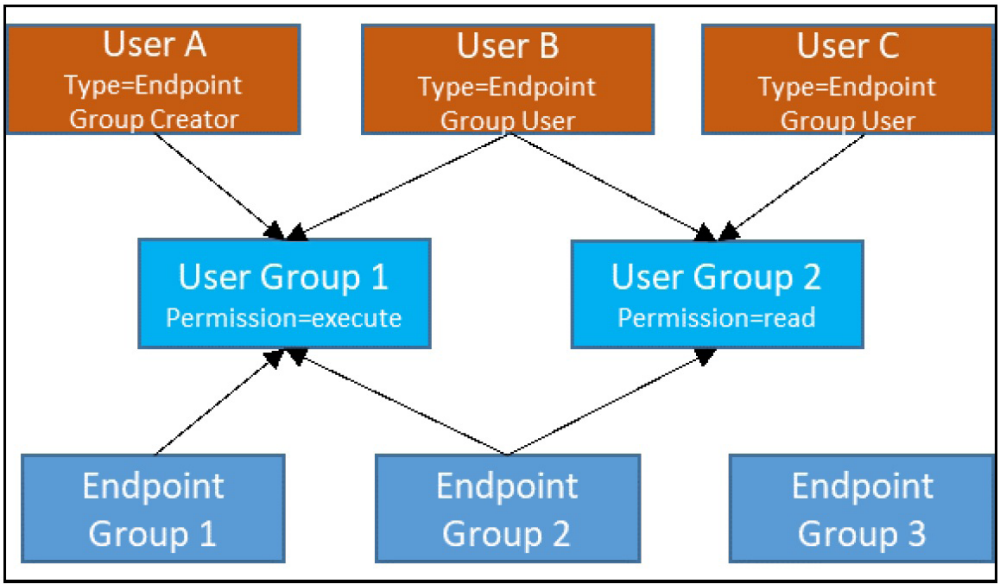
1.2.4 ユーザーグループ

ユーザーグループは、ユーザー (エンドポイント・グループ作成者またはエンドポイント・グループ・ユーザー) のリストと、それらのユーザーが関係するエンドポイント・グループで構成されます。ユーザーは複数のユーザーグループに属することができます (下図の「User B」)。あるユーザーがあるエンドポイント・グループにアクションを実行するには、そのエンドポイント・グループとユーザーが同一のユーザーグループに関連付けられている必要があります (「User B」と「Endpoint Group 2」はともに実行権限を持つ「User Group 1」に属しているため、「User B」は「Endpoint Group 2」に対してアクションを実行できます)。ただし、テナント管理者ユーザーは例外で、どのグループにも属すことなく、すべてのエンドポイント・グループに対してアクションを実行できます。

ユーザーグループに付与される権限により、メンバーユーザーが実行できるアクション (読み取り、実行など) が決まります。

- ユーザーグループは「読み取り」または「実行」権限のいずれかを持つことができます。
- 各テナント内のエンドポイント・グループ作成者とエンドポイント・グループ・ユーザーは、0 個以上のユーザーグループと関連付けできます。
- 各テナント内のエンドポイント・グループは、0 個以上のユーザーグループと関連付けできます。

図 2 : ユーザー、ユーザーグループ、エンドポイント・グループの関係



1.2.5 インテル® EMA エージェント

インテル® EMA エージェントは、クライアント・エンドポイントにインストールされるソフトウェアです。インテル® EMA エージェントは、クライアント・エンドポイントからインテル® EMA サーバーへの接続を支援し、インテル® EMA サーバーがエンドポイントを管理できるようにします。エージェントは実際には EmaAgent.exe と EmaAgent.msh という 2 つのファイルで構成されます。エージェントが動作するには、この 2 つのファイルが管理対象のエンドポイント上に存在している必要があります (セクション 4 参照)。

エージェントは、エージェントのサーバーへの接続に関する基本情報を表示できるコマンド・ライン・インターフェイスも備えています。これは、エンドポイントへのエージェント導入時に接続をトラブルシューティングするのに役立ちます。詳細については、セクション 4.5 を参照してください。

1.2.5.1 エージェントの前提条件

インテル® EMA エージェントをセットアップするために必要な前提条件を以下に記載します。

- **オペレーティング・システム:** インテル® EMA エージェントは、Microsoft* Windows* 7 と Windows* 10 (いずれも 32 ビットと 64 ビットの両方) のオペレーティング・システムで正式にサポートされています。
- **注記:** 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。
- **ファイアウォール :** インテル® EMA エージェントをインストールすると、インストールされたエージェントのバイナリープロセスに Windows* ファイアウォールの以下のインバウンド・ルールがセットアップされます。その他のファイアウォールをご利用の場合、インストールされたエージェントのバイナリープロセスに対して、以下のインバウンド・ルールが設定されていることを確認してください。
  - ピアツーピア・トラフィック:ローカルポート 16990 の UDP、ローカルおよびリモートアドレスの任意の IP、エッジ・トラバーサルはブロックされます。
  - ピアツーピア・トラフィック:ローカルポート 16990 の TCP、ローカルおよびリモートアドレスの任意の IP、エッジ・トラバーサルはブロックされます。
  - ローカル・ループバック管理トラフィック : ローカルポート 16991 の TCP、ローカルおよびリモートアドレスの 127.0.0.1、エッジ・トラバーサルはブロックされます。
- **インテル® アクティブ・マネジメント・テクノロジー (インテル® AMT) :** インテル® EMA は、インテル® AMT 11.8 以上のみをサポートしています。アウトオブバンドのエンドポイント管理にのみ必要です。後述のセクション 1.2.6 を参照してください。

  以下の表は、エンドポイントで USBR over CIRA を使用するためのインテル® AMT バージョンの必要最低要件を示しています。

インテル® AMT バージョン	ビルド番号
インテル® AMT 11.8	すべて
インテル® AMT 12	12.0.70.1607 以降
インテル® AMT 14	14.0.45.1341 以降
インテル® AMT 15	すべて

  USBR の詳細については、セクション 1.2.8 を参照してください。

1.2.6 インバンドとアウトオブバンド

インテル® EMA エージェントは、管理対象エンドポイント上のオペレーティング・システムで動作します。この接続を「インバンド」接続と呼びます。この接続に依存する機能はすべて、インバンド機能と呼ばれます。インテル® AMT に依存する機能はすべて、アウトオブバンド機能と呼ばれます。

注記：インバンド機能には、管理対象のエンドポイント上で稼働状態のオペレーティング・システムが動作していることが必要です。オペレーティング・システムが稼働していないか存在しないエンドポイントとやり取りするには、インテル® AMT を介したアウトオブバンド接続を使用する必要があります。

インテル® AMT がエンドポイントにセットアップされると、インテル® EMA は次のいずれかのアプローチを使用してインテル® AMT とやり取りできるようになります。

- **TLS Relay（TLS リレー）：**このアプローチでは、その他のインテル® EMA エージェントがインテル® AMT コマンドを対象のエンドポイント上の対象のインテル® AMT にリレーします。エージェントがリレーとして動作するには、それらのエージェントが同じサブネットに属しており、同じエンドポイント・グループに登録されている必要があります。エンドポイントが再起動すると、そのエージェントは同じグループ/サブネット内のその他のインテル® EMA エージェントにブロードキャストし、TLS リレーのために近くのエージェントとの接続を確立します。インテル® EMA エージェントが対象のインテル® AMT と通信するときはインテル® AMT TLS ポートが使用されます。この方法が「TLS リレー」と呼ばれるのはそのためです。
- **インテル® AMT CIRA（Client Initiated Remote Access）：**このアプローチでは、エンドポイント・システムのインテル® AMT は、ポート 8080 の TCP TLS 接続を介してインテル® EMA サーバーに接続します（インバンド インテル® EMA エージェントも、ポート 8080 の TCP TLS 接続を介してインテル® EMA サーバーに接続することに注意してください）。インテル® AMT CIRA は独自の暗号化トンネルを作成するため、TLS は必要ありません。CIRA が有効化されたとき、またはエンドポイント・システムが再起動されたとき、インテル® AMT は接続を複数回試行します。その試行がすべて失敗した場合、インテル® AMT はエンドポイント・システムが次に再起動されるまで接続試行を再開しません。ただし、接続が確立された後は、エンドポイントが常にサーバーに接続できるよう、CIRA によってインテル® EMA サーバーとエンドポイント間の通信が維持されます。

  インテル® AMT CIRA は、インテル® AMT の機能である「環境検出」を利用します。エンドポイント・システムのネットワーク・ドメインが構成済みの CIRA ドメインと一致した場合、インテル® AMT は CIRA 接続を開始しません。その場合は、インテル® EMA サーバーは TLS リレーと類似した通信アプローチを使用します。

  インテル® AMT が常に CIRA トンネルを開くように強制するには、インテル® AMT プロファイルを作成するときに、General（全般）の設定の CIRA intranet suffix（CIRA イントラネット・サフィックス）フィールドにフェイクのドメイン・サフィックスを入力します。このフェイクのドメイン・サフィックスは、他人に推測されない複雑なものにする必要があります。これにより、CIRA 接続とローカル管理ポートの開放を防止するために使用します。セクション 3.2.1 を参照してください。

1.2.7 インテル® EMA によるインテル® AMT のプロビジョニング/セットアップ・フロー

このセクションでは、管理対象のエンドポイント・システムに対してインテル® AMT の自動セットアップを有効化するとき（セクション 3.5）、またはインテル® AMT のオンデマンド・セットアップを手作業で実行するとき（セクション 6.1）に、プログラムによって実行される内容について説明します。

注記：インテル® AMT のセットアップのことを「プロビジョニング」と呼ぶこともあります。

インテル® EMA は、**ホスト・ベース・コンフィグレーション（HBC）**を使用して、インテル® AMT をエンドポイントにプロビジョニングします。HBC は、エンドポイントのオペレーティング・システムを介してインバンドで実行されます。PKI（Public Key Infrastructure）証明書をアップロードしていない場合、エンドポイントのインテル® AMT は、インテル® EMA によってクライアント・コントロール・モード（CCM）に設定されます。CCM の使用には、インテル® EMA の一部のリモート接続機能を実行するには各エンドポイントにおいてユーザーの同意が必要になるなどの制約があります。PKI 証明書をアップロードすると、エンドポイントのインテル® AMT は、インテル® EMA によって管理者コントロール・モード（ACM）に設定されます。LAN レスのエンドポイントには、インテル® MEBX の手作業による更新が必要です（下記のラウンド 1 を参照）。PKI 証明書と ACM によってセキュリティーが強化されるため、インテル® EMA がエンドポイントのインテル® AMT に接続してユーザーの同意なしで遠隔操作できるようになります。インテル® AMT プロファイルと、そのための PKI 証明書のアップロードについてはセクション 3.2 で説明します。

注記：ホスト・ベース・コンフィグレーション、クライアント・コントロール・モード、管理者コントロール・モードの詳細については、インテル® AMT の資料（https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm）を参照してください。

プロビジョニング/セットアップは、次の 2 つのラウンドに分けられます。

1. **ラウンド 1：**エンドポイントをクライアント・コントロール・モードに設定します。PKI 証明書がアップロード済みで、インテル® AMT の自動セットアップでセットアップ方法として TLS-PKI が選択されている場合、インテル® EMA によって、エンドポイントがクライアント・コントロール・モードから管理者コントロール・モードに変更されます。

   注記：LAN レスのエンドポイントでは、インテル® EMA がエンドポイントをクライアント・コントロール・モードから管理者コントロール・モードに変更するには、先にエンドポイントのインテル® MEBX を手動で更新して、アップロードされた PKI 証明書の DNS サフィックスを追加する必要があります。それを行わない場合、エンドポイントは CCM のままになります。詳細については、セクション 3.3.1 を参照してください。

2. **ラウンド 2:**ラウンド 1 が完了した後(インテル® AMT が CCM か ACM のいずれかで正常にプロビジョニングされた後)、インテル® EMA はインテル® AMT のその他の設定(電力ポリシー、KVM インターフェイス、CIRA など)をします。

ラウンド 1 が失敗した場合、インテル® EMA はエンドポイントのプロビジョニングを解除してから、3 分おきにプロビジョニング/セットアップを自動的に再試行します。再試行は、プロビジョニング/セットアップが成功するか、1 時間経過するまで続けられます。

ラウンド 2 が失敗した場合、インテル® EMA はエンドポイントのプロビジョニングを解除することなく、ラウンド 2 のセットアップを 3 分おきに再試行します。再試行は、プロビジョニング/セットアップが成功するか、1 時間経過するまで続けられます。

注記：インテル® AMT のプロビジョニング解除 (非アクティブ化) については、プロビジョニング解除に失敗した場合、インテル® EMA は自動的に 3 分おきに再試行します。再試行は、プロビジョニング/セットアップが成功するか、1 時間経過するまで続けられます。すべてのケース(ラウンド 1、ラウンド 2、プロビジョニング解除)で、インテル® EMA がエンドポイントから切断されると、エンドポイントに再接続された後にプロセスの再試行が実行されます。

1.2.7.1 プロビジョニング解除

エンドポイントがインテル® AMT クライアント･コントロール･モードの場合、インテル® AMT を出荷時のデフォルト設定にリセットするため、インテル® EMA はインテル® EMA エージェントを使って、インテル® MEI ドライバーを介して CFG_Unprovision コマンドを発行しようとします。

それに失敗した場合、またはエンドポイントがインテル® AMT 管理者コントロール･モードの場合、インテル® EMA は WSMAN リクエスト AMT_SetupAndConfigurationService\Unprovision を送信してインテル® AMT を出荷時のデフォルト設定にリセットします。

また、このエンドポイント･グループが 802.1X セットアップを伴うインテル® AMT プロファイルを使用している場合、インテル® EMA は 802.1X 構成用に作成された Active Directory* オブジェクトのクリア/削除も試みます。

注記：

- インテル® EMA インスタンスがプロビジョニングを解除できるのは、そのインスタンスがプロビジョニングしたエンドポイントのみです。別のインテル® EMA インスタンスによってプロビジョニングされたエンドポイントのプロビジョニングを解除することはできません。分散サーバー環境では、その分散サーバー環境内のすべてのサーバーが同一のインテル® EMA インスタンスとみなされます。
- インテル® EMA はインテル® AMT の完全なプロビジョニング解除を実行し、インテル® AMT 設定からカスタム・ルート証明書ハッシュと PKI DNS サフィックスをすべて削除します。そのため、リモート･ネットワーク上のシステムのプロビジョニングを解除した後、管理者コントロール・モードを使用してそのシステムを再プロビジョニングするには、物理的にそのシステムを触る必要がある可能性があります。

1.2.8 USB リダイレクト

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。この機能は、起動可能なイメージファイルをマウントし、マウントしたイメージファイルに対して管理対象エンドポイントを再起動したり、マウントされたイメージの内容を KVM を介して管理対象エンドポイントのコンソールから参照したりするために使用できます (KVM の通信のため、イメージに USB キーボードおよびマウス用ドライバーを含める必要があります)。イメージファイルがマウントされたら、マウントしたイメージに対してエンドポイントを再起動します。管理対象エンドポイントにイメージをマウントする方法については、セクション 6.4.6 を参照してください。マウントされたイメージに対して再起動する方法については、セクション 6.4.6.2 を参照してください。

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。CIRA の詳細については、セクション 1.2.6 を参照してください。管理機能サーバーの設定については、セクション 9.3 を参照してください。

インテル® EMA の UI の左側のナビゲーション・バーでアクセスできる Storage (ストレージ) ページを使用すると、後でエンドポイントにマウントするためのイメージファイル (.iso または .img) をアップロードおよび保存できます。詳細については、セクション 7 を参照してください。

以下の表は、エンドポイントで USBR over CIRA を使用するためのインテル® AMT バージョンの必要最低要件を示しています。

インテル® AMT バージョン	**ビルド番号**
インテル® AMT 11.8	すべて
インテル® AMT 12	12.0.70.1607 以降
インテル® AMT 14	14.0.45.1341 以降
インテル® AMT 15	すべて

1.2.9 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。

2　インテル® EMA へのログイン

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（不明な場合、インテル® EMA のグローバル管理者に問い合わせます）。分散サーバー型のインストールでは、Ajax およびウェブサーバーのロードバランサーの URL になります。
2. ログインページで、グローバル管理者によって割り振られたテナント管理者ユーザーのユーザー名（メールアドレス）とパスワードを入力します。その他のユーザーの場合、テナント管理者またはアカウント・マネージャーによって割り振られたユーザー名とパスワードを入力します。

注記：

- インテル® EMA ウェブサイト・ユーザー・インターフェイス（UI）は Cookie を使用します。ブラウザーの Cookie を無効化すると、インテル® EMA ウェブサイト UI は動作しません。
- インテル® EMA のインストール方法により、自動的に Overview（概要）ページが表示される場合と、その前にインテル® EMA の資格情報が要求される場合があります。
- インテル® EMA にログインし、ブラウザーで新しいタブを開くと、ログインページが表示されます。これは Server Settings（サーバー設定）ページでインテル® EMA のウェブサーバーの設定を sessionStorage から localStorage に変更することで変更可能ですが（セクション 9「付録 - コンポーネント・サーバーの設定変更」（45 ページ）を参照）、ブラウザーによってはタブ間でセッション Cookie が共有されないことに注意してください。
- （インテル® EMA に別のタブですでにログインしているときに）新しいタブで別のユーザーとしてログインすることはサポートされていません。新しいタブでログインは完了できますが、元のタブにエラーが表示されます。
- 間違ったパスワードを何回も入力すると、アカウントが 24 時間ロックされます。その場合、グローバル管理者に連絡してください。

2.1　Overview（概要）ページ

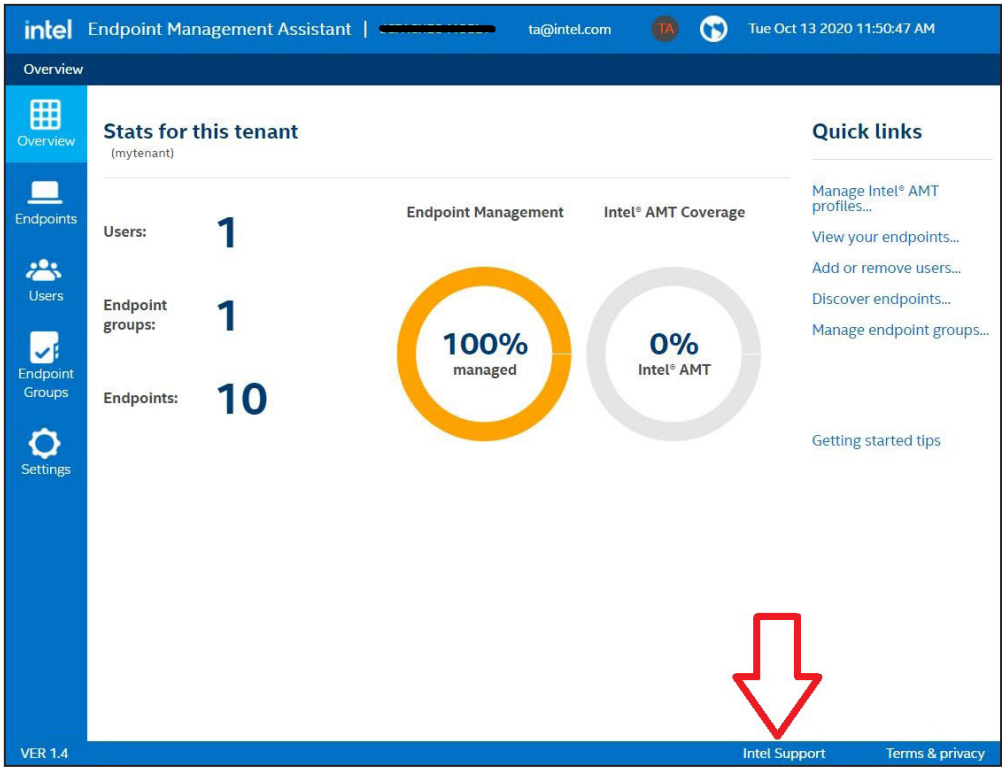
インテル® EMA にログインすると、Overview（概要）ページが表示されます。このページは、ログイン中のユーザーロールによって異なります。下の図は、テナント管理者の Overview（概要）ページを示しています。

注記：初めてログインするときは、Getting Started（はじめに）ページが表示されます。このページは最初のエンドポイント・グループを作成するまで表示されます。

右側の Quick Links（クイックリンク）から、以降のセクションで説明するテナント管理者タスクのほとんどに簡単にアクセスできます。このページに表示された統計情報の計算方法については、セクション 11 を参照してください。

サポートが必要な場合、ページ下部の **Intel Support（インテルサポート）**リンクをクリックします。

図 3：テナント管理者の Overview（概要）ページ



3　テナントのセットアップ

本セクションでは、インテル® EMA サーバーに特定のテナントをセットアップおよび構成する方法について説明します。特に断りがない限り、本セクションのタスクはテナント管理者ユーザーによって実行されます。その他のユーザーが実行できるアクションは、各アクションのサブセクションの冒頭に記載されています。

注記：組織によっては、このセクションのすべてのタスクが必要とは限りません。さらに、新規ユーザーの追加、新規エンドポイント・グループの追加など、タスクの多くは組織の拡大と変化に合わせてたびたび実行される可能性があります。

テナントをセットアップする基本的なプロセスを以下に述べます。各ステップは、以降のサブセクションで詳しく説明します。

1. **ネットワーク・プロファイルの作成 -** 本番環境で Wi-Fi* または 802.1X を使用する予定の場合、インテル® AMT プロファイル作成時に選択するだけで、これらのネットワーク・テクノロジー用のプロファイルを簡単に構成できます。これらのネットワーク・プロファイルは、インテル® AMT プロファイル作成フローの一部として作成することもできますが、複数のインテル® AMT プロファイルでネットワーク・プロファイルを再利用する予定なら、ネットワーク・プロファイルを事前に作成しておく方が簡単です。**ロール：**テナント管理者。実際の環境で Wi-Fi* または 802.1X を使用しない場合は、このステップ（セクション 3.1）は省略できます。
2. **インテル® AMT プロファイルの作成 -** アウトオブバンド（OOB）機能（エンドポイントのオペレーティング・システムが利用できない場合にも動作するエンドポイント管理機能）を使用してエンドポイントを管理する予定がある場合、エンドポイントにインテル® AMT を構成する必要があります。インテル® AMT は、エンドポイント一つひとつに対して手作業で構成することも、インテル® EMA によってすべてのエンドポイント上に自動的に構成することもできます。インテル® EMA がインテル® AMT を自動的にセットアップできるようにするためには、インテル® EMA が使用するインテル® AMT プロファイルを少なくとも 1 つ構成する必要があります。**ロール：**テナント管理者、エンドポイント・グループ作成者。インテル® AMT の自動セットアップを使用しない場合、インテル® AMT プロファイルを構成する必要はなく、このステップ（セクション 3.2）は省略できます。
3. **インテル® AMT PKI 証明書のアップロード -** インテル® AMT PKI 証明書は PKI プロビジョニングに使用され、管理者コントロール・モードでインテル® AMT の自動セットアップを有効化する予定の場合に必要になります。インテル® AMT PKI 証明書をお持ちでない場合、インテル® AMT の自動セットアップをクライアント・コントロール・モードで有効化する場合、このステップ（セクション 3.3）は省略します。**ロール：**テナント管理者。
4. **エンドポイント・グループの作成 -** エンドポイント・グループは、組織構造に基づくエンドポイントの論理的なグループ分けです。例えば、経理部のエンドポイント・グループ、技術部のエンドポイント・グループなどを作成できます。これにより、グループごとに異なる IT ポリシーを設定できます。このプロセスの残りのステップをすべて実施してエンドポイント・グループを完全に構成してから、必要に応じてこのステップに戻り、追加のエンドポイント・グループを作成して構成することをお勧めします。**ロール：**テナント管理者、エンドポイント・グループ作成者。
5. **インテル® AMT の自動セットアップの有効化 -** 上述のとおり、インテル® AMT の自動セットアップとは、インテル® EMA がエンドポイントにインテル® AMT を自動的にセットアップできるようにする機能です。インテル® EMA の OOB エンドポイント管理機能を使用する予定の場合、エンドポイントにインテル® AMT がセットアップされている必要があります。ACM モードでインテル® AMT の自動セットアップを有効化するには、インテル® AMT PKI 証明書とインテル® AMT プロファイルが必要になります。**ロール：**テナント管理者と実行権限を持つユーザー。エンドポイントでインテル® AMT の自動セットアップを有効化しない場合、このステップ（セクション 3.5）は省略できます。
6. **各エンドポイント・グループに対するインテル® EMA エージェント・ファイルの作成 -** OOB 機能を使用するかどうかにかかわらず、インテル® EMA でエンドポイントを管理するには、エンドポイントにインテル® EMA エージェントをインストールして構成する必要があります。このステップでは、エンドポイント・グループの構成（ポリシー、インテル® AMT プロファイルなど）に基づいてエージェント・ファイルのペアを作成します。**ロール：**テナント管理者、グループの関連付けに基づいて実行権限を持つユーザー。
7. **インテル® EMA エージェント・ファイルの管理対象エンドポイントへのデプロイ -** インテル® EMA エージェント・ファイルの作成が完了したら、それをエンドポイント・システムにデプロイする必要があります。このセクションでは、コマンドラインまたは GUI インストーラーを使用して、エージェント・ファイルを特定のエンドポイント・システム上に手作業で直接インストールする方法を説明します。コマンドラインの手順は、一括導入ツールを活用して自動デプロイメント・パッケージを作成するために利用できます。**ロール：**管理対象のエンドポイント・システムに対する管理権限を持つすべてのユーザー。

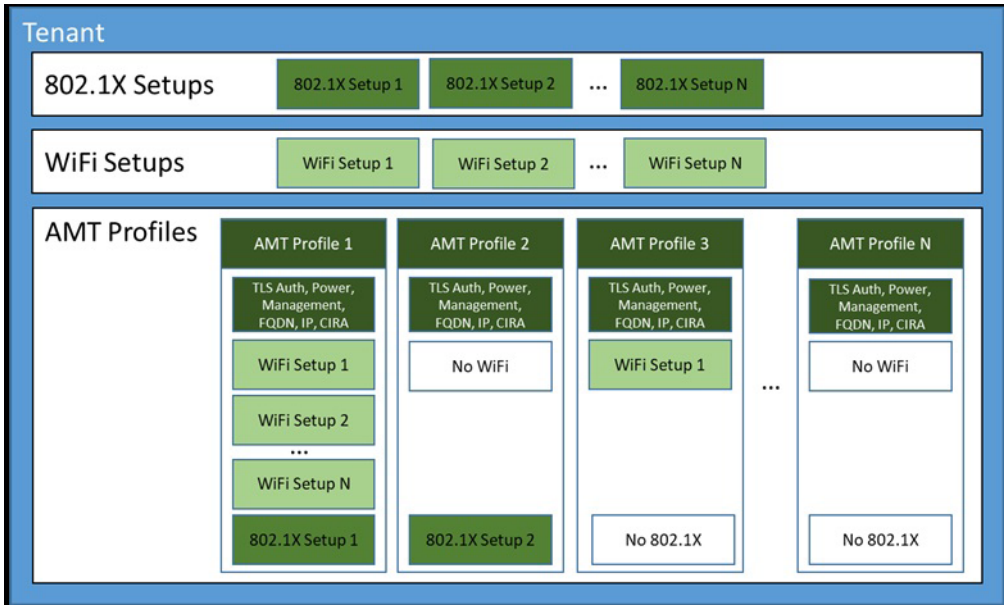
8. **必要に応じた追加のユーザーとユーザーグループの作成 -** 組織の規模や複雑度に応じて、エンドポイントの管理に役立つ追加のユーザーを作成する場合もあります (ユーザーロールの詳細については、セクション 1.2.2 を参照)。これらのユーザーは、必要に応じてユーザーグループにグループ化できます。**ロール:**テナント管理者、アカウント・マネージャー。

3.1 ネットワーク・プロファイルの作成

ロール：テナント管理者

ネットワーク・プロファイルは、インテル® AMT プロファイル作成時に同時に作成することも可能ですが、事前に作成しておく方が簡単です。そうすることで、インテル® AMT プロファイル作成時には、既存のネットワーク・プロファイルを選択するだけで済みます。以下の図は、ネットワーク・プロファイル (「Setup」) とインテル® AMT プロファイルの関係を示しています。

図 4：ネットワーク・プロファイルとインテル® AMT プロファイル



実際の環境で Wi-Fi* または 802.1X を使用しない場合、このセクションは省略できます。

3.1.1 Wi-Fi* プロファイルの新規作成

Wi-Fi* プロファイルを新規作成する手順は以下のとおりです。

左側のナビゲーション・バーで **Endpoint Groups (エンドポイント・グループ)** を選択し、**Intel® AMT Profiles (インテル® AMT プロファイル) > Manage WiFi Profiles (WiFi プロファイルの管理)** を選択して **New Profile (新規プロファイル)** をクリックします。新規 Wi-Fi* プロファイルは、インテル® AMT プロファイルの作成ワークフロー (セクション 3.2) の一部として作成することもできます。

Define the WiFi Profile (WiFi プロファイルの定義) ダイアログで以下の操作を行います。

1. **WiFi profile name (WiFi プロファイル名)** フィールドに Wi-Fi* プロファイルの名前を入力します。セットアップ名は最大 32 文字で、(/ \ < > : ; * | ? ") の文字を含めることはできません。
2. **SSID** フィールドに特定の Wi-Fi*i ネットワークを識別する SSID (Service Set Identifier) を入力します (最大 32 文字)。**SSID** を空欄にした場合、インテル® AMT はこの Wi-Fi* プロファイルに定義された暗号化を使用するすべての Wi-Fi* ネットワークに接続しようとします。
3. **Security type (セキュリティー・タイプ)** ドロップダウン・リストで次のいずれかを選択します。
    - **WPAPSK：** Wi-Fi* 保護アクセス鍵管理プロトコルを使用します。フィールドに **Security key (セキュリティー・キー)** (パスフレーズ) を入力します (8 ~ 63 文字の印字可能な ASCII 文字を含める必要があります)。

- **WPA2PSK:** 堅牢なセキュリティー・ネットワーク (WPA2) 鍵管理プロトコルを使用します。フィールドに **Security key (セキュリティー・キー)** (パスフレーズ) を入力します (8 ~ 63 文字の印字可能な ASCII 文字を含める必要があります)。
- **WPAIEEE802_1 :** Wi-Fi* 保護アクセス鍵管理プロトコルを使用します。ドロップダウン・リストから既存の **802.1X setup (802.1X セットアップ)** を選択します。
- **WPA2IEEE802_1 :** 堅牢なセキュリティー・ネットワーク (WPA2) 鍵管理プロトコルを使用します。ドロップダウン・リストから既存の **802.1X setup (802.1X セットアップ)** を選択します。

4. Encryption (暗号化) ドロップダウン・リストで次のいずれかを選択します。
   - **Temporal Key Integrity Protocol (TKIP) (一時鍵インテグリティー・プロトコル)**
   - **Counter mode CBC MAC Protocol (CCMP) (カウンターモード CBC MAC プロトコル)**

新しいセットアップを作成すると、その優先順位は既存のセットアップの最高値よりも大きい値になります。

3.1.1.1 Wi-Fi* プロファイルの編集と削除

1. 左側のナビゲーション・バーで **Endpoint Groups (エンドポイント・グループ)** を選択し、**Intel® AMT Profiles (インテル® AMT プロファイル) > Manage WiFi Profiles (WiFi プロファイルの管理)** を選択します。
2. Wi-Fi* プロファイルを編集または削除するには、そのプロファイルの横の省略記号 (**...**) をクリックします。インテル® AMT プロファイルに関連付けられたネットワーク・プロファイルは削除できません。

Wi-Fi* プロファイルは優先順位に従ってリストで並び替えられます。優先順位番号が最も小さいものがリストの一番上、最も大きいものがリストの一番下に表示されます。

プロファイルの優先順位を変更するには、青色の上または下向き矢印をクリックして Wi-Fi* プロファイルを上下に移動します。

3.1.2 新規 802.1x プロファイルの作成

IEEE802.1x ネットワーク・プロトコルは LAN に接続しようとするデバイスに対して認証メカニズムを提供し、ポイント・ツー・ポイント接続を確立するか、認証に失敗した場合は接続を許可しません。IEEE802.1x はほとんどの無線 802.11 アクセスポイントに使用されており、拡張認証プロトコル (EAP) をベースとしています。定義した 802.1x プロファイルを無線および有線接続のプロファイルに含めることができます (「EAP (GTC)」プロトコルは、802.1x 有線プロファイルのみで使用できます)。

802.1X ネットワーク・プロトコルを使用する予定がない場合、このステップは省略できます。

注記 :

- 802.1x プロファイルには、Active Directory* とエンタープライズ・ルート CA との統合が必要です。
- 必ず組織のネットワーク認証要件を把握してください。それらの要件が満たされない場合、インテル® AMT が正しく動作しないことがあります。例えば、IT 組織によっては、AD コンピューター・オブジェクトと有効な 802.1x 証明書以外の 802.1x アクセスポリシー (許可されるネットワーク・ハードウェア・タイプのパスリストなど) が設定されている場合があります。

802.1X プロファイルを新規作成する手順は以下のとおりです。

左側のナビゲーション・バーで **Endpoint Groups (エンドポイント・グループ)** を選択し、**Intel® AMT Profiles (インテル® AMT プロファイル) > Manage 802.1x Profiles (802.1x プロファイルの管理)** を選択して **New Profile (新規プロファイル)** をクリックします。新規 802.1X プロファイルは、インテル® AMT プロファイルの作成ワークフロー (セクション 3.2) の一部として作成することもできます。

Definition (定義) ダイアログで次の操作を行います。

1. (オプション) **Enable (有効化)** チェックボックスをオフにし、有線接続でこのセットアップを無効にします。
2. この 802.1x プロファイルの **Name (名前)** を入力します。名前は最大 32 文字で、(/ \ < > : ; * | ? ") の文字を含めることはできません。
3. **Protocol (プロトコル)** フィールドは変更せずそのままにします。現在サポートされているのは EAP_TLS のみです。

4. **Active Directory*** に次の情報を入力します。

    - **Active Directory Organizational Unit（ADOU）（Active Directory 組織ユニット）:** AD でオブジェクトが保存される場所です。ADOU は、“OU=Out of Band Management,DC=vprodemo,DC=com” のような識別名フォーマットで入力する必要があります。
    - **Security Groups（セキュリティー・グループ）:** インテル® AMT エンドポイント用に作成された AD オブジェクトは、デフォルトでは「Domain Computers」という名前の AD セキュリティー・グループに自動的に追加されます。オブジェクトを追加する先のセキュリティー・グループを追加で定義できます。例えば、一部の RADIUS サーバーでは、オブジェクトが特定のセキュリティー・グループに属することが要求されます。新しい行を使用して、次のような識別名フォーマットで新規エントリーを入力します。"CN=vPro8021XComputers,DC=VPRODEMO,DC=COM"

5. **Client Authentication（クライアント認証）**の **How to create the certificate（証明書の作成方法）**で、インテル® AMT エンドポイントにインストールする証明書のソースを選択します。**From Microsoft CA（Microsoft CA から）**を推奨します。インテル® EMA サーバーはその Microsoft CA にアクセスできる必要があります。

    - **Certificate Authority（証明書認証局）**ドロップダウン・リストで、インテル® EMA が証明書をリクエストするのに使用する、RADIUS サーバーが認証可能なエンタープライズ CA を選択します。
    - **Server Certificate Template（サーバー証明書テンプレート）**ドロップダウン・リストで、クライアント証明書の作成に使用されるテンプレートを選択します。証明書認証局サーバーで有効なテンプレートを作成する方法については、インテル® AMT の資料を参照してください。
    - 生成される証明書のサブジェクト名に含まれる **Common Names（コモンネーム）** を定義します。**Default（デフォルト）**では、Common Name for Subject Name（サブジェクト名のコモンネーム）は User Principal Name（ユーザー・プリンシパル名）で、Common Names for Subject Alternative Name（サブジェクトの別名のコモンネーム）は User Principal Name（ユーザー・プリンシパル名）、DNS FQDN、ホスト名、SAM アカウント名、インテル® AMT を表す新しい AD オブジェクトの UUID、識別名です。**User Defined（ユーザー定義）**では、Subject Alternative Name（サブジェクトの別名）に入力する Common Names（コモンネーム）を選択し、Subject Name（サブジェクト名）を選択します。
    - **From database（データベースから）:** インテル® EMA データベースに事前に読み込まれた証明書を使用できます。証明書をアップロードする方法についてはセクション 3.3 を参照してください。証明書を特定するには、ターゲット証明書のサムプリント値を入力します。
    - **No certificate（証明書なし）:** このオプションは、選択したプロトコルでクライアント認証がオプションである場合のみ表示されます。
    - **Roaming Identity（ローミング・アイデンティティー）** は、ID 値によってユーザー アカウントを RADIUS サーバーに接続する場合に有効にします。この値は、802.1X プロトコル交換において、クリアテキストとして送信された 802.1X「アイデンティティー・リクエスト」メッセージへの応答として Radius AAA サーバーに提示されます。この文字列のフォーマットは AAA サーバーによって決まります。AAA サーバーがサポートするフォーマットには、< ドメイン >\< ユーザー名 >、< ユーザー名 >@< ドメイン > があります。この機能は、選択されたターゲットプロトコルによってサポートされている場合に有効になります。

6. **Server Authentication – Trusted Root Certificate（サーバー認証 – 信頼できるルート証明書）** の **How to get the certificate（証明書を取得する方法）** で、インテル® AMT エンドポイントにインストールする証明書のソースを選択します。**From Microsoft CA（Microsoft CA から）**を推奨します。インテル® EMA サーバーはその Microsoft* CA にアクセスできる必要があります。

    - **Certificate Authority（証明書認証局）**ドロップダウン・リストから、インテル® EMA が使用するエンタープライズ・ルート CA を選択します。
    - **From the database（データベースから）:** インテル® EMA データベースに事前に読み込まれた証明書を使用できます。証明書をアップロードする方法についてはセクション 3.3 を参照してください。証明書を特定するには、ターゲット証明書のサムプリント値を入力します。
    - **No certificate（証明書なし）:** このオプションは、選択したプロトコルでサーバー認証がオプションである場合のみ表示されます。

7. **Advanced（高度）**の **Available in S0（S0 で利用可能）**オプションはデフォルトでオンになっています。これにより、エンドポイントが S0 状態だが、サーバーへの認証に失敗する場合に、インテル® AMT がインテル® EMA サーバーへの認証を処理できます。認証が正常に行われるまで、インテル® EMA サーバーはエンドポイントにアクセスできないことに注意してください。
    - このプロファイルでインテル® AMT によるインテル® EMA サーバーへの認証を実行しない場合のみ、このオプションを無効（チェックボックスをオフ）にします。
    - **PXE Timeout（タイムアウト）**では、インテル® AMT がタイムアウトまでに認証済みの 802.1X セッションを保持する時間の長さを設定します（範囲は 0 ~ 86400 秒、すなわち 1 日）。PXE ブート実行中、インテル® AMT はここで設定された時間の間 802.1X ネゴシエーションを管理します。タイムアウト後、ネゴシエーションのコントロールはエンドポイントに渡されます。この設定は有線接続に適用されます。
8. **Radius Server Validation（Radius サーバーの検証）**で、次のいずれかを選択し、RADIUS AAA サーバーによって提供された証明書のサブジェクト名をインテル® AMT が検証する方法を指定します。
    - Do not verify（検証しない）
    - Verify using FQDN（FQDN を使用して検証）
    - Verify using Domain Suffix（ドメイン・サフィックスを使用して検証）

3.1.2.1 802.1X プロファイルの編集と削除

1. 左側のナビゲーション・バーで **Endpoint Groups（エンドポイント・グループ）**を選択し、**Intel® AMT Profiles（インテル® AMT プロファイル）> Manage 802.1x Profiles（802.1x プロファイルの管理）**を選択します。
2. プロファイルを編集または削除するには、そのプロファイルの横の省略記号（**...**）をクリックします。インテル® AMT プロファイルに関連付けられたネットワーク・プロファイルは削除できません。

3.2 インテル® AMT プロファイルの作成

ロール：テナント管理者、エンドポイント・グループ作成者

アウトオブバンド（OOB）機能（エンドポイントのオペレーティング・システムが利用できない場合にも動作するエンドポイント管理機能）を使用してエンドポイントを管理する予定がある場合、エンドポイントにインテル® AMT を構成する必要があります。インテル® AMT は、エンドポイント一つひとつに対して手作業で構成することも、インテル® EMA によってすべてのエンドポイント上に自動的に構成することもできます。インテル® EMA がインテル® AMT を自動的にセットアップできるようにするためには、インテル® EMA が使用するインテル® AMT プロファイルを少なくとも 1 つ構成する必要があります。

インテル® AMT の自動セットアップを使用しない場合、インテル® AMT プロファイルを構成する必要はなく、このステップは省略できます。

インテル® AMT プロファイルを新規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・バーで **Endpoint Groups（エンドポイント・グループ）**を選択し、**Intel® AMT Profiles（インテル® AMT プロファイル）**タブをクリックします。
2. **New Intel® AMT Profile（新規インテル® AMT プロファイル）**をクリックし、新しいインテル® AMT プロファイルの各セクション（General（一般）、Power States（電源状態）など）でフィールドに入力したら、**Save（保存）**をクリックします。

3.2.1 General（全般）の設定

Profile Name（プロファイル名）と Profile Description（プロファイルの説明）を入力した後、インテル® EMA サーバーがエンドポイントのインテル® AMT と通信する方法（CIRA または TLS リレーか）を指定します。CIRA と TLS の詳細については、セクション 1.2.6 を参照してください。

CIRA を指定する場合、次のことに注意してください。

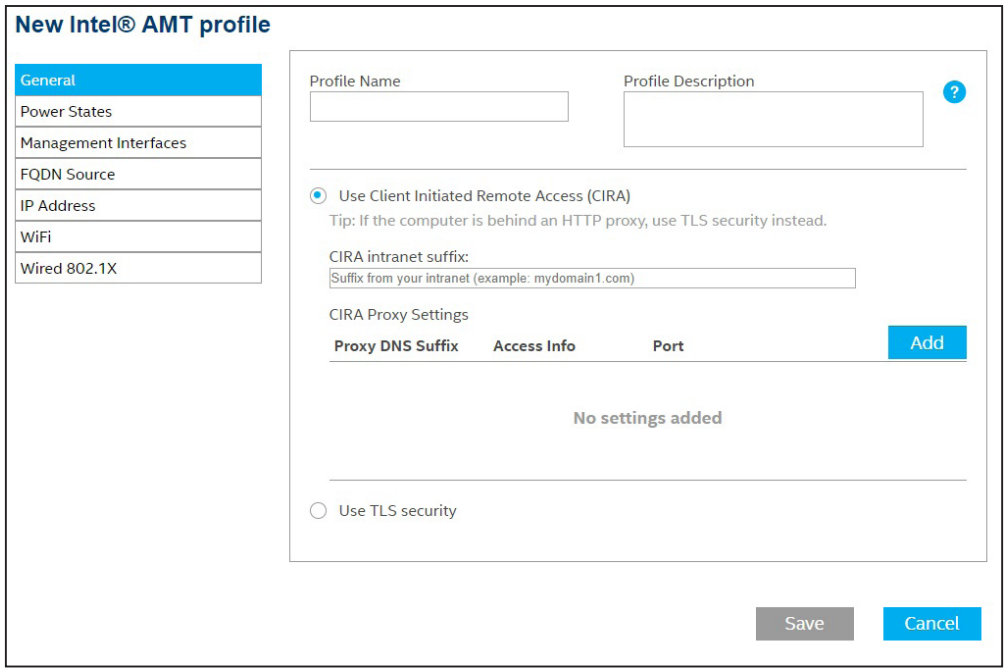
- インテル® EMA は CIRA 通信に自己署名証明書を使用します。

- イントラネット・サフィックスを定義する必要があります。インテル® AMT エンドポイントがここで定義されたイントラネット・サフィックスに一致するネットワークにある場合、インテル® AMT は CIRA を停止して TLS リレーを使用します。

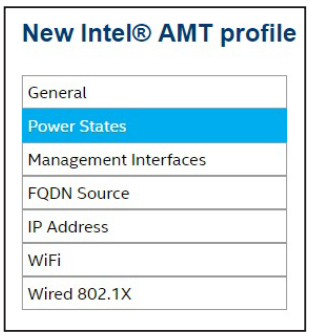
  注記：インテル® AMT が常に CIRA トンネルを開くように強制するには、インテル® AMT プロファイルを作成するときに、General（全般）の設定の CIRA intranet suffix（CIRA イントラネット・サフィックス）フィールドにフェイクのドメイン・サフィックスを入力します。このフェイクのドメイン・サフィックスは、他人に推測されない複雑なものにする必要があります。これにより、CIRA 接続とローカル管理ポートの開放を防止するために使用します。インテル® EMA の旧バージョンで作成されたプロファイルを表示すると、自動付与されたドメイン・サフィックスが表示されます。

- インテル® AMT 12 以降のエンドポイントには、インテル® AMT がインテル® EMA サーバーに接続するために使用するプロキシーを追加するオプションがあります。

図 5：プロファイルの作成 – General（全般）の設定

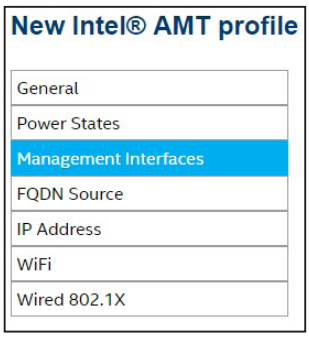


3.2.2 Power State（電力状態）の設定



デフォルトであり、推奨されるオプションは Any time the system is connected to power through all system power state (S0 – S5)（システムが任意の電力状態（S0 ~ S5）で電源に接続されているときはいつでも）です。

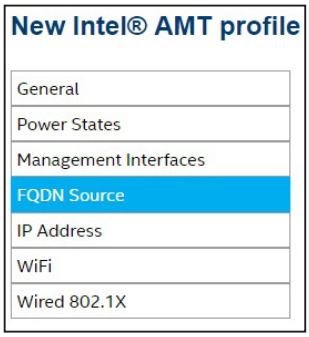
3.2.3 Management Interface（管理インターフェイス）の設定



エンドポイントで開くインターフェイスを選択します。

- **KVM redirection（KVM リダイレクト）–** キーボード/ビデオ/マウス（KVM）リダイレクト・インターフェイスを開きます。これにより、手元のキーボード、ビデオ、マウスがエンドポイント・システムに物理的に接続されているかのようにエンドポイントを操作できます。
- **Web-based user interface（ウェブベースのユーザー・インターフェイス）–** ブラウザーベースのインターフェイスを使用してインテル® AMT システムを保守管理できるようにします。
- **Serial over LAN –** キーストロークや文字表示データを TCP/IP ストリームにカプセル化し、インテル® AMT システムをリモートで管理できるようにします。
- **IDE/USB redirection（IDE/USB リダイレクト）–** IDER は、インテル® AMT システム上のドライブをリモートのイメージまたはドライブにマッピングできるようにします。この機能は、一般的に、インテル® AMT システムを代替ドライブから再起動するために使用されます。USBR は、インテル® AMT システム上のドライブをリモートのイメージまたはドライブにマッピングできるようにします。IDER と異なるのは、IDER がリモートのフロッピーまたは CD ドライブをホストマシンに内蔵されているかのように表示するのに対し、USBR はリモートドライブを USB ポートで接続されているかのように表示する点です。

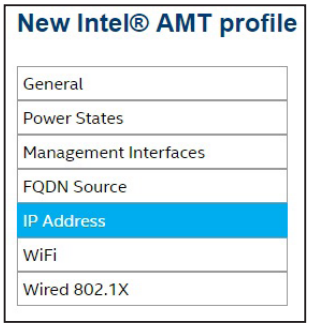
3.2.4 FQDN の設定



ホスト名とドメイン・サフィックスをインテル® AMT 上で設定する方法を選択します。

- **Shared with host OS（OS と共有）：** ホスト名は OS から取得されたホスト名になります。ドメイン・サフィックスは空欄にします。
- **On-board connection-specific DNS（オンボードのコネクションごとの DNS）：** ホスト名は OS から取得されたホスト名になります。ドメイン・サフィックスは、オンボード有線 LAN インターフェイス上の「Connection-specific DNS suffix」になります。
- **DNS lookup（DNS ルックアップ）：** オンボード有線 LAN インターフェイスの IP アドレスに対する DNS ルックアップで返される値を使用します。このオプションには、DNS と逆引き参照ゾーンが正しく構成されていることが必要です。
- **Primary DNS（プライマリー DNS）：** ドメイン・サフィックスの両方のホスト名（プライマリー DNS サフィックス）が OS から取得されます。

3.2.5 IP Address（IP アドレス）の設定

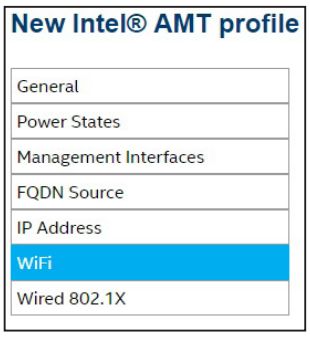


インテル® AMT がエンドポイント（ホスト）から IP アドレスを取得する方法を選択します。

- **From the DHCP server（DHCP サーバーから）-** ホストの IP アドレスが DHCP から自動的に割り当てられている場合に使用します。
- **Use a static IP address from host（ホストからの静的 IP アドレスを使用）-** ホストに IP アドレスが静的に割り当てられている場合に使用します。

注記：静的 IP アドレスで構成されたエンドポイントでは、インテル® AMT CIRA の環境検出は動作しません。

3.2.6 Wi-Fi* の設定



次のオプションから選択します。

- **Allow WiFi connection without a WiFi profile(WiFi プロファイルなしの WiFi 接続を許可)** – Wi-Fi* セットアップなしで Wi-Fi* 接続を許可する場合に選択します(ホストの Wi-Fi* 設定を使用)。
- **Use the selected WiFi profiles (選択した WiFi プロファイルを使用)** – Wi-Fi* セットアップを定義する場合に選択します。構成可能な Wi-Fi* セットアップの総数は、インテル® AMT のバージョンによって異なります。詳細については、セクション 3.1.1 を参照してください。

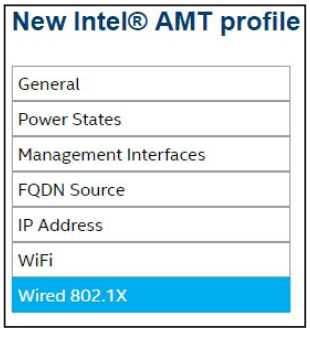
インテル® AMT には無線プロファイル同期機能があります。この機能を使用して、オペレーティング・システムの無線プロファイルをインテル® AMT エンドポイントで定義された Wi-Fi* セットアップに同期できます。**Synchronize with host platform WiFi profiles(ホスト・プラットフォーム WiFi プロファイルと同期)** チェックボックスがオンのとき、この機能のサポートが有効化されています。この機能を使用してプロファイルを同期するには、オペレーティング・システムにインテル® PROSet/Wireless ソフトウェアがインストールされている必要があります。詳細については、インテル® PROSet/Wireless ソフトウェアの資料を参照してください。

注記: ホスト・プラットフォームの管理者は最大 16 個の事前構成済み Wi-Fi* プロファイルを指定できますが、インテル® AMT は最大 8 つのプロファイルにしか同期できません。そのため、全 8 つのプロファイルが同期されている状態で新しい Wi-Fi* プロファイルをホストに追加した場合、インテル® EMA 内の最も古い同期プロファイルが新しいプロファイルによって置き換えられます。

デフォルトでは、Wi-Fi* 接続によるインテル® AMT エンドポイントへの接続は、オペレーティング・システムが S0 電力状態である場合のみ可能です。(すべての電力状態で Wi-Fi* 接続を有効化すると、バッテリ電力の消費が増加します) S0 ~ S5 のすべての電力状態で Wi-Fi* 接続を有効化する場合、**Enable WiFi connection in all system power states (S1-S5) (すべてのシステム電力状態 (S1 ~ S5) で WiFi 接続を有効化)** を選択します。

新しい Wi-Fi* プロファイルを作成するには、**New... (新規)** をクリックし、セクション 3.1.1 に記載したとおりに **Define the WiFi Profile(WiFi プロファイルの定義)** ダイアログに入力します。

3.2.7 Wired 802.1x (有線 802.1x) の設定



有線ネットワーク接続に使用する既存の 802.1X セットアップを選択します。詳細については、セクション 3.1.2 を参照してください。

新しい 802.1X プロファイルを作成するには、**New... (新規)** をクリックし、セクション 3.1.2 に記載したとおりに **Define the WiFi Profile(WiFi プロファイルの定義)** ダイアログに入力します。

3.3 インテル® AMT PKI 証明書のアップロード

ロール: テナント管理者

ユーザーの同意なくリモート接続可能な管理者コントロール・モード (ACM) でインテル® AMT をエンドポイントにプロビジョニングするには、インテル® AMT PKI 証明書が必要です。PKI 証明書がない場合、インテル® EMA はインテル® AMT をクライアント・コントロール・モード (CCM) でプロビジョニングします。CCM では、各エンドポイントにおいてリモート操作についてユーザーの同意が必要になります。

注記 : LAN レスのエンドポイントでは、インテル® EMA がエンドポイントをクライアント・コントロール・モードから管理者コントロール・モードに変更するには、先にエンドポイントのインテル® MEBX を手動で更新して、アップロードされた PKI 証明書の DNS サフィックスを追加する必要があります。それを行わない場合、エンドポイントは CCM のままになります。詳細については、セクション 3.3.1 を参照してください。

証明書は、それがインテル® AMT PKI 証明書であることを示す正しい OID または OU を持つ、有効なインテル® AMT PKI 証明書である必要があります。インテル® EMA は証明書の情報を検証しません。ただし、プロビジョニング・プロセスが実行されるドメインについて証明書の値が間違っている場合、プロビジョニングは失敗します。

注記 :

- ACM と CCM の詳細、有効なインテル® AMT PKI 証明書を取得するための要件およびプロセスについては、インテル® AMT の資料を参照してください。
- インテル® ME 11.0 では、デフォルトの SHA1 証明書ハッシュがファームウェアから削除されました。ハッシュは製造時に、あるいはインテル® MEBX または WS-MAN コマンドを使用することによって追加可能です。
- インテル® ME 15.0 のデスクトップ向けファームウェア、インテル® ME 16.0 の全プラットフォーム向けファームウェア以降、インテルはインテル® AMT プロビジョニングでの SHA1 ルート証明書と 2048 ビットより小さい RSA キーサイズのサポートを廃止しました。以降のリリースでは、SHA1 ハッシュを追加できません。
- 証明書の期限が切れる場合、新しい証明書をアップロードして、新しい **Entry Name (エントリー名)** と **Password (パスワード)** を入力します。新しい証明書をアップロードするとき、既存または期限切れの証明書の **Entry Name (エントリー名)** を再利用しないでください。期限切れの証明書を使用するエンドポイント・グループの構成は、新しい証明書の **Entry Name (エントリー名)** で更新する必要があります。
- Windows Server* 2012 または 2016 (ビルド 1709 より前) が動作するマシンにインテル® EMA サーバーをインストールした場合、証明書 PFX ファイルに「AES256-SHA256」暗号化が使用されている場合、インテル® EMA への証明書のアップロードが失敗します。有効なパスワードが提供されていたとしても、無効なパスワードのエラーが表示されます。
  対応策については、セクション 8 の**トラブルシューティング**を参照してください。

証明書は、インテル® EMA データベースに格納され、パフォーマンス最適化のためにメモリーに読み込まれます。更新された証明書ファイル (証明書チェーンの任意の証明書を含む) が変更されて再アップロードされた場合、変更が処理されて使用に反映されるまでに最長 15 分かかります。

あるテナントに複数の証明書をアップロードできます。また、同じ証明書を複数のテナントにアップロードすることもできます。ただし、あるテナント内の各エンドポイント・グループは 1 つの PKI 証明書にのみ関連付けられます。

証明書をアップロードする手順は次のとおりです。

1. 左側のナビゲーション・バーで **Settings (設定)** をクリックし、**Server Settings (サーバー設定) > Certificates (証明書)** を選択します。利用可能な証明書のリストが表示されます。インテル® AMT PKI 証明書は、青色の「PKI Certificate (PKI 証明書)」ラベルで示されます。その他は PKI 証明書によって使用されるルート証明書です。
2. **Upload (アップロード)** をクリックします。
3. **Certificate (証明書)** ダイアログが表示されます。アップロードする証明書がインテル® AMT PKI 証明書でない場合、**PKI certificate (PKI 証明書)** チェックボックスはオフにします。
4. **Entry Name (エントリー名)** と **Password (パスワード)** を入力し、**Choose File (ファイルの選択)** をクリックします。アップロードする証明書ファイルは 1MB より小さくなければなりません。PKI 証明書ファイルをアップロードする場合、秘密鍵を含む証明書チェーン全体をファイルに含める必要があります。すでに使用されている **Entry Name (エントリー名)** を再利用してはなりません。
5. **Certificate (証明書)** ダイアログで、**Upload (アップロード)** をクリックします。

証明書をダウンロードしたり削除したりすることもできます。証明書が（証明書チェーン内の）別の証明書によって使用中の場合や、インテル® AMT プロファイルまたはインテル® AMT セットアップで使用中の場合、その証明書は削除できません。

3.3.1 インテル® MEBX による正しい PKI DNS サフィックスの設定または検証

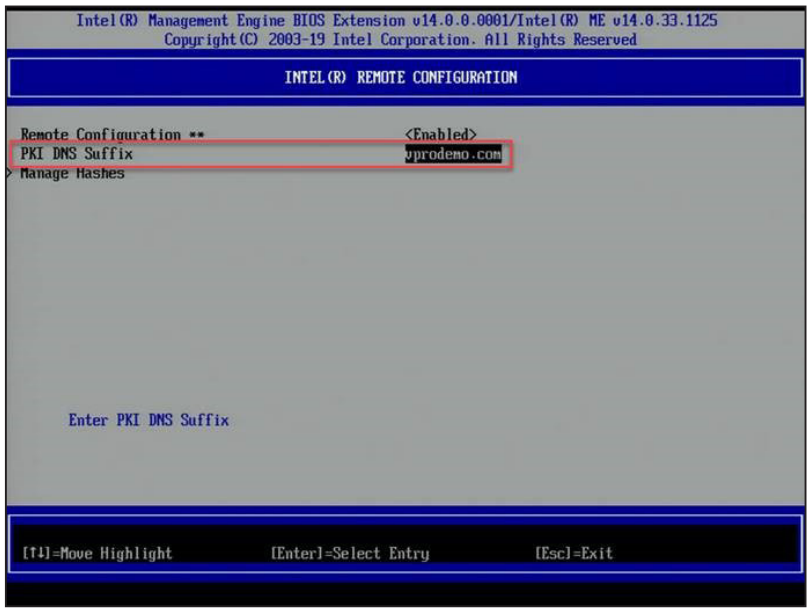
この手順は、LAN レス・エンドポイントに管理者コントロール・モード（ACM）でインテル® AMT を構成するために必要になります。LAN レスデバイスでは、現在、そのデバイスが PKI 証明書の DNS サフィックスと同じドメインにあることをインテル® AMT が知る手段はありません。そのため、LAN レスのエンドポイントのインテル® AMT を ACM で構成するためには、先に LAN レス・エンドポイントのインテル® MEBX に PKI 証明書の DNS サフィックスを手作業で追加しておく必要があります。その手順を以下に説明します。

インテル® マネジメント・エンジン BIOS 拡張（インテル® MEBX）は、インテル® AMT システムの BIOS メニューの拡張機能です。このメニューは、インテル® AMT 設定の一部を確認し、手動構成するために使用できます。このメニューは、コンピューターの再起動中に特別なキーの組み合わせ（通常 <Ctrl-P>）を押したときのみ表示されます。

インテル® MEBX へのアクセスはパスワードによって制御されます。この資料では、このパスワードをインテル® MEBX パスワードと呼びます。インテル® MEBX メニューに初めてアクセスする場合、デフォルトのパスワード（通常「admin」）を置き換える新しいパスワードが必要になります。

1. LAN レス・エンドポイントを再起動し、起動中に **Ctrl-P** を押します。
2. **Intel MEBX Login（インテル MEBX ログイン）**を選択し、インテル® MEBX パスワードを入力します。
3. **Intel(R) AMT Configuration（インテル (R) AMT 構成）> Remote Setup and Configuration（リモート・セットアップおよび構成）> TLS PKI > PKI DNS Suffix（PKI DNS サフィックス）**を選択すると、以下に示すような画面が開きます。このメニュー選択は、インテル® AMT がそのデバイスにプロビジョニングされていない場合のみ表示されることに注意してください。
4. PKI DNS サフィックスの値を確認または設定して、PKI 証明書のドメイン・サフィックスの値に一致させます。

図 6：インテル® MEBX による PKI DNS サフィックスの構成



注記：インテル® EMA はインテル® AMT の完全なプロビジョニング解除を実行し、インテル® AMT 設定からカスタム・ルート証明書ハッシュと PKI DNS サフィックスをすべて削除します。そのため、リモート・ネットワーク上のシステムのプロビジョニングを解除した後、管理者コントロール・モードを使用してそのシステムを再プロビジョニングするには、物理的にそのシステムを触る必要がある可能性があります。

3.4 エンドポイント・グループの作成

エンドポイント・グループは、組織構造に基づくエンドポイントの論理的なグループ分けです。例えば、経理部のエンドポイント・グループ、技術部のエンドポイント・グループなどを作成できます。これにより、グループごとに異なる IT ポリシーを設定できます。

3.4.1 エンドポイント・グループのポリシーセットについて

1 つのエンドポイント・グループにつき、1 つのポリシーセットが関連付けられます。各ポリシーセットに含まれるポリシーには以下のものがあります。

Power Operations (電源操作)	• **Wake-up (ウェイクアップ) :** このポリシーを選択すると、エンドポイントのリモート・ウェイクアップ/ブートアップが有効になります。 • **Sleep (スリープ) :** このポリシーを選択すると、エンドポイントのスリープおよびハイバネート・モードのリモートアクティブ化が有効になります。 • **Turn off or restart (電源オフまたは再起動) :** このポリシーを選択すると、エンドポイントのリモート電源オフおよび再起動が有効になります。
Messaging and Alerts (メッセージとアラート)	• **TCP traffic relay (TCP トラフィック・リレー) :** このポリシーは、以降のすべてのポリシーの土台になります。このポリシーを選択しない場合でも、エンドポイントはインテル® EMA サーバーに接続できます。ただし、インテル® EMA は、インテル® AMT のセットアップを含め、エンドポイントに対して何のアクションも実行できません。 • **Alert messages (アラートメッセージ) :** このポリシーを選択すると、エンドポイント上でアラートメッセージの表示が有効になります。 • **Console prompts (コンソールプロンプト) :** このポリシーを選択すると、エンドポイント上でスケジュールされたリモート実行が有効になります。このポリシーは、リモート・ターミナル・アクセスを制御するために使用する必要があります。アウトオブバンドのターミナルアクセスの場合、インテル® AMT セットアップ中に使用されるインテル® AMT プロファイルでもこのポリシーを有効にする必要があります。 • **Location information (位置情報) :** このポリシーを選択すると、エンドポイントのリモート位置情報のクエリーが有効になります。この機能は現在サポートされていません。 • **Peer-to-peer communication (ピアツーピア通信) :** このポリシーは、同じネットワーク上のエンドポイント (インテル® EMA エージェント) 間の通信に適用されます。このポリシーを選択しない場合、エージェントはネットワーク内の他のエージェントを検出せず、他のエージェントからの通信を受け付けません。そのため、インテル® EMA エージェントのリレー (TLS リレーによるインテル® AMT セットアップなど) は動作しません。
Remote Control (リモート制御)	• **Remote KVM (リモート KVM) :** このポリシーを選択すると、リモート KVM が有効になります。アウトオブバンドの KVM の場合、インテル® AMT セットアップ中に使用されるインテル® AMT プロファイルでもこのポリシーを有効にする必要があります。 • **Remote file access (リモート・ファイル・アクセス) :** このポリシーを選択すると、エンドポイントへの (ファイルブラウザー、スケジュールされたファイルデリバリー、またはファイル検索による) リモートのインバンド・ファイル・アクセスが有効になります。 • **Remote management(WMI) (リモート管理 (WMI)) :** このポリシーを選択すると、エンドポイント上でリモート WMI クエリーとリモート・プロセス操作 (WMI 経由) が有効になります。このポリシーにより、インテル® EMA がエンドポイントを BIOS にリモートで設定できるかどうかも制御されます。

	• **User consent for in-band KVM (インバンド KVM のユーザー同意)**：有効にすると、次のロジックが適用されます。
	  • ターゲットのエンドポイントがユーザーセッション中でない場合 (ロック済み、ログアウト済みなど)、KVM はタイムアウト後に拒否されます。
	  • ターゲットのエンドポイントがユーザーセッション中の場合、ユーザーに承認または拒否を求めるポップアップ・ウィンドウが表示されます。ユーザーが承認すると、インバンド KVM が通り、ターゲットのエンドポイントのシステム・トレイ・アイコンに KVM セッションの存在が通知されます。
	  • 無効にすると、ユーザーの同意は不要になります。

アウトオブバンド機能 (インテル® AMT によって提供) について

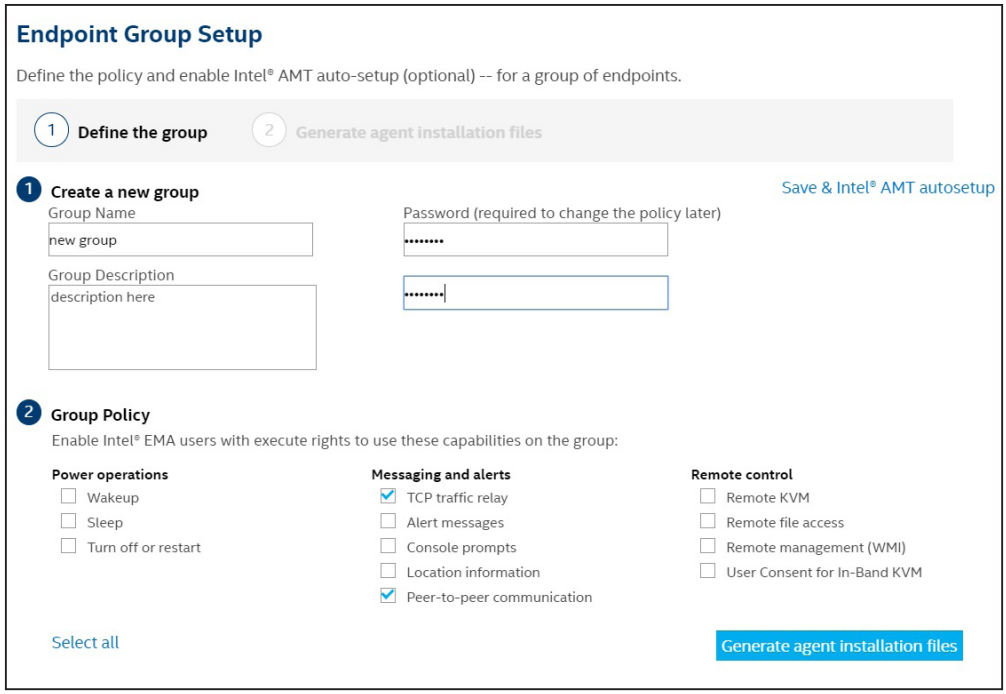
- アウトオブバンド・ターミナルとアウトオブバンド KVM は、コマンドポリシーと KVM ポリシーによって制御されます。これらのポリシーのいずれかが許可されると、両方の機能が許可されます。
- 次の WSMAN 電源アクションは、指定されたエンドポイント・グループ・ポリシーに対してチェックされます。CIM_Power-ManagementService \ RequestPowerStateChange

3.4.2 エンドポイント・グループの新規作成

ロール：テナント管理者、エンドポイント・グループ作成者

1. 左側のナビゲーション・バーで **Endpoint Groups (エンドポイント・グループ)** を選択し、**New Endpoint Group (新規エンドポイント・グループ)** を選択します。
2. フィールドに入力し、グループに含まれるエンドポイントで利用可能にする **Group Policy (グループポリシー)** 機能を選択します。
3. このグループ内のエンドポイントに対して、インテル® EMA によるインテル® AMT の自動セットアップを行う場合、**Save & Intel® AMT autosetup (保存およびインテル® AMT の自動セットアップ)** をクリックします。それ以外の場合は、**Generate agent installation files (エージェント・インストール・ファイルの生成)** をクリックします。

図 7：Endpoint Group Setup (エンドポイント・グループのセットアップ) ページ



3.4.2.1　エンドポイント・ユーザー・グループの自動作成

ロール：エンドポイント・グループ作成者のみ

エンドポイント・グループ作成者ユーザーが新しいエンドポイント・グループを作成するとき、インテル® EMA により、実行権限付きで現在のユーザーを含むユーザーグループが自動的に作成されます。また、このユーザーグループは新しいエンドポイント・グループに自動的に関連付けられます。この内部的に自動作成されたユーザーグループの名前は、[作成されたエンドポイント・グループ名]_EndpointGroupCreators の形式になります。そのため、エンドポイント・グループへのアクセス制御はユーザーグループによって管理されます。

注記：テナント管理者は特定のユーザーグループに属さないため、テナント管理者が新しいエンドポイント・グループを作成しても、このようなユーザーグループの自動作成は行われません。

3.4.3　エンドポイント・グループの表示と削除

ロール：テナント管理者（削除、表示）、エンドポイント・グループ作成者（削除、表示）、エンドポイント・グループ・ユーザー（表示）

エンドポイント・グループ作成者は、自分と同じユーザーグループ（実行権限を持つ）に属するエンドポイント・グループのみを削除できます。エンドポイント・グループ作成者は、自分と同じユーザーグループ（表示権限を持つ）に属するエンドポイント・グループのみを表示できます。

エンドポイント・グループ・ユーザーは、自分と同じユーザーグループに属するエンドポイント・グループのみを表示できます。

そのエンドポイント・グループの横の省略記号（**...**）をクリックし、**View Configuration（構成の表示）**を選択します。

このエンドポイント・グループを削除するには、**Delete Group（グループの削除）**をクリックします。

注記：エンドポイント・グループを削除した場合、そのグループに属するエンドポイントはインテル® EMA サーバーに接続できなくなります。

3.5　インテル® AMT の自動セットアップの有効化

ロール：テナント管理者、エンドポイント・グループ作成者†

†このグループに対して実行権限を持つこと

注記：インテル® AMT のセットアップは「プロビジョニング」と呼ばれることもあります。

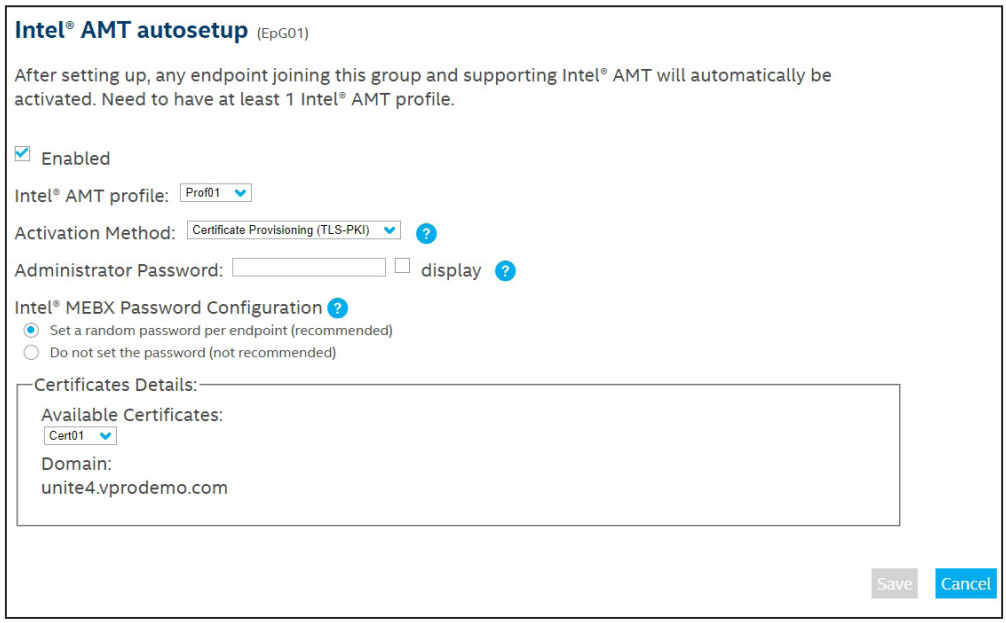
インテル® AMT の自動セットアップは、エンドポイント・グループごとに有効と無効を切り替えられます。有効にすると、インテル® EMA はこのエンドポイント・グループに登録されるすべてのエンドポイントのセットアップを試みます。このセットアップは、エンドポイントが切断された後にインテル® EMA サーバーに再接続するときや、エージェントのデプロイ前にインテル® AMT の自動セットアップが定義され、エージェントが最初に接続するときにトリガーされます。

自動セットアップを有効化する手順は次のとおりです。

1. 左側のナビゲーション・バーで **Endpoint Groups（エンドポイント・グループ）**を選択し、ターゲットのエンドポイント・グループの横の省略記号（**...**）をクリックして **View Configuration（構成の表示）**を選択します。
2. そのエンドポイント・グループの構成ページで **Intel® AMT Autosetup（インテル® AMT の自動セットアップ）**をクリックします。
3. **Enabled（有効化）**チェックボックスをオンにし、**Intel® AMT profile（インテル® AMT プロファイル）**であらかじめ作成したプロファイルを選択します。
4. 使用する **Activation Method（アクティブ化方法）**を選択します。TLS-PKI アクティブ化方法は、そのテナントに対して有効なインテル® AMT PKI 証明書が少なくとも 1 つある場合にのみ表示されます。テナント管理者は Settings（設定）ページを使用して利用可能な PKI 証明書を管理できます（セクション 3.3）。アクティブ化方法の詳細については、セクション 1.2.6 および 1.2.7 を参照してください。
5. **Administrator Password（管理者パスワード）**を入力します。ここで入力する管理者パスワードが、エンドポイント・システムでのインテル® AMT の「admin」アカウントのパスワードとして設定されます。

6. このインテル® AMT プロファイルで構成されるエンドポイントのインテル® マネジメント・エンジン BIOS 拡張 (インテル® MEBX) にランダムなパスワードを設定するかどうかを選択します。エンドポイントにはインテル® EMA によってランダムなインテル® MEBX パスワードを設定することが推奨されます。エンドポイントのランダムなパスワードは、必要な場合、インテル® EMA API を使用して取得できます。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。
7. **Available Certificates (利用可能な証明書)** から証明書を選択します (利用可能なものが存在する場合)。
8. **Save (保存)** をクリックします。

図 8：インテル® AMT autosetup (インテル® AMT の自動セットアップ) 画面



自動セットアップの構成が変更されると (インテル® AMT プロファイルの変更など)、インテル® EMA は、インバンド接続されたすべてのエンドポイントに対してこの変更をほぼ即座に適用します。接続されていないエンドポイントには、インテル® EMA サーバーに再接続した時点で変更が適用されます。

ただし、証明書またはアクティブ化方法 (ホストベースまたは TLS-PKI) が変更された場合、インテル® EMA はこのような変更を自動的に適用することはできません。その場合、はじめにエンドポイントのプロビジョニングを解除する必要があります。

3.6 管理対象エンドポイントの導入に使用するエージェント・ファイルの作成

ロール： テナント管理者、エンドポイント・グループ作成者†、エンドポイント・グループ・ユーザー†

†このグループに対して実行/表示権限を持つこと

1. 左側のナビゲーション・バーで **Endpoint Groups (エンドポイント・グループ)** を選択し、ターゲットのエンドポイント・グループの横の省略記号 (...) をクリックして **Create Agent Files (エージェント・ファイルの作成)** を選択します。
2. 使用するプラットフォーム (32 ビットまたは 64 ビット) を選択します。
3. Agent policy file (エージェント・ポリシー・ファイル) の横の **Download (ダウンロード)** をクリックしてから、**Done (完了)** をクリックします。

図 9：Generate agent installation files（エージェント・インストール・ファイルの生成）

どちらのファイルも、インテル® EMA のウェブベース UI を使用するシステムの **Downloads** フォルダー内に作成されます。これらのファイルはまとめて保管し、インテル® EMA で管理するエンドポイント・システムにコピーします。インストール・プロセスは次のセクションで説明します。

注記：

- エンドポイント・グループとユーザーグループの関連付けによるユーザーアクセス管理の詳細については、セクション 5.3 を参照してください。
- エンドポイントへのエージェントのインストールのトラブルシューティングについては、セクション 4.5 を参照してください。

4　エンドポイントへのエージェントの導入

ロール：該当なし。特定のインテル® EMA ユーザーロールによらない

このセクションでは、インテル® EMA エージェントを対象のエンドポイント・システムに手作業でインストールする方法について説明します。この手順は、多数のエンドポイント・システムに対してインテル® EMA エージェントを一括で導入するスクリプトを作成する方にも役立ちます。

前のセクションで作成した 2 つのエージェント・ファイル、**EMAAgent.exe** と **EMAAgent.msh** を、インテル® EMA で管理する各エンドポイント・システムにコピーする必要があります。各エンドポイント・システムに手動でコピーすることも、一括導入ツールを使用することもできます。どちらの場合も、2 つのファイルはそのエンドポイント・システム内の同じフォルダーに配置し、同じファイル名接頭辞 (EMAAgent) を持つ必要があります。複数のバージョン (32 ビット版と 64 ビット版) をダウンロードした場合、どちらの実行可能ファイル (.exe) がどちらのポリシーファイル (.msh) に対応するか分かるよう、ペアの名前を変更してください。

注記：コンソールとしてインテル® EMA エージェントをインストールする方法の詳細については、セクション 12 を参照してください。

次の表で、これらのファイルのプロパティーを説明します。

表 1：インテル® EMA エージェント・ファイル

ファイル名	説明
EmaAgent.exe	エージェントのインストール・ファイルです。インスタンスをインストール/更新/アンインストールするには、このファイルを管理者権限で実行する必要があります。
EmaAgent.msh	ポリシーファイルです。このファイルによってエンドポイントが属するエンドポイント・グループが決定され、インテル® EMA エージェントがインテル® EMA サーバーに通信できるようになります。

エンドポイント・システムへのインストール：

1. 2 つのエージェント・ファイル (EMAAgent.exe、EMAAgent.msh) を、これらが作成されたシステムの Downloads フォルダーからターゲットのエンドポイント・システムにコピーします。両ファイルは必ず同じフォルダーにコピーしてください。
2. エンドポイント・システムで、管理者権限でコマンドウィンドウ (cmd.exe) を開き、2 つのエージェント・ファイルがあるフォルダーに移動します。
3. 以下のコマンドを実行し、インテル® EMA エージェントをインストールします。

```
EmaAgent.exe -fullinstall
```

アンインストールする場合：

```
EmaAgent.exe -fulluninstall
```

エージェント・インストーラーのヘルプを表示する場合：

```
EmaAgent.exe -?
```

注記：Windows* エクスプローラーで EmaAgent.exe ファイルを右クリックし、Run as Administrator (管理者として実行) を選択すると、エージェント・インストーラーを GUI で実行できます。インストーラー・ダイアログで、Install/Update (インストール/更新) をクリックしてください。

インストールの検証とトラブルシューティングの詳細については、セクション 4.5 を参照してください。

4.1　インストール・ディレクトリー

Win32 サービスのデフォルトのインストール・ディレクトリーは、C:\Program Files (x86)\Intel\Ema Agent です。

Win64 サービスのデフォルトのインストール・ディレクトリーは、C:\Program Files\Intel\Ema Agent です。

両方のサービスに以下のファイルが含まれています。

- EmaAgent.exe：実行可能サービスファイルです。
- EmaAgent.log：ローカルロギングに使用されます。
- EmaAgent.msh：インストールされたポリシーファイルです。
- EmaAgent.db：インテル® EMA エージェントのデータベースです。

4.2 インテル® EMA エージェント・データベース

エージェント・サービスがインストールされると、設定と証明書を保存するためにローカル・データベースが生成されます。データベースは、エージェントが実行する実行可能バイナリーと同じパスに保存されます。

4.3 Windows* サービス情報

エージェントが Windows* サービスとしてインストールされた後、Windows* のサービス・マネージャーを使用してエージェントにアクセスできます。

1. Window* キー +R を押して **[ファイル名を指定して実行]** ウィンドウを開きます。
2. **[ファイル名を指定して実行]** ウィンドウに **services.msc** と入力します。
3. **Enter** キーを押します。
4. Windows* にインストールされたサービスがすべて表示されます。
5. エージェント サービスを見つけるには、**Intel(R) EMA Agent background service (インテル (R) EMA エージェント・バックグラウンド・サービス)** の名前を探します。
6. エージェント・サービスを選択し、正常に動作しているか確認します。
7. このとき、必要に応じてサービスを停止または再起動できます。サービスがすでに停止している場合、起動できます。

4.4 プロキシーの構成

Internet Explorer* の Windows* プロキシー設定でエンドポイントにプロキシーを設定した場合、エージェントはインストール・ディレクトリー内に **EmaAgent.proxy** という名前のファイルを作成し、そこに HTTPS プロキシーの値を格納します。

4.5 エージェントのインストールの検証とトラブルシューティング

インテル® EMA エージェントのコマンド・ライン・インターフェイスを使用して、インテル® EMA サーバーへの接続情報を表示できます。エージェントがインストールされているエンドポイント上で、次のステップを行います。

1. コマンド・プロンプト・ウィンドウを管理者として開きます。
2. インテル® EMA エージェントのインストール・ディレクトリー (セクション 4.1 を参照) に移動します。
3. 以下のコマンドのいずれかを実行します。

エージェントが動作しているかどうかをテストするには

コマンド：

```
tasklist /fi "imagename eq EmaAgent.exe"
```

例 (成功時)：

```
λ tasklist /fi "imagename eq EmaAgent.exe"
Image Name                     PID Session Name        Session#       Mem Usage
```

```
========================= ======== ================ =========== ============
EmaAgent.exe                  15396 Services                0      42,816 K
```

例(失敗時):

```
λ tasklist /fi "imagename eq EmaAgent.exe"
INFO:No tasks are running which match the specified criteria.
```

エージェントが接続されているかどうかをテストするには

コマンド:

```
netstat -nao | find "8080"
```

例(成功時):

```
λ netstat -nao | find "8080"
TCP   <agent IP>:<random port> <swarm server IP>:8080   ESTABLISHED
<process ID>


TCP 192.168.1.100:51662 192.168.0.18:8080 15396
```

例(失敗時):

```
λ netstat -nao | find "8080"
(空の結果を返す)
```

swarm サーバー名を取得するには

コマンド:

```
EMAAgent.exe -swarmserver
```

例(成功時):

```
EMAAgent.exe -swarmserver
Intel(R) EMA Swarm server address and port are 192.168.0.18:8080
```

例(失敗時):

```
EMAAgent.exe -swarmserver
Unable to read Intel(R) EMA Agent database.
```

エージェントのノード ID を取得するには

コマンド:

```
EMAAgent.exe -nodeidhex
```

例(成功時):

```
λ EMAAgent.exe -nodeidhex
Intel(R) EMA Agent node is: <HEX ID>
```

例(失敗時):

```
λ EMAAgent.exe -nodeidhex
Not defined, start the Intel(R) EMA Agent to create a nodeid.
```

プロキシーサーバー情報を取得するには

コマンド :

```
EMAAgent.exe -agentproxy
```

例 (成功時) :

```
EMAAgent.exe -agentproxy
Intel(R) EMA Agent Proxy: example.com:12345
```

例 (失敗時) :

```
EMAAgent.exe -agentproxy
No Intel(R) EMA Agent proxy found.
```

5　ユーザーとユーザーグループの管理

組織の規模や複雑度に応じて、エンドポイントの管理に役立つ追加のユーザーを作成する場合もあります (ユーザーロールの詳細については、セクション 1.2.2 を参照)。

ユーザーがエンドポイント・グループ内のエンドポイントを管理するには、そのユーザーが管理対象のエンドポイント・グループと同じユーザーグループに割り当てられている必要があります (セクション 1.2.4 参照)。

5.1　ユーザーの追加、変更、削除

ロール：テナント管理者、アカウント・マネージャー、グローバル管理者

1. 左側のナビゲーション・バーで **Users (ユーザー)** をクリックします (または **Overview (概要)** ページの **Quick Links (クイックリンク)** で **Add or remove users (ユーザーの追加または削除)** をクリックします)。
2. ユーザーを追加するには、**New User... (新規ユーザー)** をクリックします。
3. ユーザー情報を入力し、**Save (保存)** をクリックします。
4. ユーザーグループに新しいユーザーを追加するには、新規ユーザーの横の省略記号 (**...**) をクリックして **Group memberships (グループ・メンバーシップ)** を選択し、このユーザーを追加するグループを選択します。

注記：

- ユーザーが自身のユーザーアカウントのパスワードを変更する場合、現在のパスワードを最初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、省略記号 (**...**) をクリックしてユーザーを編集し、アカウントのロックを解除します。
- そのテナントでクライアント資格情報アカウントが作成されている場合、テナント管理者のロールを持つユーザーの一覧と、メールアカウントの形式ではないユーザー名 (user@domain.com) が表示されることがあります。クライアント資格情報アカウントの詳細については、セクション 13「付録 - マシンツーマシン・クライアント・アプリケーションからのインテル® EMA エンドポイント処理の実行」(55 ページ) を参照してください。
- 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)。

既存のユーザーを編集または削除するには、そのユーザーの横の省略記号 (**...**) をクリックし、**Edit (編集)** または **Delete (削除)** を選択します。

5.2　ユーザーグループの新規作成

ロール：テナント管理者、アカウント・マネージャー、グローバル管理者 (更新および削除のみ)

1. 左側のナビゲーション・バーで **Users (ユーザー)** を選択し、**User Groups (ユーザーグループ)** タブをクリックします。
2. **User Groups (ユーザーグループ)** タブを選択して **New Group (新規グループ)** をクリックしたら、**Group Name (グループ名)** と **Description (説明)** を入力し、このユーザーグループのユーザーに付与するアクセス許可レベルを指定します。

   注記：Description (説明) は必須フィールドであり、値を入力しないとグループを保存できません。
3. **Members (メンバー)** をクリックし、このユーザーグループに追加するユーザーを選択します (または、後で新規ユーザーを作成した時点でこれを実行します)。
4. **Endpoint Groups (エンドポイント・グループ)** をクリックし、このユーザーグループがアクセスできるエンドポイント・グループを選択します。

既存のユーザーグループを編集または削除するには、そのユーザーグループの横の省略記号 (**...**) をクリックし、**Edit (編集)** または **Delete (削除)** を選択します。ユーザーグループを削除しても、そのユーザーグループに関連付けられていたユーザーおよびエンドポイントは影響を受けません。

5.3 ユーザーグループへのエンドポイント・グループの割り当て

ロール：テナント管理者、エンドポイント・グループ作成者†

†このグループに対して実行権限を持つこと

セクション 1.2.4 で説明したとおり、ユーザーグループはエンドポイント・グループに対するユーザーアクセスを管理するために使用されます。結果として、ユーザーグループによってエンドポイント自体へのアクセスが管理されます。ユーザーが特定のエンドポイント・グループのエンドポイントに対して管理タスクを実行するためには、ユーザーとそのエンドポイント・グループが同じユーザーグループに属している必要があります。

1. 左側のナビゲーション・バーで **Users（ユーザー）**を選択し、**User Groups（ユーザーグループ）**タブをクリックします。
2. ターゲットのユーザーグループの省略記号（**...**）をクリックし、**Assign Endpoint Groups（エンドポイント・グループの割り当て）**を選択します。
3. ダイアログボックスでターゲットのエンドポイント・グループと関連付ける権限を選択し、**Save（保存）**をクリックします。

6　エンドポイントの管理

ロール：テナント管理者、エンドポイント・グループ作成者（グループと権限に基づく）、エンドポイント・グループ・ユーザー（グループと権限に基づく）

組織構造を反映するようにテナントをセットアップすると、インテル® EMA を使用してエンドポイント・システムを管理する準備は完了です。

6.1　インテル® AMT のオンデマンド・セットアップ

インテル® AMT のセットアップは「プロビジョニング」と呼ばれることもあります。

インテル® AMT のセットアップ/クリーンアップ・アクションは、一つひとつのエンドポイントに対してオンデマンドで実行できます。ただし、オンデマンド・セットアップではインテル® AMT プロファイルは使用できません。Intel® AMT profile（インテル® AMT プロファイル）ドロップダウン・メニューは無効化されます。オンデマンド・セットアップでは、ごく基本的な構成を実行します。詳細については、セクション 1.2.7 を参照してください。

このページにアクセスするには、エンドポイントのアクション・ドロップダウン・メニューを開き、**Provision Intel® AMT（インテル® AMT のプロビジョニング）**を選択します。このオプションは、対象のエンドポイントがインテル® AMT に対応している場合のみ有効化されます。このページを使用して、インテル® AMT をプロビジョニングまたはプロビジョニング解除できます。

Activation Method（アクティブ化方法）について

- TLS-PKI アクティブ化方法は、そのテナントに対して有効なインテル® AMT PKI 証明書が少なくとも 1 つある場合に表示されます。テナント管理者は Settings（設定）ページを使用して利用可能な PKI 証明書を管理できます。詳細については、セクション 3.3 を参照してください。
- TLS-PKI が選択されている場合でも、インテル® EMA はインテル® AMT のセットアップにホストベースのフローを使用します。

Administrator Password（管理者パスワード）に入力したパスワードは、インテル® AMT の「admin」アカウントのパスワードとして設定されます。

エンドポイントのインテル® マネジメント・エンジン BIOS 拡張（インテル® MEBX）にランダムなパスワードを設定するかどうかを選択します（PKI プロビジョニングのみで利用可能）。エンドポイントにはインテル® EMA によってランダムなインテル® MEBX パスワードを設定することが推奨されます。エンドポイントのランダムなパスワードは、必要な場合、インテル® EMA API を使用して取得できます。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。

注記：エンドポイントのプロビジョニングを解除すると、ランダムなインテル® MEBX パスワードはインテル® EMA データベースから削除され、API で取得することはできなくなります。エンドポイントのプロビジョニングを解除する前に、必ずインテル® MEBX パスワードを取得してメモしておきます。これは、再プロビジョニングする前にインテル® MEBX で PKI DNS サフィックスをリセットする必要がある LAN レスのシステムでは特に重要です。LAN レスのシステムの詳細については、セクション 3.3.1 を参照してください。

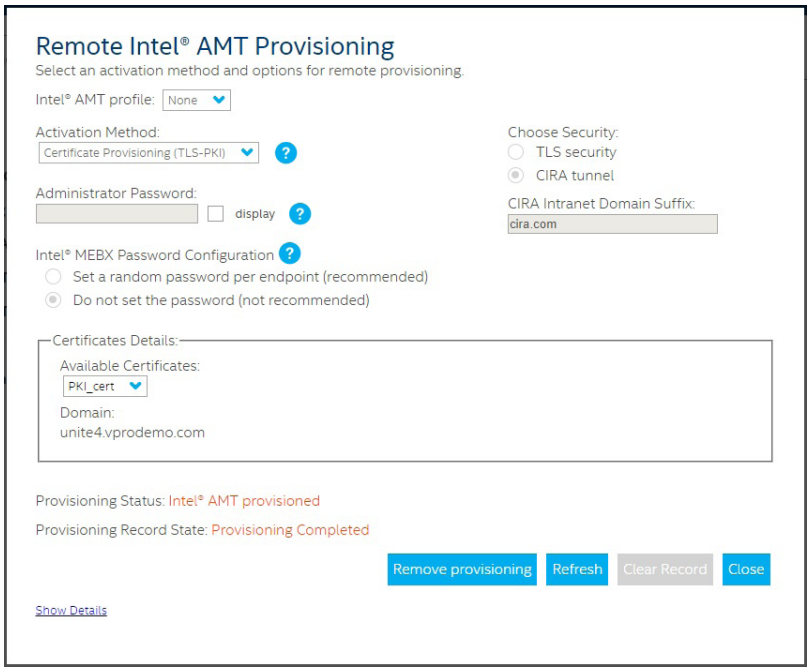
CIRA または TLS リレーの詳細については、セクション 1.2.6 を参照してください。

Provision Status（プロビジョニング・ステータス）：これはターゲットのインテル® AMT のプロビジョニング・ステータスです。

Provision Record State（プロビジョニング・レコードの状態）：これは現在のセットアップ/クリーンアップ・アクションのステータスです。インテル® EMA は、各インテル® AMT セットアップのセットアップ/プロビジョニング・レコードを保持します。このレコードは、エンドポイントのセットアップ・ステータスを示します。セットアップ/プロビジョニングが失敗した場合、インテル® EMA はこのレコードを再開して定期的にリトライします。そのため、セットアップ/プロビジョニング・プロセス進行中には、Clear Record（レコードのクリア）ボタンが表示されます。レコードをクリアした場合、インテル® EMA はそれ以上プロビジョニング処理を試行しません。

Provision Status（プロビジョニング・ステータス）が Provisioned（プロビジョニング済み）になり、Provision Record State（プロビジョニング・レコードの状態）が Complete（完了）になると、ターゲットのインテル® AMT のセットアップは完了です。

図 10：インテル® AMT のオンデマンド・プロビジョニング



6.2 インテル® EMA エージェント

インテル® EMA エージェントは、TCP とポート 8080 を介してインテル® EMA サーバーに接続します。インテル® EMA エージェントをインストールすると、インストールされたエージェントのバイナリープロセスに Windows* ファイアウォールの以下のインバウンド・ルールがセットアップされます。その他のファイアウォールをご利用の場合、インストールされたエージェントのバイナリープロセスに対して、以下のインバウンド・ルールが設定されていることを確認してください。

- ピアツーピア・トラフィック：ローカルポート 16990 の UDP、ローカルおよびリモートアドレスの任意の IP、エッジ・トラバーサルはブロックされます。
- ピアツーピア・トラフィック：ローカルポート 16990 の TCP、ローカルおよびリモートアドレスの任意の IP、エッジ・トラバーサルはブロックされます。
- ローカル・ループバック管理トラフィック：ローカルポート 16991 の TCP、ローカルおよびリモートアドレスの 127.0.0.1、エッジ・トラバーサルはブロックされます。

インテル® EMA エージェントのトラブルシューティングについては、セクション 4.5 を参照してください。

6.3 エンドポイントの表示

テナント管理者、エンドポイント・グループ作成者、エンドポイント・グループ・ユーザーは、**Managed Endpoints（管理対象のエンドポイント）**ページで、各自がアクセス権（実行権限または表示権限）を持つエンドポイントを表示できます。

エンドポイントのリストを表示するには、左側のナビゲーション・バーで **Endpoints（エンドポイント）**を選択し、**Managed Endpoints（管理対象のエンドポイント）**タブを選択します。

注記：表示される **Connection（接続）**ステータスはインバンド接続のステータスです。

特定のエンドポイントの詳細を表示するには、リスト内の任意のエンドポイントについて **View（表示）**をクリックすると、その情報ページにアクセスできます。このページの各タブについて、以下のサブセクションで説明します。

6.3.1 General（全般）タブ

選択したエンドポイントについて全般的情報を表示します。

注記：

- **Manage this endpoint（このエンドポイントを管理）**ドロップダウン・メニュー・オプションについては、セクション 6.4 で説明します。
- 接続済みのステータスは、インバンド接続用です。
- エンドポイントのインテル® AMT ファームウェアがインテル® EMA によってセットアップ/プロビジョニングされると、Device Page（デバイスページ）リンクが有効化され、そのエンドポイントのインテル® AMT のデフォルト・ウェブ・インターフェイスにアクセスできるようになります。
- このページにはインテル® AMT セットアップ・ステータスが表示されます。インテル® AMT がセットアップ済みにもかかわらず、インテル® EMA にセットアップ・レコードがない場合、警告が表示されます。

6.3.2 Intel® AMT（インテル® AMT）タブ

多くのアウトオブバンド・インテル® AMT 操作を実行できます。操作をするには、インテル® AMT が現在のインテル® EMA インスタンスで構成されたものでなければなりません。異なるインテル® EMA インスタンスによって構成されたエンドポイントは、このタブでは操作できません。

左側のペインのリストから、実行するアクションを選択します。

注記：

- このタブを使ってインテル® AMT の設定を変更しないでください。エンドポイントの管理性が低下する場合があります。
- このタブは、インテル® マネージャビリティー・コマンダー（インテル® MC）をインテル® EMA のユーザー・インターフェイスに組み込んだものです。このタブのアクションはインテル® MC を介して実行されます。リストで利用できるアクションの詳細については、インテル® MC のユーザー資料を参照してください。
- Intel® AMT（インテル® AMT）タブでは、CIRA 向けにプロビジョニングされたエンドポイントの IP アドレスは **unknown（不明）**としてレポートされます。一方、インテル® AMT ウェブページでは、そのようなエンドポイントの IP アドレスは **0.0.0.0** としてレポートされます。

6.3.3 Desktop（デスクトップ）タブ

インバンドのリモート KVM 機能を使用して、次の設定を変更できます。

- **Choose display（ディスプレイの選択）：**エンドポイントにディスプレイが複数ある場合、表示するターゲット・ディスプレイを選択できます。
- **Change scale percentage（スケール率の変更）：**これは、レンダリング解像度のパーセント値です。値が小さいほど、解像度は低くなります。50%（半分）または 100%（フルスケール）を使用すると最良の結果が得られます。
- **Change bitmap quality（ビットマップ品質の変更）：**これは、ビットマップ圧縮のレベルです。値が小さいほど、圧縮率は高くなりますが、解像度が低下します。
- **Rotate the rendered display on Intel® EMA（インテル® EMA に表示するディスプレイの回転）：**ターゲットのエンドポイント・ディスプレイが縦置きの場合に便利です。
- **Send the “Ctrl + Alt + Del” key combination（Ctrl + Alt + Del キーの送信）：**いくつかの特別なキーの組み合わせは、ウェブブラウザーを実行する Windows* オペレーティング・システムによって遮断されます。このオプションを使うことで、Ctrl + Alt + Del キーをリモートのシステムに送信できます。
- **Expand KVM to full screen（KVM の全画面への拡大）：**これはウェブブラウザーの全画面 API を使用して、リモート KVM を全画面モードに拡大します。このモードを解除するには、ウェブブラウザーの制御（**Esc** キーなど）を使用します。

次のいずれかの条件が成立する場合、このタブは無効化されます。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- エンドポイントがインテル® EMA にインバンド接続されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。

注記：

- この機能の動作は、インバンド KVM に対するユーザーの同意による影響を受けます。詳細については、セクション 3.4.1 を参照してください。
- 複数のユーザー（ウェブブラウザー）が同一のエンドポイントの KVM に接続する場合、次のことに注意してください。
  - 前の同意リクエストが有効な場合、ユーザーの同意は再度リクエストされません。
  - マウスとキーボードの入力について、すべてのセッションが競合します。
  - スケール、ビットマップ品質、ディスプレイの選択はすべてのセッションに影響します。
  - 回転は現在のブラウザーのみに影響します。

6.3.4 Terminal（ターミナル）タブ

インバンドとアウトオブバンド両方のリモートターミナル機能を提供します。テキストベースのコマンドのみがサポートされます。次のいずれかの条件が成立する場合、このタブは無効化されます。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。
- そのエンドポイントがプロビジョニングされていない、また、そのエンドポイントがインテル® EMA にインバンド接続されていない。

そのエンドポイント上にインテル® AMT がセットアップ/プロビジョニングされている場合、**Start Intel® AMT Terminal（インテル® AMT ターミナルの起動）**ボタンが表示されます。あるいは、**Start Terminal（ターミナルの起動）**ボタンを使用します。

注記：Intel® AMT terminal（インテル® AMT ターミナル）は、Serial-Over-LAN（SOL）ターミナルです。動作させるには、まず、別のツールを使用してエンドポイント・システムを再起動して BIOS に入り、BIOS で SOL を有効化する必要があります。この手順の例を以下に示します。

1. エンドポイントをプロビジョニングし、BIOS モード中にインテル® AMT 処理を実行できるようにします。
2. エンドポイントを再起動して BIOS で SOL を有効化するツールを選択します。例えば、インテル® EMA の JavaScript* ライブラリーのサンプルファイル EndpointAMTOperations.html では、BIOS へのリセットを実行すると SOL を有効に設定するため、ツールとして使用できます。サンプルファイルをホストする方法については、インテル® EMA 管理者にお問い合わせください。
3. インテル® EMA ウェブサイトで、エンドポイントの Terminal（ターミナル）タブに移動します。
4. 選択したツールで、エンドポイントを BIOS にリセットします。BIOS は、テキストバージョンの BIOS である必要があります。
5. **Terminal（ターミナル）**タブで **Start Intel® AMT Terminal（インテル® AMT ターミナルを開始）**をクリックします。任意のキー（上向きまたは下向き矢印キーなど）を押して、接続後にディスプレイを更新します。

注記：

ターミナルウィンドウで Windows* PowerShell* を実行する場合、コマンド入力時に大文字（Shift+< 文字キー >）を入力しないでください。Windows* PowerShell* が終了し、コマンドプロンプトに戻ってしまいます。Ctrl+< 任意のキー > でも同様です。すべてのコマンドを小文字のみを使用して入力してください。ほとんどのコマンドは大文字と小文字を区別しません。大文字と小文字の区別については、次の情報を参照してください。

https://devblogs.microsoft.com/scripting/weekend-scripter-unexpected-case-sensitivity-in-powershell/

また、Caps Lock を有効にすると、Windows* PowerShell* を終了することなく大文字を入力できます。

終了したら、**Disconnect（切断）**をクリックします。

6.3.5 Files（ファイル）Tab

インバンドのリモートファイル参照機能を提供します。

次のいずれかの条件が成立する場合、このタブは無効化されます。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- エンドポイントがインテル® EMA にインバンド接続されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。

6.3.6 Processes（プロセス）タブ

インバンドのリモートプロセス管理機能を提供します。この機能は、Windows* Management Instrumentation（WMI）によって実装されます。これは以下の用途で使用します。

- 実行中のプロセスのリストを表示する。
- 管理対象のエンドポイント上で新しいプロセスを起動する。ターゲットの実行可能ファイルに有効なローカルパスを提供する必要があります。
- プロセスを終了させる。

次のいずれかの条件が成立する場合、このタブは無効化されます。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- エンドポイントがインテル® EMA にインバンド接続されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。

6.3.7 WMI タブ

ターゲットのエンドポイントに対して Windows* Management Instrumentation（WMI）クエリーまたは WMI アクションを実行できます。

次のいずれかの条件が成立する場合、このタブは無効化されます。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- エンドポイントがインテル® EMA にインバンド接続されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。

6.4 エンドポイントにおけるアクションの実行

Managed Endpoints（管理対象のエンドポイント）ページで、エンドポイントを少なくとも 1 つ選択し、**Select an endpoint action（エンドポイント・アクションを選択）**ドロップダウン・メニューをクリックします。

利用可能なエンドポイント・アクションについて、以下のサブセクションで説明します。

6.4.1 ウェイクアップ

1 つまたは複数のエンドポイントに対し、インテル® AMT または Wake-On-LAN 経由でウェイクリクエストを送信します。

注記：Wake-On-LAN はインテル® vPro® プラットフォームでのみサポートされています。

エンドポイントを 1 つだけ選択し、以下のいずれかの条件が成立した場合、アクションは実行されません。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。

6.4.2 スリープ/ハイバネート/電源オフ/再起動

このアクションは、1 つまたは複数のエンドポイントに対して実行できます。

ターゲットのエンドポイントがインバンド接続の場合、インバンドの電源操作がエンドポイントのオペレーティング・システムを介して実行されます。ターゲットがインバンド接続でないが、完全なインテル® AMT 構成レコードを持つ場合、関連付けられたインテル® AMT 電源アクション (ディープスリープ、ハイバネート、ソフト電源オフ、ソフト電源サイクル) が実行されます。

エンドポイントを 1 つだけ選択し、以下のいずれかの条件が成立した場合、アクションは実行されません。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。

6.4.3 アラートの送信

1 つまたは複数のエンドポイントに、アラートメッセージをポップアップ・ウィンドウとして (インバンド接続を介して) 送信できます。

アラートを送信するには、表示するメッセージを入力し、メッセージを表示する時間の長さを選択し、Send (送信) をクリックします。

エンドポイントを 1 つだけ選択し、以下のいずれかの条件が成立した場合、アクションは実行されません。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。
- エンドポイントがインテル® EMA にインバンド接続されていない。

6.4.4 リモートファイル検索

1 つまたは複数のエンドポイントに対して、リモートファイル検索を (インバンド接続を介して) 実行できます。ファイル検索は Windows* の検索インデックスに依存します。

検索する文字列を入力し、Search (検索) をクリックします。結果ファイルをダウンロードするには、ファイルをクリックします。

エンドポイントを 1 つだけ選択し、以下のいずれかの条件が成立した場合、アクションは実行されません。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。
- エンドポイントがインテル® EMA にインバンド接続されていない。

6.4.5 エンドポイントの管理の停止

ターゲットのエンドポイントをインテル® EMA から削除できます。ただし、これはエンドポイントが将来的にインテル® EMA に再接続し再登録することを妨げるものではありません。また、システムはプロビジョニングされたままです。

このアクションは、次の両方の条件が成立する場合にのみ有効化されます。

- エンドポイントが 1 つだけ選択されている。
- ログイン中のユーザーが選択したエンドポイントに対する実行権限を持っている。

6.4.6 イメージのマウント

保存されたイメージファイル (.iso または .img) を、USB リダイレクト (USBR) を介して現在のエンドポイントにマウントします。USBR の詳細については、セクション 1.2.8 を参照してください。このメニューオプションには、エンドポイントの Details (詳細) ページからのみアクセスできます。

注記：ターゲット・エンドポイントのインテル® AMT ファームウェアがクライアント・コントロール・モード (CCM) でプロビジョニングされた場合、または管理者コントロール・モード (ACM) で Consent Required (同意を要求) をオンにしてプロビジョニングされた場合、エンドポイントにイメージをマウントする前に、Intel® AMT (インテル® AMT) タブの KVM で、ターゲット・エンドポイントのユーザーから同意を得る必要があります。Intel® AMT (インテル® AMT) タブからエンドポイントに KVM セッションを開始すると、User Consent Code (ユーザー同意コード) がエンドポイントのユーザーに表示されます。User Consent Code (ユーザー同意コード) を入力すると、そのエンドポイントにイメージをマウントできるようになります。CCM と ACM の詳細については、セクション 1.2.7 を参照してください。Intel® AMT (インテル® AMT) タブについては、セクション 6.3.2 を参照してください。さらに、ACM、CCM、ユーザー同意の詳細については、インテル® AMT の資料 (https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm) が参考になります。

Endpoint Actions (エンドポイント・アクション) ドロップダウン・リストから **Mount an Image (イメージのマウント)** を選択して、マウントする保存済みイメージを選択し、**Start (開始)** をクリックしてイメージをマウントします。アクションが完了したら、エンドポイントの Details (詳細) ページの左下に、そのエンドポイントへのアクティブな USBR セッションとマウントされたイメージファイル名を示す **Storage Redirection (ストレージ・リダイレクト)** バナーが表示されます。

イメージファイルのマウントを解除するには、Details (詳細) ページの **Storage Redirection (ストレージ・リダイレクト)** バナーの下にある **Unmount Image (イメージのマウント解除)** をクリックします。

イメージファイルのアップロードと保存の詳細については、セクション 7 を参照してください。

6.4.6.1 イメージに関する推奨事項

エンドポイントがマウントされたイメージを使用して再起動する間のタイムアウトを防止するため、可能な限りサイズの小さいイメージを使用してください。さらに、再起動後のエンドポイントを KVM 経由で操作するには、起動するイメージに USB キーボードおよびマウスのドライバーを含める必要があります。

マウントされたイメージを使用してエンドポイントを再起動する際は、2 分割のイメージを使用することを推奨します。まず、ネットワーク上でエンドポイントを起動できる、小さいイメージでエンドポイントを起動します。次に、そのイメージを使用して、エンドポイントからより多くのコンテンツにアクセスします。

注記：インテル® AMT による USBR を介した一部の UDF フォーマット・イメージの起動には、既知の問題があります。UDF フォーマットのイメージが起動されない、あるいは完全に起動されないことがあります。この問題が解消されるまでは、CDFS フォーマットのイメージを使用することを推奨します。

6.4.6.2 指定したイメージを使用した起動

選択したエンドポイントをマウントされたイメージファイル (.iso または .img) を使用して再起動します。

注記：このアクションを実行するには、事前にイメージファイルをエンドポイントにマウントする必要があります。イメージファイルのマウントの詳細については、セクション 6.4.6 を参照してください。

そのエンドポイントにイメージをマウントしたら、Details (詳細) ページの **Storage Redirection (ストレージ・リダイレクト)** の下の **Boot to this Image (このイメージを使用して起動)** をクリックします、

注記：BIOS のセキュアブートによって署名なしのイメージの読み込みがブロックされるため、署名済みのイメージファイルの使用を推奨します。セキュアブートによってイメージの読み込みがブロックされた場合、エンドポイントは内部ドライブで起動することがあります。

エンドポイントの起動処理が成功したかどうかを検証するには、Intel® AMT (インテル® AMT) タブを使用して、再起動したエンドポイントで KVM セッション (リモート・デスクトップ) を実行し、エンドポイントが選択したイメージで起動したことを確認します。イメージには、KVM 操作向けに USB キーボードおよびマウスのドライバーを含める必要があります。

6.4.7 インテル® AMT のプロビジョニング

インテル® AMT のプロビジョニング情報を開きます。詳細については、セクション 3.5 を参照してください。

このアクションは、以下のすべての条件が成立する場合にのみ有効化されます。

- エンドポイントが 1 つだけ選択されている。

- 選択したエンドポイントがインテル® AMT に対応している。
- 選択したエンドポイントがインテル® EMA にインバンド接続されている。
- ログイン中のユーザーが選択したエンドポイントに対する実行権限を持っている。

6.4.8 デスクトップの表示

1 つまたは複数のエンドポイントの複数のリモート・インバンド KVM を (リモート入力制御なしに) 表示できます。

注記: この機能の動作は、インバンド KVM に対するユーザーの同意による影響を受けます。詳細については、セクション 3.4.1 を参照してください。

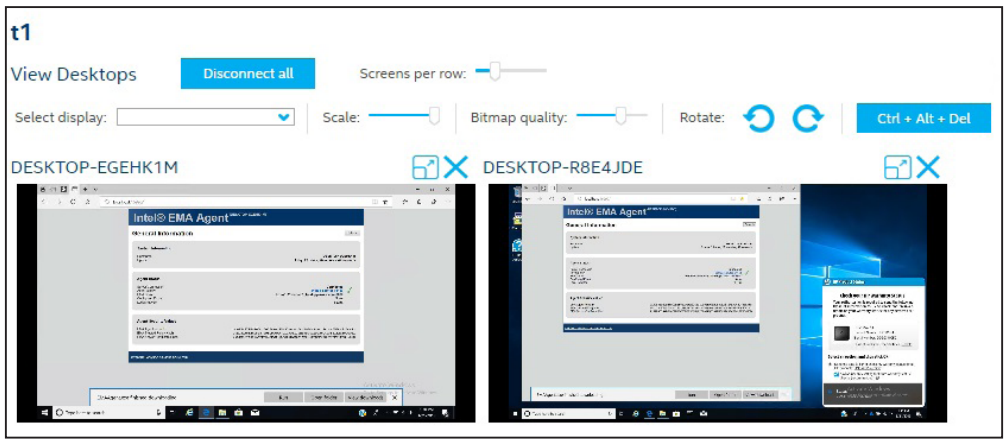
エンドポイントを 1 つだけ選択し、以下のいずれかの条件が成立した場合、アクションは実行されません。

- そのアクションがエンドポイント・グループ・ポリシーで許可されていない。
- ログイン中のユーザーがそのエンドポイントに対する実行権限を持っていない。
- エンドポイントがインテル® EMA にインバンド接続されていない。

エンドポイントのターゲット KVM を選択します。ターゲット・エンドポイントが強調表示されたら、ディプレイ設定を変更し、そのターゲット KVM に対して **Ctrl+Alt+Del** を押せます。

各 KVM の展開ボタンをクリックして、そのエンドポイントに対する Remote KVM (リモート KVM) タブを開くこともできます。

図 11 : マルチデスクトップ表示



7　ディスクイメージの管理

ロール：テナント管理者

インテル® EMA では、起動可能ディスク・イメージ・ファイル (*.iso および *.img) をアップロードし、保存できます。デフォルトのイメージファイルの保存場所は、**USBR Images Root Directory (USBR イメージのルート・ディレクトリー)** の Manageability Server (管理機能サーバー) の設定を編集することで定義できます。コンポーネント・サーバーの設定 (Manageability Server (管理機能サーバー) 配下) の更新については、セクション 9「付録 - コンポーネント・サーバーの設定変更」(45 ページ) を参照してください。

注記：インテル® EMA の自動クリーンアップ・プロセスにより、USBR ルート・ディレクトリー内にある、インテル® EMA 以外によって作成されたフォルダーおよびファイルは定期的に削除されます。このクリーンアップ・プロシージャー **fileuploadcleanup** を手動で実行することもできます (「インテル® EMA シングル・サーバー・インストール・ガイド」の「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」を参照してください)。

USBR 機能の詳細については、セクション 1.2.8 を参照してください。

7.1　イメージファイルのアップロード

ディスク・イメージ・ファイルをアップロードする手順は次のとおりです。

1. 左側のナビゲーション・バーで **Storage (ストレージ)** を選択し、**Disk Images (ディスクイメージ)** タブをクリックします。
2. **Upload (アップロード)** ボタンをクリックします。
3. **Upload Image File (イメージファイルのアップロード)** ダイアログで、オプションで **Description (説明)** を入力し、**Choose File (ファイルの選択)** をクリックします。
4. 目的のファイルを参照して選択し、**Open (開く)** をクリックします。ダイアログに、ファイルサイズと、デフォルトのイメージファイル保存場所の利用可能なディスク容量が表示されます。USBR イメージのルート・ディレクトリーの設定 (Manageability Server (管理機能サーバー) 配下) の更新については、セクション 9「付録 - コンポーネント・サーバーの設定変更」(45 ページ) を参照してください。

   注記：選択したファイルのサイズが利用可能なディスク容量より大きい場合、エラーメッセージが表示され、**Upload (アップロード)** ボタンは無効化されます。
5. **Upload (アップロード)** をクリックします。進捗状況バーが表示されます。アップロードをキャンセルするには、**Cancel (キャンセル)** をクリックします (キャンセルを確認するメッセージが表示されます)。
6. ファイルのアップロードが完了したら、**Done (完了)** をクリックします。アップロードしたファイルが保存済みファイルのリストに表示されます。

7.2　保存されたイメージファイルの編集と削除

アップロードしたイメージファイルを編集したり削除したりできます。手順は次のとおりです。

1. 左側のナビゲーション・バーで **Storage (ストレージ)** を選択し、**Disk Images (ディスクイメージ)** タブをクリックします。
2. **Storage (ストレージ)** ページのファイルリストで、編集または削除するファイルの行にある省略記号 (**...**) をクリックし、ドロップダウン・メニューで **Edit (編集)** か **Delete (削除)** を選択します。**Delete (削除)** を選択すると、確認メッセージが表示されます。**Edit (編集)** を選択すると、ダイアログボックスが表示されます。使用中のイメージファイルを削除したり名前変更することはできません。
3. エディター・ダイアログ・ボックスで、必要に応じてファイル名や **Description (説明)** を編集します。

   注記：ファイル名に使用できる拡張子は .img と .iso のみです。
4. **Save (保存)** をクリックして変更を保存し、**Storage (ストレージ)** ページに戻ります。

7.3 アクティブなセッションの表示および管理

現在のテナントでアクティブなセッションを表示および管理するには、左側のナビゲーション・バーで **Storage（ストレージ）**を選択し、**Active Sessions（アクティブなセッション）**タブをクリックします。

アクティブなセッションのリストには、以下の情報が表示されます。

Endpoint Name（エンドポイント名）	エンドポイントの名前。
File name（ファイル名）	ストレージ・リダイレクトによって、現在エンドポイントにマウントされているイメージファイル。
Idle Time（アイドル時間）	セッションがアイドル状態であった時間の長さ。
Session Length（セッション長）	セッションが開始されてからの合計時間。
User（ユーザー）	セッションを開始したユーザー。
End Session（セッションを終了）	そのエンドポイントのセッションを切断するリンクをクリックします。

アクティブなリダイレクト・セッションを切断するには、表のターゲット・エンドポイントの行で **End session（セッションを終了）**をクリックします。アクションを確認するメッセージが表示されます。

7.4 イメージに関する推奨事項

エンドポイントがマウントされたイメージを使用して再起動する間のタイムアウトを防止するため、可能な限りサイズの小さいイメージを使用してください。さらに、再起動後のエンドポイントを KVM 経由で操作するには、起動するイメージに USB キーボードおよびマウスのドライバーを含める必要があります。

マウントされたイメージを使用してエンドポイントを再起動する際は、2 分割のイメージを使用することを推奨します。まず、ネットワーク上でエンドポイントを起動できる、小さいイメージでエンドポイントを起動します。次に、そのイメージを使用して、エンドポイントからより多くのコンテンツにアクセスします。

注記：インテル® AMT による USBR を介した一部の UDF フォーマット・イメージの起動には、既知の問題があります。UDF フォーマットのイメージが起動されない、あるいは完全に起動されないことがあります。この問題が解消されるまでは、CDFS フォーマットのイメージを使用することを推奨します。

8　付録：トラブルシューティング

インテル® EMA ウェブサイトにログインできない	インテル® EMA ウェブサイト・ユーザー・インターフェイス (UI) は Cookie を使用します。ブラウザーの Cookie を無効化すると、インテル® EMA ウェブサイト UI は動作しません。
インテル® EMA エージェントがインテル® EMA サーバーに接続できない	インテル® EMA エージェントのトラブルシューティングについては、セクション 4.5 を参照してください。
エンドポイント・リストのウェブページにエンドポイントが表示されない	エンドポイント・リストのウェブページにエンドポイントが 1 つも表示されない場合、以下を行います。 1. セクション 1.2 を理解していること、現在のログイン・ユーザー・アカウントがターゲット・エンドポイントに対して正しいアクセス権を持つことを確認します。 2. インテル® EMA エージェントをターゲット・エンドポイントにインストールするとき、正しいエンドポイント・ポリシーファイルを使用していることを確認します。 3. 上記に問題がない場合、上述の**インテル® EMA エージェントがインテル® EMA サーバーに接続できない**の手順を行ってください。
KVM に真っ黒な画面が表示される	インテル® AMT KVM に接続すると、物理的モニターが接続されていない場合、真っ黒な画面が表示される。 エンドポイントがヘッドレスの場合、オペレーティング・システム経由でのリクエストがない場合、グラフィックス・プロセシング・ユニット (GPU) がオフになります。その場合、エンドポイントを再起動するか、BIOS 起動したときに接続済みのモニターが検出されず、真っ黒な何もない画面が表示されます。
インテル® EMA エージェント – アンインストールまたは更新中のエラー	サービスをアンインストールする、または既存のインストール上にサービスをインストール/更新するには、既存のインテル® EMA エージェントと同じアーキテクチャー・タイプ (32 ビット・サービスか 64 ビット・サービス) を持つインテル® EMA エージェント・インストーラーが必要です。
インテル® EMA エージェントのログ	インテル® EMA エージェントで以下のログが作成されます。 • エージェント実行中に発生したエラーに関する一般的なログ • デバッグ情報用のデバッグログ • インストール/アンインストール・プロセス中に検出されたエラーに関するインストール・ログ **インテル® EMA エージェントの一般的なエラーのログ** 一般的なログはデフォルトで有効化されており、インテル® EMA エージェント・サービスのエラーをレポートします。ファイル名は **EmaAgent.log** です。 **EmaAgent.log** ファイルはインテル® EMA エージェントのインストール・ディレクトリーにあり、win32 では **Program Files x86** フォルダー、win64 では **Program Files** フォルダーです。 ログには、エラーの日時、エラーのパスとファイル名、行番号、パラメーター、エラーの簡単な説明が含まれます。

	ログファイルのシンタックス： [日時] ファイルパス：行番号 (パラメーター 1、パラメーター 2) メッセージ **インテル® EMA エージェントのインストール・ログ** このログはインストール/アンインストール処理中にエラーが検出されたときに生成されます。ログファイルの名前は、使用されたインストーラーに基づき、インストーラーと同じフォルダーに配置されます。インストール/アンインストール処理中にエラーが検出されない場合、ログは作成されません。 **注記：**特定のエラーメッセージ「Error removing the installation directory file (インストール・ディレクトリー・ファイルの削除エラー)」に対応するには、アンインストール時にインストール・ディレクトリー内に開いているファイルまたは保護されたファイルが存在しないことを確認します。アンインストールを開始する前に、必ずすべてのファイルを閉じます。
インテル® EMA により、エンドポイントが別のツールによって管理されているというメッセージが出る	エンドポイントが現在、別の管理アプリケーションによって管理されている可能性があります。インテル® EMA で管理できるようにするには、そのエンドポイントのプロビジョニングを解除してから、インテル® EMA を使用して再プロビジョニングする必要があります。プロビジョニング解除の詳細については、インテル® AMT の資料 (下記) を参照してください。 https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm
Windows Server* 2012 または 2016 で PKI 証明書のインポートが失敗する	Windows Server* 2012 または 2016 (ビルド 1709 より前) が動作するマシンにインテル® EMA サーバーをインストールした場合、証明書 PFX ファイルに「AES256-SHA256」暗号化が使用されている場合、インテル® EMA への証明書のアップロードが失敗します。有効なパスワードが提供されていたとしても、無効なパスワードのエラーが表示されます。 これは、Windows* 自体がこの暗号化を使用した PFX ファイルをサポートしていないことによる Windows* の問題です。この問題は、Windows Server* 2016 ビルド 1709 以降では修正されています。 https://github.com/dsccommunity/CertificateDsc/pull/154/files **対策：** 1. PFX ファイルを 暗号化「AES256-SHA256」を使用する PFX ファイルをサポートするシステムに (Windows* 10 デスクトップなど) にインストールします。そのためには、PFX ファイルをダブルクリックして Certificate Import Wizard (証明書インポートウィザード) を開きます。デフォルトでは、現在ログイン中のユーザーの個人証明書ストアにインストールされます。必ず **Mark this key as exportable (この鍵をエクスポート可能としてマーク)** と **Include all extended properties (すべての拡張プロパティーを含める)** をオンにします。 2. 現在のユーザー 証明書で Microsoft* 管理コンソールを開きます。 3. インストールした証明書を右クリックし、**All Tasks (すべてのタスク) > Export....(エクスポート)**を選択します。Certificate Export Wizard (証明書エクスポート・ウィザード) 4. ウィザードで **Yes、export the private key (はい、秘密鍵をエクスポートします)** を選択し、**Next (次へ)** をクリックします。

	5. **Personal Information Exchange (.PFX)** を選択し、**Include all certificates in path (パスにすべての証明書を含める)**、**Export all extended properties (すべての拡張プロパティーをエクスポートする)**、**Enable certificate privacy (証明書プライバシーの有効化)** を選択します。必要に応じて、**Delete the private key if successful (成功したら秘密鍵を削除)**を選択します(中間システムから証明書と鍵を削除する場合)。**Next(次へ)**をクリックします。 6. セキュリティー画面の **Encryption(暗号化)**で TripleDES-SHA1 を選択します。古いバージョンの Windows* では「AES256-SHA256」の PFX ファイルをサポートしていないのが根本的な原因です。この暗号化は実際の証明書に対するものではなく、画面上に提供されるパスワードとともに使用され、PFX ファイル形式にエクスポートされるときに、証明書に関連付けられた秘密鍵を保護します。 7. エクスポート・ウィザードを終了し、新しい PFX ファイルを作成します。この新しい PFX ファイルは、インテル® EMA サーバーをインストールした古い Windows* システムでも問題なく使用できます。

9　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。

9.1　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。

9.2 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)。
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)。

9.3 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。

設定	説明
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。
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、データレータをスロットルするために必要になります。

設定	説明
	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。 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。

9.4 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。

10 付録 - インテル® AMT 検出

ロール：テナント管理者

10.1 概要

インテル® AMT 検出は、ネットワーク・アダプターの IP アドレス宛に RMCP (Remote Management and Control Protocol) タイプの ping を送信して、ネットワーク内でインテル® AMT 対応エンドポイントを識別するプロセスです。インテル® EMA の管理機能サーバーは、管理機能サーバーがインストールされているマシンのネットワーク・アダプターを使用して RMCP ping を送信しています。

検出には主に 2 つのタイプがあります。

- **Manual (手動)：**このタイプの検出では、同じタイプとパラメーターを使用した 2 つ以上の同時検索が可能です。このタイプの検出のセットアップと結果は、実行するテナントに固有です。
- **Automatic (自動)：**このタイプの検出は、一度に 1 プロセスずつのみ実行されます。有効にするとプロセスが定期的に実行されます。このタイプの検出のセットアップと結果は、すべてのテナントに共有されます。

いくつか制限事項があります。

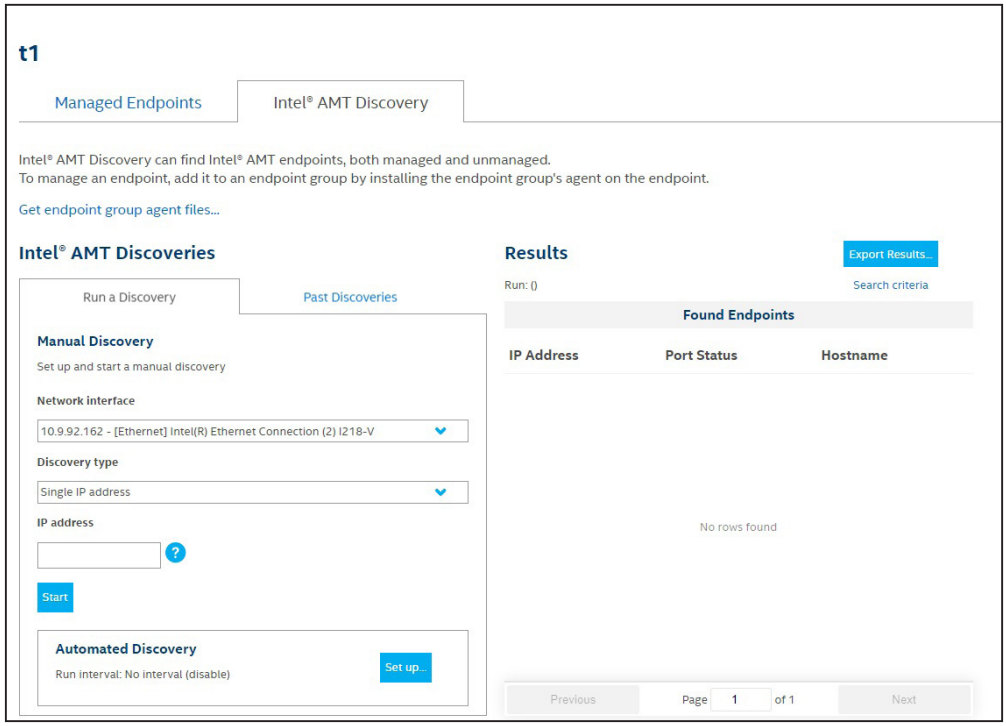
- エンドポイントはイーサネット・ポートを介して接続しなければならない。
- インテル® AMT は IP アドレスを取得できなければならない。
- 一部のインテル® AMT プロビジョニング・プロセスでは、IP 設定を自動取得するために有線接続が設定される。つまり、インテル® AMT はホスト・オペレーティング・システムでネットワーク・インターフェイスに設定された静的 IP アドレスと異なる IP アドレスを持つ。
- クラウドベースのインテル® EMA インストールを使用している場合、検出機能ではクラウド・ホスティング環境のローカル・ネットワークが検索される。インターネット上のデバイスは検出されない。
- CIRA モードで実行されるよう構成されたエンドポイントは、エンドポイントに同時に実行される CIRA 接続がある場合、結果を返さないことがある。CIRA 接続は、検出中にインテル® AMT にクエリーを行うために使用されるネットワーク・ポートを無効化する。

10.2 検出の管理

一般的な使用例は次のとおりです。

- 新しい検出の作成：以下の図に示すページを使用して、手動検出を実行するか、自動検出をセットアップできます。インテル® EMA の 1 つのインストールについて、サポートされる自動検出セットアップは 1 つだけであることに注意してください。新しいセットアップを作成すると、前のセットアップが置き換えられます。
- 過去の検出のチェック：Past Discoveries (過去の検出) サブタブをクリックして、履歴を確認します。選択した過去の検出の結果が、ページの右側に表示されます。自動検出では、最新の結果のみが保存されることに注意してください。

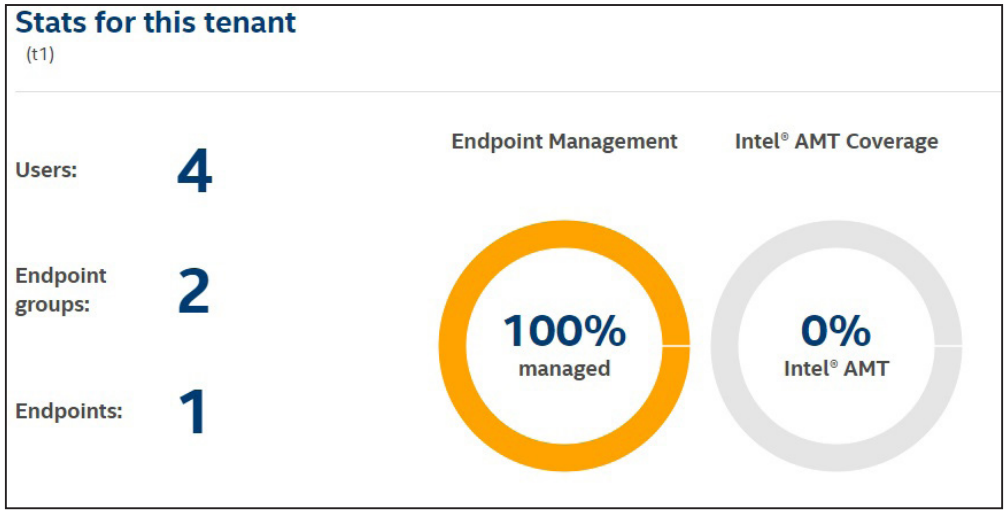
図 12：インテル® AMT 検出



11 付録 - テナント統計情報の計算方法

テナント管理者ユーザーの Overview (概要) ページには、現在管理されているエンドポイントの割合、インテル® AMT が構成およびアクティブ化されているインテル® AMT 対応デバイスの割合に関する統計情報が表示されます。

図 13：テナントの Overview (概要) ページの統計情報



Endpoint Management (エンドポイント管理) のパーセント値は以下の式で計算されます。

C1 / (C1 + C2)

- C1：インテル® EMA エージェントを介してインテル® EMA サーバーに接続されているエンドポイントの数。
- C2：インテル® EMA サーバーの自動検出および手動検出によって検出された、インテル® AMT 機能を備えるエンドポイントの数。

注記：オペレーティング・システムが使用する IP アドレスと、インテル® AMT ファームウェアが使用する IP アドレスは異なることがあります。その結果、同じエンドポイントが C1 と C2 の両方でカウントされることがあります。そのため、統計表示は概算値です。

Intel® AMT Coverage (インテル® AMT カバレージ) のパーセント値は以下の式で計算されます。

C3 / C1

- C1：インテル® EMA エージェントを介してインテル® EMA サーバーに接続されているエンドポイントの数。
- C3：C1 のうち、インテル® AMT でプロビジョニング/セットアップされたエンドポイントの数。

12 付録 - インテル® EMA エージェント・コンソール Win32 および Win64

インテル® EMA エージェントは通常、サービスとしてインストールされ、実行されます。しかしながら、コンソールまたはスタンドアロンの実行可能アプリケーションとして実行することも可能です。これは、エージェントをインストールしてサービスとして実行するのではなく、手動で「オンデマンド」でエージェントを実行する場合に役立ちます。機能は、サービスのバージョンと変わりません。

インテル® EMA エージェント・コンソールは、インテル® EMA API からダウンロードできます。

注記：

- 使用先のシステムに合わせて、適切なエージェント・コンソール・バージョン (32 ビットまたは 64 ビット) を使用する必要があります。
- エージェント実行ファイルのコンソール・バージョンは、サービスバージョンと同じファイル名 (EmaAgent.exe) を持ちます。そのため、すでにサービスとしてインストールされたエージェントを含むシステムにコンソール・エージェントをダウンロードする場合、サービス・エージェントが上書きされないよう、必ずコンソールバージョンの名前を変更してください。
- エージェント・コンソールは、コマンド・ライン・ツールであり、グラフィカル・ユーザー・インターフェイスは持ちません。
- エージェント・コンソールは、サービス・バージョンと同じように、エージェント・インストールのトラブルシューティングに使用できます。詳細については、セクション 4.5 を参照してください。

12.1 ファイル

インテル® EMA エージェントをコンソールまたはスタンドアロンの実行可能アプリケーションとしてインストールするには、2 つのファイルが必要です。これらのファイルのプロパティーを次の表で説明します。これらの 2 つのファイルは同じディレクトリーに配置する必要があります。エージェント・コンソール・アプリケーションは、ダウンロード先システムのアーキテクチャーに合わせて、適切なフォルダーに配置してください (C:\Program Files (x86)\Intel\Ema Agent or C:\Program Files\Intel\Ema Agent)。

表 2：ファイルのプロパティー

ファイル名	説明
EmaAgent.exe	エージェントのインストール・ファイルです。インスタンスをインストール/更新/アンインストールするには、このファイルを管理者権限で実行する必要があります。
EmaAgent.msh	ポリシーファイルです。このファイルによってエンドポイントが属するエンドポイント・グループが決定され、インテル® EMA エージェントがインテル® EMA サーバーに通信できるようになります。

インテル® EMA エージェントをコンソールとして実行するには、管理対象のエンドポイント・システムで次の手順を行います。

1. 管理者権限でコマンドウィンドウ (cmd.exe) を開き、インテル® EMA エージェント コンソールの実行可能ファイルがあるパスに移動します。
2. 次のコマンドを実行し、コンソールモードでインテル® EMA エージェントを開始します (ファイル名を変更した場合は、そのファイル名を使用してください)。

   ```
   EmaAgent.exe
   ```

3. コンソールモードのインテル® EMA エージェントを停止するには、CTRL + C のキーの組み合わせを使用します。

12.2 Windows* レジストリーの場所

エージェントのインストールによって作成されるレジストリー・キーは、Microsoft* Windows* OS とインテル® EMA エージェント (コンソールおよびサービス) のアーキテクチャーによって変わります。アーキテクチャーごとのインテル® EMA エージェントのレジストリー・パスを以下に示します。

- Win32 と EMA エージェント Win32：
  - HKEY_LOCAL_MACHINE -> “Software\Intel\EmaAgent”
- Win64 と EMA エージェント Win32：
  - HKEY_LOCAL_MACHINE -> “Software\Wow6432Node\Intel\EmaAgent”
- Win64 と EMA エージェント Win64：
  - HKEY_LOCAL_MACHINE -> “Software\Intel\EmaAgent”

12.3 インテル® EMA エージェント・データベース

エージェントのコンソールが動作を開始すると、設定と証明書の値を保存するためにローカル・データベースが生成されます。データベースは、コンソールのバイナリーフォルダーに保存されます。

現在のユーザー値は、Windows* にログ記録された実際のセッションのユーザー名です。

12.4 プロキシーの構成

コンソールモードで使用するプロキシーを構成するには、コンソール起動時にプロキシー引数を追加する必要があります。次のコマンドを実行します。

```
EmaAgent.exe -proxy:host:port
```

- ホスト：プロキシーの HTTPS ホスト名。
- ポート：プロキシーのポート番号。

12.5 リソース消費

リソース消費は、CPU、RAM、ネットワーク・トラフィックごとに分割されます。

次のすべてのテストは、有線ローカル LAN ネットワーク上で DELL 製ノートブック PC のモデル Latitude* E7270、Windows* 10 Professional 64 ビット、インテル® Core™ i5-6300 プロセッサー (2.40GHz – 2.50GHz)、16GB RAM を使用して実行されました。

CPU

- エージェントのコンソールに接続していないときの最大平均値は 0.01%。
- リモート・デスクトップ使用時の最大平均値は 5.53%。
- ターミナル使用時の最大平均値は 0.29%。これは、コンソールコマンドと ipconfig、ipconfig /all、netstat などの操作を使用した結果です。
- ファイル・マネージャー使用時の最大平均値は 3.11%。アップロードされたファイルは 133 MB です。

RAM

このセクションの値は、Windows* リソースモニターのワーキングセット (KB) の列から取得されました。

- エージェントのコンソールに接続していないときの最大平均値は 33,380 KB。
- リモート・デスクトップ使用時の最大平均値は 51,040 KB。

- ターミナル使用時の最大平均値は 33,632 KB。
    - これは、コンソールコマンドと ipconfig、ipconfig /all、netstat などの操作を使用した結果です。スクリプトのメモリー使用量が多い場合、この平均値は大幅に増加することがあります。メモリーリークのあるスクリプトを実行しないように注意してください。
- ファイル・マネージャー使用時の最大平均値は 31,180 KB。アップロードされたファイルは 133 MB です。

ネットワーク・トラフィック

- エージェントのコンソールに接続していないときの最大トラフィックを以下に示します。
    - 1 秒あたりの最大送信バイト数：137
    - 1 秒あたりの最大受信バイト数：42
    - 1 秒あたりの最大合計転送バイト数：180
- リモート・デスクトップ使用時の最大トラフィックを以下に示します。
    - 1 秒あたりの最大送信バイト数：469,925
    - 1 秒あたりの最大受信バイト数：230,886
    - 1 秒あたりの最大合計転送バイト数：700,811
- ターミナル使用時の最大トラフィックを以下に示します。
    - 1 秒あたりの最大送信バイト数：16,683
    - 1 秒あたりの最大受信バイト数：5,691
    - 1 秒あたりの合計転送バイト数：22,373
    - これは、コンソールコマンドと ipconfig、ipconfig /all、netstat などの操作を使用した結果です。スクリプトのデータ送受信量が多い場合、この平均値は大幅に増加することがあります。
- ファイル・マネージャー使用時の最大トラフィックを以下に示します。
    - 1 秒あたりの最大送信バイト数：533,827
    - 1 秒あたりの最大受信バイト数：1,040,282
    - 1 秒あたりの合計転送バイト数：1,574,109
    - アップロードされたファイルは 133 MB です。アップロード/削除するファイルのサイズとネットワーク帯域幅により、これらの値は変わることがあります。

13 付録 - マシンツーマシン・クライアント・アプリケーションからのインテル® EMA エンドポイント処理の実行

インテル® EMA API は、マシンツーマシン (M2M) アプリケーションをサポートしており、M2M クライアント・アプリケーションから直接インテル® EMA インバンドおよびアウトオブバンド・エンドポイント処理を実行できます。M2M アプリケーションをサポートするため、インテル® EMA API はクライアント資格情報認証フローを提供しています。

まず、インテル® EMA API を使用して、インテル® EMA サーバー上でクライアント資格情報アカウントを作成する必要があります。このアカウントは M2M クライアントがインテル® EMA にログインし、アクセストークンをリクエストするために使用されます。これにより、クライアントはインテル® EMA サーバー上でインテル® EMA インバンドおよびアウトオブバンド API コール (「リソース」と呼ぶ) を実行できるようになります。クライアント資格情報アカウントは特定のテナントに固有で、テナント 1 つあたりのクライアント資格情報アカウントは 1 つだけです。クライアント資格情報アカウントは、グローバル管理者ユーザーと、クライアント資格情報アカウントを作成するテナントのテナント管理者ユーザーのみが作成できます。

クライアント資格情報アカウントの作成後、M2M クライアント・アプリケーションからインテル® EMA API を呼び出してアクセストークンをリクエストする必要があります。そのため、クライアント資格情報アカウントを使用してインテル® EMA にログインします。アクセストークンには有効期限があり、その期間はクライアント資格情報アカウントの作成時に設定されます。

M2M クライアント・アプリケーションは、リクエストしたアクセストークンを受信後、インテル® EMA サーバーに API コールを実行できます。

注記：インテル® EMA API の詳細については、インテル® EMA API ガイドを参照してください。

13.1 クライアント資格情報アカウントの新規作成

新しいクライアント資格情報アカウントを作成するには、インテル® EMA サーバーにグローバル管理者またはテナント管理者としてログオンし、**POST api/v3/ClientCredentials** にインテル® EMA API を使用して、次の値を指定します。

- **client_secret** - 任意の秘密の文字列。パスワードやパスフレーズのようなものです。
- **maxFailedLogins** - クライアント資格情報アカウントがロックされるまでのログイン試行回数。
- **tokenLifetimeHours** - トークンの有効時間 (単位：時間)
- **tenantID** - クライアント資格情報アカウントを作成するテナントの ID。これはグローバル管理者のみに必要で、**api/v3/Tenants** API コールを使用して特定できます。テナント管理者の場合、値は管理者が属するテナントのテナント ID によって自動的に決まるため、必要ありません。

13.2 クライアント資格情報を使用したトークンのリクエスト

M2M クライアント・アプリケーションからクライアント資格情報アカウントを作成後、**POST /api/token** API を使用して、アクセストークンをリクエストします。**grant_type** を client_credentials にします。

トークン API コールの例を以下に示します。

```
POST /api/token

grant_type=client_credentials

&client_id=xxxxxxxxxx

&client_secret=xxxxxxxxxx
```

M2M クライアント・アプリケーションがトークン API を実行してアクセストークンを受信すると、(トークンの期限が切れるまで) インテル® EMA インスタンスに対してインバンドおよびアウトオブバンド処理のインテル® EMA API コールを直接実行できるようになります。