



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

快速入门指南

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

版权所有 2018-2023 英特尔公司。

本软件和相关文档是英特尔的版权材料，您对这些材料的使用受到为您提供这些材料所基于的明确许可证（“许可证”）的控制。除非许可证另有规定，否则未经英特尔事先书面许可，不得使用、修改、复制、发布、分发、披露或传播本软件或相关文档。

本软件和相关文档按原样提供，没有任何明示或暗示的保证，许可证中明确声明的保证除外。

英特尔技术可能需要支持的硬件、软件或服务激活。

没有任何产品或组件能保证绝对安全。

您的成本和结果可能会有所不同。

本文档未授予任何公司或其他机构知识产权许可（明示或暗示、允诺禁反言或其他方式）。

英特尔不承诺任何明示或暗示的担保，包括但不限于对适销性、特定用途适用性和不侵权的暗示担保，以及由履约习惯、交易习惯和贸易惯例引起的任何担保。

所描述的产品和服务可能包含可能导致产品和服务与公布的技术规格有所偏离的瑕疵或误差，一经发现将被收入勘误说明。可应要求提供当前的勘误表。

英特尔技术特性和优势取决于系统配置，并可能需要支持的硬件、软件或服务激活。性能会因系统配置的不同而有所差异。没有任何计算机系统能保证绝对安全。英特尔对数据或系统丢失或被盗、以及因此而导致的任何其它损失不承担任何责任。请咨询您的系统制造商或零售商，也可登录 <http://www.intel.com/technology/vpro> 获取更多信息。

英特尔、英特尔标志和其他英特尔标识是英特尔公司或其子公司的商标。文中涉及的其它名称及商标属于各自所有者资产。

1 简介	1
2 支持的操作系统	2
3 安装前提条件	3
3.1 计算机	3
3.2 操作系统	3
3.3 数据库	3
3.4 适用于 Microsoft Azure AD 环境的预安装说明	4
3.5 网页服务器	4
3.6 英特尔® 主动管理技术 PKI 证书	5
3.7 Microsoft .NET 框架版本	5
3.8 防火墙	5
3.9 网络	5
3.10 网络端口	5
4 安装或更新英特尔® EMA 服务器	8
4.1 初始服务器安装	8
4.1.1 服务器主机配置	9
4.1.2 数据库设置	9
4.1.3 负载均衡器信息	11
4.1.4 要部署的服务器组件	13
4.1.5 Platform Manager 配置	13
4.1.6 用户身份验证	13
4.1.6.1 本地帐户	14
4.1.6.2 域身份验证	14
4.1.6.3 Azure Active Directory 身份验证	14
4.1.7 全局管理员帐户设置	15
4.1.8 完成	15
4.1.9 摘要	16
4.1.10 修改 Azure AD 的服务器设置	16
5 使用全局管理员界面	17
6 租户设置和端点代理部署	18
6.1 创建您的端点组	18
6.2 创建代理文件以部署到托管端点	18
6.3 创建您的英特尔® 主动管理技术配置文件	19
6.4 启用英特尔® 主动管理技术自动设置	19
6.5 将代理部署到端点	20
7 英特尔® EMA 服务器管理	21
7.1 创建新的用户组	21

7.2 添加、修改和删除用户	21
7.3 将端点组分配给用户组	21
8 重要文件和目录位置	22

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

本文档概述了在试验或概念容量验证中安装英特尔 EMA 的基础步骤，并介绍了开始使用此系统所需的一些基本配置。本文档旨在用于教程、试验或概念验证活动中，不一定反映在实际生产环境中实施英特尔 EMA 所需的所有设置和配置。

本文档中的程序用来指导您在同一台计算机（或虚拟机）上安装全部英特尔 EMA 服务器组件（即 Swarm 服务器、Ajax 服务器等），因为这是最简单的配置。当您在同一台计算机上安装全部组件时，不需要使用实际负载均衡器。因此，当安装过程中要求您配置负载均衡器时，仅需输入全部英特尔 EMA 服务器组件所安装的系统 IP 地址或 FQDN。并且，您不需要执行用于安装其他服务器的步骤。

有关完整的安装、设置和配置说明（包括建议安全设置），请参阅《英特尔® EMA 服务器安装和维护指南》和《英特尔® EMA 管理和使用指南》。

2 支持的操作系统

作为独立应用程序，英特尔® EMA 代理可以安装在以下操作系统上：

- Microsoft Windows 10
- Microsoft Windows 11

可以在以下操作系统上安装英特尔 EMA 服务器：

- Microsoft Windows Server 2019 (**注意**：getPFX API 要求在 Windows Server 2019 或更高版本上安装英特尔 EMA 服务器)
- Microsoft Windows Server 2022 (**注意**：Windows Server 2022 上会默认禁用英特尔 ME 11 系统加密)

3 安装前提条件

这是设置英特尔® EMA 服务器所需的先决条件的列表。

3.1 计算机

具有足够功能以应对预期流量的计算机或虚拟机。不符合这些最低规格的系统可能会遇到性能问题。

2 个英特尔® 至强® 处理器，16 线程，24 GB RAM，1 TB 镜像：此配置应能够处理超过 20k 的连接。

3.2 操作系统

请参阅支持的操作系统，第 2 节。

当前，英特尔 EMA 不提供国际化支持。操作系统需要具有英语-美国 Windows 显示语言，英语-美国系统语言环境和英语-美国格式（与 Windows 显示语言匹配）。

3.3 数据库

安装 Microsoft SQL Server*。该数据库可以在网络上的单独服务器上运行，也可以在与英特尔 EMA 服务器相同的系统上运行。针对演示或测试目的，如果安装了高级功能，则可以使用 Microsoft SQL Server Express 版本。针对生产环境，我们建议使用 Microsoft SQL Server Enterprise。需要具有安装、配置和使用 SQL 和 Active Directory 的扎实知识（如果使用 802.1x）。




重要提示： 为了深入了解安全性，建议使用 Microsoft SQL Server Enterprise 并启用“透明数据加密”。另外，建议将 Windows 身份验证模式作为身份验证模式。



注意：

- 支持 Microsoft SQL Server 2017、2019 和 2022（仅限美式英语版本）。
- 运行 SQL Server 的计算机的操作系统必须是受支持的操作系统版本，并且必须具有英语-美国 Windows 显示语言、英语-美国系统语言环境和英语-美国格式（与 Windows 显示语言匹配）。请参阅支持的操作系统，第 2 节。
- SQL Server 中的**排序规则**值必须设置为 **SQL_Latin1_General_CP1_CI_AS**。
- 确保为 SQL Server 分配足够的资源（CPU、内存、固态硬盘等）。如果您的 SQL Server 资源是动态分配的，请确保分配了有足够保证的固定资源。如果不是，您可能在程序文件 **Program Files (x86)\Intel\Platform Manager\Emalog** 中的组件服务器日志文件中看到诸如“无法获得数据库连接，所有连接正忙”的错误消息。
- 英特尔 EMA 在 SQL Server 中使用查询通知来减少数据库读取次数。该功能要求在 SQL Server 中启用“Service Broker”。如果禁用了 Service Broker，您将在程序文件 **Program Files (x86)\Intel\Platform Manager\Emalog** 中的组件服务器日志文件中看到与此相关的警告。
- 如果在安装过程中选择 SQL 身份验证，则需要提供两个数据库连接字符串。一个字符串面向权限更大的帐户，用于安装数据库；另一个字符串面向英特尔 EMA 服务使用的权限更小的帐户，用于在安装完成后访问数据库。
- 在安装英特尔 EMA 之前，请确保 SQL Server 上存在一个帐户，英特尔 EMA 安装程序可以使用该帐户连接到 SQL Server 并创建英特尔 EMA 数据库。如果您不是 SQL 数据库管理员 (SQL DBA)，请联系 SQL DBA 以设置此帐户。在安装英特尔 EMA 之前，此帐户必须存在，因为在安装过程中会要求您指定 SQL 连接帐户。此帐户可以是 Windows 身份验证下的 Windows 帐户，或者 SQL 身份验证下的 SQL 帐户。此外，SQL 帐户必须配置默认数据库。默认数据库可以是 SQL 服务器上的任何现有数据库。需要此默认数据库，以便英特尔 EMA 安装程序可以确认指定的 SQL 帐户/用户能够连上 SQL 服务器及其数据库。

- 在安装英特尔 EMA 之前，请确保英特尔 EMA SQL 连接字符串中用于创建数据库的 SQL 帐户具有 sysadmin 权限（可以为 IIS 默认应用池身份创建新帐户），并且至少具有 dbcreator 权限，以便它创建、修改和删除任何数据库。另外，该帐户必须具有数据库级别的角色 db_owner、db_datawriter 和 db_datareader。需要具备“sysadmin”权限，才能为 SQL 服务器创建新用户“IIS APPPOOL\DefaultAppPool”（如果其不存在）。如果它已经存在，或者您没有将该帐户用于英特尔 EMA 网站的 IIS 应用程序池，那么为了创建英特尔 EMA 数据库，在安装过程中所需的角色是“dbcreator”。请记住，仅在英特尔 EMA 安装过程中才需要“sysadmin”或“dbcreator”权限。最后，您必须向英特尔 EMA 数据库用户授予“SUBSCRIBE QUERY NOTIFICATIONS”的权限。

 **重要提示：**如果您没有将“sysadmin”权限授予 SQL 连接帐户，安装仍将成功完成，但会出现与无法创建上述 IIS APPPOOL 用户相关的错误。**如果您没有将“sysadmin”权限授予 SQL 连接帐户，则您必须在安装完成后在 SQL 服务器上手动创建此用户，以便英特尔 EMA 正常工作。**

有关更改这些权限和角色的详细信息，请参阅 1.17 节。

3.4 适用于 Microsoft Azure AD 环境的预安装说明

如果您打算在现有 Microsoft Azure AD 环境中安装英特尔 EMA，请遵照下面的步骤，以使英特尔 EMA 能够成功连接到 Azure AD 环境。我们建议您在安装英特尔 EMA 之前执行这些步骤。虽然也可以在安装后再执行，但您将无法添加用户或执行其他英特尔 EMA 操作，直到在 Azure AD 中执行这些步骤之后此情况才会改变。



注意：配置为使用 Azure AD 身份验证的英特尔 EMA 实例不支持从脚本或外部应用程序通过 REST API 进行个人用户身份验证。使用客户端凭据是这些实例上可支持的一种替代方案。如果您需要使用会调用英特尔 EMA API 的集成应用程序或管理脚本，请在进行生产部署之前验证它们是否能使用 Azure AD 身份验证。

1. 在您的 Azure AD 租户（请注意，这与英特尔 EMA 租户不同）中，创建一个新的应用注册。此应用将在英特尔 EMA 安装后与之关联，而英特尔 EMA 将通过此应用与 Azure AD 进行交互，从而交换信息。
 - a. 转到 **Azure Active Directory > App Registration**，然后创建新的应用注册。
 - b. **Supported account types**（新应用）必须是 **Accounts in this organizational directory only**。
 - c. 配置 Redirect URI，选择 Web 作为平台。
 - d. 输入 `https://<EMA FQDN or IP>/api/latest/azureLogin` 作为 **Redirect URI** 值（请注意，此 URI 区分大小写）。
2. 在新注册应用的 **Certificates & Secrets** 部分，添加新的客户端密钥：
 - a. 在创建客户端密钥时，请记录该密钥的值，因为它只出现一次。在安装英特尔 EMA 的 Web 服务器之后，将需要使用该值对其设置进行配置。请确保此敏感信息的安全。
 - b. 考虑客户端密钥的到期日期。请注意，在其到期之前，您需要创建新的客户端密钥，并更新英特尔 EMA 中的 Web 服务器设置。
3. 在新注册应用的 API permissions 部分，添加所需的权限：
 - a. 请确保适用于 **Microsoft Graph** 的“Delegated”权限类型已存在，并且具有“User.Read”权限。
 - b. 添加适用于 **Microsoft Graph** 的权限，使其具有“Application”类型和“User.Read.All”权限。
 - c. 单击 **Grant admin consent** 以授予这些 API 权限。
4. 转到新注册应用的 **Overview** 部分，并复制/记录 Azure AD Directory（租户）ID、Azure AD 应用程序（客户端）ID，以对应之前创建的 Azure AD 客户端密钥值。在服务器初始安装后，使用这些值对英特尔 EMA 的 Web 服务器进行配置，如第 4.1.10 节所述。

3.5 网页服务器

英特尔 EMA 使用 Microsoft Internet Information Server (IIS)。使用最新 IIS 10 版本。

为目标 IIS 安装 IIS URL Rewrite Module。如果已安装，英特尔 EMA 会设置网站设置，以从响应标题中删除 IIS 服务器版本。此外，重写模块会添加 HSTS 标题、将 Cookie 的 SameSite 属性设置为 strict，并从 HTTP 自动重定向到 HTTPS。如果未安装，则不会应用这些设置。



注意： 如果已安装 IIS，请确保禁用除“Anonymous”和“Windows”之外的所有身份验证方法（应仅启用这两种方法）。这仅适用于 Windows 身份验证模式。

Authentication		
Group by: No Grouping		
Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

3.6 英特尔® 主动管理技术 PKI 证书

英特尔主动管理技术管理员控制模式 (ACM) 预配要求具备由受信任机构颁发的与目标英特尔主动管理技术端点的域名匹配的证书。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： 从英特尔 ME 15 系统开始，已在英特尔主动管理技术 PKI 证书链中删除对 SHA1 根证书或大小小于 2048 的 RSA 密钥的支持。

3.7 Microsoft .NET 框架版本

英特尔 EMA 服务器软件使用 Microsoft .NET Framework 4.8 构建。操作系统必须具有 Microsoft .NET Framework 4.8 或更高版本。如果未安装 .NET Framework 4.8 或更高版本，则英特尔 EMA 安装程序将显示一个对话框，提示您下载和安装 .NET Framework 4.8 运行时。

3.8 防火墙

我们建议使用防火墙软件以确保仅授权端口可用于连接。Windows 内置的防火墙软件可以执行此任务。

3.9 网络

在安装过程中，您必须指定用于在各个组件之间进行通信的值（主机名或 IP 地址）。如果选择主机名或 FQDN，则需要确保该值可由网络中的 DNS 服务器解析。如果没有 DNS 服务器，则在安装过程中应使用固定的 IP 地址。错误的主机名/IP 地址将导致英特尔 EMA 功能无法正常运行。在分布式服务器架构实施中，如果使用 Active Directory，请确保所有计算机（包括托管负载均衡器的计算机）都列于 Active Directory 中。

所选的 FQDN 和/或 IP 地址用于各种目的：

- Swarm 服务器负载均衡器 FQDN/IP 地址是将在代理配置文件中提供的位置，用于与端点代理、英特尔主动管理技术或英特尔® Standard Manageability 连接。
- Ajax & Web 服务器负载均衡器 FQDN/IP 地址用于英特尔 EMA 主网站的 HTTPS URL。
- 恢复服务器负载均衡器 FQDN/IP 地址用于支持“一键恢复”。

这些设置在安装后无法更改。请确保它们在 DNS 中均正确解析，并考虑选择适用的 FQDN，以便在需要时可以灵活地重新配置到其他服务器（例如，动态 DNS 条目）。

3.10 网络端口

表 1 列出了用于服务器组件之间各种通信的服务器网络端口。

- 对于某些功能/用途，AJAX 服务器和可管理性服务器将与 Swarm 服务器建立 TCP 连接（本地或远程）。
- 端点和 Swarm 服务器通过安全的 TCP 连接进行通信。英特尔主动管理技术 (CIRA) 和 Swarm 服务器通过安全的 TCP 连接进行通信。
- Platform Manager 服务使用命名管道与同一台计算机上的其他英特尔 EMA 组件服务器进行通信。Platform Manager 客户端应用程序通过安全的 TCP 连接与 Platform Manager 服务进行对话。

表 1: 服务器网络端口

协议	端口	用途
TCP	443	HTTPS 网页服务器端口。在 Web 浏览器和网页服务器之间使用。
TCP	1433	SQL Server 远程访问。这在内部英特尔 EMA 服务器和内部 SQL 服务器之间使用。仅当英特尔 EMA 服务器和 SQL 服务器不在同一台计算机上时才需要。这是 SQL Server 使用的默认端口。
TCP	8000	Platform Manager 服务和 Platform Manager 客户端之间进行通信的默认 TCP 端口。您可以在安装过程中更改此端口。
TCP	8080 [†]	代理、控制台和英特尔主动管理技术 CIRA 端口。这存在于客户端端点和英特尔 EMA Swarm 服务器之间。请参阅下面的注释。
TCP	8084	Web 重定向端口。在 Web 浏览器和网页服务器之间使用。
TCP	8085	恢复端口。由恢复组件服务器使用。如果您在“Server Settings”页面的“Recovery Server”选项卡上更改此端口，系统将提示您更新端口绑定。请参阅第 1 页的“附录 - 修改组件服务器设置”。
TCP	8089	各种英特尔 EMA 组件服务器和英特尔 EMA Swarm 服务器之间的通信。此端口号是默认端口号，可以在“服务器设置”页面中更改。请参阅第 1 页的“附录 - 修改组件服务器设置”。
TCP	8092	Ajax 组件服务器用来侦听内部组件间通信的端口。此端口号是默认端口号，可以在“服务器设置”页面中更改。请参阅第 1 页的“附录 - 修改组件服务器设置”。
TCP	8093	Swarm 组件服务器用来侦听内部组件间通信的端口。此端口号是默认端口号，可以在“服务器设置”页面中进行更改。请参阅第 1 页的“附录 - 修改组件服务器设置”。
TCP	8094	可管理性组件服务器用来侦听内部组件间通信的端口。此端口号是默认端口号，可以在“服务器设置”页面中更改。请参阅第 1 页的“附录 - 修改组件服务器设置”。
TCP	8095	恢复组件服务器用来侦听内部组件间通信的端口。此端口号是默认端口号，可以在“服务器设置”页面中更改。请参阅第 1 页的“附录 - 修改组件服务器设置”。
LDAPS/LDAP	636/389	LDAPS 安全端口是 636。标准的非安全 LDAP 端口是 389。这些端口用于 Active Directory 和/或 802.1x 配置。
全局编录 (安全/非安全)	3269/3268	安全 (3269) 和非安全 (3268) 全局编录端口。这些端口用于 Active Directory 和/或 802.1x 配置。

[†]您可以更改代理和英特尔主动管理技术 CIRA 用于连接到英特尔 EMA 服务器的端口。



1. 在负载均衡器上，创建转发规则以将所需端口（例如 8081）路由到后端 Swarm 服务器端口 8080。请注意，Swarm 服务器仍在侦听端口 8080，但这使您可以为外部网络设置其他端口。

2. 在可管理性服务器上，将服务器设置 **ciraserver_port** 从 8080 更改为所需的端口（在此示例中为 8081）。停止并重新启动可管理性服务器。有关更改英特尔 EMA 组件服务器设置的信息，请参阅第 1 页“附录 - 修改组件服务器设置”。
3. 对于网页服务器设置，请将服务器设置 **SwarmServerPort** 从 8080 更改为所需的端口。与此更改同步 IIS 应用程序设置。有关更改英特尔 EMA 组件服务器设置的信息，请参阅第 1 页“附录 - 修改组件服务器设置”。
4. 创建一个新的端点组（请注意，现有端点组将不具有新的 **SwarmServerPort** 信息），然后将端点注册到该新端点组。然后在端点上配置英特尔主动管理技术。查阅《英特尔® EMA 管理和使用指南》获取有关端点组的信息以及在端点上提供英特尔主动管理技术的信息。

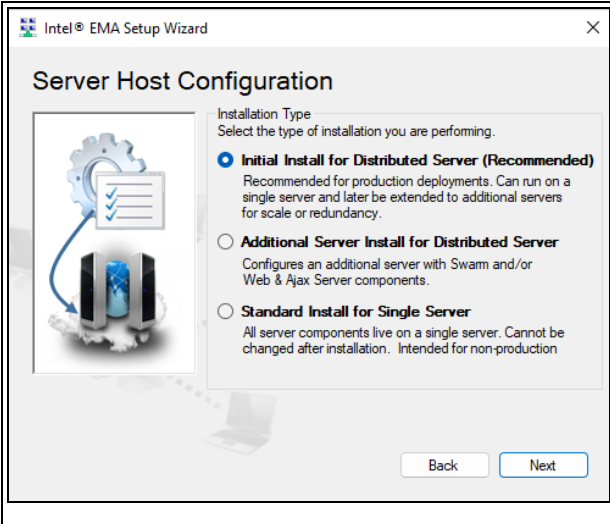
4 安装或更新英特尔® EMA 服务器

请按照以下步骤在分布式架构安装中安装英特尔® EMA 服务器。

4.1 初始服务器安装

	<p>解压缩安装 ZIP 文件，打开文件夹，然后右键单击 EMAServerInstaller.exe 并选择 Run as administrator。如果初始检查已通过，则安装程序将打开，底部的状态栏将显示“就绪”。</p> <p>单击左上方的图标开始安装过程。</p> <p> 注意：如需帮助，请单击 Help > Intel Support</p>
	<p> 警告！对于首次安装，如果继续安装过程，则英特尔 EMA 设置向导将删除 c:\inetpub\wwwroot 文件夹中的所有内容。在继续安装过程之前，请确保备份所有需要的文件。</p> <p>从之前的英特尔 EMA 版本更新时，这将不适用，尽管 IIS 绑定将设置为默认值。单击“Welcome”屏幕上的 Next 继续安装过程。显示许可协议时，接受许可可以继续。</p> <p>单击“Welcome”屏幕上的 Next 继续安装过程。</p>

4.1.1 服务器主机配置

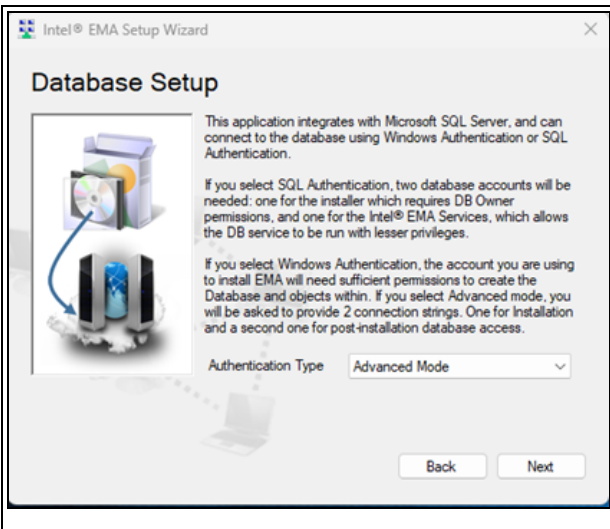


分布式服务器架构的初始安装

此服务器计算机上已安装一个或多个服务器组件，并且可以使用以下 **Additional Server Install** 选项在其他服务器计算机上安装组件的其他实例。

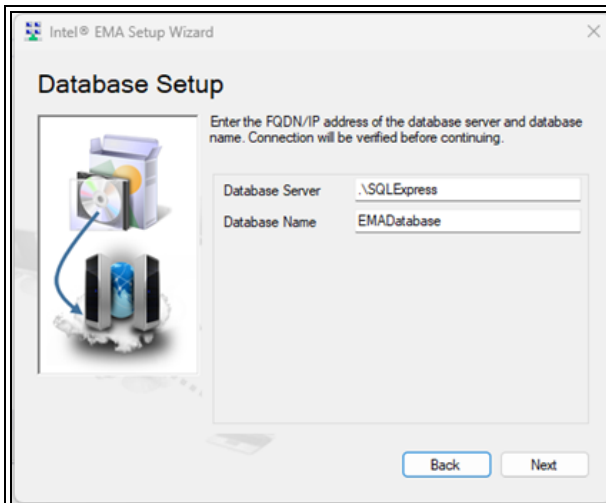
注意： 如果您正在一台计算机上安装全部组件，则不需要执行 **Additional Server Install** 章节中的步骤。

4.1.2 数据库设置



选择所需身份验证类型：Windows 身份验证、SQL 身份验证或高级模式。

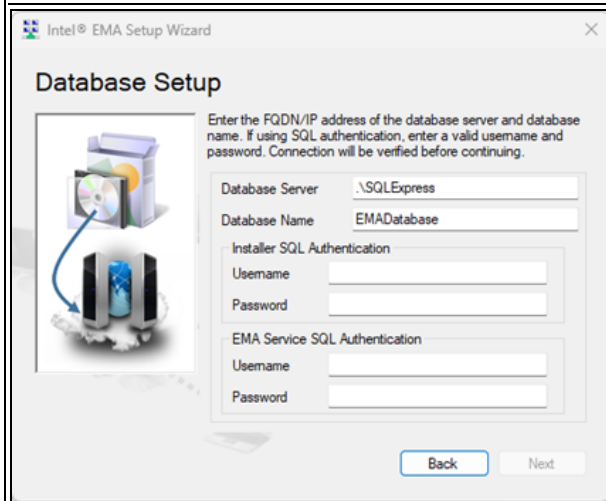
注意： 为了安全起见，建议将 Windows 身份验证模式用于 SQL 身份验证。如果使用 SQL 身份验证，则必须首先确保在 SQL 服务器中设置了目标凭据。



如果选择 Windows 身份验证，则安装所用的帐户将用于对 SQL Server 进行身份验证并创建数据库。

指定托管数据库的服务器。实际值取决于您安装的数据库服务器。有关详细信息，请参考 SQL 安装。

英特尔 EMA 安装完成后，您可以在 Windows 服务设置中修改英特尔平台管理器服务的设置，从而更改用于访问数据库的帐户。

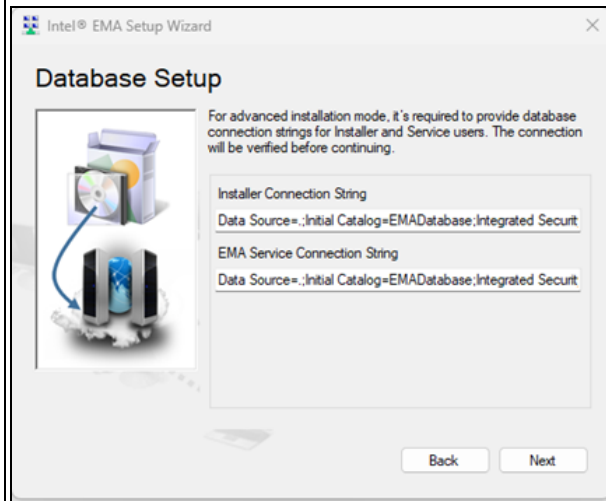


如果选择 SQL 身份验证或高级模式，则需要输入两组凭证



注意：

- 系统管理员必须提前创建这两个帐户
 - 一个帐户供安装程序使用，它需要 db_owner、sysadmin 或 db_creator 权限。
 - 一个帐户供英特尔 EMA 服务在安装后使用，以便以较低权限运行数据库服务。
 - 必须向此帐户授予连接到英特尔 EMA 数据库的权限，并授予针对数据库所有者、可管理性和安全架构的执行权限。
 - 如果向英特尔 EMA 服务使用的帐户授予 sysadmin 角色，但稍后移除了该角色，则对数据库的访问权限将不再有效。
- 如果使用的 SQL Server 与英特尔® EMA 安装在同一台计算机上，则可以使用 localhost。
- 如果使用的是远程 SQL Server，请确保为 IIS 默认应用程序池设置了 SQL Server 帐户以进行连接。



SQL 身份验证：

- 指定托管数据库的服务器。实际值取决于您安装的数据库服务器。有关详细信息，请参考 SQL 安装。
- 指定将用于创建数据库的 SQL Server 帐户，以及


	<p>英特尔 EMA 服务在安装完成后用于访问数据库的帐户。</p> <p>高级模式：</p> <ul style="list-style-type: none"> 指定两个自定义数据库连接字符串。一个字符串用于安装数据库，一个字符串供英特尔 EMA 服务在英特尔 EMA 安装完成后使用。 <p>有关连接字符串的更多信息，请参阅 https://docs.microsoft.com/zh-cn/dotnet/framework/data/adonet/connection-string-syntax。请注意，英特尔® EMA 可能不支持此页面上的部分示例。</p> <p>注意： 参数“MultipleActiveResultSets=True”是必需的。有关更多信息，请参阅 https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/enabling-multiple-active-result-sets。</p> <p>连接字符串经过加密并存储在 <code>c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config</code> 中。</p> <p>重要提示： 如果要安装分布式服务器架构，请将这些自定义连接字符串复制到文本文件中保存，以在安装其他服务器时使用。</p> <p>注意： 在升级期间会显示连接信息，但在安装流程中无法编辑这一信息。</p>
--	---

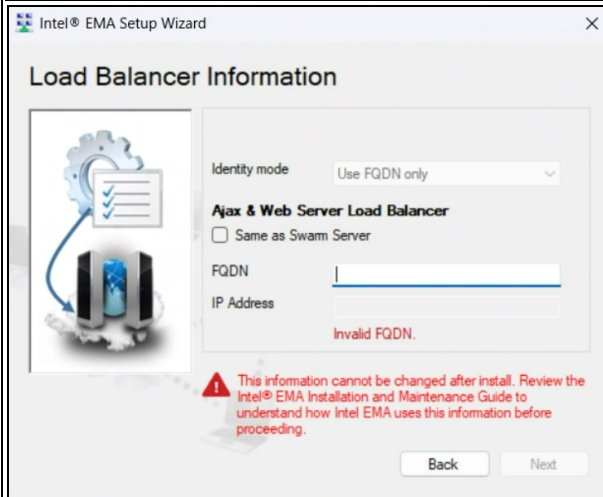
4.1.3 负载均衡器信息

	<p>对于身份模式：</p> <ul style="list-style-type: none"> Use FQDN only: 仅使用 FQDN 处理请求。我们建议输入可寻址的完整 FQDN。 Use FQDN first: 使用 FQDN 处理请求，但也可以通过 IP 地址查找网站。 Use IP address: 仅使用 IP 地址处理请求 <p>注意：</p> <ul style="list-style-type: none"> 使用英特尔主动管理技术的一键恢复功能需要完整的 FQDN。如果您打算使用一键恢复功能，则必须输入完整的 FQDN (server_name.domain)，而不仅仅是主机名。此外，如果您计划使用一键恢复，请勿选择 Use IP Address。
---	--

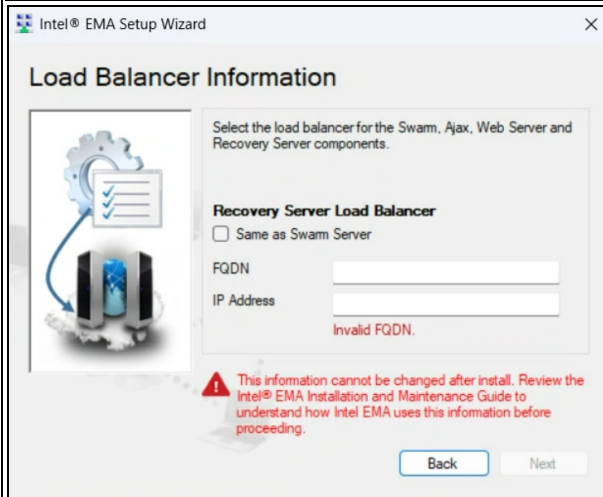
- 英特尔主动管理技术依赖 DNS 查找来解析远程主机。如果选择对服务器使用简称/主机名称，而不是 DNS 可解析 FQDN，则英特尔主动管理技术远程管理功能可能无法正常工作。

输入 Swarm 服务器的负载均衡器的 **FQDN** 和/或 **IP Address** (或两者，取决于身份模式)。


 **注意：** 如果要在同一台计算机 (或 VM) 上安装全部英特尔 EMA 服务器组件，请输入要在其上安装英特尔 EMA 的计算机或 VM 的 FQDN 和/或 IP 地址。



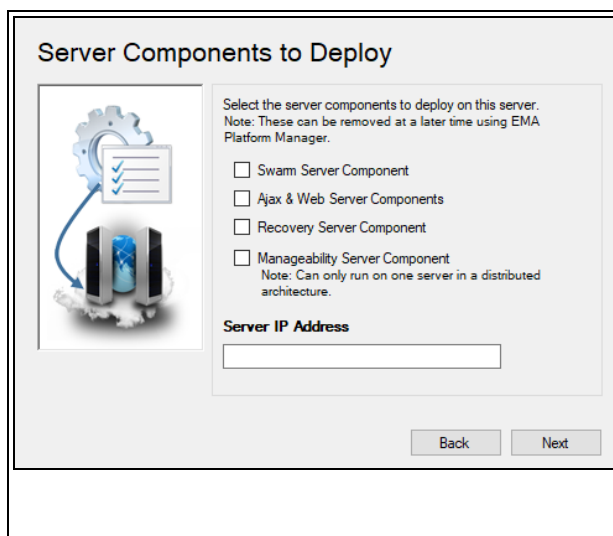
输入 Ajax 服务器和网页服务器组件 (或选择 **Same as Swarm Server**) 的负载均衡器的 **FQDN** 和/或 **IP Address** (或两者，取决于身份模式)。



输入恢复服务器组件 (或选择 **Same as Swarm Server**) 的负载均衡器的 **FQDN** 和/或 **IP Address** (或两者，取决于身份模式)。

 **注意：** 如果计划使用域/Windows 身份验证模式 (Kerberos)，则需要为支持 Ajax 和网页服务器的负载均衡器设置服务主体名称 (SPN)。

4.1.4 要部署的服务器组件



Server Components to Deploy


Select the server components to deploy on this server.
Note: These can be removed at a later time using EMA Platform Manager.

- Swarm Server Component
- Ajax & Web Server Components
- Recovery Server Component
- Manageability Server Component
Note: Can only run on one server in a distributed architecture.

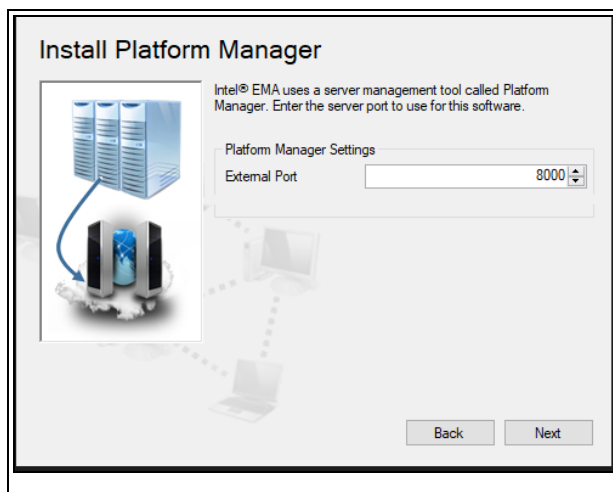
Server IP Address

Back Next

指定要在此服务器计算机上部署的服务器组件，然后验证此服务器计算机的 **IP Address**（默认情况下填写的字段）。

 **注意：** 只有一台计算机可以运行可管理性服务器组件。

4.1.5 Platform Manager 配置



Install Platform Manager

Intel® EMA uses a server management tool called Platform Manager. Enter the server port to use for this software.

Platform Manager Settings

External Port

Back Next

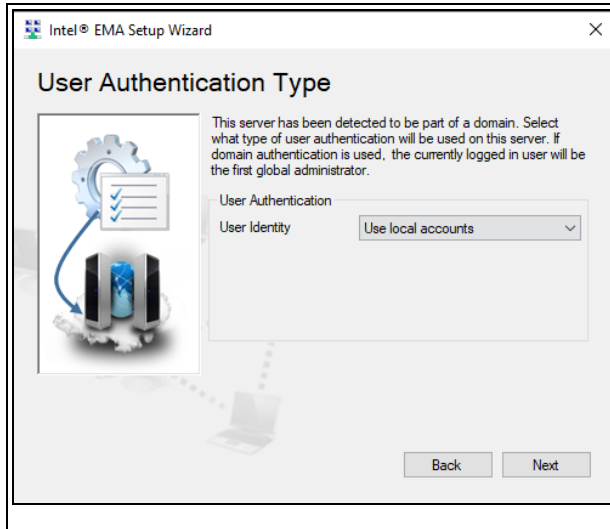
External Port 在此英特尔 EMA 服务器上运行的英特尔® EMA Platform Manager 服务使用接受来自英特尔 EMA Platform Manager 客户端应用程序的连接。确保您指定的端口在基础网络中打开。

无法在更新模式下编辑此屏幕。

4.1.6 用户身份验证

选择您想要使用何种身份验证方式。

4.1.6.1 本地帐户



如果您选择 **Use local accounts**，那么英特尔® EMA 将保留一个内部用户数据库。

这是安装过程的默认设置。这会将安装的实例置于用户名/密码模式。

4.1.6.2 域身份验证



如果您的服务器已加入 Active Directory 域，则可以选择 **Use domain authentication**。

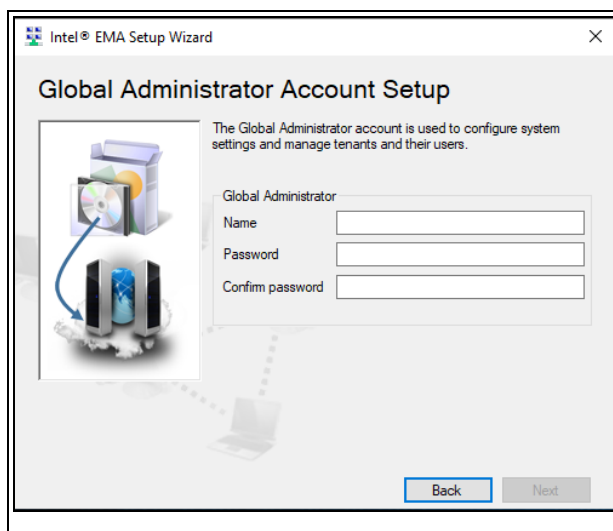
当前登录的用户将自动以“全局管理员”角色添加到英特尔 EMA（在左侧屏幕中显示为“站点管理员”）。

4.1.6.3 Azure Active Directory 身份验证



如果您的 IT 环境包含 Azure Active Directory，则可以选择 **Use Azure AD Authentication**。此选项允许您输入第一个全局管理员角色帐户的用户名和密码。Azure Active Directory 中无需包含此帐户。完成安装后，您可以使用此帐户登录和创建随后的用户，后者必须位于 Azure Active Directory 中。

4.1.7 全局管理员帐户设置

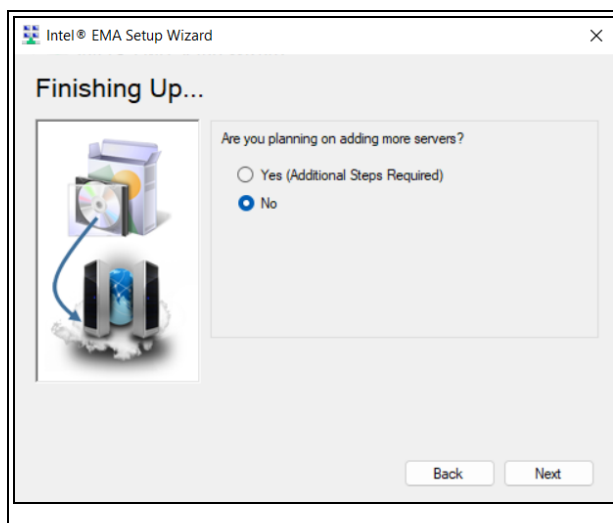


如果您已为用户身份验证选择了“普通帐户”或“Azure AD 身份验证”，则该视屏仅出现于设置期间。如果使用域帐户，则将使运行安装程序的用户成为全局管理员。

注意：必须以电子邮件地址（即 name@domain）的形式输入 **Name** 字段。

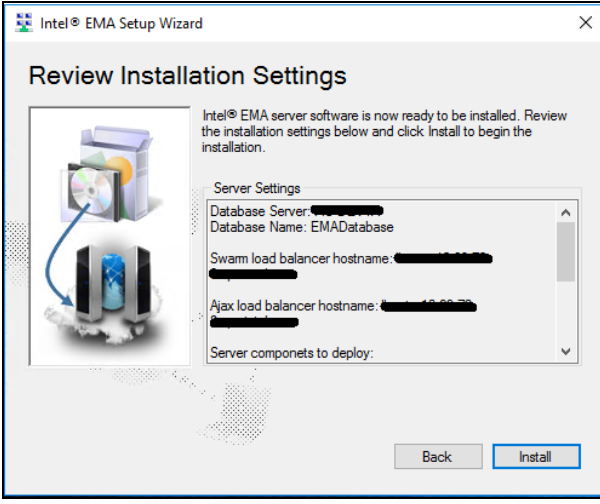
Global Administrator：此角色能够执行用户管理、租户创建和服务管理。此角色不执行设备管理。在 Azure AD 环境中，需要使用此帐户按照第 4.1.10 节中的描述来配置英特尔 EMA。

4.1.8 完成



在此视屏上选择 **No**。

4.1.9 摘要

	<p>查看您的安装设置，然后单击 Install。</p> <p>将安装所有必需的 Windows 组件，然后安装英特尔® EMA 软件本身。</p> <p>重要提示： 在安装完成之前，请勿中止或退出安装程序。不支持安装回滚。</p> <p>安装状态显示在安装程序主菜单的底部。安装期间无法使用安装选项。</p> <p>要在安装过程中检查日志文件，请单击 File > Advanced Mode。要退出高级模式，请再次单击 File > Advanced Mode。</p> <p>安装后，您可以在与英特尔 EMA 安装程序相同的文件夹中检查日志文件 EMALog-Intel®EMAInstaller.txt。</p>
---	--

注意： 无论是通过本地 SQL Server 还是通过远程 SQL Server 进行安装，安装日志文件中都会出现以下警告。通过远程 SQL Server 安装时，可以忽略此消息。通过本地 SQL Server 安装时，请确保将帐户设置为允许 IIS 默认应用程序池连接。

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

4.1.10 修改 Azure AD 的服务器设置

注意： 仅当您使用 Azure AD 身份验证模式安装了英特尔 EMA 后，才需要执行这些步骤。

在英特尔 EMA 用户界面的“Server Settings”选项卡上执行以下步骤。必须先执行这些步骤，您才可以在 Azure AD 身份验证模式中添加其他用户。

1. 使用初始全局管理员 (root GA) 帐户及其用户名和密码登录到英特尔 EMA。
2. 导航到 "Server Settings" 页面，然后到 Web 服务器设置。
3. 使用您在第 3.4 节中复制并保存的值，输入 **Azure AD Directory (tenant) ID**、**Azure AD Application (client) ID** 和 **Azure AD Client Secret Value**。


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**。

当这些设置更新后，英特尔 EMA 服务器将进行测试，验证能否成功连接到 Azure AD 环境。

5 使用全局管理员界面

英特尔® EMA 的全局管理员页面用于管理租户、用户和用户组。

要登录英特尔 EMA，请执行以下操作：


1. 打开浏览器并导航到安装期间指定的 FQDN/主机名。
2. 在登录页面上，输入全局管理员的用户名（例如：电子邮件地址）和密码。
 **注意：**如果指定了域身份验证，将自动显示全局管理员“Overview”页面。
3. 在 **Overview** 页面底部的 **Getting Started** 下，单击 **View Getting Started tips**。
4. 在 **Getting started** 页面上，按照步骤（按顺序）**Create a Tenant**、**Add a Tenant Administrator**，然后 **Add Additional Users**（如果需要）。请注意，您必须为您创建的每个租户至少创建一个租户管理员。全局管理员无法执行租户中的许多任务。

注销

要注销，请单击 **Overview** 页面顶部栏中的用户名，然后选择 **Log out**。

6 租户设置和端点代理部署

本节介绍如何在英特尔® EMA 服务器上设置租户工作空间以及如何将英特尔 EMA 代理部署到托管端点系统。

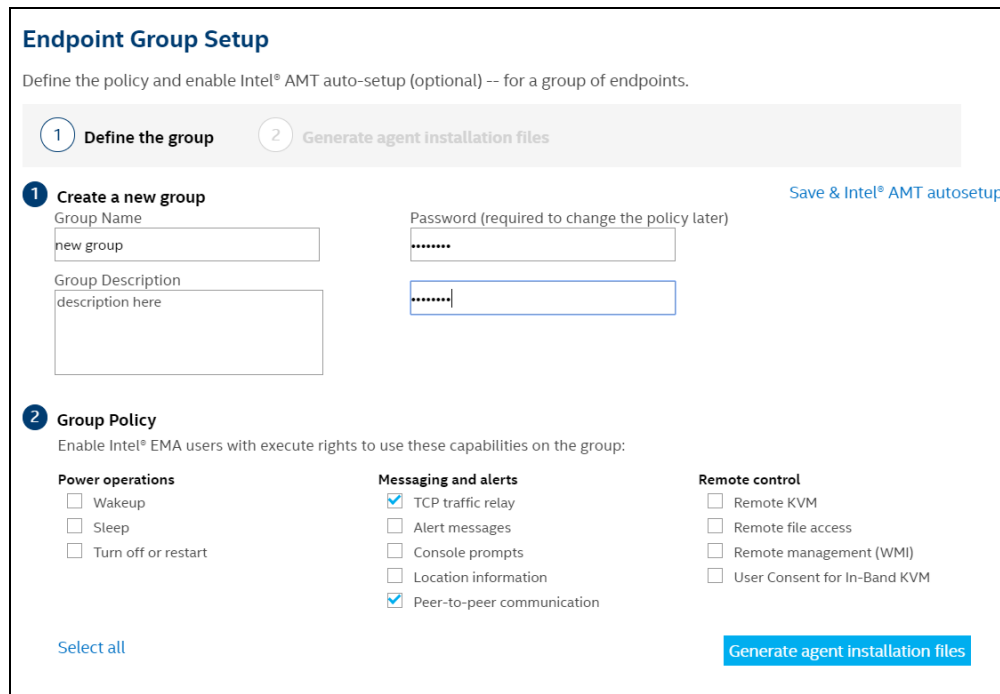
 **注意：** 您必须以具有“租户管理员”特权的用户身份登录到英特尔 EMA 服务器，才能执行本节中的步骤。

要登录英特尔 EMA，请执行以下操作：

1. 打开浏览器并导航到服务器安装期间指定的 FQDN/主机名。
2. 在登录页面上，输入租户管理员用户的用户名（即电子邮件地址）和密码。

6.1 创建您的端点组

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功能 **Group Policy**。
3. 单击 **Generate agent installation files**。



6.2 创建代理文件以部署到托管端点

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**。

Generate Agent Installation Files

After the files are installed on endpoints, the endpoints will join this group:

Windows (64-bit) Service 


Also download the agent policy file

Agent policy file 

Now, go copy the agent policy file and the appropriate agent file to each endpoint (manually or using a distribution tool).

Install the agent by running the agent as administrator for that endpoint

Tip: keep the agent and agent policy files together. The file names (other than the extensions) must be the same




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。

6.3 创建您的英特尔® 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**。
 - **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。

6.4 启用英特尔® 主动管理技术自动设置

1. 选择 **Enabled** 复选框，然后选择您先前创建的 **Intel® AMT profile**。
2. 选择要使用的 **Activation Method**。要快速启动，请使用 **Host Based Provisioning**。
3. 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。

4. 单击 **Save**。
5. 如果您正在执行初始租户设置，请继续执行第 6.5 节的操作，以将代理文件部署到您的端点。

6.5 将代理部署到端点



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
```

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”。

7 英特尔® EMA 服务器管理



注意：要执行本节中的步骤，请以租户管理员用户身份登录到英特尔® EMA 服务器。有关用户角色的信息以及全局管理员和租户管理员用户之间的区别，请参阅《英特尔® EMA 管理和使用指南》中的“用户角色”。

7.1 创建新的用户组

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。

7.2 添加、修改和删除用户

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。

7.3 将端点组分配给用户组

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**。

8 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 <ul style="list-style-type: none">• 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。