英特尔® Endpoint Management Assistant （英特尔® EMA）

管理和使用指南

英特尔® EMA 版本：1.12.1

文件更新日期：2024 年 1 月 10 日星期三

法律免责声明

1 简介

英特尔® Endpoint Management Assistant（英特尔® EMA）是一种软件应用程序，它提供了一种简便的方法来管理云内部和外部防火墙中基于英特尔® vPro® 平台的设备。英特尔® EMA 旨在使英特尔® 主动管理技术易于配置和使用，以便 IT 人员可以管理配备了英特尔® vPro® 平台技术的设备，而不会中断工作流程。反过来，这简化了客户管理，可以帮助降低 IT 组织的管理成本。

英特尔 EMA 及其管理控制台通过提供在云上远程安全地连接英特尔® 主动管理技术设备的能力，为 IT 提供了复杂而灵活的管理解决方案。优点包括：

- 英特尔 EMA 可以在英特尔® vPro® 平台上配置和使用英特尔® 主动管理技术进行带外硬件级管理
- 操作系统运行时，英特尔® EMA 可以使用其基于软件的代理在非英特尔® vPro® 平台上或未激活英特尔® 主动管理技术的英特尔® vPro® 平台上管理系统
- 英特尔 EMA 可以安装在本地或云中
- 您可以使用英特尔 EMA 的内置用户界面或通过 API 调用英特尔 EMA 功能

本文档介绍完成英特尔 EMA 服务器安装后如何设置和配置英特尔 EMA 以管理您的端点。它还描述了随着组织的发展和变化，如何维护和修改您的英特尔 EMA 使用环境（称为租户；请参阅下方的第 1.2.1 节）。此外，它定义了使用英特尔 EMA 的关键概念和术语，包括哪些用户角色可以在英特尔 EMA 租户环境中执行哪些任务。最后，它介绍了您可以在托管端点上执行的管理操作，并提供了执行这些操作的分步说明。

1.1 使用要求

为了使用英特尔® EMA 管理端点，需要以下组件：

- 支持的网络浏览器：Chrome* 63+（自 2017 年 12 月起）、Firefox* 52+（自 2017 年 3 月起）。
- 英特尔® 主动管理技术知识：您必须具备英特尔主动管理技术解决方案的一般知识。您应该知道适当的设置/配置方法和各种控制模式。英特尔 EMA 仅支持英特尔® 主动管理技术 11.8.79 或更高版本。

  注意：仅当您计划使用带外功能时，才需要英特尔® 主动管理技术知识（请参阅第 1.2.6 节）。

有关英特尔主动管理技术的其他信息，请参阅以下文档：

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

1.1.1 代理必备条件

注意： 英特尔 EMA 代理并不适合在目标端点上的 VM 中运行，即使在基础管理程序上也是如此。LAN/WLAN 无法正确解读多个 IP 地址。未写入任何管理程序以适应使用英特尔主动管理技术所需的地址转换。这会影响代理连接到英特尔主动管理技术和在端点上执行带外 (OOB) 操作的能力。在这种情况下，或许可以有效执行带内操作，但并不确定。

以下是设置英特尔 EMA 代理所需的必备条件的列表：

- **操作系统：** Microsoft Windows 10 和 Windows 11（64 位操作系统）都正式支持英特尔® EMA 代理。32 位代理已弃用，并且将不再发布。运行 32 位代理的系统应该进行更新（手动更新程序）。
- **防火墙：** 安装英特尔 EMA 代理后，它将为已安装的代理二进制进程设置以下 Windows 防火墙入站规则。如果使用其他防火墙，请确保为已安装的代理二进制进程设置了以下入站规则：
  - 点对点流量：阻止本地端口为 16990 的 UDP、本地和远程地址的任何 IP 以及边缘遍历。
  - 点对点流量：阻止本地端口为 16990 的 TCP、本地和远程地址的任何 IP 以及边缘遍历。
  - 本地环回管理流量：阻止本地端口为 16991 的 TCP、本地和远程地址 127.0.0.1 以及边缘遍历。

- **英特尔® 主动管理技术：** 英特尔 EMA 仅支持英特尔® 主动管理技术 11.8.79 或更高版本。只有在进行带外端点管理时才是必需的。 请参阅下方的第 1.2.6 节。
  下表列出了在端点上使用 USBR over CIRA 所需的最低英特尔主动管理技术版本。

英特尔主动管理技术版本	版本号
英特尔主动管理技术 11	11.8.79 或更高版本
英特尔主动管理技术 12	12.0.70.1607 或更高版本
英特尔主动管理技术 14	14.0.45.1341 或更高版本
英特尔主动管理技术 15	全部
英特尔主动管理技术 16	全部

  有关 USBR 的更多信息，请参阅第 1.2.8 节。

1.2 主要概念

以下各节描述了英特尔® EMA 解决方案中使用的主要工具、组件、角色和过程。

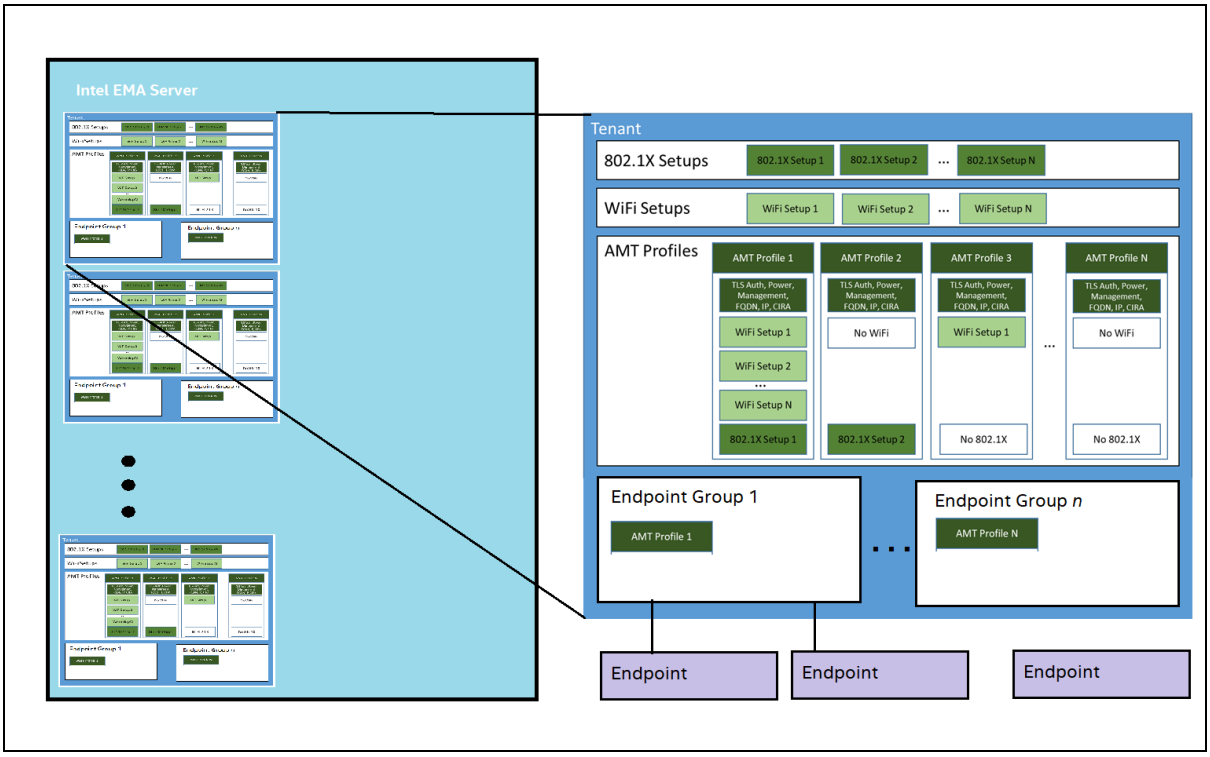
1.2.1 租户

租户是英特尔® EMA 服务器中代表业务实体的使用空间。例如，租户可以是公司，也可以是公司内的组织或办公室位置。一台英特尔 EMA 服务器可以支持多个租户。租户下的用户、端点组和端点与另一租户下的用户、端点组和端点是分离的。

注意： 英特尔® EMA 安装程序不会为初始租户创建租户管理员用户，因此您必须在安装之后使用全局管理员用户创建租户管理员用户，然后才能进行租户设置。

下图说明了英特尔 EMA 服务器与其租户之间的关系。其他概念，诸如端点组、配置文件和端点，将在后续章节中进行介绍。

图 1: 英特尔® EMA 服务器和租户



1.2.2 用户角色

一位用户只能拥有一个角色。但是，一个角色可以由多位用户执行。可用角色为：

- **全局管理员：**该角色执行用户管理、租户管理和服务器管理。全局管理员不执行端点管理，并且不（也不能）属于任何端点组。全局管理员的控制范围涵盖单个英特尔® EMA 服务器安装实例中的所有租户。
- **租户管理员：**该角色是特定租户专有的，并且可以在该租户下执行所有操作（用户管理、端点管理）。因此，租户管理员不（也不能）属于其租户中的任何用户组。租户管理员用户不能管理全局管理员用户。
- **客户经理：**该角色是特定租户专有的，并且只能执行用户管理。但是，客户经理无法管理拥有更高级别角色的用户（例如：租户管理员或全局管理员）。客户经理无法执行端点管理，因此不能属于任何用户组。
- **端点组创建者：**该角色是特定租户专有的。它可以执行端点管理，以及创建新的端点组和管理英特尔主动管理技术配置文件。端点组创建者可以是多个用户组的成员，并且可以管理它们所属的所有组。端点组创建者无法执行用户管理。但是，他们可以看到该租户中所有用户组的列表，以及所有端点组创建者和端点组用户的列表（即：该租户中的用户角色在用户角色层次结构中处于同等或较低的位置；他们看不到客户经理、租户管理员或全局管理员）。
- **端点组用户：**该角色是特定租户专有的，并且只能执行端点管理。端点组用户可以是多个用户组的成员，但是他们不能执行用户管理，只能查看自己的用户信息。

1.2.3 端点组

端点组是共享通用配置和权限的端点的集合。一个端点只能加入 1 个端点组，但可以变更至其他端点组。创建端点组时，必须指定以下通用设置：

1. 策略集：此策略集控制可以在此端点组中的端点上执行哪种操作。有关更多详细信息，请参阅第 3.4.1 节。
2. 英特尔® 主动管理技术自动设置：英特尔® EMA 将尝试使用此通用英特尔主动管理技术配置来设置加入此端点组的所有端点。

如需配置/设置端点以连接到英特尔® EMA 服务器，您需要下载并运行带有目标端点组的策略文件的英特尔 EMA 代理安装程序。然后，端点将连接到英特尔 EMA 服务器并加入此策略文件中指定的端点组。

1.2.4 用户组

用户组由用户列表（端点组创建者或端点组用户）和这些用户可以与之交互的端点组构成。一个用户可以是多个用户组的成员（下图中的用户 B）。端点组和用户必须与同一用户组关联，这样用户才能在该端点组上执行操作（用户 B 可以在端点组 2 上执行操作，因为它们都在用户组 1 中）。租户管理员用户是一个例外，他们不是任何组的成员，但仍可以在任何端点组上执行操作。

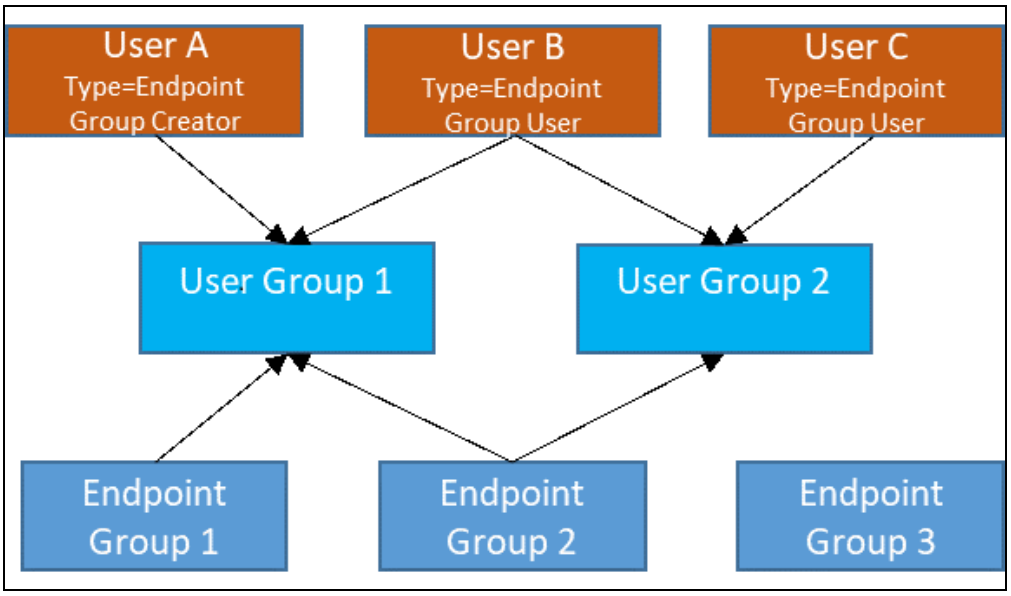
授予用户组的访问权限决定了该组成员用户可执行的操作。

- 用户组分配有特定访问权限，如桌面、终端、电源操作，USB 重定向等。您可以选择所有权限，也可为该组单独选择特定权限。

  注意：如果用户属于多个用户组，则会具有其所属的所有用户组的所有权限。例如，如果用户组 1 仅具有终端权限，但用户组 2 具有电源操作权限，则用户 B 将同时具有端点组 2 的终端和电源操作权限（该端点组同时属于这两个用户组）。但是，用户 B 将仅具有端点组 1 的终端权限（该端点组仅属于用户组 1）。

- 租户中的端点组创建者和端点组用户可以与零个或多个用户组关联。
- 租户中的端点组可以与零个或多个用户组关联。

图 2: 用户、用户组和端点组之间的关系



1.2.5 英特尔® EMA 代理

英特尔® EMA 代理 是安装于客户端端点上的软件。英特尔 EMA 代理可帮助客户端端点连接到英特尔 EMA 服务器，从而使英特尔 EMA 服务器可以管理端点。代理实际上由两个文件组成，即 EmaAgent.exe 和 EmaAgent.msh，托管端点上必须存在这两个文件，代理才能正常工作（请参阅第 4 节）。

代理还具有命令行界面，可用于显示有关代理与服务器的连接的基本信息。在代理部署期间对端点连接进行故障排除时，这将很有帮助。请参阅第 4.5 节获取详细信息。

1.2.5.1 代理必备条件

注意： 英特尔 EMA 代理并不适合在目标端点上的 VM 中运行，即使在基础管理程序上也是如此。LAN/WLAN

无法正确解读多个 IP 地址。未写入任何管理程序以适应使用英特尔主动管理技术所需的地址转换。这会影响代理连接到英特尔主动管理技术和在端点上执行带外 (OOB) 操作的能力。在这种情况下，或许可以有效执行带内操作，但并不确定。

以下是设置英特尔 EMA 代理所需的必备条件的列表：

- **操作系统：** Microsoft Windows 10 和 Windows 11（64 位操作系统）都正式支持英特尔® EMA 代理。32 位代理已弃用，并且将不再发布。运行 32 位代理的系统应该进行更新（手动更新程序）。
- **防火墙：** 安装英特尔 EMA 代理后，它将为已安装的代理二进制进程设置以下 Windows 防火墙入站规则。如果使用其他防火墙，请确保为已安装的代理二进制进程设置了以下入站规则：
  - 点对点流量：阻止本地端口为 16990 的 UDP、本地和远程地址的任何 IP 以及边缘遍历。
  - 点对点流量：阻止本地端口为 16990 的 TCP、本地和远程地址的任何 IP 以及边缘遍历。
  - 本地环回管理流量：阻止本地端口为 16991 的 TCP、本地和远程地址 127.0.0.1 以及边缘遍历。
- **英特尔® 主动管理技术：** 英特尔 EMA 仅支持英特尔® 主动管理技术 11.8.79 或更高版本。只有在进行带外端点管理时才是必需的。 请参阅下方的第 1.2.6 节。
  下表列出了在端点上使用 USBR over CIRA 所需的最低英特尔主动管理技术版本。

英特尔主动管理技术版本	版本号
英特尔主动管理技术 11	11.8.79 或更高版本
英特尔主动管理技术 12	12.0.70.1607 或更高版本
英特尔主动管理技术 14	14.0.45.1341 或更高版本
英特尔主动管理技术 15	全部
英特尔主动管理技术 16	全部

有关 USBR 的更多信息，请参阅第 1.2.8 节。

1.2.5.2 代理 Windows 注册表信息

代理安装所创建的注册表项取决于 Microsoft Windows 操作系统和英特尔 EMA 代理（控制台和服务）的架构。这些是架构提供的英特尔 EMA 代理的注册表路径：

- Win64 服务：
  - HKEY_LOCAL_MACHINE -> “Software\Intel\EmaAgent”
- Win64 控制台：
  - HKEY_CURRENT_USER -> “Software\Intel\EmaAgent”

在安装/运行英特尔 EMA 代理时，此注册表项根中应存在以下注册表项：

- **MeshId** - 包含 MSH 文件中端点组 ID 的 REG_SZ；如果不存在 MSH 文件，则该值为空。
- **MeshName** - 包含 MSH 文件中端点组名称的 REG_SZ；如果不存在 MSH 文件，则该值为空。
- **NodeId** - 包含端点 ID 的 REG_SZ。

  注意： 端点 ID 与代理根证书相关联。服务/控制台使用不同的根证书。

- **Version** - 包含正在运行的 EmaAgent 的版本号的 REG_DWORD。
- **EnhancedLoggingLevel** - 包含日志记录级别的 REG_DWORD。默认情况下，此项设置为 3，这会禁用增强型调试日志记录。要启用增强型调试日志记录，请编辑注册表并将 EnhancedLoggingLevel 设置为 4。

1.2.6 带内与带外

英特尔® EMA 代理 在托管端点上的操作系统中运行。我们将此连接称为“带内”连接。依赖此连接的所有功能都称为带内功能。依赖于英特尔® 主动管理技术的所有功能都称为带外功能。

注意：带内功能要求在托管端点上运行正常的操作系统。要与操作系统不起作用或不存在的端点进行交互，必须通过英特尔® 主动管理技术使用带外连接。

一旦在端点上设置了英特尔® 主动管理技术，英特尔 EMA 就可以通过以下方法之一与英特尔® 主动管理技术进行对话：

- **TLS 中继：**通过这种方法，其他英特尔 EMA 代理 将英特尔主动管理技术命令中继到目标端点上的目标英特尔主动管理技术。要成为中继，代理必须位于同一子网中并注册到同一端点组。端点重新启动时，其代理会广播到组/子网中的其他英特尔 EMA 代理，并与其“邻居”建立联系以进行 TLS 中继。当英特尔 EMA 代理与目标英特尔主动管理技术通信时，它将使用英特尔主动管理技术 TLS 端口。这就是它被称为 TLS 中继的原因。
- **英特尔® 主动管理技术 CIRA（客户端发起的远程访问）：**英特尔主动管理技术 CIRA 可用于 DHCP 或静态 IP 地址。在这种方法中，端点系统的英特尔主动管理技术通过端口 8080 的 TCP TLS 连接功能连接到英特尔 EMA 服务器（请注意，带内英特尔 EMA 代理也通过端口 8080 的 TCP TLS 连接到英特尔 EMA 服务器）。英特尔主动管理技术 CIRA 会创建自己的加密隧道，因此不需要额外的 TLS。启用 CIRA 或重启端点系统后，英特尔® 主动管理技术会尝试多次连接。然而如果所有尝试均失败，则英特尔® 主动管理技术将不会继续尝试连接，直到下次重新启动端点系统。但是一旦连接，CIRA 将维持英特尔 EMA 服务器与端点之间的通信，以便端点始终可以访问服务器。

  如果将英特尔主动管理技术配置文件设置为使用 DHCP，则英特尔主动管理技术 CIRA 将使用英特尔主动管理技术的“环境检测”功能。当端点系统的网络域与配置的 CIRA 域匹配时，英特尔主动管理技术将不会启动 CIRA 连接。在这种情况下，英特尔 EMA 服务器使用类似于 TLS 中继的通信方法。使用静态 IP 地址时，将忽略“环境检测”功能，并且 CIRA 始终连接。

  使用 DHCP 时，您可以在创建英特尔主动管理技术的配置文件时选择 "Always Use Intel AMT CIRA" 或在常规设置下 CIRA 内部网后缀字段中输入伪造的域后缀，从而强制英特尔主动管理技术始终打开 CIRA 隧道。这个伪造的域后缀应该足够复杂，防止任何人猜中，从而使用它来阻止 CIRA 连接并打开本地管理端口。请参阅第 3.4.1 节。

1.2.7 英特尔® EMA 中的英特尔® 主动管理技术设置/设置流程

本节介绍为托管端点系统启用英特尔® 主动管理技术自动设置（第 3.6 节）或手动执行英特尔主动管理技术的按需设置（第 6.1 节）时以编程方式发生的情况。

注意： 英特尔® 主动管理技术设置也称为配置。

英特尔® EMA 使用**基于主机的配置 (HBC)** 在您的端点上配置英特尔主动管理技术。HBC 通过端点的操作系统在带内执行。如果您没有上传公钥基础架构 (PKI) 证书，则英特尔 EMA 在端点上将英特尔主动管理技术设置为客户端控制模式 (CCM)。使用 CCM 时存在一些限制，例如需要在每个端点上征得用户同意才能执行某些英特尔 EMA 的远程连接功能。上传 PKI 证书可使英特尔 EMA 将端点的英特尔主动管理技术设置为管理员控制模式 (ACM)。无局域网端点需要手动更新（参见下面的第 1 轮）。PKI 证书和 ACM 的附加安全性使英特尔 EMA 可以与端点的英特尔主动管理技术连接并执行远程操作，而无需用户同意。英特尔主动管理技术配置文件以及为它们上传 PKI 证书在第 3.4 节中进行了讨论。

注意：有关基于主机的配置、客户端控制模式和管理员控制模式的更多信息，请参阅英特尔® 主动管理技术文档。https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm

配置/设置分为 2 轮。

1. **第 1 轮：** 将端点设置为客户端控制模式。然后，如果您已上传 PKI 证书并在您的英特尔主动管理技术自动设置中选择 TLS-PKI 作为设置方法，则英特尔 EMA 会将端点从客户端控制模式转到管理控制模式。

注意： 对于无局域网端点，必须首先手动更新端点的英特尔 MEBX 来添加已上传 PKI 证书的 DNS 后缀，以便英特尔 EMA 将端点从客户端控制模式切换到管理员控制模式。否则，端点将保留在客户端控制模式。查看章节3.5.2了解详情。

2. **第 2 轮：**第 1 轮完成后（例如：在 CCM 或 ACM 中成功配置了英特尔主动管理技术），英特尔® EMA 会配置其他英特尔主动管理技术设置，例如电源政策、KVM 接口、CIRA 等。

如果第 1 轮失败，则英特尔 EMA 将取消配置端点，然后每三分钟自动重试该配置/设置，直到成功或直到一小时内未成功为止。

如果第 2 轮失败，则英特尔 EMA 将继续设置端点，并继续每三分钟尝试第 2 轮设置，直到成功或直到一小时内未成功为止。

注意： 对于取消配置（取消激活）英特尔® 主动管理技术，如果取消配置失败，则英特尔 EMA 将每三分钟自动重试一次，直到成功或直到一小时内未成功为止。在所有情况下（第 1 轮、第 2 轮或未配置），如果英特尔 EMA 与端点断开连接，它将在尝试重新连接至端点时重试尝试的进程。

1.2.7.1 取消配置

如果端点处于英特尔® 主动管理技术客户端控制模式，则英特尔 EMA 尝试使用英特尔 EMA 代理通过英特尔® MEI 驱动程序发出 CFG_Unprovision 命令，以将英特尔主动管理技术重置为默认出厂设置。

如果以上操作失败或端点处于英特尔主动管理技术管理员控制模式，则英特尔 EMA 向 WSMAN 发送请求 AMT_SetupAndConfigurationService\Unprovision，以将英特尔主动管理技术重置为默认出厂设置。

如果此端点组正在使用采用 802.1X 设置的英特尔主动管理技术配置文件，则英特尔 EMA 也尝试清除/删除为 802.1X 配置创建的 Active Directory 对象。

注意：

- 英特尔 EMA 实例只能取消配置的端点。由一个英特尔 EMA 实例配置的端点不能由另一个实例取消配置。请注意，分布式服务器环境中的所有服务器均被视为同一英特尔 EMA 实例。
- 英特尔 EMA 完全取消了英特尔主动管理技术的设置，并从英特尔主动管理技术设置中删除了任何自定义根证书哈希和 PKI DNS 后缀。这样，如果您取消配置远程网络上的系统，然后又想使用“管理控制模式”来重新配置该系统，则可能需要物理接触该系统才能执行此操作。

1.2.8 USB 重定向

使用英特尔 EMA 的 USB 重定向 (USBR) 和一键恢复 (OCR) 功能，可以通过英特尔主动管理技术将远程磁盘映像（.iso 或 .img）安装到托管端点。 您可以使用此功能来安装可引导映像文件，并将托管端点重新引导到所安装映像文件，或者通过 KVM 从托管端点的控制台中浏览所安装映像内容（映像必须包含 USB 键盘和鼠标驱动程序才能进行 KVM 交互）。在您安装映像文件后，可以将端点重新引导至安装的映像。请参阅第 6.4.9 节，了解如何将映像安装到托管端点的详细信息。请参阅第 6.4.9.2 节，了解重新引导至已安装映像的详细信息。

注意：

- 使用 USBR 时，强烈建议执行基于 CIRA 的调配。USBR 对延迟很敏感，并且英特尔 EMA 已针对 CIRA 调配的端点优化了 USBR。如果您将 TLS 与中继结合使用，则需要以“全局管理员”身份在“服务器设置”中“可管理性服务器”部分下调整“USBR 重定向限制速率”。此设置取决于您的独特网络环境。我们建议从 10 毫秒的设置开始，然后以 10 为增量增加，直到找到非常适合网络环境的速率为止。您不太可能需要超过 50 毫秒。请注意，增加此设置将降低 USBR 引导性能，尤其是对于 CIRA 端点，并且只能用于含纯中继实例的 TLS。 请参阅第 1.2.6 节了解 CIRA 的相关信息。请参阅第 9.3 节了解有关设置可管理性服务器设置的信息。
- 强烈建议您不要上传机密数据。

使用可以从英特尔 EMA UI 左侧的导航窗格访问的“存储”页面，可上传和存储映像文件（.iso 或 .img），以供日后安装到端点时使用。有关详细信息，请参阅第 7 节。

下表列出了在端点上使用 USBR over CIRA 所需的最低英特尔主动管理技术版本。

英特尔主动管理技术版本	版本号
英特尔主动管理技术 11	11.8.79 或更高版本
英特尔主动管理技术 12	12.0.70.1607 或更高版本
英特尔主动管理技术 14	14.0.45.1341 或更高版本
英特尔主动管理技术 15	全部
英特尔主动管理技术 16	全部

1.2.9 远程安全擦除

远程安全擦除 (RSE) 是英特尔主动管理技术的一项功能，让 IT 管理员能够远程擦除客户端设备的硬盘。此功能可在“Hardware Manageability”选项卡上的英特尔® EMA 用户界面中使用（请参阅第 6.3.2 节），也可在英特尔® EMA API 中使用。请参阅《英特尔® EMA API 指南》，以详细了解使用英特尔 EMA RSE 实施的特定 API 调用。

RSE 功能在员工离开组织时比较实用，在这种情况下，IT 部门可以远程擦除整个驱动器（可引导分区），然后使用英特尔 EMA 的 KVM 和 USBR 功能将操作系统和应用程序远程重新安装到该设备上，以便将设备发给其他员工。

注意： 为了让英特尔 EMA 在设备上执行此功能（通过用户界面或 API），目标设备（第 12 代英特尔® 酷睿™ 平台或更高版本）必须是英特尔 EMA 中托管的端点，并且其英特尔主动管理技术必须由英特尔 EMA 预配。此外，目标设备必须具有支持此功能的 BIOS 和普通硬盘。

有关英特尔主动管理技术的远程安全擦除功能及其要求的更多信息，请前往以下链接查看《英特尔主动管理技术开发人员指南》：

https://software.intel.com/content/www/us/en/develop/documentation/amt-developer-guide/top/remote-secure-erase/remote-secure-erase-implementation.html

注意： 使用英特尔 EMA API 时，如果尝试的擦除操作失败，则不会清除英特尔主动管理技术引导选项。在重试擦除操作之前，必须先清除此引导选项数据。英特尔 EMA 提供 API，**POST /api/latest/endpointOOBOperations/Single/SecureErase/{endpointId}/clear**，可清除指定设备上的英特尔® 主动管理技术引导选项，以便重试擦除操作。有关此特定 API 调用的详细信息，请参阅《英特尔® EMA API 指南》。

1.2.10 英特尔® Remote Platform Erase 概述

英特尔® Remote Platform Erase（英特尔® RPE）让您能够远程擦除所有平台信息，包括平台的英特尔主动管理技术信息（可选）。由此一来，您无需手动擦除固态硬盘即可重复使用平台。

注意： 为了让英特尔 EMA 在设备上执行此功能（通过用户界面或 API），目标设备（第 12 代英特尔® 酷睿™ 平台或更高版本）必须是英特尔 EMA 中托管的端点，并且其英特尔主动管理技术必须由英特尔 EMA 预配。此外，目标设备必须具有支持此功能的 BIOS 和普通硬盘。

借助英特尔 RPE，您可以在处置或转售设备之前清除设备中的所有用户和公司数据，从而保护公司资产和个人信息。

有关如何在英特尔 EMA 用户界面中使用此项英特尔主动管理技术功能的信息，请参阅第 6.4.11 节。

有关英特尔 RPE 的更多信息，请参阅以下链接中的《英特尔主动管理技术开发人员指南》：

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/WordDocuments/Secure_Remote_Platform_Erase.htm

1.2.11 一键恢复

一键恢复 (OCR) 让您能够在指定端点上启动恢复进程。借助此功能，您可以将端点的操作系统恢复到上次已知的正常状态，以及从非正常状态、裸机情况或连接问题中恢复。此功能需要英特尔® 主动管理技术带外 (OOB) 功能。

注意： 为了让英特尔 EMA 在设备上执行此功能（通过用户界面或 API），目标设备（第 12 代英特尔® 酷睿™ 平台或更高版本）必须是英特尔 EMA 中托管的端点，并且其英特尔主动管理技术必须由英特尔 EMA 预配。此外，目标设备必须具有支持此功能的 BIOS 和普通硬盘。

英特尔 EMA 通过安装和部署恢复服务器（作为其组件服务器之一）来实施此功能。有关恢复服务器设置的信息，请参阅第 9 节。

英特尔 EMA 对一键恢复的实施让您能够使用来自端点本身的预配置恢复映像以及您已上传到英特尔 EMA 服务器的映像（请参阅第 6.4.10 节）。

如果您计划选用使用 HTTPS 的恢复映像，则必须在端点的 BIOS 中启用 HTTPS 引导，如下所示：

1. **在 BIOS 中启用安全引导：** “Boot Maintenance Manager”菜单 >“Secure Boot Config”菜单 > Attempt Secure Boot = 选中
2. **在 BIOS 中启用 HTTPS 引导：** “BIOS Menu path–Intel Advanced”菜单 > PCH-IO Configuration > EFI Network <Onboard NIC>
3. **更改引导顺序并将 HTTPv4 设置为优先项：**
    1. Boot to Bios >“Boot Maintenance Manager”菜单
    2. “Boot Options”菜单 > Change Boot Order
    3. 保存并重新启动。

有关“一键恢复”的更多信息，请参阅以下链接中的英特尔® 主动管理技术在线文档：

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/WordDocuments/oneclickrecovery.htm

1.2.12 Microsoft Azure AD 身份验证

如果您有现成的 Microsoft Azure Active Directory (Azure AD) 环境，则可以安装英特尔 EMA 以使用 Azure AD 身份验证。有关安装详情，请参阅《英特尔® EMA 服务器安装和维护指南》。

在此模式下安装英特尔 EMA 之前，必须先在您的环境中完成 Azure AD 的设置和配置。此外，在 Azure AD 模式下安装英特尔 EMA 之前，您必须完成几个手动步骤。请参阅《英特尔® EMA 服务器安装和维护指南》中的”开始之前“章节。

在 Azure AD 身份验证模式下安装后，英特尔 EMA 将在登录视屏上提供两种登录选择（请参阅第 2 节），允许您使用 Azure AD 单点登录 (SSO) 凭据登录。如果选择 **Login with Azure SSO Credentials**，则将显示 Microsoft SSO 登录进程，以便您输入您的 SSO 凭据。您输入的用户必须已在 Azure AD 中存在。

注意： 如果在安装后初次登录到英特尔 EMA，请使用英特尔 EMA 凭据进行登录并使用您在安装期间创建的初始用户名。初次登录后，您可以在英特尔 EMA 中创建更多与 Azure AD 用户相对应的用户。

在英特尔 EMA（安装于 Azure AD 模式下）中创建的任何用户必须在此创建之前已存在于 Azure AD 中。此外，英特尔 EMA 用户的名称必须与相应 Azure AD 用户的通用主体名称 (UPN) 属性相匹配。并且，任何您想要创建相应英特尔 EMA 用户的 Azure AD 用户不能是“访客帐户”或“外部帐户”。因为英特尔 EMA 依赖于 UPN，如果用户是访客或外部帐户，则英特尔 EMA 无法从 Azure AD 获取 UPN。

此外，有些公司为 Web 浏览器设置了政策，使其始终将当前登录的 Windows 帐户用作为 SSO 凭据。对于 Chrome 和 Edge 尤其如此。要使用不同的用户，请以“无痕”模式打开 Web 浏览器。

如果您的 Web 浏览器中有任何插件或扩展程序会阻止 `login.microsoftonline.com`，则需要将它们删除或禁用。

英特尔 EMA 安装程序的 "Advanced Mode" 菜单栏中有个菜单选项可将您的现有英特尔 EMA 实例从 Windows AD 身份验证切换为 Azure AD 身份验证。详情请参阅《英特尔® EMA 服务器安装和维护指南》中的“英特尔 EMA 安装程序 ‘Advanced Mode’ 菜单栏”章节。

1.2.13 英特尔 LMS 的功能和安装

英特尔® Local Manageability Service（英特尔® LMS）是一项服务，可通过启用以下用例来增强您的英特尔 EMA 使用体验。英特尔 LMS 不属于英特尔 EMA 的一部分，也不是英特尔 EMA 按设计运行的必要条件，因为英特尔 EMA 确实包含内置的“微型 LMS”。但是，英特尔 LMS 确实可以促进托管端点上的以下用例，而这些用例只有在端点上安装了完整英特尔 LMS 服务的情况下才能受到支持。

注意：如果托管端点上存在英特尔 LMS，则英特尔 EMA 会自动使用它，而非使用内置微型 LMS。如果您的端点上不存在英特尔® LMS，请参阅下面的第 1.2.13.2 节。

1.2.13.1 功能和用例

- 英特尔® Management and Security Status（英特尔® IMSS）- 隐私要求
- 时间同步
- WiFi 配置文件同步
- 静态 IP 同步
- WMI 供应商
- 在系统事件日志中记录事件
- 正常重置（尽管英特尔 EMA 代理会在英特尔 EMA 内部处理此问题）

有关英特尔 LMS 的更多信息，请参阅以下链接中的英特尔主动管理技术参考指南：

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm?turl=WordDocuments%2Flocalmanageabilityservice.htm

1.2.13.2 获取和安装英特尔 LMS

许多 PC OEM 在其 PC 平台上配备英特尔® LMS。如果您的端点没有安装英特尔 LMS，可以执行以下操作，以在您的托管端点上获取和安装英特尔 LMS：

1. 访问 https://www.intel.com/content/www/us/en/download/682431/intel-management-engine-drivers-for-windows-7-windows-8-1-and-windows-10.html。
2. 在托管端点上，下载最新英特尔管理引擎驱动程序包 zip 文件 (**ME_SW_<version>.zip**)。
3. 下载完成后，在托管端点上解压缩下载的文件。
4. 打开解压出来的文件夹 (**ME_SW_<version>**)，然后打开 **Drivers > LMS** 文件夹。
5. 右键单击 **LMS.inf**，然后选择 **Install**。
6. 在安装完成后，打开“设备管理器”并确保显示 **Intel(R) Management and Security Application Local Management** 设备。

1.2.14 重要文件和目录位置

<Installer Directory>/EMALog-Intel®EMAInstaller.txt	安装日志
C:\Program Files (x86)\Intel\Platform Manager\Platform Manager Server\settings.txt	包含 Platform Manager 的设置，包括端口号和密码。
C:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\app.config and connections.config	包含数据库连接字符串（加密）。
C:\Program Files (x86)\Intel\Platform Manager\EMALogs • EMALog-XXX.txt • TraceLog-XXX.txt	每个服务器组件的日志。它们与您在平台管理器的事件日志中看到的日志消息相同。
C:\Program Files\Intel\EMA Agent	64 位英特尔 EMA 代理文件的安装位置。
C:\inetpub\wwwroot	IIS 网站位置。

2 登录到英特尔® EMA

要登录英特尔 EMA，请执行以下操作：

1. 打开浏览器，然后导航到安装期间指定的 FQDN/主机名（如果不确定，请咨询您的英特尔 EMA 全局管理员）。在分布式服务器安装中，这将是 Ajax 和 Web 服务器负载均衡器的 URL。
2. 如果您已在 Azure AD 模式下安装了英特尔 EMA，请选择或 **Login with Azure SSO Credentials** 或 **Login with Intel EMA Credentials**。否则，请转到步骤 4。

   注意： 如果这是安装后立即在 Azure AD 模式下进行的初始登录，则必须选择 **Login with Intel EMA Credentials** 并输入您在安装期间为初始用户创建的凭据。

3. 对于 Azure SSO 凭据，请输入适用的 Microsoft Azure 单点登录凭据。
4. 对于英特尔 EMA 凭据，请输入全局管理员为您分配的租户管理员用户的用户名称（即电子邮件地址）和密码。对于其他用户，请输入由租户管理员或帐户管理员分配给您的用户名和密码。

注意：

- 英特尔 EMA 网站用户界面 (UI) 使用了 Cookie。如果在浏览器中禁用 Cookie，则英特尔 EMA 网站 UI 将无法正常运行。
- 根据英特尔 EMA 的安装方式，“概述”页面可能会自动显示，或者可能会首先要求您提供英特尔 EMA 凭证。
- 如果您登录到英特尔 EMA 并在浏览器中打开一个新标签，您将转到登录页面。您可以在“服务器设置”页面上，通过英特尔 EMA 的 Web 服务器设置将 sessionStorage 更改为 localStorage 来更改此设置（请参阅第 9 节“附录 - 修改组件服务器设置”，P50），但请注意，某些浏览器不会跨选项卡共享会话 cookie 。
- 不支持以其他用户身份在新选项卡上登录（当已在另一个选项卡中登录英特尔 EMA 时）。您可以在新选项卡上完成登录，但是原登录选项卡上将显示错误。
- 如果您输入错误密码的次数过多，则您的帐户将被锁定 24 小时。如果发生这种情况，请咨询您的全局管理员。

2.1 概述页面

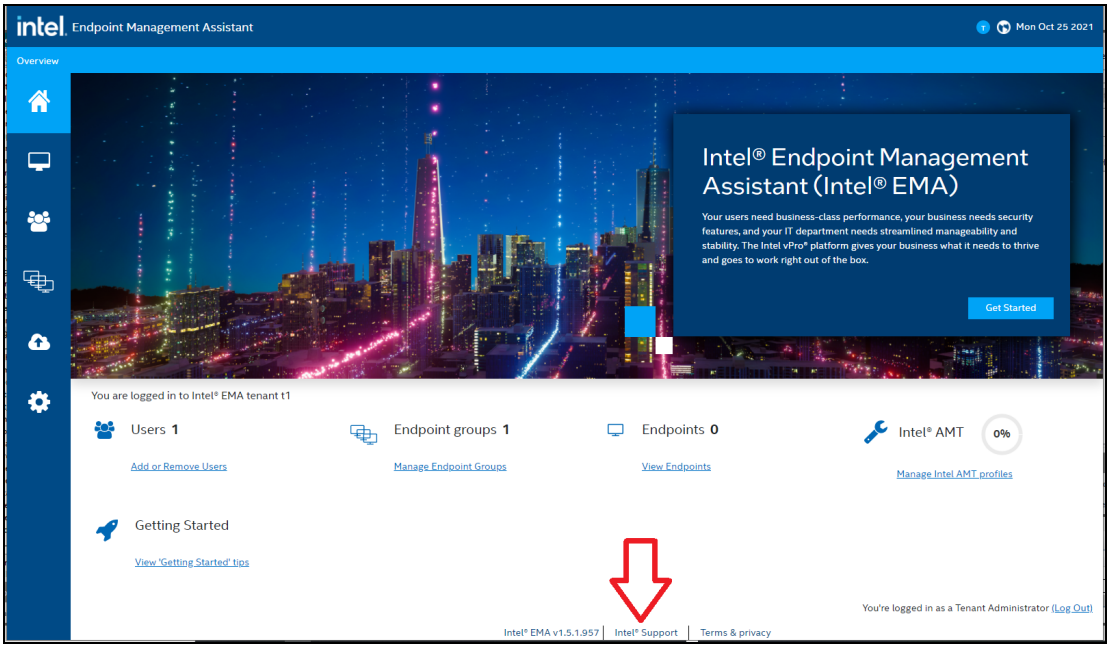
登录到英特尔® EMA 之后，将显示概述页面。该页面的内容取决于您以哪个用户角色登录。下图显示了租户管理员的“Overview”页面。

注意： 首次登录时，将显示“开始”链接。在创建第一个端点组之前，将一直显示该页面。“开始”页面中的任务在第 3 节中进行了更详细的介绍。

底部的快速链接提供对大多数租户管理员任务的便捷访问，本指南的后续部分将介绍这些任务。

要获得帮助，请单击页面底部的 **Intel Support** 链接。

图 3: 租户管理员概述



2.1.1 在页脚中添加或删除服务器名称

默认情况下，英特尔 EMA Web UI 页面的页脚不会显示英特尔 EMA 服务器的名称。但是，如果需要，您可以使用以下指令将其添加到页脚。

1. 在英特尔 EMA 服务器计算机上，打开 IIS。
2. 在左侧的导航窗格中，选择 **Default Web Site**，然后选择 **Configuration Editor**。
3. 打开 **appSettings**。
4. 在项目列表中添加一个项目，**key** 列为“name2”，**value** 列为“(*<server_name>*)”，其中 *<server_name>* 为英特尔 EMA 服务器的名称。请注意，**value** 列是一个简单字符串，因此，您在必填的括号中键入的内容即为将在页脚中显示的内容。
5. 保存该配置，然后退出 ISS。下次启动英特尔 EMA 时，您应该会在底部的页脚中看到服务器名称。

3 设置您的租户

本节介绍如何在英特尔® EMA 服务器上设置和配置特定的租户。除非另有说明，否则本部分中的任务由租户管理员用户执行。可以由其他用户执行的操作会在该操作的小节开头注明。

重要提示！您必须以具有租户管理员权限的用户身份登录英特尔 EMA 服务器，才能执行本节中的步骤。如《英特尔® EMA 服务器安装和维护指南》或《英特尔® EMA 分布式服务器安装和维护指南》第 3 节所述，在英特尔 EMA 安装之后的“开始”步骤中，全局管理员应该已经创建了至少一个租户和租户管理员用户。如有必要，请参阅这些安装指南。

注意：根据您组织的实际情况，可能不一定需要完成本节中的所有任务。此外，随着组织的发展和变化，许多任务（例如添加新用户和创建新端点组）可能会随着时间的推移定期执行。

以下是设置租户的基本过程。在随后的小节中将详细说明这些步骤。

1. **创建您的端点组 -** 端点组是基于组织对端点的逻辑分组。例如，您可以为您的会计部门创建一个端点组，为工程部门创建一个端点组。这使您可以为不同的组制定不同的 IT 策略。我们建议您通过完成此过程中的其他步骤来完全配置端点组，然后根据需要返回此步骤以创建和配置其他端点组。**角色：**租户管理员，端点组创建者。
2. **为每个端点组创建英特尔® EMA 代理文件 -** 无论是否计划使用 OOB 功能，都必须在端点上安装和配置英特尔 EMA 代理，以便英特尔 EMA 可以对其进行管理。此步骤根据您的端点组配置（政策，英特尔® 主动管理技术配置文件等）创建一对代理文件。**角色：**租户管理员，具有基于组关联的适当访问权限的用户。
3. **创建您的网络配置文件 -** 如果您打算在生产环境中使用 WiFi 或 802.1X，则可以为这些网络技术配置配置文件，并且可在创建英特尔® 主动管理技术配置文件时轻松选择这些配置文件。您也可以在英特尔® 主动管理技术配置文件创建流程中创建这些网络配置文件，但是，如果您打算在多个英特尔® 主动管理技术配置文件中重复使用网络配置文件，则预先创建网络配置文件可能更轻松。**角色：**租户管理员。如果您的环境中不使用 WiFi 或 802.1X，则可以跳过此步骤（第 3.1 节）。
4. **创建您的英特尔® 主动管理技术配置文件 -** 如果您打算使用带外 (OOB) 功能来管理端点（即，在端点操作系统不可用时可以运行的端点管理功能），则必须在端点上配置英特尔® 主动管理技术。您可以在每个端点上手动配置英特尔® 主动管理技术，或者可以让英特尔 EMA 自动在所有端点上设置英特尔® 主动管理技术。为了使英特尔 EMA 自动设置英特尔主动管理技术，您必须至少配置一个英特尔主动管理技术配置文件供英特尔 EMA 使用。**角色：**租户管理员，端点组创建者。如果您不想使用英特尔® 主动管理技术自动设置，则不需要配置英特尔® 主动管理技术配置文件，可以跳过此步骤（第 3.2 节）。
5. **上传您的英特尔® 主动管理技术 PKI 证书 -** 英特尔主动管理技术 PKI 证书用于 PKI 设置，如果您打算在管理控制模式下启用英特尔主动管理技术自动设置，则必须使用该证书。如果您没有英特尔® 主动管理技术 PKI 证书，或者想在客户端控制模式下启用英特尔® 主动管理技术自动设置，请跳过此步骤（第 3.3 节）。**角色：**租户管理员。
6. **启用英特尔® 主动管理技术自动设置 -** 如上所述，英特尔主动管理技术自动设置允许英特尔 EMA 在您的端点上自动设置英特尔主动管理技术。如果您打算使用英特尔® EMA 的 OOB 端点管理功能，则必须在端点上设置英特尔® 主动管理技术。您必须具有英特尔® 主动管理技术 PKI 证书和英特尔® 主动管理技术配置文件才能在 ACM 模式下启用英特尔® 主动管理技术自动设置。**角色：**租户管理员和具有适当访问权限的用户。如果您不想在端点上启用英特尔® 主动管理技术自动设置，则可以跳过此步骤（第 3.5 节）。
7. **将英特尔® EMA 代理文件部署到托管端点 -** 创建英特尔 EMA 代理文件后，需要将其部署到端点系统。本节提供了有关使用命令行或 GUI 安装程序直接在给定的端点系统上手动安装代理文件的说明。可以通过批量部署工具利用命令行过程来创建自动部署程序包。**角色：**在托管端点系统上具有管理员权限的任何用户。
8. **根据需要创建其他用户和用户组 -** 根据组织的规模和复杂性，您可能决定需要更多用户来帮助管理端点（请参阅第 1.2.2 节了解有关用户角色的详细信息）。可以根据需要将这些用户分组为“用户组”。**角色：**租户管理员，帐户管理员。

3.1 创建您的端点组

端点组是基于组织的端点逻辑分组。例如，您可以为您的会计部门创建一个端点组，为工程部门创建一个端点组。这使您可以为不同的组制定不同的 IT 策略。

3.1.1 关于端点组策略集

每个端点组都有一个关联的策略集。一个策略集包括以下内容：

电源操作	• **唤醒：** 如果选择此策略，则启用端点的远程唤醒/启动。 • **睡眠：** 如果选择此策略，则会在端点上启用远程激活睡眠和休眠模式。 • **关闭或重新启动：** 如果选择此策略，则启用远程关机和端点重启。
消息和提醒	• **TCP 流量中继：** 此策略构成以下所有策略的基础。如果未选择此策略，则端点仍可以连接到英特尔® EMA 服务器。但是，英特尔 EMA 无法在端点上执行任何操作，包括英特尔® 主动管理技术设置。 • **提醒消息：** 如果选择此策略，则启用了在端点上显示提醒消息。 • **控制台提示：** 如果选择此策略，则启用在端点上运行计划的远程执行。此策略应用于控制远程终端访问。对于带外终端访问，在英特尔主动管理技术设置过程中使用的英特尔主动管理技术配置文件也需要启用此策略。 • **地点信息：** 如果选择此策略，则启用查询端点的远程位置信息。当前不支持此功能。 • **点对点通信：** 此策略适用于同一网络中的端点（英特尔 EMA 代理）之间的通信。如果未选择此策略，则代理将不会在其网络内寻找其他代理，也不会接受来自其他代理的通信。因此，需要英特尔 EMA 代理中继的功能（例如“带中继的 TLS”下的英特尔主动管理技术设置）将不起作用。

远程控制	• **远程 KVM：** 如果选择此策略，则启用远程 KVM。对于带外 KVM，在英特尔® 主动管理技术设置过程中使用的英特尔主动管理技术配置文件也需要启用此策略。
	• **远程文件访问：** 如果选择此策略，则启用对端点的远程带内文件访问（通过文件浏览器、计划的文件传递或文件搜索）。
	• **远程管理 (WMI)：** 如果选择此策略，则在端点上启用远程 WMI 查询和远程过程操作（通过 WMI）。此策略还控制英特尔® EMA 是否可以将端点远程设置为 BIOS。
	• **用户同意带内 KVM：** 如果启用，则会应用以下逻辑：：
	  ◦ 如果目标端点不在用户会话中（锁定、注销等），则超时后将拒绝 KVM。
	  ◦ 否则，如果目标端点处于用户会话中，则用户会收到一个弹出窗口以选择接受或拒绝。如果用户同意，则带内 KVM 会通过，并且目标端点上的系统任务栏图标会显示以表明它处于 KVM 会话中。
	  ◦ 否则如果禁用，则无需用户同意。

关于带外功能（英特尔主动管理技术提供的功能）：

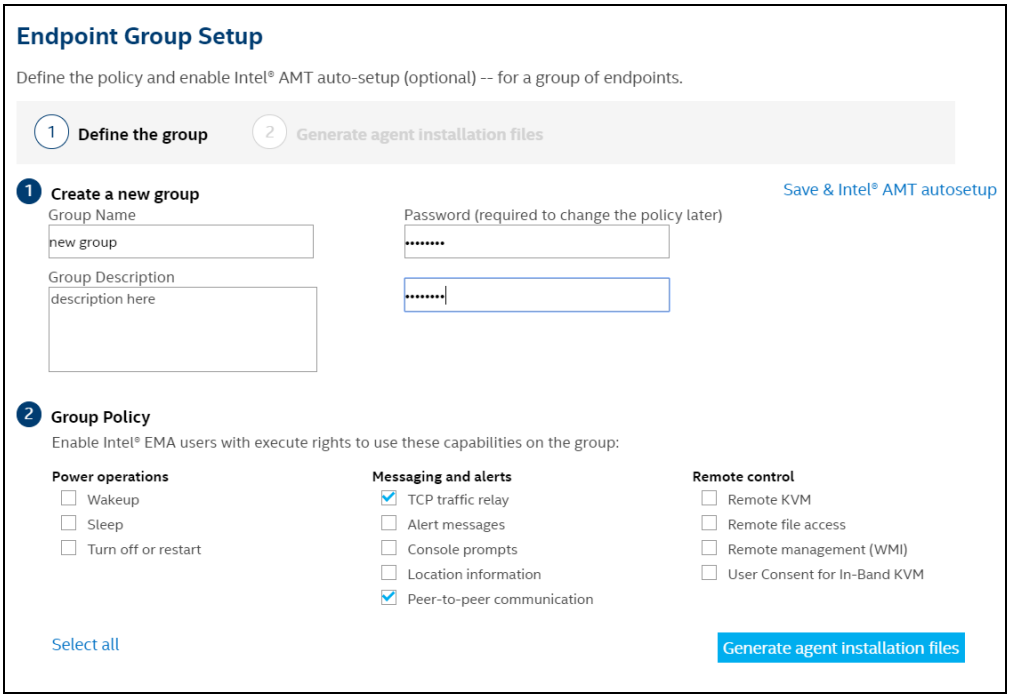
- 带外终端和带外 KVM 由命令策略和 KVM 策略控制。如果允许这些策略之一，则两个功能均被允许。
- 根据指定的端点组策略检查以下 WSMAN 电源操作：CIM_PowerManagementService \ RequestPowerStateChange。

3.1.2 创建新的端点组

角色：租户管理员，端点组创建者

1. 从左侧的导航栏中选择 **Endpoint Groups**，然后选择 **New Endpoint Group**。
2. 填写各字段并选择该组中的端点应具有的 **Group Policy** 功能。
3. 如果您计划在英特尔主动管理技术配置文件中使用 WiFi 或 802.1x 配置文件，请单击 **Generate agent installation files** 并继续执行第 3.2 节的操作。您可以在创建网络配置文件和英特尔主动管理技术配置文件后，启用英特尔主动管理技术自动设置。如果您想直接在该组中的端点上设置英特尔主动管理技术自动设置，请单击 **Save & Intel® AMT autosetup** 并继续执行第 3.4 节的操作。

图 4: “Endpoint Group Setup”页面



3.1.2.1 自动创建端点用户组

角色：仅端点组创建者

当端点组创建者用户创建新的端点组时，英特尔 EMA 会自动创建具有适当访问权限的用户组，并将当前用户纳入该组中。它还会自动将此用户组关联到新的端点组。内部自动创建的用户组使用[创建的端点组名称]_ EndpointGroupCreators 格式命名。因此，用户组仍然保持对端点组的访问控制。

注意：创建新端点组的租户管理员将不会看到此自动创建的用户组，因为该租户管理员不属于任何特定用户组。

3.1.3 查看和删除端点组

角色：租户管理员（删除，查看），端点组创建者（删除，查看），端点组用户（查看）

端点组创建者只能删除与该端点组创建者属于同一用户组（具有执行权限）的端点组。端点组创建者只能查看与端点组创建者属于同一用户组（具有查看权限）的端点组。

端点组用户只能查看与端点组用户属于同一用户组的端点组。

单击目标端点组旁边的向下箭头，然后选择 **View Configuration**。

要删除此端点组，请单击 **Delete Group**。

注意：如果删除此端点组，则该组中的端点将无法连接到英特尔® EMA 服务器。

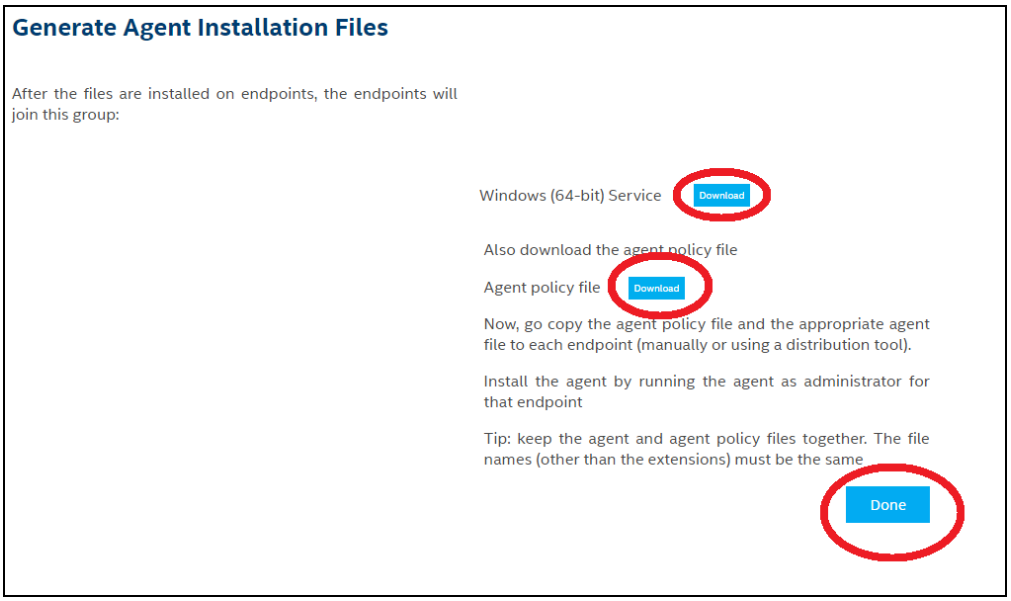
3.2 创建代理文件以部署到托管端点

角色：租户管理员、端点组创建者†、端点组用户†

†具有此组的访问权限

1. 如果您不是从上一节接续操作，可以从左侧的导航栏访问此屏幕，选择 **Endpoint Groups**，然后单击目标端点组旁边的向下箭头并选择 **Create Agent Files**。
2. 对于 Windows 64 位服务代理文件，请单击 **Download**。
3. 单击 **Download** 以获取代理策略文件，然后单击 **Done**。

图 5: 生成代理安装文件



这两个文件都在使用英特尔 EMA 基于 Web 的 UI 系统上的 **Downloads** 文件夹中创建。将这些文件放在一起，然后将它们复制到要使用英特尔 EMA 管理的端点系统。第 4 节对该安装过程进行了介绍，建议按照第 3.3 节中的小节顺序进行操作。

注意：

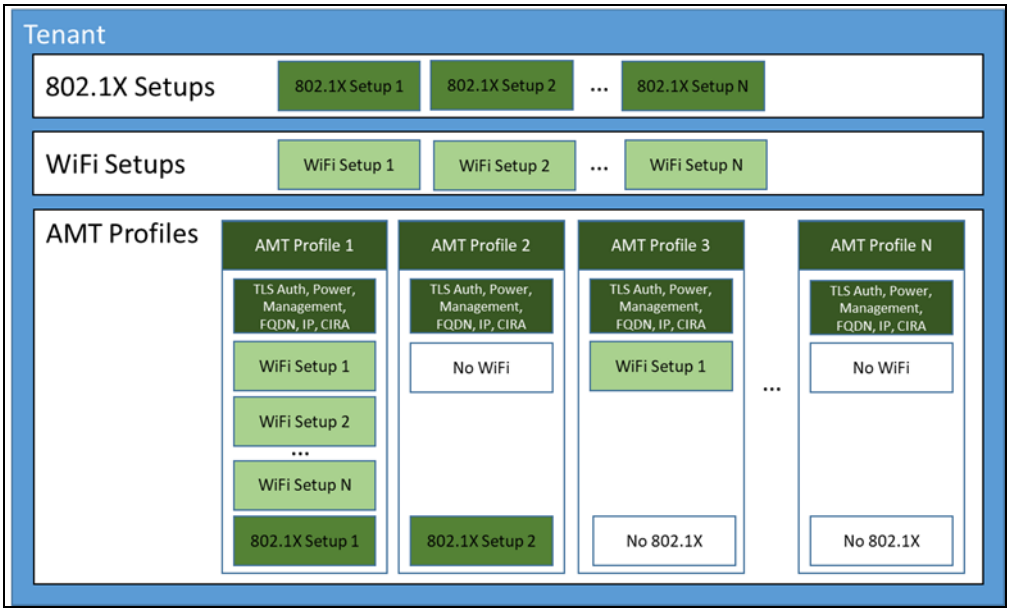
- 有关将端点组与用户组关联以管理用户对其的访问的信息，请参阅第 5.3 节。
- 有关端点上的代理安装故障排除的信息，请参阅第 4.5 节。

3.3 创建您的网络配置文件

角色：租户管理员

尽管在创建英特尔® 主动管理技术配置文件时可以创建网络配置文件，但您可能会发现预先创建网络配置文件是更容易的做法。通过这种方式，您就可以在创建英特尔主动管理技术配置文件时简单地选择一个现有的网络配置文件。下图说明了网络配置文件或“设置”与英特尔主动管理技术配置文件之间的关系。

图 6: 网络配置文件和英特尔® 主动管理技术配置文件



如果您的环境中不使用 Wi-Fi 或 802.1X，则可以跳过本节。

3.3.1 创建新 WiFi 配置文件

要创建新的 WiFi 配置文件:

从左侧的导航栏中选择 **Endpoint Groups**，然后选择 **Intel® AMT Profiles > Manage WiFi Profiles** 并单击 **New Profile**。您还可以在英特尔® 主动管理技术配置文件创建工作流程（第 3.4 节）中创建新的 WiFi 配置文件。

在 **Define the WiFi Profile** 对话框中，请执行以下操作:

1. 在 **WiFi profile name** 字段中，输入 WiFi 配置文件的名称。设置名称最多可以包含 32 个字符，并且不能包含 (/ \ < > : ; * | ? ”) 字符。
2. 在 **SSID** 字段中，输入用于标识特定 WiFi 网络的服务集标识符（最多 32 个字符）。
3. 从 **Security type** 下拉列表中选择以下选项之一:
    - **WPAPSK:** 使用 WiFi 保护访问密钥管理协议。在提供的字段中输入 **Security key**（密码）（必须包含 8 到 63 个可打印 ASCII 字符）。
    - **WPA2PSK:** 使用强大的安全网络（或 WPA2）密钥管理协议。在提供的字段中输入 **Security key**（密码）（必须包含 8 到 63 个可打印 ASCII 字符）。
    - **WPAIEEE802_1:** 使用 WiFi 保护访问密钥管理协议。从下拉列表中选择一个现有的 **802.1X setup**。
    - **WPA2IEEE802_1:** 使用强大的安全网络（或 WPA2）密钥管理协议。从下拉列表中选择一个现有的 **802.1X setup**。
4. 从 **Encryption** 下拉列表中选择以下选项之一:
    - **Temporal Key Integrity Protocol (TKIP)**
    - **Counter mode CBC MAC Protocol (CCMP)**

创建新设置时，其优先级值比现有设置的最高值大一。

3.3.1.1 编辑和删除 Wi-Fi 配置文件

1. 从左侧导航栏中选择 **Endpoint Groups**，然后选择 **Intel® AMT Profiles > Manage WiFi Profiles**。
2. 单击目标 Wi-Fi 配置文件旁边的向下箭头以对其进行编辑或删除。您不能删除与英特尔主动管理技术配置文件关联的网络配置文件。

Wi-Fi 配置文件按其优先级在此列表中排序，最小的优先级数字位于列表顶部，最大的优先级数字（将最后使用）位于列表底部。

要更改配置文件的优先级，请单击蓝色向上和向下箭头按钮，向上或向下移动 WiFi 配置文件。

3.3.2 创建一个新的 802.1x 配置文件

IEEE802.1x 网络协议为希望连接到 LAN 的设备提供了一种身份验证机制，可以建立点对点连接，或者在身份验证失败时阻止该连接。它用于大多数无线 802.11 接入点，并基于可扩展身份验证协议 (EAP)。您可以在配置文件中包含为无线和有线连接定义的 802.1x 配置文件。

如果您不打算使用 802.1X 网络协议，则可以跳过此步骤。

注意：

- 802.1x 配置文件需要与 Active Directory 和企业级 CA 集成。
- 确保您了解组织的网络身份验证要求。如果不满足这些要求，则英特尔主动管理技术可能无法正常运行。例如，某些 IT 组织具有超出 802.1x 访问策略的要求，而不仅仅是需要 AD 计算机对象和有效的 802.1x 证书（如允许的网络硬件类型的密码列表）。
- 有关为 Microsoft Active Directory (AD) 域服务配置 802.1x 身份验证（包括创建用于 802.1x 配置文件的 AD 组织单位 (OU)）的信息，请参阅《英特尔® EMA 服务器安装和维护指南》和《英特尔® EMA 分布式服务器安装和维护指南》的附录。**如果您计划将 802.1x 用于 AD 域服务，请在创建 802.1x 配置文件之前，确保您的全局管理员执行本附录中所述的为 Active Directory 配置 802.1x 的过程。**

要创建新的 802.1X 配置文件：

从左侧的导航栏中选择 **Endpoint Groups**，然后选择 **Intel® AMT Profiles > Manage 802.1x Profiles** 并单击 **New Profile**。您还可以在英特尔® 主动管理技术配置文件创建工作流程中创建新的 802.1X 配置文件（第 3.2 节）。

在 **Definition** 对话框中，请执行以下操作：

1. （可选）取消选中 **Enable** 复选框以禁用此设置的有线连接。
2. 为 802.1x 配置文件输入 **Name**。名称最多可以包含 32 个字符，并且不能包含 (/ \ < > : ; * | ? ”) 字符。
3. 为 **Protocol** 选择 **EAP_TLS** 或 **EAP_PEAP_MSCHAP_V2**。
4. 在 **Active Directory** 下方，输入以下信息：
   - **Active Directory Organizational Unit (ADOU)**Active Directory Organizational Unit (ADOU)：这是将对象存储在 AD 中的位置。必须使用专有名称格式输入 ADOU。例如，“OU=带外管理，DC=vprodemo，DC=com”。
   - **Security Groups**Security Groups：默认情况下，为英特尔主动管理技术端点创建的 AD 对象自动添加到名为“Domain Computers”的 AD 安全组中。您可以定义将对象添加到的其他安全组。例如，某些 RADIUS 服务器要求对象必须是特定安全组的成员。使用可分辨名称格式将新行用于新条目；例如：“CN=vPro8021XComputers，DC=VPRODEMO，DC=COM”。
5. 此步骤仅适用于 EAP_TLS。如果您选择 **Client Authentication**，则不显示屏幕的 **EAP_PEAP_MSCHAP_V2** 部分。在 **Client Authentication** 下，对于 **How to create the certificate**，选择将在英特尔® 主动管理技术端点中安装的证书的来源。 **From Microsoft CA** 建议使用，并且英特尔 EMA 服务器需要能够访问 Microsoft CA。
   - 来自 **Certificate Authority** 下拉列表，选择英特尔 EMA 将用于请求 RADIUS 服务器可以认证的证书的企业 CA。这需要配置企业根 CA，以便在进行 AD 查询时将其显示为根证书颁发机构。如果您没有看到要使用的企业根 CA，则需要使用下面列出的 **From the database** 选项。

- 从 **Server Certificate Template** 下拉列表中，选择将用于创建客户端证书的模板。有关如何在证书颁发机构服务器上创建有效模板的信息，请参阅英特尔主动管理技术文档。
- 定义将包含在生成的证书的使用者名称中的 **Common Names**。对于 **Default**，使用者名称的通用名称是用户主体名称，使用者备用名称的通用名称是用户主体名称、DNS FQDN、主机名、SAM 帐户名称、代表英特尔® 主动管理技术的新 AD 对象的 UUID 以及专有名称。对于 **User Defined**，选择要在“Subject Alternative Name”中输入的通用名称，然后从下拉列表中选择 **CN for Subject Name**。

  注意：

  - 您可以选择将专有名称包含在证书的主题备用名称中，但 **CN for Subject Name** 下拉列表中不包含专有名称，因为证书的主题名称中不允许使用专有名称。
  - 连接到 802.1x 网络时，英特尔® 主动管理技术固件将主题名称用作 Radius 用户名，因此在配置 Radius 服务器时，主题名称的值必须是有效的用户名。

- **From database**From Database：用户可以使用英特尔® EMA 数据库中的预上传证书。有关如何上传证书的详细信息，请参阅第 3.5.1 节。输入目标证书指纹值以找到证书。

6. 在 **Server Authentication – Trusted Root Certificate** 下，对于 **How to get the certificate**，选择将在英特尔® 主动管理技术端点中安装的证书的来源。
   - 从 **Certificate Authority** 下拉列表中，选择英特尔 EMA 将使用的企业根 CA。
   - **From the database**From the database：用户可以使用英特尔 EMA 数据库中的预上传证书。有关如何上传证书的详细信息，请参阅第 3.5.1 节。输入目标证书指纹值以找到证书。
7. 在 **Advanced** 下，**Available in S0** 选项默认情况下处于启用状态，如果端点处于 S0 状态但无法向服务器验证，则默认情况下该选项允许英特尔主动管理技术处理对英特尔 EMA 服务器的验证。请注意直到成功进行身份验证之后，英特尔 EMA 服务器才能访问端点。
   - 仅当您不希望英特尔主动管理技术使用此配置文件对英特尔® EMA 服务器执行身份验证时，才禁用（取消选中）此选项。
   - 对于 **PXE Timeout**，设置超时之前以秒为单位的英特尔主动管理技术保持经过身份验证的 802.1X 会话的持续时间（范围为 0-86400 秒或一天）。在设置的持续时间内，英特尔主动管理技术在进行 PXE 引导时管理 802.1X 协商。超时后，协商控制权将传递给端点。此设置适用于“Wired Connections”。
8. 在 **Radius Server Validation** 下，选择以下选项之一以指定您希望英特尔主动管理技术如何验证 RADIUS AAA 服务器提供的证书中的使用者名称。
   - Do not verify
   - Verify using FQDN
   - Verify using Domain Suffix

3.3.2.1 编辑和删除 802.1x 配置文件

1. 从左侧的导航栏中选择 **Endpoint Groups**，然后选择 **Intel® AMT Profiles > Manage 802.1x Profiles**。
2. 单击目标配置文件旁边的向下箭头以对其进行编辑或删除。您不能删除与英特尔主动管理技术配置文件关联的网络配置文件。

3.4 创建您的英特尔® 主动管理技术配置文件

角色：租户管理员，端点组创建者

如果您打算使用带外 (OOB) 功能来管理端点（例如：当端点操作系统不可用时可以使用的端点管理功能），则必须在端点上配置英特尔® 主动管理技术。您可以在每个端点上手动配置英特尔主动管理技术，或者可以让英特尔® EMA 自动在所有端点上设置英特尔主动管理技术。为了使英特尔 EMA 自动设置英特尔主动管理技术，您必须至少配置一个英特尔主动管理技术配置文件供英特尔 EMA 使用。

如果您不想使用英特尔主动管理技术自动设置，则不需要配置英特尔主动管理技术配置文件，可以跳过此步骤。

要创建新的英特尔® 主动管理技术配置文件：

1. 在左侧的导航栏中，选择 **Endpoint Groups**，然后单击 **Intel AMT Profiles** 选项卡。
2. 单击 **New Intel AMT Profile**，填写新的英特尔主动管理技术配置文件各个部分的字段（“General”、“Power States”等），然后单击 **Save**。这些部分的内容将在以下小节中详细介绍。
3. 如果您正在执行初始租户设置，请在填写英特尔主动管理技术配置文件的各个部分并单击 **Save** 后，继续执行第 3.5.1 节中的操作，以在启用英特尔主动管理技术自动设置之前上传英特尔主动管理技术 PKI 证书。

3.4.1 常规设置

输入 **Profile Name** 和 **Profile Description**，然后指定英特尔 EMA 服务器将如何与端点的英特尔主动管理技术（CIRA 或 TLS 中继）进行通信。有关 CIRA 和 TLS 的更多信息，请参阅第 1.2.6 节。

- **Always Use Intel AMT CIRA** - 此选项设置随机 CIRA 主域。将始终使用 CIRA（无 TLS 中继）。
- **Use Intel AMT CIRA unless on a specified network** - 显示 CIRA 主域并允许您输入其他域。如果检测到指定域，则使用 TLS 中继。
- **Use TLS Relay** - 仅使用 TLS 中继（无 CIRA）。

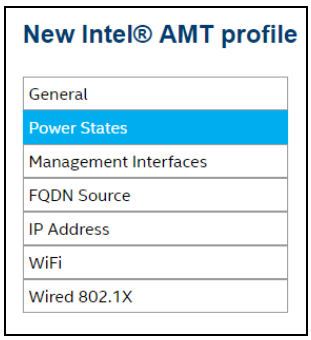
如果指定 CIRA，请注意以下几点：

- 英特尔 EMA 使用自签名证书进行 CIRA 通信。
- 您必须定义一个内部网后缀。当英特尔主动管理技术端点位于与定义的内部网后缀匹配的网络上时，英特尔主动管理技术将停止 CIRA 并改用 TLS 中继。

  注意：要强制英特尔主动管理技术始终打开 CIRA 隧道，请在创建英特尔主动管理技术配置文件时在“General”设置下的 CIRA 内部网后缀字段中输入伪造的域后缀。这个伪造的域后缀应该足够复杂，防止任何人猜中，从而使用它来阻止 CIRA 连接并打开本地管理端口。如果查看使用以前版本的英特尔 EMA 创建的配置文件，则将在此处自动填写域后缀。

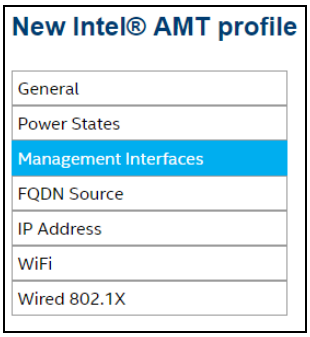
- 对于具有英特尔主动管理技术 12 或更高版本的端点，您可以选择添加用于英特尔主动管理技术的代理以连接到英特尔 EMA 服务器。

3.4.2 电源状态设置



默认值和建议的选择是“任何时候通过所有系统电源状态 (S0 – S5) 将系统连接到电源”。

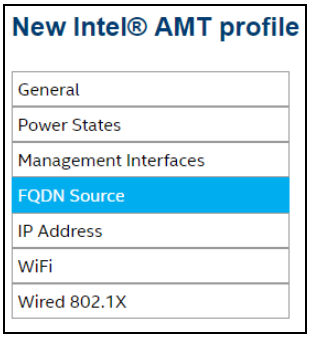
3.4.3 管理接口设置



选择要在端点上打开的接口：

- **KVM redirection** – 打开键盘/视频/鼠标 (KVM) 重定向界面，该界面使您可以与端点进行交互，类似您的键盘、视频和鼠标已物理连接到该系统一样。
- **User Consent** - 向目标端点的用户提供同意代码，以允许与端点进行远程管理交互。选择 **KVM** 或 **KVM + Advanced Boot Options**（在远程执行高级引导操作时使用，例如 USBR 或远程安全擦除）。如果选择其中之一，则在通过 KVM 连接或尝试执行高级引导操作时，系统将提示您输入端点用户提供的同意代码。如果端点处于客户端控制模式，则无论在此处选择什么选项，都会强制执行用户同意。您还可以修改 **timeout** 时间段（以秒为单位）。
- **Web-based user interface** – 使您能够使用基于浏览器的界面来管理和维护英特尔® 主动管理技术系统。
- **Serial over LAN** – 通过将按键和字符显示数据封装在 TCP/IP 流中，使您能够远程管理英特尔主动管理技术系统。
- **IDE/USB redirection** – IDER 使您可以将英特尔主动管理技术系统上的驱动器映射到远程映像或驱动器。此功能通常用于从备用驱动器重新引导英特尔主动管理技术系统。USBR 使您可以将英特尔主动管理技术系统上的驱动器映射到远程映像或驱动器。与将远程软盘或 CD 驱动器呈现为好像已集成在主机中的 IDER 相比，USBR 将远程驱动器呈现为似乎是通过 USB 端口连接的。
- **OCR (One Click Recovery)** - 启动恢复过程，以安全的方式将指定端点的操作系统恢复到上次已知的正常状态。使用英特尔主动管理技术带外 (OOB) 连接。
- **RPE (Remote Platform Erase)** - 启动以安全方式远程擦除所有平台信息的进程，包括平台的英特尔主动管理技术信息（可选）。使用英特尔主动管理技术带外 (OOB) 连接。

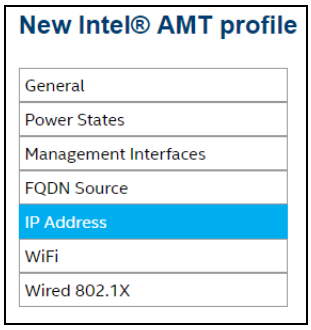
3.4.4 FQDN 设置



选择如何在英特尔主动管理技术上设置主机名和域后缀。

- **Shared with host OS:** 主机名是操作系统中的主机名。域后缀为空白。
- **On-board connection-specific DNS:** 主机名是操作系统中的主机名。域后缀是板载有线 LAN 接口的“连接特定 DNS 后缀”。
- **DNS lookup:** 使用 dnslookup 在板载有线 LAN 接口的 IP 地址上返回的值。此选项需要使用反向查找区域正确配置的 DNS。
- **Primary DNS:** 域后缀（主 DNS 后缀）的主机名均来自操作系统。

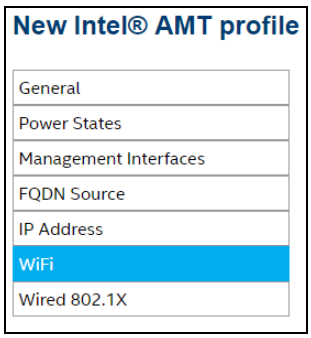
3.4.5 IP 地址设置



选择英特尔主动管理技术如何获取端点（主机）的 IP 地址。

- **From the DHCP server** - 从 DHCP 自动为主机分配 IP 地址时，请使用此选项。
- **Use a static IP address from host** - 当主机具有静态分配的 IP 地址时，请使用此选项。

3.4.6 WiFi 设置



从下列选项中选择:

- **Allow WiFi connection without a WiFi profile** – 如果希望在未设置 WiFi 的情况下（使用主机 WiFi 设置）允许建立 WiFi 连接，选择此选项。
- **Use the selected WiFi profiles** – 如果要定义 WiFi 设置，请选择此选项。可配置的 WiFi 设置总数取决于英特尔主动管理技术的版本。有关更多详情，请参阅第 3.3.1 节。

英特尔主动管理技术包含无线配置文件同步功能。此功能使操作系统中的无线配置文件与英特尔主动管理技术端点中定义的 WiFi 设置同步。当 **Synchronize with host platform WiFi profiles** 复选框被选中，启用了对此功能的支持。要使用此功能同步配置文件，必须在端点上安装英特尔管理引擎组件。请咨询端点的原始设备制造商 (OEM) 以获取这些驱动程序。

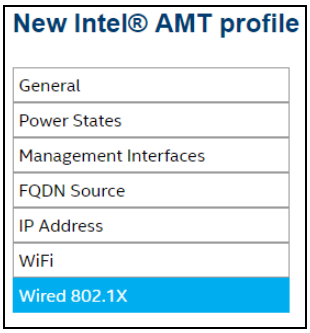
注意： 尽管主机平台的管理员最多可以指定 16 个预配置的 WiFi 配置文件，但是英特尔主动管理技术最多只能同步 8 个配置文件。因此，如果当前已同步所有 8 个配置文件，并且在主机上添加了新的 WiFi 配置文件，则英特尔 EMA 中最旧的同步配置文件将被替换为新的配置文件。

默认情况下，仅当操作系统处于 S0 电源状态时，才可以通过 WiFi 连接连接到英特尔主动管理技术端点。如果要在所有 S0-S5 电源状态下启用 WiFi 连接，请选择 **Enable WiFi connection in all system power states (S1-S5)**。

要启用一键恢复 (OCR) 功能，使其以无线方式运行，请选择 **Enable WiFi profile sharing with UEFI BIOS**。有关 OCR 的更多信息，请参阅第 1.2.11 节。

要创建新的 WiFi 配置文件，请单击 **New…**，然后完成“Define the WiFi Profile”对话框，如第 3.3.1 节所述。

3.4.7 有线 802.1x 设置



选择一个现有的 802.1X 设置以用于有线网络。有关更多详情，请参阅第 3.3.2 节。

要创建新的 802.1X 配置文件，请单击 **New…** 并完成 **Define the 802.1x profile** 对话框，如第 3.3.2 节所述。

3.5 上传证书

角色： 租户管理员

本节介绍了如何上传各种证书，包括企业根证书和英特尔主动管理技术 PKI 证书。

要上传证书：

1. 在左侧的导航窗格中，单击 **Settings**，然后选择 **Server Settings > Certificates**。显示可用的证书列表。
2. 单击 **Upload**。
3. 显示证书对话框。
4. 输入 **Entry Name**，然后单击 **Choose File**。名称以 .CER 结尾的证书文件无需密码。名称以 .PFX 结尾的证书文件需要密码。请注意，上传的证书文件必须小于 1 MB。
5. 在“Certificate”对话框中，单击 **Upload**。

该证书存储在英特尔 EMA 数据库中，并加载到内存中以实现最佳性能。如果进行更改时重新上传了更新的证书文件（包括证书链中的任何证书），则可能需要最多 15 分钟来处理并反映该文件，以使其可供使用。

您也可以下载和删除证书。请注意，如果证书仍被（证书链中的）另一个证书使用，或者在英特尔主动管理技术配置文件或英特尔主动管理技术设置中使用，则无法将其删除。

如果您正在执行初始租户设置，请继续执行第 3.6 节的操作以启用英特尔® 主动管理技术自动设置。

3.5.1 上传英特尔® 主动管理技术 PKI 证书

如果要在管理员控制模式 (ACM) 下在端点上预配英特尔® 主动管理技术，则需要英特尔® 主动管理技术 PKI 证书，这样可以配置用户同意要求。没有 PKI 证书，英特尔® EMA 会以客户端控制模式 (CCM) 预配英特尔® 主动管理技术，这需要用户同意才能在每个端点上执行远程操作。证书文件需要具有完整的证书链。此外，还需要为其发布受支持的 OID 2.16.840.1.113741.1.2.3（这是唯一的英特尔主动管理技术 OID）。

注意： 对于无局域网端点，必须首先手动更新端点的英特尔 MEBX 来添加已上传 PKI 证书的 DNS 后缀，以便英特尔 EMA 将端点从客户端控制模式切换到管理员控制模式。否则，端点将保留在客户端控制模式。查看章节 3.5.2了解详情。

该证书必须是具有正确 OID 或 OU 的有效英特尔主动管理技术 PKI 证书，表明其是英特尔主动管理技术 PKI 证书并包含私钥。英特尔 EMA 不验证证书信息。但是，如果证书值对于正在运行预配过程的域不正确，则预配将失败。

注意：

- 有关 ACM 和 CCM 的更多信息，请参阅英特尔® 主动管理技术文档，以发现获取有效的英特尔® 主动管理技术 PKI 证书的要求和过程。
- 在英特尔® ME 11.0 中，已从固件中删除默认的 SHA1 证书哈希值。但仍可在制造过程中，或者通过英

特尔 MEBX 或 WS-MAN 命令添加哈希值。

- 从英特尔® ME 15.0 台式机固件和英特尔® ME 16.0 全平台固件起，英特尔去掉了对用于英特尔主动管理技术配置且大小小于 2048 字节的 SHA1 根证书和 RSA 密钥的支持。在上述版本和后续版本中，无法再添加 SHA1 哈希值。
- 如果证书即将到期，则必须上传新证书并输入新的 **Entry Name** 和 **Password**。在上传新证书时，请勿将 **Entry Name** 重复用于现有即将过期的证书。您将需要使用新证书的 **Entry Name** 更新使用即将到期证书的任何端点组配置。
- 如果您在运行 Windows Server 2016（低于内部版本 1709）的计算机上安装了英特尔 EMA 服务器，并且证书 PFX 文件使用“AES256-SHA256”加密，则将证书上传到英特尔 EMA 将会失败。即使提供有效的密码，也会显示有关密码无效的错误。
  请参阅第 8 节中“附录：故障排除”了解有关如何适应这种情况的信息。

该证书存储在英特尔 EMA 数据库中，并加载到内存中以实现最佳性能。如果进行更改时重新上传了更新的证书文件（包括证书链中的任何证书），则可能需要最多 15 分钟来处理并反映该文件，以使其可供使用。

您可以为给定的租户上传多个证书，也可以将同一证书上传到多个租户。但是，给定租户中的每个端点组只能具有一个与其关联的 PKI 证书。

有关上传证书的步骤，请参阅第 3.5 节。

您也可以下载和删除证书。请注意，如果证书仍被（证书链中的）另一个证书使用，或者在英特尔主动管理技术配置文件或英特尔主动管理技术设置中使用，则无法将其删除。

如果您正在执行初始租户设置，请继续执行第 3.6 节的操作以启用英特尔® 主动管理技术自动设置。

3.5.2 在英特尔® MEBX 中设置或验证正确的 PKI DNS 后缀

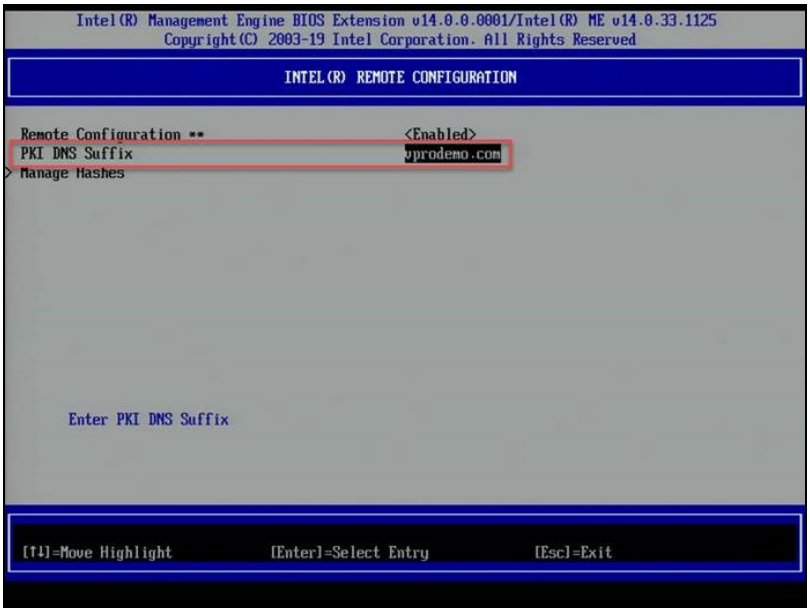
需要完成此过程，以便在无局域网端点上的管理员控制模式 (ACM) 中配置英特尔主动管理技术。对于无局域网设备，英特尔主动管理技术目前没有办法确定是否与 PKI 证书的 DNS 后缀处于同一个域上。因此，为了在 ACM 中配置无局域网端点的英特尔主动管理技术，必须首先手动将 PKI 证书的 DNS 后缀添加到无局域网端点的英特尔 MEBX，如下所述。

英特尔® Management Engine BIOS Extension（英特尔® MEBX）是英特尔主动管理技术系统上的一个 BIOS 菜单扩展。此菜单可用于查看和手动配置某些英特尔主动管理技术设置。只有在重新启动计算机时按专用组合键（通常是 <Ctrl-P>），才会显示该菜单。

对英特尔 MEBX 的访问由密码来控制，在本文档中是指英特尔 MEBX 密码。首次进入英特尔 MEBX 菜单需要设置新密码来替换默认密码（通常是“admin”）。

1. 重新启动无局域网端点并在启动过程中按 **Ctrl-P**。
2. 选择 **Intel MEBX Login**，然后输入英特尔 MEBX 密码。
3. 选择 **Intel(R) AMT Configuration > Remote Setup and Configuration > TLS PKI > PKI DNS Suffix**，进入如下所示的屏幕。请注意，仅当未在此设备上调配英特尔® 主动管理技术时，此菜单选项才可用。
4. 验证或设置 PKI DNS 后缀值，确保与 PKI 证书的域后缀值匹配。

图 7: 英特尔 MEBX PKI DNS 后缀配置



注意： 英特尔 EMA 完全取消了英特尔主动管理技术的设置，并从英特尔主动管理技术设置中删除了任何自定义根证书哈希和 PKI DNS 后缀。这样，如果您取消配置远程网络上的系统，然后又想使用“管理控制模式”来重新配置该系统，则可能需要物理接触该系统才能执行此操作。

3.6 启用英特尔® 主动管理技术自动设置

角色： 租户管理员，端点组创建者†

†具有此组的适当访问权限

注意： 英特尔® 主动管理技术设置也称为英特尔主动管理技术预配。

可以为每个端点组启用或禁用英特尔主动管理技术自动设置。如果启用，则英特尔 EMA 将尝试设置在此端点组中注册的所有端点。如果在部署代理之前定义了英特尔® 主动管理技术自动设置，则当端点断开连接再重新连接到英特尔® EMA 服务器时，或者当代理先连接时，就会触发此设置。

要启用自动设置：

1. 在左侧的导航栏中，选择 **Endpoint Groups**，然后单击目标端点组旁边的下拉箭头并选择 **View Configuration**。
2. 在该端点组的配置页面上，单击 **Intel® AMT Autosetup**。
3. 选择 **Enabled** 复选框，然后选择您先前创建的 **Intel® AMT profile** 。
4. 选择要使用的 **Activation Method** 。仅当此租户至少有一个有效的英特尔主动管理技术 PKI 证书时，才将显示 TLS-PKI 激活方法。租户管理员可以使用“Settings”页面来管理可用的 PKI 证书。请参阅第 3.5.1 节，了解有关 PKI 证书的更多信息。
   有关激活方法的更多详细信息，请参见第 1.2.6 节和第 1.2.7 节。
5. 如果您取消选中“Randomize”复选框（默认选中），则必须输入 **Administrator Password**。您输入的管理员密码将被设置为端点系统上英特尔主动管理技术中“admin”帐户的密码。建议在所有端点上使用随机管理员密码，这样可以确保在一个端点的管理员密码泄露的情况下，其它端点的管理员密码不会泄露。如有必要，可使用英特尔 EMA API 检索端点的随机密码。有关更多信息，请访问 https://www.intel.com/content/www/us/en/support/articles/000055621/software/manageability-products.html，单击 **Detailed HTML API Documentation**，并在浏览器中打开下载的 **Vxswagger.html** 文件，查看《英特尔® EMA API 指南》和在线提供的 API 详细信息。

6. 如果使用 TLS-PKI 激活方法，请选择是否在使用此英特尔主动管理技术配置文件配置的端点上为英特尔® Management Engine BIOS Extension（英特尔® MEBX）设置随机密码。建议让英特尔 EMA 在端点上设置随机的英特尔 MEBX 密码。同样，如有必要，可使用英特尔 EMA API 检索随机密码。如果使用基于主机的预配，将不会显示此操作。
7. 从 **Available Certificates** 中选择一个证书（如果有）。
8. 单击 **Save**。
9. 如果您正在执行初始租户设置，请继续执行第 4 节的操作，以将代理文件部署到您的端点。

如果更改了自动设置中的配置（即更改了英特尔® 主动管理技术配置文件），则英特尔® EMA 将尝试几乎立即将这些更改应用于带内连接的所有端点。对于未连接的端点，当它们重新连接到英特尔® EMA 服务器时，将应用更改。

但是，如果更改了证书或激活方法（即基于主机或 TLS-PKI），则英特尔® EMA 无法自动应用此类更改。您将需要先取消预配端点。

如果管理员密码从随机密码更改为指定密码、从指定密码更改为随机密码，或从指定密码更改为更新的指定密码，则端点系统的管理员帐户密码会更新。

4 将代理部署到端点

角色：不适用；不是任何英特尔 EMA 用户角色专有的

本节介绍如何在目标端点系统上手动安装英特尔 EMA 代理。此程序也适用于希望将英特尔 EMA 代理以脚本形式大规模部署到大量端点系统的用户。

端点主机名称：从英特尔 EMA 1.12.0 开始，端点主机名称支持 Unicode 字符。之前的英特尔 EMA 版本仅支持在主机名称中使用 ASCII 字符。

必须将您在第 3.2 节中创建的两个代理文件 **EMAAgent.exe** 和 **EMAAgent.msh** 复制到您要使用英特尔 EMA 管理的每个端点系统。可以手动将它们复制到端点系统，也可以使用大规模部署工具。无论采用哪种方式，这两个文件都必须位于端点系统上的同一文件夹中，并且必须使用相同的文件名前缀（即 EMAAgent）。

注意：有关如何将英特尔 EMA 代理安装为控制台的信息，请参阅第 10 节。

下表描述了每个此类文件的属性。

表 1: 英特尔® EMA 代理文件

文件名	描述
EmaAgent.exe	这是代理安装文件。要安装/更新/卸载任何实例，就必须以管理员权限执行此文件。
EmaAgent.msh	这是策略文件。此文件确定了该端点将属于哪个端点组，并使英特尔 EMA 代理能够联系英特尔 EMA 服务器。

注意： 英特尔 EMA 代理并不适合在目标端点上的 VM 中运行，即使在基础管理程序上也是如此。LAN/WLAN 无法正确解读多个 IP 地址。未写入任何管理程序以适应使用英特尔主动管理技术所需的地址转换。这会影响代理连接到英特尔主动管理技术和在端点上执行带外 (OOB) 操作的能力。在这种情况下，或许可以有效执行带内操作，但并不确定。

要在端点系统上进行安装：

1. 将两个代理文件 EMAAgent.exe 和 EMAAgent.msh 从创建它们的系统上的“下载”文件夹复制到目标端点系统。确保将两个文件放在同一文件夹中。
2. 在端点系统上，打开具有管理员权限的命令窗口 (cmd.exe)，然后转到两个代理文件所在的文件夹。
3. 运行以下命令以安装英特尔® EMA 代理。

```
EmaAgent.exe -fullinstall
```

注意：如果您希望代理能够访问代理网络，则必须在该端点上为代理配置代理网络。请参阅第 4.4 节

卸载：

```
EmaAgent.exe -fulluninstall
```

要查看代理安装程序的相关帮助：

```
EmaAgent.exe -?
```

注意：也可通过在 Windows 资源管理器中右键单击 EmaAgent.exe 文件并选择“以管理员身份运行”，将代理安装程序作为 GUI 运行。在“安装程序”对话框中，单击“安装/更新”。

有关安装验证和故障排除信息，请参阅第 4.5 节。

4.1 安装目录

Win64 服务的默认安装目录是 C:\Program Files\Intel\Ema Agent。

两种服务都将包括以下文件：

- EmaAgent.exe：可执行服务文件。
- EmaAgent.log：用于本地日志记录。
- EmaAgent.msh：安装的策略文件
- EmaAgent.db：英特尔 EMA 代理数据库

4.2 英特尔® EMA 代理数据库

安装代理服务后，将生成一个本地数据库来保存设置和证书。数据库与代理正在运行的可执行二进制文件存储在同一路径中。

4.3 Windows 服务信息

将代理安装为 Windows 服务后，可以使用 Windows 服务管理器对其进行访问。

1. 同时按 Windows 键和 R 键打开 **Run** 窗口。
2. 在 **Run** 窗口中输入 **services.msc**。
3. 按 **Enter** 键。
4. 这将显示 Windows 中所有已安装的服务。
5. 要查找代理服务，请查找 **Intel(R) EMA Agent background service** 名称。
6. 选择代理服务，然后检查其是否正常运行。
7. 此时，可以根据需要停止或重新启动服务。如果该服务已经停止，则可以启动它。

4.4 代理服务器配置

如果您希望端点上的代理能够访问代理网络，则必须在该端点上为代理配置代理网络。

要在端点上安装代理并同时指定代理网络，请在目标端点上使用以下命令：

```
EmaAgent.exe -fullinstall -proxy:<address>:<port>
```

代理在端点上的安装目录中创建一个名为 **EmaAgent.proxy** 的文件，其中存储您指定的 HTTPS 代理的值。

如果您在运行安装程序时不使用 -proxy 参数，则当前在 Windows“控制面板”的“LAN 设置”对话框中为您在运行安装程序时的登录用户配置的任何 Windows 代理网络设置都将应用于代理（即，存储在 EmaAgent.proxy 文件中）。请注意，英特尔 EMA 不处理 **Automatic configuration** 设置（即，“LAN 设置”对话框的上半部分）；仅存储 **Proxy server**（下半部分）设置。

4.5 代理安装验证和故障排除

您可以使用英特尔 EMA 代理的命令行界面来显示有关与英特尔 EMA 服务器的连接的信息。在安装代理的端点上执行以下步骤。

1. 以管理员身份打开命令提示符窗口。
2. 将目录更改为英特尔 EMA 代理安装目录（请参阅第 4.1 节）。
3. 执行以下命令之一。

测试代理是否正在运行

命令:

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

示例 (成功) :

```
λ tasklist /fi "imagename eq EmaAgent.exe"
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
EmaAgent.exe                 15396 Services                   0     42,816 K
```

示例 (失败) :

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

测试代理是否已连接

命令:

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

示例 (成功) :

```
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
```

示例 (失败) :

```
λ netstat -nao | find "8080"
(returns empty results)
```

获取 Swarm 服务器名称

命令:

```
EMAAgent.exe -swarmserver
```

示例 (成功) :

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

示例 (失败) :

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

获取代理节点 ID

命令:

```
EMAAgent.exe -nodeidhex
```

示例 (成功) :

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

示例 (失败) :

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

获取代理服务器信息

命令:

```
EMAAgent.exe -agentproxy
```

示例 (成功) :

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

示例 (失败) :

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

测试是否可以访问英特尔® EMA 服务器

命令:

```
powershell.exe test-netconnection -computername <ema-fqdn> -port 8080
```

示例 (成功) :

```
ComputerName : <ema-fqdn>
RemoteAddress : <server IP address>
RemotePort : 8080
InterfaceAlias : Ethernet 2
SourceAddress : <client IP address>
TcpTestSucceeded : True
```

示例 (失败)

```
ComputerName : <ema-fqdn>
RemoteAddress : <server IP address>
```

```
RemotePort : 8080
InterfaceAlias : Ethernet 2
SourceAddress : <client IP address>
PingSucceeded : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded : False
```

5 管理用户和用户组

根据组织的规模和复杂性，您可能决定需要更多用户来帮助管理端点（有关用户角色的信息，请参阅第 1.2.2 节）。

为了使用户能够管理端点组中的端点，必须将用户分配给与其要管理的端点组相同的用户组（请参阅第 1.2.4 节）。

5.1 添加、修改和删除用户

角色： 租户管理员，客户经理，全局管理员

1. 在左侧导航条上选择 **Users**（或单击 **Overview** 页面上 **Users** 下的 **Add or remove users**）。
2. 要添加用户，请单击 **New User…**。
3. 输入用户信息，然后单击 **Save**。
4. 要将新用户添加到用户组，请单击新用户旁边的向下箭头并选择 **Group memberships**，然后选择该用户应属于的组。

注意：

- 要更改您自己的用户帐户的密码，必须首先输入当前密码。如果您正在编辑其他帐户（您的角色可以管理的账户），则无需输入用户的当前密码。
- 对于“锁定”用户，请单击向下箭头并编辑用户以解锁帐户。
- 如果已在此租户中创建了一个客户端凭据帐户，则您可能会看到列出了一个具有租户管理员角色，并且用户名格式不是电子邮件帐户格式（即 user@domain.com）的用户。有关客户端凭据帐户的信息，请参阅第 11 节“附录 - 从计算机到计算机客户端应用程序执行英特尔® EMA 端点操作”，P63。
- 如果您将英特尔 EMA 配置为使用 Active Directory 身份验证，请确保您创建的任何用户的用户名都与 Active Directory 用户的 userPrincipalName 属性相对应。在此模式下，未显示或不需要“密码”字段。
- 如果您已将英特尔 EMA 配置为使用 Azure AD 身份验证，则无法删除您在安装过程中创建的初始帐户，也无法编辑此帐户的角色。但是，您可以编辑初始帐户的密码。此外，请确保您创建的任何用户的用户名与 Azure AD 用户的通用主体名称 (UPN) 相匹配。在此模式下，不显示或不需要密码字段。
- 如果您已将英特尔 EMA 配置为使用正常（用户名/密码）身份验证，则在创建新用户或更新现有用户的密码时，将根据密码策略检查密码。全局管理员可以使用 **Security Settings** 中的 **Settings** 来配置密码策略。默认情况下，密码策略要求密码最小长度为 8 个字符，最大长度为 255 个字符，要求使用复杂密码（大写/小写/数字/特殊字符），并会对照禁用密码列表进行检查。

要编辑或删除现有用户，请单击该用户旁边的向下箭头，然后选择 **Edit** 或 **Delete**。

5.2 创建新的用户组

角色： 租户管理员，客户经理，全局管理员

1. 在左侧导航栏上选择 **Users**，然后单击 **User Groups** 选项卡。
2. 选择 **User Groups** 选项卡，单击 **New Group** 并输入 **Group Name** 和 **Description**，然后选择准备向该用户组中的用户授予的访问权限。

   注意：

   - 如果您尚未创建至少一个租户（只有全局管理员），则 **New Group** 按钮将被禁用（显示为灰色）。

     Description 是必填字段，在提供该值前，您将无法保存该组。

3. 单击 **Members** 并选择要添加到此用户组的用户（或者您可以稍后在创建新用户时执行此操作）。
4. （对全局管理员不可用）单击 **Endpoint Groups**，然后选择该用户组将有权访问的端点组。

要编辑或删除现有用户组，请单击该用户组旁边的向下箭头，然后选择 **Edit** 或 **Delete**。如果删除用户组，则与该组关联的用户和端点不受影响。

5.3 将端点组分配给用户组

角色： 租户管理员，端点组创建者†

†具有此组的适当访问权限

如第 1.2.4 节所述，用户组用于管理用户对端点组的访问，从而管理对端点本身的访问。为了使用户能够在特定端点组中的端点上执行管理任务，该用户和端点组必须属于同一用户组。

1. 在左侧导航栏上选择 **Users**，然后单击 **User Groups** 选项卡。
2. 单击目标用户组的向下箭头并选择 **Assign Endpoint Groups**。
3. 在对话框中，选择目标端点组及其关联的权限，然后单击 **Save**。

6 管理端点

角色： 租户管理员，端点组创建者（基于组和权限），端点组用户（基于组和权限）

设置租户以反映组织的结构之后，就可以开始使用英特尔® EMA 来管理端点系统了。

6.1 英特尔® 主动管理技术按需设置

英特尔® 主动管理技术设置也称为英特尔主动管理技术预配。

可以在单个端点上按需执行英特尔主动管理技术设置/清除操作。但是，不能在按需设置中使用英特尔主动管理技术配置文件。英特尔主动管理技术配置文件下拉菜单被停用。按需设置将执行非常基本的配置。有关更多详情，请参阅第 1.2.7 节。

要访问此页面，请打开端点的操作下拉菜单，然后选择“Provision Intel® AMT”。仅当目标端点支持英特尔主动管理技术时，才启用此选项。然后，您可以使用此页面来预配或取消预配英特尔主动管理技术（要取消预配，请使用如图 8 所示的 **Remove provisioning** 按钮。

关于激活方法：

- 当此租户至少有一个有效的英特尔主动管理技术 PKI 证书时，将显示 TLS-PKI 激活方法。租户管理员可以使用“Settings”页面来管理可用的 PKI 证书。有关更多详情，请参阅第 3.5.1 节。
- 即使选择了 TLS-PKI，英特尔 EMA 仍然使用基于主机的流程来设置英特尔主动管理技术。

您输入的管理员密码将设置为英特尔主动管理技术中管理员帐户的密码。

选择是否在端点上为英特尔® Management Engine BIOS Extension（英特尔® MEBX）设置随机密码（仅适用于 PKI 调配）。建议让英特尔 EMA 在端点上设置随机的英特尔 MEBX 密码。如有必要，可使用英特尔 EMA API 检索端点的随机密码。有关更多信息，请参阅《英特尔® EMA API 指南》。

注意： 如果您取消调配端点，则将从英特尔 EMA 数据库中删除随机的英特尔 MEBX 密码，因此 API 无法检索该密码。取消调配端点之前，请确保检索其英特尔 MEBX 密码并记下该密码。这对于没有 LAN 的系统尤其重要，因为在重新调配之前，可能需要重置英特尔 MEBX 中的 PKI DNS 后缀。有关没有 LAN 的系统的更多信息，请参阅第 3.5.2 节。

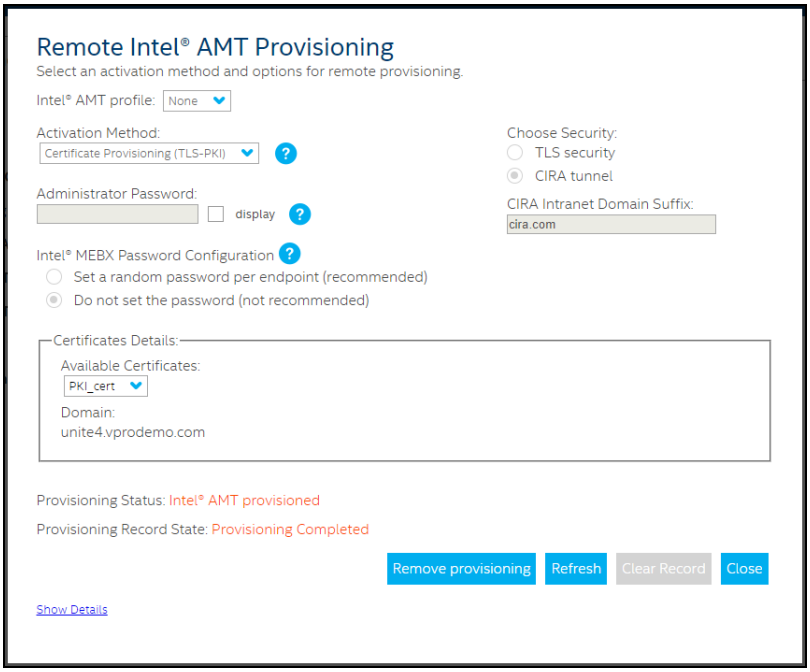
对于 CIRA 或 TLS 中继，请参阅第 1.2.6 节以获取详细信息。

Provision Status: 这是目标英特尔主动管理技术的预配状态。

Provision Record State: 这是当前的设置/清除操作状态。英特尔 EMA 会维护每个英特尔主动管理技术设置的设置/预配记录。该记录指示端点的设置状态。如果设置/预配过程失败，英特尔 EMA 将再次选取该记录并定期重试。因此，在进行设置/预配的过程中，您将看到“Clear Record”按钮。如果清除了记录，则英特尔 EMA 将不会尝试任何进一步的预配操作。

当“Provision Status”为“Provisioned”且“Provision Record”状态为“Complete”时，说明目标英特尔主动管理技术的设置已完成。

图 8: 按需预配英特尔® 主动管理技术



6.2 英特尔® EMA 代理

英特尔® EMA 代理通过 TCP 和端口 8080 连接到英特尔 EMA 服务器。安装英特尔 EMA 代理后，它将为已安装的代理二进制进程设置以下 Windows 防火墙入站规则。如果使用其他防火墙，请确保为已安装的代理二进制进程设置了以下入站规则：

- 点对点流量：阻止本地端口为 16990 的 UDP、本地和远程地址的任何 IP 以及边缘遍历。
- 点对点流量：阻止本地端口为 16990 的 TCP、本地和远程地址的任何 IP 以及边缘遍历。
- 本地环回管理流量：阻止本地端口为 16991 的 TCP、本地和远程地址 127.0.0.1 以及边缘遍历。

有关英特尔 EMA 代理故障排除的信息，请参阅第 4.5 节。

6.2.1 代理 Windows 注册表信息

代理安装所创建的注册表项取决于 Microsoft Windows 操作系统和英特尔 EMA 代理（控制台和服务）的架构。这些是架构提供的英特尔 EMA 代理的注册表路径：

- Win64 服务：
  - HKEY_LOCAL_MACHINE -> “Software\Intel\EmaAgent”
- Win64 控制台：
  - HKEY_CURRENT_USER -> “Software\Intel\EmaAgent”

在安装/运行英特尔 EMA 代理时，此注册表项根中应存在以下注册表项：

- **MeshId** - 包含 MSH 文件中端点组 ID 的 REG_SZ；如果不存在 MSH 文件，则该值为空。
- **MeshName** - 包含 MSH 文件中端点组名称的 REG_SZ；如果不存在 MSH 文件，则该值为空。
- **NodeId** - 包含端点 ID 的 REG_SZ。

  注意： 端点 ID 与代理根证书相关联。服务/控制台使用不同的根证书。

- **Version** - 包含正在运行的 EmaAgent 的版本号的 REG_DWORD。

- **EnhancedLoggingLevel** - 包含日志记录级别的 REG_DWORD。默认情况下，此项设置为 3，这会禁用增强型调试日志记录。要启用增强型调试日志记录，请编辑注册表并将 EnhancedLoggingLevel 设置为 4。

6.3 查看端点

租户管理员、端点组创建者和端点组用户可以在 **Managed Endpoints** 页面上查看他们有权访问（具有适当访问权限）的端点。

在左侧导航栏中选择 **Endpoints**，然后选择 **Managed Endpoints** 选项卡。

如果您当前管理的端点数量不超过 1000 个，则会自动加载这些端点以供显示。如果您管理的端点数量超过 1000 个，请单击 **Load all Endpoints** 按钮以查看当前管理的所有端点。这一过程可能需要花几分钟时间。

您还可以在 **Search** 字段中输入搜索条件，搜索与指定条件匹配的端点。

显示结果后，左侧会出现 **Filter** 面板。要筛选结果，请选择所需的筛选条件。

注意：显示的 **Connection** 状态是带内连接状态。

有关特定端点的更多信息，请单击 **View** 列表中的某个端点以访问其信息页面。以下小节将介绍此页面上的选项卡。

6.3.1 “General”选项卡

显示有关所选端点的常规信息。

注意：

- **Manage this endpoint** 下拉菜单选项在第 6.4 节中有所描述。
- 连接状态为带内连接。
- 当英特尔® EMA 设置/配置了端点的英特尔® 主动管理技术固件后，如果在英特尔主动管理技术的配置文件管理接口设置中已启用基于 Web 的用户界面，则能够使用“设备页面”链接访问该端点上英特尔主动管理技术的默认 Web 界面。如果没有启用基于 Web 的用户界面，则将不会显示“设备页面”链接。
- 英特尔® 管理引擎版本和设置状态在此页面显示。如果设置了英特尔® ME，但英特尔® EMA 没有设置记录，则会显示警告。

6.3.2 “Hardware Manageability”选项卡

允许您执行许多带外英特尔® 主动管理技术操作。为了使它正常工作，必须由当前的英特尔® EMA 实例配置英特尔® 主动管理技术。也就是说，无法使用此选项卡对由其他英特尔 EMA 实例配置的端点进行操作。

从左侧窗格的操作列表中选择要执行的操作。

注意：

- 请勿使用此选项卡更改任何英特尔® 主动管理技术设置。这样做可能会导致端点失去可管理性。
- 此选项卡将英特尔® Manageability Commander（英特尔® MC）集成到英特尔 EMA 用户界面中。此选项卡上的操作通过英特尔® MC 来执行。有关该列表中可用操作的信息，请参阅以下链接提供的英特尔® MC 用户文档。
  https://downloadmirror.intel.com/27807/Intel%20Manageability%20Commander%20User%20Guide.pdf
- 为 CIRA 预配的端点的 IP 地址将在 “Hardware Manageability” 选项卡上报告为 **unknown** 。但是，在英特尔® AMT 网页上，此端点的 IP 地址将报告为 **0.0.0.0**。
- 如果端点使用新式待机，则为了成功从新式待机唤醒，端点必须安装英特尔 HID（人机界面驱动程序）事件过滤器器件驱动程序，并实施支持英特尔专有唤醒功能的 BIOS。另外，通过远程桌面建立连接或使用鼠标/键盘也会将系统从新式待机唤醒。

6.3.3 “Desktop”选项卡

允许您使用带内远程 KVM 功能更改以下设置：

Disconnect	断开当前的带内 KVM 会话。
Select display	如果端点有多个显示，则可以选择要查看的目标显示。
Scale	调整屏幕呈现分辨率的缩放百分比。值越小意味着分辨率降低得越多。如果使用 50%（一半）或 100%（全部），则将获得最佳结果。
Quality	调整位图压缩级别。较小的值表示更多的压缩，但分辨率降低。
	旋转呈现在英特尔® EMA 上的显示。当目标端点显示处于纵向模式时，此功能很有帮助。
	通过带内 KVM 将纯文本从控制台系统的剪贴板（即运行英特尔 EMA Web 版用户界面的计算机）粘贴到当前目标端点。  **注意：** • 在剪贴板功能中使用“粘贴”之前，您必须为浏览器提供剪贴板的访问权限。对于 Internet Explorer 和 Chrome，首次单击“粘贴”图标时，您将收到自动提示。对于 Firefox，您必须在 Firefox 中手动更新偏好设置，将以下两项设置为“True”：**dom.events.asyncClipboard** 和 **dom.events.testing.asyncClipboard**。 • 如果您发现目标端点上的粘贴输出中出现意外的字符或大小写，请参阅第 8 节“附录：故障排除”，P47下的主题“从剪贴板进行带内KVM 粘贴导致意外的字符或大小写”。
Ctrl + Alt + Del	发送“Ctrl + Alt + Del”组合键。Web 浏览器所运行的 Windows 操作系统会拦截几种特殊的组合键。使用此选项将“Ctrl + Alt + Del”发送到远程系统。
	将 KVM 扩展为全屏显示。此功能利用 Web 浏览器的全屏 API 将远程 KVM 扩展为全屏模式。要退出此模式，请使用 Web 浏览器的内置控件（例如：**Esc** 键）。

如果满足以下任一条件，则将禁用此选项卡：

- 端点组政策不允许执行此操作
- 端点未带内连接至 Intel EMA
- 已登录用户没有对端点的适当访问权限

 **注意：**

- 用户同意带内 KVM 将影响此功能的行为。有关详细信息，请参阅第 3.1.1 节。
- 首次启动带内 KVM 会话时，将显示连接到端点的所有显示器的内容。
- 在 1.12.0 之前的英特尔 EMA 版本中，Windows 显示 UAC 提示或注销 Windows 等事件会导致显示所有显示器。发生此类事件时，英特尔 EMA 1.12.0 及更高版本将保留显示器选择。
  - 如果发生此类事件之一时正查看 Windows 中主显示器之外的显示器，则可能会看到黑屏，并需要使用显示器选择下拉菜单切换到主显示器。
- 如果选择的显示器在带内 KVM 远程控制会话期间不可用，则英特尔 EMA 将默认在远程控制窗口中显示所有可用显示器。

- 在多个用户（即 Web 浏览器）连接到同一端点的 KVM 的情况下，请注意以下几点：
  - 如果先前的同意请求仍处于活跃状态，则不会再次请求用户同意
  - 所有会话将与鼠标和键盘输入竞争
  - 比例、位图质量和显示选择将影响所有会话
  - 旋转只会影响当前的浏览器

6.3.4 终端选项卡

提供带内和带外远程终端功能。仅支持基于文本的命令。

如果满足以下任一条件，则将禁用此选项卡：

- 端点组政策不允许执行此操作
- 已登录用户没有对该端点的适当访问权限
- 如果未设置端点，并且该端点未带内连接到英特尔® EMA。

“英特尔® 主动管理技术终端”是 LAN 串行 (SOL) 终端。如果与端点的 BIOS 交互，则 BIOS 必须是文本版本的 BIOS。

单击 **Actions** 菜单并从以下选项中选择：

- **Start Terminal** - 用于未配置英特尔主动管理技术的端点。带内。
- **Start Intel AMT Terminal** - 如果未预配端点，则处于禁用状态。用于在已配置英特尔主动管理技术的端点上与除 BIOS 以外的 SOL 工具和应用程序（例如，Windows PowerShell）交互。
- **Boot to BIOS** - 如果未预配端点，则处于禁用状态。用于将已配置英特尔主动管理技术的端点引导至文本版本的 BIOS，并在引导后与 BIOS 交互。请注意，端点的 BIOS 必须支持此功能。此外，BIOS 的显示方式可能会因具体的 BIOS 实施方式而异。显示的信息来自端点的 BIOS，并且退出 BIOS 后文本可能不会被清除，具体取决于 BIOS 的实施方式。您还必须选择 **Start Intel AMT Terminal** 才能看到显示的 BIOS 文本。此功能需要用户同意，这会触发端点屏幕上显示的 6 位数用户同意代码。您必须联系端点用户并输入此代码，才能执行此操作。
- **Disconnect** - 断开会话。

注意：
如果在终端窗口中运行 Windows PowerShell，请在输入命令时不要使用大写字母（Shift + <字母键>），因为这将导致 Windows PowerShell 退出并返回命令提示符。Ctrl + <任意键>也是如此。仅使用小写字母输入所有命令。大多数命令都不区分大小写。有关区分大小写的信息，请参阅以下链接：

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

请注意，启用 Caps Lock 允许您输入大写字母而无需退出 Windows PowerShell。

6.3.5 “Files Tab”选项卡

提供带内远程文件浏览功能。从英特尔 EMA 1.12.0 开始，文件名支持 Unicode 字符。之前的英特尔 EMA 版本仅支持 ASCII 文件名。

如果满足以下任一条件，则将禁用此选项卡：

- 端点组政策不允许执行此操作
- 端点未带内连接至 Intel EMA
- 已登录用户没有对端点的适当访问权限

6.3.6 进程选项卡

提供带内远程进程管理功能。此功能是通过 Windows Management Instrumentation (WMI) 实现的。使用它来执行以下操作：

- 查看正在运行的进程列表。
- 在托管端点上启动新进程。您必须提供目标可执行文件的有效本地路径。
- 终止进程。

如果满足以下任一条件，则将禁用此选项卡：

- 端点组政策不允许执行此操作
- 端点未带内连接至 Intel EMA
- 已登录用户没有对端点的适当访问权限

6.3.7 “WMI”选项卡

允许您在目标端点上运行 Windows Management Instrumentation (WMI) 查询或 WMI 操作。

如果满足以下任一条件，则将禁用此选项卡：

- 端点组政策不允许执行此操作
- 端点未带内连接至 Intel EMA
- 已登录用户没有对端点的适当访问权限

6.4 在端点上执行操作

在 **Managed Endpoints** 页面上，至少选择一个端点，然后单击 **Select an endpoint action** 下拉菜单。

以下各子节介绍了可用的端点操作。

6.4.1 唤醒

通过英特尔® 主动管理技术或 LAN 唤醒向一个或多个端点发送唤醒请求

注意：仅在英特尔® vPro® 平台上支持 LAN 唤醒。

如果仅选择一个端点，则如果满足以下任一条件，将不执行该操作：

- 如果端点组的策略不允许执行此操作
- 如果已登录用户没有对该端点的适当访问权限

6.4.2 设置闹钟

此项英特尔主动管理技术功能允许您为端点设置最多 5 个闹钟。闹钟在指定的日期和时间将端点唤醒。

注意：

- 要查看现有闹钟，用户必须处于与目标端点组关联的用户组中。
- 具有 HasPowerOperationsAccess 权限的端点组用户和端点组创建者用户角色可以查看、创建和删除闹钟。
- 有关用户角色的更多信息，请参阅第 1.2.2 节。有关用户组和权限的更多信息，请参阅第 1.2.4 节。

要设置闹钟：

1. 从 "Endpoint Details" 页面选择 **Actions > Alarm Clock**。
2. 在 "Alarm Clock" 对话框中，单击 **Add New Alarm**。

3. 输入闹钟的名称。
4. 使用 **Wake up this endpoint at** 下的控件来设置闹钟的日期和时间。
5. 如果您希望闹钟将来可重复执行，请选择 **Recurring**，然后指定重复周期的天数、小时数和分钟数。
6. 如果您希望闹钟在执行后即删除，请选择 **Delete on Completion**。
7. 单击 **OK** 设置指定的闹钟。
8. 现在新的闹钟名称将显示在 "Alarm Clock" 对话框的第一行中。

要删除闹钟：

要删除闹钟，请从 "Endpoint Details" 页面选择 **Actions > Alarm Clock**，然后从 "Alarm Clock" 对话框的第一行中选择所需的闹钟，并单击 **Delete**。

6.4.3 睡眠/休眠/关机/重启

可以在一个或多个端点上执行此操作。

如果目标端点采用带内连接，则通过端点的操作系统执行带内电源操作。如果目标不是带内连接的，但具有完整的英特尔® 主动管理技术配置记录，则将执行关联的英特尔主动管理技术电源操作（分别处于深度睡眠、休眠、软关机、软关机并重新开机）。

如果仅选择一个端点，则如果满足以下任一条件，将不执行该操作：

- 如果端点组的策略不允许执行此操作
- 如果已登录用户没有对该端点的适当访问权限

6.4.4 发送提醒

允许您以弹出窗口的形式向一个或多个端点（通过带内连接）发送提醒消息。

要发送提醒，请输入要显示的消息，然后选择显示消息的持续时间，然后单击“发送”。

如果仅选择一个端点，则如果满足以下任一条件，将不执行该操作：

- 如果端点组的策略不允许执行此操作
- 如果已登录用户没有对该端点的适当访问权限
- 如果端点不是带内连接到英特尔 EMA

6.4.5 远程文件搜索

允许您对一个或多个端点（通过带内连接）执行远程文件搜索。文件搜索依赖于 Windows 索引。

输入要搜索的字符串，然后单击搜索。要下载结果文件，只需单击即可。

如果仅选择一个端点，则如果满足以下任一条件，将不执行该操作：

- 如果端点组的策略不允许执行此操作
- 如果已登录用户没有对该端点的适当访问权限
- 如果端点不是带内连接到英特尔 EMA

6.4.6 停止管理端点

允许您从英特尔® EMA 删除此目标端点。但是，这不会阻止端点将来重新连接并重新注册到英特尔 EMA。此外，系统仍已预配。如果对系统进行了预配，就可以看到端点的管理员密码和英特尔 MEBx 密码。

注意：强烈建议您在通过此命令停止管理之前，先通过英特尔 EMA UI 取消预配托管端点上的英特尔主动管理技术（有关如何使用英特尔 EMA 取消预配英特尔主动管理技术，请参阅第 6.1 节）。如果在没有首先取消预配英特尔主动管理技术的情况下停止管理，可能会导致难以在英特尔 EMA 中重新注册端点（端点显示为属于另一个工具）。

仅当以下两项均成立时，才会启用此操作：

- 选择一个端点
- 已登录用户具有对所选端点的适当访问权限

6.4.7 配置英特尔® 主动管理技术

打开英特尔® 主动管理技术的预配信息。有关详细信息，请参阅第 6.1 节。

仅当以下所有项均成立时，才会启用此操作：

- 选择一个端点
- 所选端点具有英特尔® 主动管理技术功能
- 所选端点已带内连接至英特尔 EMA
- 已登录用户具有对所选端点的适当访问权限

6.4.8 查看台式机

允许您查看（无远程输入控制）一个或多个端点的多个远程带内 KVM。

注意： 用户同意带内 KVM 将影响此功能的行为。有关详细信息，请参阅第 3.1.1 节。

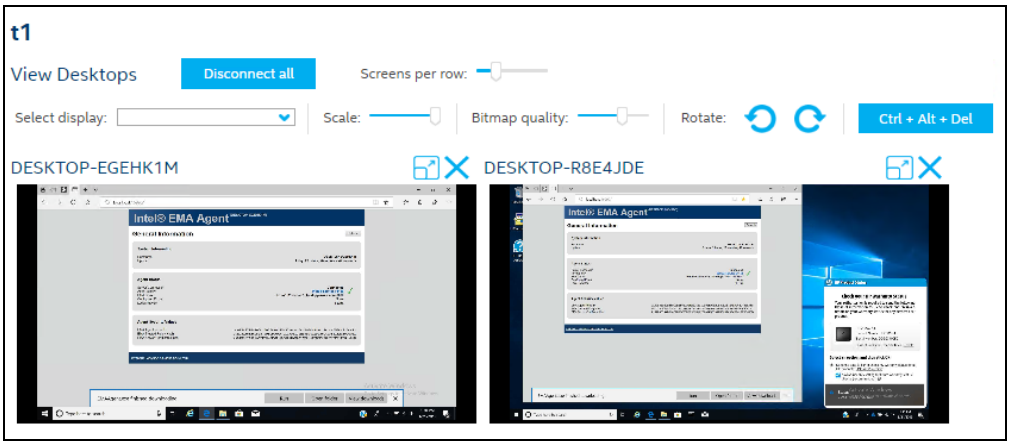
如果仅选择一个端点，则如果满足以下任一条件，将不执行该操作：

- 如果端点组的策略不允许执行此操作
- 如果已登录用户没有对该端点的适当访问权限
- 如果端点不是带内连接到英特尔® EMA

选择端点的目标 KVM。目标端点突出显示后，您可以更改显示设置，然后为该目标 KVM 按 **Ctrl+Alt+Del**。

您也可以单击每个 KVM 的展开按钮以打开该端点的远程 KVM 选项卡。

图 9: 多桌面查看



6.4.9 安装映像

通过 USB 重定向 (USBR) 将存储的映像文件（.iso 或 .img）安装到当前端点。有关 USBR 的更多信息，请参阅第 1.2.8 节。只能从端点的“Details”页面选择此菜单项。

注意： 如果目标端点的英特尔主动管理技术固件是在客户端控制模式 (CCM) 下预配的，或在启用了“Consent Required”设置的管理员控制模式 (ACM) 下预配的，则端点的屏幕上会显示 6 位数用户同意代码，您必须联系端点用户才能获得该代码。输入用户同意代码后，即可在端点上执行此操作。请参阅第 1.2.7 节了解 CCM 和

ACM 的相关信息。此外，您可以参考英特尔主动管理技术文档以获取有关 ACM、CCM 和用户同意的详细信息 (https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm)。

要装载映像，请按照以下步骤操作：

1. 从 **Endpoint Actions** 下拉列表中选择 **Mount an Image**。
2. 从列表中选择其中一个映像。
3. 单击 **Start**。这会触发端点屏幕上显示的 6 位数用户同意代码。
4. 联系端点用户并请其提供 6 位数用户同意代码，该代码应该会显示在他们的屏幕上。输入端点用户提供的代码。

操作完成后，会有一个 **Storage Redirection** 条幅出现在端点“Details”页面的左下角，指示该端点的活跃 USBR 会话以及已安装映像文件的名称。

要卸载映像文件，请在“Details”页面 **Unmount Image** 条幅下单击 **Storage Redirection**。

有关上传和存储映像文件的详细信息，请参阅第 7 节。

6.4.9.1 映像建议

尽可能使用小映像，以防止在将端点重新引导到所安装映像时发生超时。此外，如果您计划通过 KVM 与重新引导的端点进行交互，则引导到的映像必须包含 USB 键盘和鼠标驱动程序。

一种将端点重新引导到所安装映像的推荐方法是使用两部分映像。首先，将端点引导到小映像，以便在网络上启动该端点。然后使用该映像从端点访问更多内容。

注意： 当前的已知问题是英特尔主动管理技术通过 USBR 引导一些 UDF 格式化映像。有时，UDF 格式化映像可能无法引导或无法完全引导。我们建议使用 CDFS 格式化映像，直到此问题得到解决。

6.4.9.2 引导到此映像

将选定端点引导至安装的映像文件（.iso 或 .img）。

注意： 执行此操作前，必须先将映像文件安装到端点。有关安装映像文件的更多信息，请参阅第 6.4.9 节。

将映像文件安装到此端点后，请单击端点“Details”页面上 **Storage Redirection** 条幅下的 **Boot to this Image**。

注意： 建议您使用签名的映像文件，因为 BIOS 中的安全引导会阻止加载未签名的映像。如果安全引导阻止映像加载，则端点可能会引导到其内部驱动器。

要验证是否已成功完成端点引导操作，请使用“Hardware Manageability”选项卡并将 KVM 会话（远程桌面）执行到重新引导的端点，以确保端点引导至选定映像。映像必须包含用于 KVM 交互的 USB 键盘和鼠标驱动程序。

6.4.10 引导至恢复映像

使用英特尔主动管理技术的”一键恢复“功能，将端点引导至所选的恢复映像。

小心： 此操作可能会擦除端点的硬盘。请谨慎操作！

恢复映像列表由端点平台本身的预配置恢复映像以及已上传到英特尔 EMA 服务器的映像（即 .ISO）组成。但是，如果由于某种原因禁用了恢复服务器，则仅显示端点平台本身的映像（不显示从英特尔 EMA 服务器上传的映像）。

列表中显示的映像取决于端点平台支持的方法（HTTPS、PBA 或 WinRE）。如果您计划选择使用 HTTPS 的映像，则必须在端点的 BIOS 中启用 HTTPS 引导。有关这方面的说明，请参阅第 1.2.11 节。

注意： 如果目标端点的英特尔主动管理技术固件是在客户端控制模式 (CCM) 下预配的，或在启用了“Consent Required”设置的管理员控制模式 (ACM) 下预配的，则端点的屏幕上会显示 6 位数用户同意代码，您必须联系

端点用户才能获得该代码。输入用户同意代码后，即可在端点上执行此操作。请参阅第 1.2.7 节了解 CCM 和 ACM 的相关信息。此外，您可以参考英特尔主动管理技术文档以获取有关 ACM、CCM 和用户同意的详细信息 (https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm)。

要引导至恢复映像：

1. 从列表中选择一个恢复映像。
2. 单击 **Start**，确认您想要执行此操作。这会触发端点屏幕上显示的 6 位数用户同意代码。
3. 联系端点用户并请其提供 6 位数用户同意代码，该代码应该会显示在他们的屏幕上。输入端点用户提供的代码。

此时，端点重新引导至选定的恢复映像。

6.4.11 平台擦除

远程擦除所有平台信息，包括平台的英特尔主动管理技术信息（可选）。

注意： 如果目标端点的英特尔主动管理技术固件是在客户端控制模式 (CCM) 下预配的，或在启用了“Consent Required”设置的管理员控制模式 (ACM) 下预配的，则端点的屏幕上会显示 6 位数用户同意代码，您必须联系端点用户才能获得该代码。输入用户同意代码后，即可在端点上执行此操作。请参阅第 1.2.7 节了解 CCM 和 ACM 的相关信息。此外，您可以参考英特尔主动管理技术文档以获取有关 ACM、CCM 和用户同意的详细信息 (https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm)。

从下拉菜单中选择 **Platform Erase** 后，选择要执行的平台擦除选项。

Complete Factory Reset	选择所有选项
SSD Erase	通过介质擦除和加密擦除相结合的方式移除 ATA 和 NVM 驱动器中的所有内容。
Pyrite Revert	将驱动器恢复到原始出厂状态。
Clear BIOS Non-Volatile Memory	清除 BIOS 内存。
Reset BIOS Back to Factory State	将所有 BIOS 选项重置为出厂默认值。
TPM Clear	将可信平台模块 (TPM) 重置为默认状态，清除所有存储的密钥。
OEM Custom	擦除所有由制造商添加的自定义内容。
Unconfigure Intel CSME	取消为远程管理进行的英特尔主动管理技术预配。 **小心：** 如果选择此选项，则会完全取消英特尔主动管理技术的配置，您将无法在此端点上执行任何带外 (OOB) 操作，包括挂载恢复映像。但是，取消英特尔主动管理技术的配置后，您可以像在任何全新端点上一样，使用正常的英特尔 EMA 进程在此端点上重新配置英特尔主动管理技术。
SSD Master Password	如果选择 **SSD Erase**，则需要填写此项。
Pyrite Password	如果选择 **Pyrite Revert**，则需要填写此项。

选择了所需选项后，单击 **Start Erase**。确认您想要执行此操作。

7 管理磁盘映像

角色： 租户管理员

英特尔 EMA 允许您上传和存储可引导磁盘映像文件（*.iso 和 *.img）。您可以通过编辑可管理性服务器设置 USBR 映像根目录 (**USBR Images Root Directory**) 来定义默认映像文件存储位置。有关如何更新组件服务器设置（此设置位于“Manageability Server”下）的信息，请参阅第 9 节“附录 - 修改组件服务器设置”，P50。

注意： 英特尔 EMA 的自动化清理进程将定期删除 USBR 根目录中并非由英特尔 EMA 创建的任何文件夹和文件。您还可以手动运行此清理程序 **fileuploadcleanup**（请参阅《英特尔® EMA 服务器安装和维护指南》或《英特尔® EMA 分布式服务器安装和维护指南》中“使用英特尔 EMA Platform Manager 客户端应用程序”下的“在组件服务器上执行基本控制”）。

有关 USBR 功能的更多信息，请参阅第 1.2.8 节。

7.1 上传映像文件

请按照以下步骤上传磁盘映像文件。

1. 在左侧的导航栏中选择 **Storage**，然后单击 **Disk Images** 选项卡。
2. 单击 **Upload** 按钮。
3. 在 **Upload Image File** 对话框中，可以选择输入 **Description**。
4. 如果从 HTTPS 进行恢复，同时 BIOS 允许英特尔主动管理技术控制此设置，且已在 ACM 模式下预配英特尔主动管理技术，请勿选择 **Enforce Secure Boot**。否则请选择该项。
5. 单击 **Choose File**。
6. 浏览至所需文件，将其选中，然后单击 **Open**。该对话框在默认映像文件存储位置中显示文件大小和可用磁盘空间。有关如何更新“USBR Images Root Directory”设置（在“Manageability Server”下）的信息，请参阅第 9 节“附录 - 修改组件服务器设置”，P50。

   注意：

   - 如果所选文件的大小超出了可用磁盘空间，则会显示一条错误消息并禁用 **Upload** 按钮。有关如何为每个租户以及整个英特尔 EMA 实例（在“Manageability Server”下）设置存储容量上限的信息，请参阅第 9 节“附录 - 修改组件服务器设置”，P50。
   - 强烈建议您不要上传机密数据。

7. 单击 **Upload**。显示进度条。要取消上传，请单击 **Cancel**（您将收到确认取消）。
8. 文件上传完成后，单击 **Done**。现在已上传的文件将显示在已存储文件的列表中。

7.2 编辑和删除存储的映像文件

您可以编辑和删除已上传的映像文件。请执行以下步骤。

1. 在左侧的导航栏中选择 **Storage**，然后单击 **Disk Images** 选项卡。
2. 在 **Storage** 页面上的文件列表中，单击要编辑或删除的文件行中的向下箭头，然后从下拉菜单中选择 **Edit** 或 **Delete**。如果选择 **Delete**，将提示您确认此选择。如果选择 **Edit**，将显示一个对话框。无法删除或重命名使用中的映像文件。
3. 在编辑器对话框中，根据需要编辑文件名和/或 **Description**。

   注意： 对于文件名，仅接受扩展名 .img 和 .iso。

4. 单击 **Save** 以保存更改并返回 **Storage** 页面。

7.3 查看和管理活动会话

要查看和管理当前租户的活动会话，请从左侧的导航栏中选择 **Storage**，然后单击 **Active Sessions** 选项卡。

活动会话列表显示以下信息：

Endpoint Name	端点的名称。
File name	当前通过存储重定向安装到端点的映像文件。
Idle Time	会话空闲的时间长度。
Session Length	自启动会话以来的总时间长度。
User	启动会话的用户。
End Session	单击链接以断开此端点的会话。

要断开活动重定向会话，请单击目标端点的表行中的 **End session**。系统将要求您确认此操作。

7.4 映像建议

尽可能使用小映像，以防止在将端点重新引导到所安装映像时发生超时。此外，如果您计划通过 KVM 与重新引导的端点进行交互，则引导到的映像必须包含 USB 键盘和鼠标驱动程序。

一种将端点重新引导到所安装映像的推荐方法是使用两部分映像。首先，将端点引导到小映像，以便在网络上启动该端点。然后使用该映像从端点访问更多内容。

注意： 当前的已知问题是英特尔主动管理技术通过 USBR 引导一些 UDF 格式化映像。有时，UDF 格式化映像可能无法引导或无法完全引导。我们建议使用 CDFS 格式化映像，直到此问题得到解决。

8 附录：故障排除

无法登录到英特尔® EMA 网站	英特尔 EMA 网站用户界面 (UI) 使用了 Cookie。如果在浏览器中禁用 Cookie，则英特尔 EMA 网站 UI 将无法正常运行。
英特尔 EMA 代理无法连接到英特尔 EMA 服务器	请参阅第 4.5 节了解英特尔 EMA 代理故障排除的相关信息。
端点列表网页未显示任何端点或加载速度慢	如果在端点列表网页上看不到任何端点，请执行以下操作： 1. 确保您了解第 1.2 节，并且您当前的登录用户帐户具有查看目标端点的正确访问权限。 2. 在目标端点上安装英特尔 EMA 代理时，确保使用了正确的端点政策文件。 3. 如果您使用面向 Internet Explorer 和/或 Edge 的 Microsoft 企业模式架构 2，则可能需要从 Sites.xml 文件中删除英特尔 EMA 服务器的 DNS 条目。 4. 如果上述所有步骤都没问题，请按照上文**英特尔® EMA 代理无法连接到英特尔® EMA 服务器**中的步骤操作。
KVM 显示黑屏	连接到英特尔® 主动管理技术 KVM 时，如果未插入物理监视器，则会显示黑屏。 如果端点是无头的，则如果没有通过操作系统的请求，则图形处理单元 (GPU) 会关闭电源。在这种情况下，当端点关机然后开机或引导至 BIOS 时，它不会检测到已连接的显示器并关闭 GPU 的电源，从而导致黑屏/白屏。
英特尔® EMA 代理 – 卸载或更新期间失败	要卸载服务或在现有安装之上安装/更新服务，您需要使用与现有英特尔 EMA 代理具有相同架构类型（32 位服务或 64 位服务）的英特尔 EMA 代理安装程序。
英特尔® EMA 代理日志	英特尔 EMA 代理生成以下日志： • 代理运行时遇到的错误的常规日志 • 记录调试信息的调试日志 • 如果在安装/卸载过程中检测到任何错误，则为安装日志 **常规英特尔® EMA 代理错误日志** 常规日志默认情况下处于启用状态，并且报告英特尔® EMA 代理服务错误。文件名是 **EmaAgent.log**。 对于 Win64 系统，**EmaAgent.log** 文件位于 **Program Files** 文件夹中英特尔® EMA 代理的安装目录下。 日志包括错误的日期和时间、错误的路径和文件名、行号、参数以及错误的简要说明。 日志文件语法： `[Date & Time] FilePath: LineNumber (Parameter1, Parameter2) Message.` **英特尔® EMA 代理安装日志** 在安装/卸载过程中检测到错误时，将生成此日志。日志文件以使用的安装程序命名，并且位于安装程序所在的文件夹中。如果在安装/卸载过程中未检测到错误，则不会创建日志。

	注意：要解决特定的错误消息“Error removing the installation directory file”，请确保卸载时安装目录中没有打开或受保护的文件。开始卸载之前，请确保关闭所有文件。
英特尔® EMA 声明端点由其他程序管理	该端点当前可能由另一个管理应用程序管理。要允许英特尔 EMA 管理它，您需要取消预配端点，然后使用英特尔 EMA 重新预配它。有关取消预配的信息，请参阅您的英特尔® 主动管理技术文档（如下）。 https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm 或者，如果英特尔主动管理技术管理员密码已知，您可以使用 POST /api/latest/amtSetups/endpoints/adopt API 来采用端点。 有关更多信息，请参阅 swagger 文档。
在 Windows Server 2016 上导入 PKI 证书失败	如果您在运行 Windows Server 2016（低于内部版本 1709）的计算机上安装了英特尔 EMA 服务器，并且证书 PFX 文件使用“AES256-SHA256”加密，则将证书上传到英特尔 EMA 将会失败。即使提供有效的密码，也会显示有关密码无效的错误。 这是一个与 Windows 相关的问题，其中 Windows 本身不支持使用此加密创建的 PFX 文件。从 Windows Server 2016 内部版本 1709 和更高版本开始，此问题已修复。 https://github.com/dsccommunity/CertificateDsc/pull/154/files **修复方式：** 1. 在支持使用加密“AES256-SHA256”的 PFX 文件的系统上安装 PFX 文件（例如，Windows 10 桌面版）。为此，请双击 PFX 文件以启动“证书导入向导”。默认情况下，它将安装到当前登录用户的个人证书存储区中。确保选择 **Mark this key as exportable** 和 **Include all extended properties**。 2. 打开 Microsoft 管理控制台以获取当前用户证书。 3. 右键单击刚安装的证书，然后选择 **All Tasks > Export...**。这将打开“证书导出向导”。 4. 在该向导中，选择 **Yes, export the private key**，然后单击 **Next**。 5. 选择 **Personal Information Exchange (.PFX)**，然后依次选择 **Include all certificates in path**、**Export all extended properties** 和 **Enable certificate privacy**。如果需要，请选择 **Delete the private key if successful**（如果要从此中间系统中删除证书和密钥，请执行此操作）。单击 **Next**。 6. 在“安全性”屏幕中，选择 **Encryption** “TripleDES-SHA1”。这是问题的根源：Windows 的早期版本不支持使用“AES256-SHA256”的 PFX 文件。此加密不适用于实际证书，而是与此屏幕上提供的密码结合使用，以在将证书导出为 PFX 文件格式时保护与证书关联的私钥。 7. 完成导出向导屏幕，以创建新的 PFX 文件。此新的 PFX 文件可以在安装英特尔 EMA 服务器的旧 Windows 系统上成功使用。

从剪贴板进行带内 KVM 粘贴导致意外的字符或大小写	尝试通过 KVM 将纯文本从英特尔 EMA 控制台系统的剪贴板（即运行英特尔 EMA Web 版用户界面的计算机的剪贴板）粘贴到目标端点时，您可能会注意到目标端点上的粘贴输出中出现意外的大小写或大写。这与其他远程桌面应用程序的行为一致。有关更多信息，请参阅 Microsoft 提供的以下链接： https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/caps-lock-key-status-not-synced-to-client 此外，根据目标端点的操作系统语言/区域设置，可能会粘贴意外的字符。仅支持美国英语键盘字符代码。如果端点的语言/区域设置不是美国英语，则可能会在端点上粘贴无法预料的字符。 **要修复该问题（仅限大写问题），请执行以下操作：** • 在粘贴之前，请确保目标端点上的大写锁定功能处于关闭状态。如果在与该端点的 KVM 会话期间按下过 Caps Lock 键，请确保在退出 KVM 会话之前再次按下 Caps Lock 以清除（关闭）目标端点上的大写锁定。否则，端点上的大写锁定功能将保持打开状态，而当您粘贴到该端点时，所粘贴的文本将出现相应的行为（小写全部变成大写，反之亦然）。
使用服务器证书 API 导出 PFX 失败	调用 POST /api/latest/serverCertificates/{certificateName}/getPFX 会定期导致错误。如果发生此错误，请稍候，然后重新尝试调用。

9 附录 - 修改组件服务器设置

可以使用 **Server Settings** 选项卡来修改组成英特尔 EMA 服务器的各种组件服务器（Swarm 服务器、Ajax 服务器等）的设置，该选项卡可从左侧垂直导航窗格上的 **Settings** 选择中访问。要修改组件服务器的安全设置，请选择 **Security Settings** 选项卡。有关安全设置和说明的列表，请参阅第 9.5 节。

以下子节介绍了每个组件服务器可用的设置。对于每个组件服务器，按照英特尔 EMA 用户界面页面中的显示顺序列出相应的设置。

注意：如果更改任何组件服务器的 **serverIps** 或 **messagePort** 设置，则必须重新启动所有组件服务器，而不仅仅是重新设置被更改的组件服务器（在分布式服务器架构中，必须在所有服务器计算机上执行此操作）。此外，更改这两个设置时，您将需要回收英特尔 EMA 网站的 IIS 应用程序池以重新启动英特尔 EMA 网页服务器。对于其他设置，仅重新启动修改后的组件服务器就足够了。如果更改 **messagePort**，请确保新端口未被防火墙阻止。

9.1 Swarm 服务器

设置	描述
UI: Admin Port **API: adminport**	Swarm 服务器的 Admin TCP 侦听器将绑定到的端口。这是用于从其他英特尔 EMA 服务器进程到 Swarm 服务器的通信。默认为 8089。
UI: Admin Port Local **API: adminportlocal**	确定 Admin TCP 侦听器是否仅绑定到本地环回。值为 0 和 1。 0 = 分布式服务器环境 1 = 单服务器环境
UI: Agent Auto Update	布尔值。启用或禁用自动代理更新。默认：启用。
UI: Agent Update Interval (Seconds) **API: agentUpdateIntervalSeconds**	英特尔 EMA 代理更新间隔（以秒为单位）。即，如果设置为 5，则英特尔 EMA 服务器在尝试更新下一个请求更新的代理前，会先等待 5 秒。默认：10。最小值：10。最大值：120。
UI: Log File Path **API: logfilepath**	英特尔 EMA 日志文件的路径。 最大值：247 个字符 最小值：2 个字符
UI: Enable Intel CIRA Power State Polling **API: enableCIRAPowerPolling**	启用定期 CIRA 电源状态轮询。值是 True/False。默认值为 True。
UI: Maximum Number of Concurrent Database Connections **API: maxdbconnections**	此服务器的最大并发数据库连接数。
UI: Swarm Servers **API: swarmserver**	活动 Swarm 服务器列表。包括服务器 ID、服务器 IP 和端口（格式为 IP 地址：端口）。
UI: Server IPs **API: serverIps**	运行此组件服务器类型的机器 IP 地址列表。例如，如果 Swarm 服务器在机器 ip1、ip2 和 ip3 上运行，则 serverIps 将包括所有 IP 地址。
UI: Message Port **API: messagePort**	该组件服务器类型正在侦听的 TCP 端口，以接受来自其他英特尔 EMA 组件的内部流量。默认为 8093。

设置	描述
UI: TCP Connection Retry **API: tcpConnRetrySeconds**	在英特尔 EMA 服务器组件之间建立通信连接时重试之间的等待时间。
UI: TCP Connection Idle **API: tcpConnIdleSeconds**	建立通信后组件之间发送的心跳消息之间的间隔。
UI: Database Connection Wait Time (Minutes)	英特尔 EMA 等待获取数据库连接的时间（以分钟为单位）。 范围：1 - 10 默认值：2
UI: Database Lock Timeout Period (Seconds) **API: dbSetLockTimeoutSeconds**	SQL 查询保持锁定的时间（以秒为单位）。 范围：1 - 60 默认值：2
UI: Database Retry Hold Time for a Query (Milliseconds)	SQL 查询等待完成的时间（以毫秒为单位）。该值乘以 **Database Retry Attempts for a Query** 的值，以增加每次重试的维持时间。 范围：100 - 60000 默认：100
UI: Database Retry Attempts for a Query **API: dbRetryMaxAttempts**	执行失败的 SQL 查询的重试次数。达到此值后，Swarm 服务器将由于数据库中的严重故障而重新启动。 范围：3 - 100 默认值：5
UI: CIRA Keep-alive Interval (Seconds) **API: CIRAKeepAliveIntervalSeconds**	以秒为单位为 Swarm 服务器定期向目标端点的英特尔主动管理技术固件发送的消息设置时间间隔，以使 CIRA 连接保持打开状态。新安装的英特尔 EMA 的时间间隔默认值为 10 分钟。如果从 1.11.0 之前的旧版本英特尔 EMA 进行升级，则默认值为 10 秒。 默认值：10 秒 最小值：10 秒 最大值：1 小时（即 3,600 秒）

9.2 Ajax 服务器

设置	描述
UI: Ajax Cookie Auto Refresh Range **API: ajaxCookieAutoRefreshRange**	可以延长 Ajax cookie 寿命的分钟数范围。
UI: Ajax Cookie Idle Timeout **API: ajaxCookieIdleTimeout**	从添加 cookie 到过期的时间（以分钟为单位）。
UI: Http Header Access Control Allow Headers **API: httpheader_Access-Control-Allow-Headers**	为了响应 Ajax 请求而设置的其他标题。
UI: Log File Path	英特尔 EMA 日志文件的路径。

设置	描述
API: logfilepath	最大值：247 个字符 最小值：2 个字符
UI: User Access Failed Max Count **API: userAccessFailedMaxCount**	用户帐户被 Web API 锁定之前密码尝试失败的次数。
UI: Expire Sessions **API: expiresessions**	设置 Ajax 服务器是否应该使会话过期（默认启用）。
UI: Maximum Number of Concurrent Database Connections **API: maxdbconnections**	此服务器的最大并发数据库连接数。
UI: Server IPs **API: serverIps**	运行此组件服务器类型的机器 IP 地址列表。例如，如果 Ajax 服务器在机器 ip1、ip2 和 ip3 上运行，则 serverIps 将包括所有 IP 地址。
UI: Swarm Servers **API: swarmserver**	活动 Swarm 服务器列表。包括服务器 ID、服务器 IP 和端口（格式为 IP 地址：端口）。
UI: Message Port **API: messagePort**	该组件服务器类型正在侦听的 TCP 端口，以接受来自其他英特尔 EMA 组件的内部流量。默认为 8092。

9.3 可管理性服务器

设置	描述
UI: CIRA Server Host **API: ciraserver_host**	CIRA 访问服务器的主机名，即 Swarm 服务器（或分布式架构中的 Swarm 服务器负载均衡器）。仅在安装模式使用主机名时使用。在多服务器安装中使用。
UI: CIRA Server IP **API: ciraserver_ip**	CIRA 访问服务器的 IP 地址，即 Swarm 服务器（或分布式架构中的 Swarm 服务器负载均衡器）。仅在安装模式使用 IP 地址时使用。
UI: CIRA Server IP **API: ciraserver_port**	CIRA 访问服务器的端口，即 Swarm 服务器（或分布式架构中的 Swarm 服务器负载均衡器）。负载平衡器用于将传入流量（来自 CIRA）定向到 Swarm 服务器的 8080 端口。
UI: Log File Path **API: logfilepath**	英特尔 EMA 日志文件的路径。 最大值：247 个字符 最小值：2 个字符
UI: Maximum Number of Concurrent Database Connections **API: maxdbconnections**	此服务器的最大并发数据库连接数。
UI: USBR Images Root Directory **API: usbrImagesRootDirectory**	英特尔 EMA 服务器上的根目录，用于存储上传的可引导映像文件（.iso 和 .img）。默认值为 **C:\ProgramData\Intel\EMA\USBR**。 **注意：** 如果全局管理员在图像上载后对此文件夹进行过更改，则其他用户（如租户管理员）将无法看到或使用

设置	描述
	这些文件。全局管理员（系统管理员）需要先手动将内容从原始文件夹复制到新文件夹，然后其他用户才能访问这些文件。
UI: Maximum USBR Image Storage Capacity per Tenant	每个租户可用于 USBR 映像存储的磁盘空间 (GB)。 默认值：20 GB 最大值：50 GB
UI: Maximum USBR Image storage Capacity Per EMA Instance	此英特尔 EMA 实例中可用于 USBR 映像存储的总磁盘空间 (GB)（适用于所有租户）。 默认：50 GB 最大值：500 GB
UI: Maximum USBR Slot Count per Tenant **API: maxUsbrSlotCountPerTenant**	每个租户可使用的活动 USBR 会话数。
UI: Maximum USBR Idle time **API: maxUsbrIdleTimeInMinutes**	USBR 会话在被自动终止前可以处于空闲状态的时长（以分钟为单位）。
UI: USBR Redirection Manager Loop Interval	活动 USBR 会话的状态轮询间隔（以秒为单位）。
UI: USBR Redirection Throttling Rate	将 USBR 文件数据发送到目标端点英特尔主动管理技术固件的延迟。该延迟的作用是限制数据速率，因为如果数据速率太高，英特尔 EMA 中的某些内部数据流将无法正常工作。 **注意：** 使用 USBR 时，强烈建议执行基于 CIRA 的调配。USBR 对延迟很敏感，并且英特尔 EMA 已针对 CIRA 调配的端点优化了 USBR。如果您将 TLS 与中继结合使用，则需要以“全局管理员”身份在“服务器设置”中“可管理性服务器”部分下调整“USBR 重定向限制速率”。此设置取决于您的独特网络环境。我们建议从 10 毫秒的设置开始，然后以 10 为增量增加，直到找到非常适合网络环境的速率为止。您不太可能需要超过 50 毫秒。请注意，增加此设置将降低 USBR 引导性能，尤其是对于 CIRA 端点，并且只能用于含纯中继实例的 TLS。 默认值：0，最大值：1000，最小值：0。 建议值 = 从 10 开始，按 10 递增，以找到适合您网络的速率。
UI: File Upload Retention Period **API: fileUploadRetentionPeriodInDays**	保留不完整的可恢复文件上传的天数，之后会将其自动删除。
UI: File Upload Cleanup Interval **API: fileUploadCleanupIntervalInHours**	文件清理进程将运行以处理不完整的可恢复文件的间隔（小时）。
UI: Swarm Servers **API: swarmserver**	活动 Swarm 服务器列表。包括服务器 ID、服务器 IP 和端口（格式为 IP 地址：端口）。
UI: Server IPs **API: serverIps**	运行此组件服务器类型的机器 IP 地址列表。例如，如果可管理性服务器在机器 ip1、ip2 和 ip3 上运行，则 serverIps 将包括所有 IP 地址
UI: Message Port	该组件服务器类型正在侦听的 TCP 端口，以接受来自其他英特

设置	描述
API: messagePort	尔 EMA 组件的内部流量。默认为 8094。
UI: Audit Log Cleanup Interval (Hours) **API: AuditLogCleanupIntervalInHours**	清理英特尔 EMA 数据库中的审核日志记录之前的时间间隔（小时）。
UI: Audit Log Retention Period (Days) **API: AuditLogRetentionPeriodInDays**	清理英特尔 EMA 数据库中的审核日志记录之前的时间间隔（天）。
UI: Enable 8021X Certificate Auto Renewal **API: Is8021XCertificateRenewalEnabled**	布尔值，默认为“True”。用于确定是否已启用自动 802.1x 证书续订流程。如果已启用，则英特尔 EMA 会自动续订即将到期的证书。
UI: 802.1X Certificate Renewal Window (Days) **API: Ieee8021xCertificateRenewalWindowDays**	整数。设置英特尔 EMA 将于 802.1x 证书到期前多少天提醒证书续订操作。 默认：30 最大值：90 最小值：1
UI: Enable Provisioning TLS Certificate Revocation Check **API: enableProvisioningTLSCertCRLCheck**	布尔值。启用或禁用证书吊销列表 (CRL) 检查，以便预配由客户端英特尔主动管理技术系统在 TLS 预配流中提供的 TLS 证书。CRL 检查要求可管理性服务器具有活动互联网连接，以便定期下载 CRL 文件。 默认值：True。

9.4 网页服务器

注意：使用 **Save and Sync Web Settings** 按钮重新启动网页服务器。或者，您可以运行英特尔® EMA 安装程序 EMAServerInstaller.exe（以管理员身份运行），并从菜单栏中选择 **Settings > Sync Web Server Settings**。

设置	描述
UI: Access Token Time to Live **API: AccessTokenTimeToLive**	API 承载令牌的有效期限（以秒为单位）。
UI: Ajax Server Host **API: AjaxServerHost**	Ajax 服务器或 Ajax 服务器的负载平衡器的主机名或 IP 地址。
UI: Enable Allowed Domains, Allowed Domains **API: EnableAllowedDomains, AllowedDomains**	由 Ajax 服务器使用。如果启用，则网页服务器将检查传入的 Ajax/websocket 请求以接受还是拒绝。 AllowedDomains 是一个逗号分隔列表，示例为 test1.intel.com,test2.intel.com。 EnableAllowedDomains 为 0 (false) 或 1 (true)。
UI: Log File Path **API: logfilepath**	英特尔 EMA 日志文件的路径。 最大值：247 个字符 最小值：2 个字符
UI: Maximum Number of Concurrent Database Connections	此服务器的最大并发数据库连接数。

设置	描述
API: maxdbconnections	
UI: Swarm Server Host **API: SwarmServerHost**	Swarm 服务器或 Swarm 服务器的负载平衡器的主机名或 IP 地址。
UI: Swarm Server Port **API: SwarmServerPort**	单服务器安装中的 8080 或分布式服务器体系结构中的 Swarm 服务器负载平衡器暴露的 Swarm 服务器端口。
UI: Global Catalog Port **API: GlobalCatalogPort**	用于连接到 Active Directory 全局目录的端口。提供 AD 用户名和密码时，用于执行 AD 登录。默认为 3269，它是 SSL 端口。请参阅下面的 LDAP 连接端口的注释。
UI: LDAP Connection Port **API: LdapConnectionPort**	在 802.1x 配置中用于 LDAP 连接的端口。默认端口为 636 安全端口。  **注意：** 英特尔 EMA 版本 1.5.0 及更高版本默认使用 LDAPS 安全端口（LDAPS 安全端口 636 和全局编录端口 3269）。之前的英特尔 EMA 版本使用标准非安全 LDAP 端口（LDAP 端口 389 和全局编录端口 3268）。如果您要安装英特尔 EMA v 1.5.0 或更高版本，并且要使用 Active Directory 或 802.1x 集成，请确保启用 LDAPS 端口。如果您更喜欢使用标准非安全端口，那么在安装英特尔 EMA 之后，再次打开安装程序（EMAServerInstaller.exe，以管理员身份运行）并选择 **File > Advanced Mode**，然后单击 **Settings > Switch from LDAPs to LDAP**，以将英特尔 EMA 使用的 LDAP 端口重置为标准非安全端口。或者，您可以在英特尔 EMA UI 的 Server Settings 页面上的网页服务器设置中更改端口。如果您在英特尔主动管理技术预配过程中遇到 802.1x 设置问题，原因可能就出在这里。有关更多信息，请参阅以下链接：https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts。
UI: Max Access Token TTL **API: MaxAccesstokenTTL**	刷新 API 承载令牌的最长时间。
UI: Frontend Storage Type **API: frontendstoragetype**	允许您指定应将英特尔 EMA 网站运行时信息存储在浏览器本地存储还是浏览器会话存储中。如果使用本地存储，在前端网站关闭后，该会话将保留（无需再次登录）。如果使用会话存储，在前端网站关闭时，该会话将丢失。
UI: Azure AD Directory (tenant) ID **API: AzureAdTenantId**	采用 GUID 格式的 Azure AD Directory（租户）ID。仅在已选定 Azure AD 身份验证选项时使用。
UI: Azure AD Application (client) ID **API: AzureAdClientID**	采用 GUID 格式的 Azure AD 应用程序（客户端）ID。结合 Azure 密钥使用，使 Web 服务器能够连接到指定的 Azure 租户。仅在已选定 Azure AD 身份验证选项时使用。
UI: Azure AD Client Secret Value **API: AzureAdClientSecretValue**	Azure AD 客户端密钥值，仅在已选定 Azure AD 身份验证选项时使用。密钥将以加密格式存储在 SQL 数据库中。

9.5 安全设置

下列大多数安全设置适用于各种组件服务器，但有些仅适用于特定的组件服务器（如 Ajax 服务器）。其中许多设置旨在帮助防范拒绝服务 (DoS) 攻击。

注意：如果更改任何组件服务器的安全设置，则必须重新启动所有组件服务器，而不仅仅是设置已更改的组件服务器（在分布式服务器架构中，必须在所有服务器计算机上执行此操作）。此外，更改上述设置后，您将需要回收英特尔 EMA 网站的 IIS 应用程序池以重新启动英特尔 EMA 网页服务器。

设置	描述
UI: Unauthorized TCP connection timeout	布尔值。启用后，英特尔 EMA 将终止处于空闲且未完成 SSL 握手的新 TCP 连接，以帮助防范拒绝服务攻击。 默认值：true。
UI: TCP connection timeout	新 TCP TLS 连接必须在该时间限制（以毫秒为单位）内完成 SSL 握手，否则会被视为空闲并终止。 默认：5000 最大值：3,600,000（1 小时）
UI: Rate Limiter **API: enableRateLimiter**	布尔值。启用后，英特尔 EMA 将执行基于 IP 地址的 HTTPS/TCP TLS 限速请求，以帮助防范拒绝服务攻击。 默认值：true。
UI: Rate Limiter Window Size **API: rateLimiterWinSizeInMilliSeconds**	用于跟踪基于 IP 地址的限速请求的窗口期（以毫秒为单位）。 默认：200 最大值：3,600,000（1 小时）
UI: Ajax HTTP Requests Max Count **API: ajaxHttpRateLimiterMaxCount**	在拒绝对 Ajax 服务器 Web 重定向端口 (8084) 的请求之前，窗口期中每个 IP 地址允许的请求数上限。 默认：20 最大值：1,000,000
UI: Recovery HTTP Requests Max Count **API: recoveryHttpRateLimiterMaxCount**	在拒绝对恢复服务器 Web 重定向端口 (8085) 的请求之前，窗口期中每个 IP 地址允许的请求数上限。 默认：20 最大值：1,000,000
UI: Message Ports Requests Max Count (Before Authorization) **API: blastMessageBeforeAuthRateLimiterMaxCount**	在拒绝对内部组件间端口（8092、8093、8094）的请求之前，窗口期中每个 IP 地址允许的身份验证前请求数上限。 默认：100 最大值：1,000,000
UI: Message Ports Requests Max Count (After Authorization) **API: blastMessageAfterAuthRateLimiterMaxCount**	在拒绝对内部组件间端口（8092、8093、8094）的请求之前，窗口期中每个 IP 地址允许的身份验证后请求数上限。 默认：80,000 最大值：1,000,000
UI: Swarm Admin Ports Request Max Count (Before Authorization) **API: adminPortBeforeAuthRateLimiterMaxCount**	在拒绝对 Swarm 服务器管理端口 (8089) 的请求之前，窗口期中每个 IP 地址允许的身份验证前请求数上限。 默认：20,000 最大值：1,000,000
UI: Swarm Admin Ports Request Max Count (After	在限制对 Swarm 服务器管理端口 (8089) 的请求之前，窗

设置	描述
Authorization) **API: adminPortAfterAuthRateLimiterMaxCount**	口期中每个 IP 地址允许的经过身份验证的请求数上限。 默认：20,000 最大值：1,000,000
UI: Agent Port Request Max Count (Before Authorization) **API: agentPortBeforeAuthRateLimiterMaxCount**	在拒绝对 Swarm 服务器代理端口 (8080) 的请求之前，窗口期中每个 IP 地址允许的身份验证前请求数上限。 默认：20 最大值：1,000,000
UI: Agent Port Request Max Count (After Authorization) **API: agentPortAfterAuthRateLimiterMaxCount**	在限制对 Swarm 服务器代理端口 (8080) 的请求之前，窗口期中每个 IP 允许的经过身份验证的请求数上限。 默认：1000 最大值：1,000,000
UI: Connection Count Check **API: enableConnectionCountChecker**	布尔值。启用后，英特尔 EMA 将限制每个 IP 地址的 TCP TLS 连接数，以帮助防范拒绝服务攻击。 默认值：true。
UI: Message Port (connections per port) **API: blastMessageConnCountChecker**	每个 IP 地址允许连接到内部组件间端口（8092、8093、8094）的连接数上限。 默认：20 最大值：1,000,000
UI: Admin Port (connections per port) **API: swarmAdminPortConnCountChecker**	每个 IP 地址允许连接到 Swarm 服务器管理端口 (8089) 的连接数上限。 默认：20,000 最大值：1,000,000
UI: Swarm Agent Port (connections per port) **API: swarmAgentPortConnCountChecker**	每个 IP 地址允许连接到 Swarm 服务器代理端口 (8080) 的连接数上限。 默认：20,000 最大值：1,000,000
UI: User password minimum length **API: userPasswordMinLength**	用于自定义密码验证策略。 默认值：8 最小值：8 最大值：20
UI: User password maximum length **API: userPasswordMaxLength**	用于自定义密码验证策略。 默认值：255 最小值：64 最大值：255
UI: Client Credentials minimum length **API: clientCredentialsMinLength**	用于自定义密码验证策略。 默认值：12 最小值：12 最大值：20

设置	描述
UI: Client Credentials maximum length **API: clientCredentialsMaxLength**	用于自定义密码验证策略。 默认值：255 最小值：64 最大值：255
API: passwordComplexityRequired	用于自定义密码验证策略。 True/False。 默认值：True
UI: Password Disallowed List Checking **API: PasswordDisallowedListChecking**	布尔值。启用此设置并使用用户身份验证（用户名/密码）时，如果已创建新用户或已更新当前用户的密码，则会对照禁用密码列表对提供的密码进行检查。可以使用安装程序“Advanced Mode”自定义此列表。 默认值：True。

9.6 恢复服务器设置

提供以下设置以支持未来的英特尔平台。

设置	描述
UI: Log File Path **API: logfilepath**	英特尔 EMA 日志文件的路径。 最大值：247 个字符 最小值：2 个字符
UI: Maximum Number of Concurrent Database Connections **API: maxdbconnections**	此服务器的最大并发数据库连接数。
UI: Message Port **API: messagePort**	该组件服务器类型正在侦听的 TCP 端口，以接受来自其他英特尔 EMA 组件的内部流量。默认 8095。

UI: Recovery Port
API: RecoveryPort
	用于恢复的端口。默认 8085。
	注意：如果更改默认端口，则在英特尔 EMA 安装过程中，系统会提示您在每个恢复服务器上以管理员模式运行以下命令，从而更新端口绑定（<> 括号中的项在提示弹出对话框中提供）：
	`netsh http delete sslcert ipport=<original port number>`
	`netsh http add sslcert ipport=<new port number>`
	`certhash=<certificate hash>`
	`appid={3a6739cf-6707-4623-a073-34b6b7a51b1d}`

UI: Recovery Port Enabled **API: RecoveryPortEnabled**	布尔值，默认为“True”。指定是否启用恢复端口。
UI: Server IPs	运行此组件服务器类型的机器 IP 地址列表。例如，如果 Ajax 服务器在机器 ip1、ip2 和 ip3 上运行，则 serverIps 将包括所有 IP 地址。

设置	描述
API: serverIps	

10 附录 - 英特尔® EMA 代理控制台

英特尔® EMA 代理通常已安装并作为服务运行。但是，它也可以作为控制台或独立可执行应用程序运行。如果要在不希望将代理作为服务运行的系统上安装代理，而是希望通过手动执行来“按需”运行，这将很有用。功能与服务版本相同。

英特尔 EMA 代理控制台可从英特尔 EMA API 进行下载。

注意：

- 代理可执行文件的控制台版本具有与服务版本相同的文件名 (EmaAgent.exe)。因此，如果要将控制台代理下载到已将代理作为服务安装的系统，请确保重命名控制台版本，以免覆盖服务代理。
- 代理控制台是命令行工具，没有图形用户界面。
- 代理控制台可用于代理安装故障排除，就像服务版本一样。有关详细信息，请参阅第 4.5 节。

10.1 文件

要将英特尔 EMA 代理作为控制台或独立可执行应用程序安装，您需要两个文件。下表描述了这些文件的属性。这两个文件必须位于同一目录中。请务必将代理控制台应用程序下载到您当前下载系统架构的对应文件夹中 (C:\Program Files\Intel\Ema Agent)。

表 2: 文件属性

文件名	描述
EmaAgent.exe	这是代理安装文件。要安装/更新/卸载任何实例，就必须以管理员权限执行此文件。
EmaAgent.msh	这是策略文件。此文件确定了该端点将属于哪个端点组，并使英特尔 EMA 代理能够联系英特尔 EMA 服务器。

要将英特尔 EMA 代理作为控制台运行，请在托管端点系统上执行以下操作：

1. 使用管理特权打开命令窗口 (cmd.exe)，然后转到英特尔 EMA 代理控制台可执行文件所在的路径。
2. 运行以下命令以控制台模式启动英特尔 EMA 代理（如果更改了文件名，请使用选择的名称）：
   `EmaAgent.exe`
3. 要在控制台模式下停止英特尔 EMA 代理，请使用组合键 `CTRL+C`。

10.2 英特尔® EMA 代理数据库

代理控制台正在运行后，将生成一个本地数据库以保存设置和证书值。该数据库存储在控制台二进制文件夹中。

当前用户值是 Windows 中登录的实际会话的用户名。

10.3 代理服务器配置

要配置在控制台模式下使用的代理服务器，必须在启动控制台时添加代理服务器参数。运行以下命令：

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

- Host：代理服务器的 HTTPS 主机名。
- Port：代理服务器的端口号。

10.4 资源消耗

资源消耗按 CPU、RAM 和网络流量进行划分。

以下所有测试均在搭载 Windows 10 专业版 64 位、英特尔® 酷睿™ i5-6300 2.40 GHz – 2.5 GHz 处理器和 16 GB RAM，并处于使用有线网络的本地 LAN 中的戴尔 Latitude E7270 笔记本电脑机型上执行。

CPU

- 与代理控制台没有任何连接的最大平均值为 0.01%。
- 使用远程桌面的最大平均值为 5.53%。
- 使用终端的最大平均值为 0.29%。这是使用控制台命令和操作（例如 ipconfig、ipconfig /all 或 netstat）的结果。
- 使用文件管理器的最大平均值为 3.11%。上传的文件为 133 MB。

RAM

本节中的值取自 Windows 资源监视器的“工作集 (KB)”一列。

- 与代理没有任何连接的最大平均值为 33,380 KB。
- 使用远程桌面的最大平均值为 51,040 KB。
- 使用终端的最大平均值为 33,632 KB。
  - 这是使用控制台命令和操作（例如 ipconfig、ipconfig /all 或 netstat）的结果。如果脚本使用大量内存，则该平均值可能会显着增加。注意不要执行带有内存泄漏的脚本。
- 使用文件管理器的最大平均值为 31,180 KB。上传的文件为 133 MB。

网络流量

- 与代理控制台没有任何连接的最大流量如下所示：
  - 每秒发送的最大字节数：137。
  - 每秒接收的最大字节数：42。
  - 每秒传输的最大总字节数：180。
- 使用远程桌面的最大流量如下所示：
  - 每秒发送的最大字节数：469,925。
  - 每秒接收的最大字节数：230,886。
  - 每秒传输的最大总字节数：700,811。
- 使用终端的最大流量如下所示：
  - 每秒发送的最大字节数：16,683。
  - 每秒接收的最大字节数：5,691。
  - 每秒传输的总字节数：22,373。
  - 这是使用控制台命令和操作（例如 ipconfig、ipconfig /all 或 netstat）的结果。如果脚本发送或接收大量数据，则该平均值可能会大大增加。
- 使用文件管理器的最大流量如下所示：
  - 每秒发送的最大字节数：533,827。
  - 每秒接收的最大字节数：1,040,282。
  - 每秒传输的总字节数：1,574,109。
  - 上传的文件为 133 MB。这些值可能会更改，具体取决于要上传/删除的文件的大小和网络带宽。

10.5 代理 Windows 注册表信息

代理安装所创建的注册表项取决于 Microsoft Windows 操作系统和英特尔 EMA 代理（控制台和服务）的架构。这些是架构提供的英特尔 EMA 代理的注册表路径：

- Win64 服务：
  - HKEY_LOCAL_MACHINE -> “Software\Intel\EmaAgent”

- Win64 控制台：
    - HKEY_CURRENT_USER -> “Software\Intel\EmaAgent”

在安装/运行英特尔 EMA 代理时，此注册表项根中应存在以下注册表项：

- **MeshId** - 包含 MSH 文件中端点组 ID 的 REG_SZ；如果不存在 MSH 文件，则该值为空。
- **MeshName** - 包含 MSH 文件中端点组名称的 REG_SZ；如果不存在 MSH 文件，则该值为空。
- **NodeId** - 包含端点 ID 的 REG_SZ。

  注意： 端点 ID 与代理根证书相关联。服务/控制台使用不同的根证书。

- **Version** - 包含正在运行的 EmaAgent 的版本号的 REG_DWORD。
- **EnhancedLoggingLevel** - 包含日志记录级别的 REG_DWORD。默认情况下，此项设置为 3，这会禁用增强型调试日志记录。要启用增强型调试日志记录，请编辑注册表并将 EnhancedLoggingLevel 设置为 4。

11 附录 - 从计算机到计算机客户端应用程序执行英特尔® EMA 端点操作

英特尔 EMA API 支持直接从 M2M 客户端应用程序执行英特尔 EMA 带内和带外端点操作的机器对机器 (M2M) 应用程序。英特尔 EMA API 提供了客户端凭证身份验证流程以支持 M2M 应用程序。

首先，您将需要使用英特尔 EMA API 在英特尔 EMA 服务器上创建一个客户凭证帐户。M2M 客户端使用此帐户登录英特尔 EMA 并请求访问令牌，这使客户端可以在英特尔 EMA 上执行英特尔 EMA 带内和带外 API 调用（称为“资源”）服务器。客户端凭据帐户为特定租户专有。客户端凭证帐户只能由要在其中创建客户端凭证帐户的租户的全局管理员用户或租户管理员用户创建。

注意：可以为每个租户创建多个客户端凭据帐户。

设置了客户端凭证帐户后，您将需要从 M2M 客户端应用程序调用英特尔 EMA API 来请求访问令牌。这需要使用“客户端凭证”帐户登录到英特尔 EMA。访问令牌在有限的时间内有效，并且访问令牌的持续时间设置为“客户端凭证”帐户创建的一部分。

M2M 客户端应用程序收到请求的访问令牌后，便可以对英特尔 EMA 服务器进行 API 调用。有关英特尔 EMA API 的详细信息，请参阅《英特尔® EMA API 指南》。

11.1 创建一个新的客户端凭证帐户

要创建新的客户端凭证帐户，请以全局管理员或租户管理员身份登录英特尔 EMA 服务器，并使用英特尔 EMA API 进行操作：**POST api/latest/ClientCredentials**，提供以下值：

- **client_secret** - 您选择的机密字符串，类似于密码或密码短语。该值必须至少具有 12 个字符，并且至少包含一个数字，同时包含小写和大写字母，且至少包含一个特殊字符。
- **maxFailedLogins** - 客户端凭证帐户被锁定之前允许的登录尝试次数。最小值为 5，最大值为 15，默认值为 10。
- **tokenLifetimeHours** - 令牌的有效数量或时长。最小值为 1，最大值为 24，默认值为 1。
- **tenantID** - 将为其创建此客户端凭证帐户的租户的标识符。仅全局管理员需要使用，可通过 **api/latest/Tenants** API 调用找到。对于租户管理员而言这不是必需的，因为其值自动采用了管理员所属租户的 tenantID。
- **scope** - 此客户端凭据帐户的范围或用户角色。此参数为枚举类型，对于端点管理员角色，值为“1”或“EndpointManager”，对于租户管理员角色，值为“2”或“TenantManager”。您可以输入数字或角色名称。如果输入角色名称，请注意，该名称区分大小写并且不得包含空格。如果名称输入错误，或输入除 1 或 2 以外的数字，就会收到错误消息。

11.2 客户端凭据帐户范围的 API 权限

客户端凭据租户管理员有权访问支持租户管理的 API。这包括用于用户管理、端点组、创建并管理英特尔主动管理技术配置文件和英特尔主动管理技术设置的 API。

客户端凭据端点管理员有权访问支持在端点上执行操作的 API。这包括入站和出站操作、端点采用和取消配置。

请参阅 swagger 文档，以查看每个角色支持的 API 的完整列表。

11.3 使用客户端凭证请求令牌

创建了客户端凭证帐户后，请使用 M2M 客户端应用程序中的 **POST /api/token** API 来请求访问令牌。请注意，**grant_type** 必须为“client_credentials”。

令牌 API 调用的示例如下所示：

```
POST /api/token

grant_type=client_credentials

&client_id=xxxxxxxxxx

&client_secret=xxxxxxxxxx
```

M2M 客户端应用程序执行令牌 API 并收到访问令牌后，就可以直接对英特尔 EMA 实例进行带内和带外操作的英特尔 EMA API 调用（直到令牌过期）。