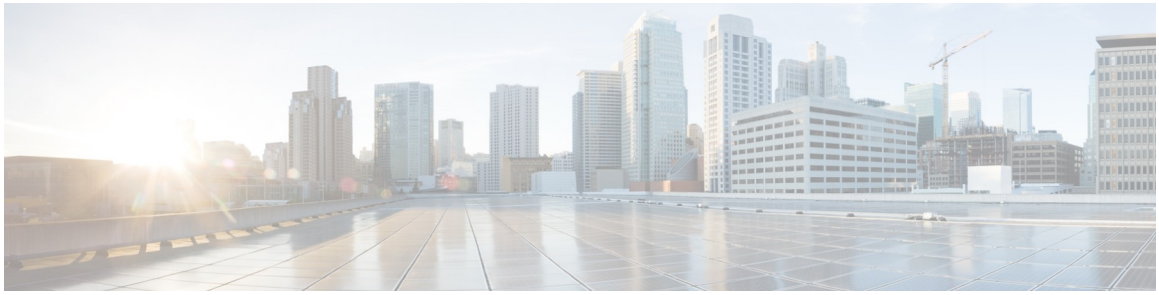


Cisco Intersight 概述

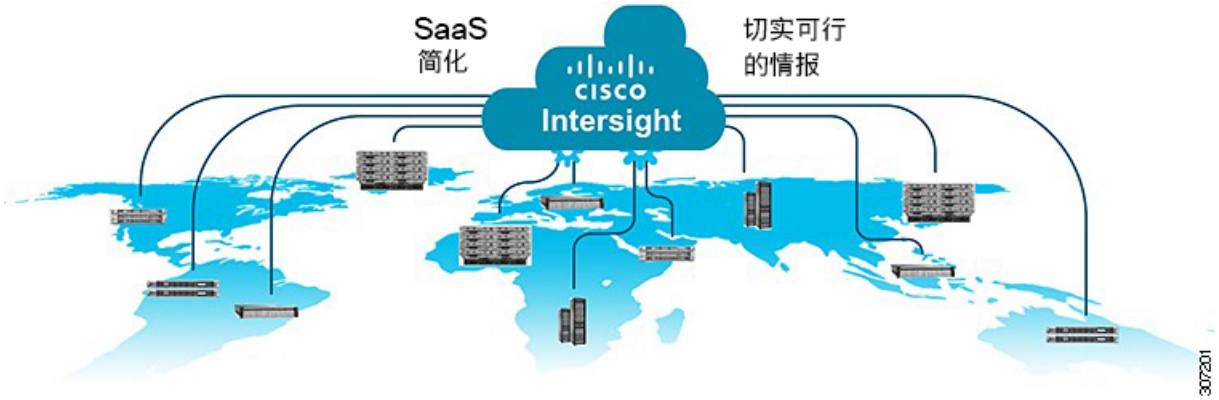
• Cisco Intersight 入门指南，第 1 页

Cisco Intersight 入门指南

Cisco Intersight 概述

Cisco Intersight™ 是以服务的形式提供的管理平台，嵌入了适用于思科和第三方 IT 基础设施的分析功能。此平台可提供智能级别的管理，相较于之前的几代工具，它让 IT 组织可以用更高级的方法对组织环境进行分析、简化并实现自动化。Cisco Intersight 为传统数据中心和边缘的资源提智能的集成式管理体验。由于有灵活的部署选项来满足复杂的安全需求，Intersight 入门非常简单快捷。

Cisco Intersight 与 Cisco UCS 和 HyperFlex 系统深度集成，可以实现远程部署、配置和持续维护。基于模型的部署适用于远程位置的单个系统或数据中心中数以百计的系统，并且支持快速、标准化的配置和部署。无论您使用的是小型配置还是大型配置，它都可以简化这些系统的维护。



Cisco Intersight 包括支持 OpenAPI 规范的 API，这是一种描述 RESTful API 的强大定义格式。由于支持 OpenAPI 规范，因此可以利用自动生成 Intersight API 文档 (intersight.com/apidocs)、API 架构和 SDK 的工具获得互通性 REST API。Intersight API 包括功能齐全的 Python 和 PowerShell SDK。

审阅稿 - 思科机密

Cisco Intersight 提供灵活的部署选择，既可以采用软件即服务 (SaaS) 的形式部署在 Intersight.com 上，又可以作为 Cisco Intersight 虚拟设备在本地运行。作为虚拟设备，它可以提供 Cisco Intersight 的优势，同时为具有更多数据位置和更高安全要求的客户提供更大的灵活性。要了解有关该虚拟设备的更多信息，请参阅 Cisco Intersight 虚拟设备入门指南。

有关 Intersight 的当前特性和功能的完整总结，请参阅支持的系统。

Cisco Intersight 设置和设备申领

要开始使用 Cisco Intersight，请确保完成以下步骤：

1. **创建 Cisco Intersight 账户**。访问 https://intersight.com/，创建 Intersight 账户。您必须具有有效的 Cisco ID 才能创建 Cisco Intersight 账户。如果没有 Cisco ID，可以在此处创建一个。
2. **申领新设备**。在“设备详细信息”页面中，点击**申领新设备**，然后完成以下步骤，以申领由 Cisco Intersight 管理的一台或多台设备：
   a. 输入相应的设备 ID。终端设备通过一个设备连接器连接至 Cisco Intersight 门户，该设备连接器嵌入在每个系统的管理控制器（即用于 Cisco UCS Director 的管理虚拟机）。该设备连接器为所连接的设备提供一种使用安全互联网连接向 Cisco Intersight 门户发送信息和从该门户接收控制指令的安全方式。下表提供了设备 ID 格式和设备连接器位置：

设备	设备 ID 格式和示例	设备连接器位置
UCS 域	主辅 FI 的序列号 ID 采用这种格式：FI-A 的序列号 & FI-B 的序列号 示例：[SAL1924GKV6&SAL1913CJ7V]	在 Cisco UCS Manager 中依次选择**管理** > **设备连接器**
Cisco UCS C 系列独立服务器	序列号 示例：NGTR12345	在 Cisco IMC 中依次选择**管理** > **设备连接器**
HyperFlex	集群 UUID 示例：xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	在 Cisco HyperFlex 中依次选择 **HyperFlex Connect UI** > **设置** > **设备连接器**
Cisco UCS Director 和思科数据中心网络管理器 (DCNM)	设备 ID 示例：xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx。	在 Cisco UCS Director 中依次选择**管理** > **设备连接**器 在 Cisco DCNM 中依次选择**管理** > **DCNM 服务器** > **设备连接器**
思科应用策略基础设施控制器 (APIC)	设备 ID 由 APIC 节点的序列号 ID 组成 示例：DIF1123FGFG& DIF2345GHJK & DIS5678SDFG	在 Cisco APIC 中依次选择**系统** > **系统设置** > **Intersight** > **Intersight 设备连接器**

审阅稿 - 思科机密

设备	设备 ID 格式和示例	设备连接器位置
思科应用服务引擎	设备 ID 由服务节点的序列号 ID 组成 示例：DIF1123FGFG& DIF2345GHJK & DIS5678SDFG	在思科应用服务引擎中依次选择 **Cisco APIC** > **应用** > **思科应用服务引擎** > **Intersight**

b. 申领节点。输入设备申领代码，然后点击**申领**。您可以在相应设备类型的 “设备连接器” 中找到此代码。

备注 在获取申领代码前，请确保设备连接器对 Cisco Intersight 具有出站网络访问权限，且处于 “未申领” 状态。

3. **添加用户。**在 “设置” 中，依次选择**用户** > **添加新用户** > **添加用户**，然后提供用户的 Cisco ID 并选择一个用户角色。您可以为新用户选择只读或管理员角色。要获得申领设备和添加新用户方面的更多帮助，请按照 Cisco Intersight 中的指导帮助进行操作。

有关在管理接口上启用 Intersight 管理和配置设备连接器的详细信息，请参阅下面列出的相应文档:

- Cisco UCS Manager 管理指南
- Cisco UCS C 系列集成管理控制器 GUI 配置指南
- 适用于 Cisco Intersight 的 Cisco HyperFlex 系统安装指南
- Cisco UCS Director 管理指南
- 思科网络洞察力文档

使用 Intersight Assist 申领设备

仅当您使用 Cisco Intersight Assist 申领设备时，才可以将终端设备（例如纯存储设备和 VMware vCenter 设备）添加到 Cisco Intersight 中。完成以下步骤，使用 Intersight Assist 来申领这些设备:

1. 在 “设备详细信息” 页面中，点击**申领新设备** > **通过 Intersight Assist 申领**。
2. 输入以下详细信息完成设备申领:
   a. **Intersight Assist**：如果有多个 Intersight Assist，请从列表中选择一个要使用的 Intersight Assist。
   b. **设备类型**：选择纯存储闪存阵列或 VMware vCenter。
   c. **主机名/IP 地址**：纯存储闪存阵列或 VMware vCenter 的管理地址，可以是 IPv4、IPv6 或完全限定域名 (FQDN)。
   d. **端口**：要连接到受管设备的端口号。此字段是可选字段。如果不指定端口号，系统将选择默认端口。

e. **协议**：用于连接到受管设备的协议，可以是 HTTPS 或 HTTP。

f. **用户名**：受管设备的登录凭证。

g. **密码**：与用户名关联的密码。

3. 点击**申领**。

   在申领设备后，您可以在**设备**选项卡中查看纯存储设备和 VMware vCenter 设备。此外，您还可以在左侧面板上查看**存储**选项卡和**虚拟化**选项卡。

取消申领设备

您可以直接从 Intersight 门户或终端上的设备连接器取消申领设备。思科建议您尽可能从 Intersight 门户取消申领设备。只有在您无法访问申领设备的原始账户或与 Intersight 失去连接并且您想要在终端本地取消申领设备时，才应使用设备连接器上的**取消申领**选项。

直接从 Intersight 门户取消申领设备可确保完全删除设备资产并将设备重置到注册账户。然后便可以重新申领设备。但是，当您从终端取消申领设备时，设备将在当前 Intersight 账户或申领设备的虚拟设备中保持**已取消申领**状态。您必须从 Intersight 用户界面中删除设备资产，使设备可以移动到注册账户，然后才能重新申领设备。

- 当您取消申领设备时，您将无法再从 Intersight 进行管理。
- 当设备被取消申领时，它会立即与相应的 Intersight 账户解除关联。
- 设备将保留在取消申领操作之前应用的任何配置，但后续任何更改配置的尝试都将失败。任何关联的配置文件都将与相应的设备取消关联。在再次分配配置文件或执行任何其他操作之前，您必须将该设备重新申领到另一个 Intersight 账户，然后重新创建和部署策略、配置文件以及其他配置设置。

要从 Intersight 用户界面删除设备，请执行以下操作:

1. 点击**设备**以查看设备表视图。
2. 选择要删除的设备，然后点击**垃圾桶**图标。以后您可以按照**申领设备**部分描述的步骤，根据需要重新申领设备。

备注 删除设备不会更改设备配置，只是将其从申领设备的 Intersight 账户中移除。仅当您重新申领设备的情况下，Intersight 才可以在删除设备后重新访问设备。

要从终端上的设备连接器取消申领设备，请仅在您无法访问申领设备的原始 Intersight 账户时采用这种方式。

1. 直接登录设备，然后导航至设备连接器。有关如何导航至设备连接器的详细信息，请参阅**申领设备**部分中的步骤 2b。
2. 点击**取消申领**。设备现在即可供申领。在终端上完成从账户取消申领后，验证**设备**表视图中与账户取消关联的设备是否显示**已取消申领**状态。请在 Intersight 用户界面中完成取消申领过程，再重新申领相应设备。

许可要求

Cisco Intersight 使用有多个级别的基于订用的许可证。您可以购买一年、三年或五年的订用持续时间，并为所选订用持续时间选择所需的 Cisco UCS 服务器卷层。您访问 Cisco Intersight 门户并申领设备后，每种思科终端（Cisco UCS 服务器、Cisco HyperFlex 系统或 Cisco UCS Director 软件）都会自动包含 Cisco Intersight Base，而不收取任何额外费用。您可以使用思科订购工具购买以下任何级别的 Intersight 许可证:

- **Cisco Intersight Essentials**。Essentials 具备 Base 级别的所有功能，此外还包括很多其他功能，例如 Cisco UCS Central 和 Cisco IMC 管理引擎授权、使用服务配置文件的基于策略的配置、固件管理，以及与硬件兼容性列表 (HCL) 的兼容性评估。
- **Cisco Intersight Advantage**。Advantage 提供 Base 和 Essentials 级别的所有特性和功能。
- **Cisco Intersight Premier**。除了 Advantage 级别提供的功能之外，Intersight Premier 还包括 Cisco UCS Director 的全部订用授权，而不收取任何额外费用。

注意 作为技术预览提供的 Cisco Intersight 功能（如在平台用户界面中 “技术预览指定” 所示）是以正在开发的功能的预览形式提供的，这些功能（包括 GUI 和 API 接口）的技术预览可能会与全面上线时不一样。此外，技术预览交付的级别可能与功能全面上线时提供的许可证级别不同。

下表列出了按许可证级别分配的 Intersight 特性和功能。有关在不同平台上支持的功能的细分，请参阅 “支持的系统”。

Cisco Intersight 许可模式

功能	Base	Essentials	Advantage	Premier
Cisco HyperFlex 安装	✓	✓	✓	✓
运行状况和资产状况全局监控	✓	✓	✓	✓
集成思科技术支持中心 (TAC)	✓	✓	✓	✓
用户可自定义的控制面板	✓	✓	✓	✓
搜索和标记	✓	✓	✓	✓

审阅稿 - 思科机密

功能	Base	Essentials	Advantage	Premier
元素管理器的情景启动	✓	✓	✓	✓
支持合同状态	✓	✓	✓	✓
远程管理和 vKVM	✓ 仅适用于 HyperFlex	✓	✓	✓
与硬件兼容性列表 (HCL) 的兼容性		✓	✓	✓
使用服务配置文件进行基于策略的配置		✓	✓	✓
Intersight 虚拟设备部署		✓	✓	✓
固件管理		✓	✓	✓
服务器操作、详细信息、图形服务器视图		✓	✓	✓
REST API		✓	✓	✓
服务器配置文件、策略和详细信息		✓	✓	✓
Intersight 移动应用		✓	✓	✓
适用于 ServiceNow 的 Cisco Intersight ITSM 插件		✓	✓	✓
操作系统安装		✓ **功能预览**	✓ **功能预览**	✓ **功能预览**
自定义指标构件		✓ **功能预览**	✓ **功能预览**	✓ **功能预览**
通告		✓ **功能预览**	✓ **功能预览**	✓ **功能预览**
HyperFlex 集群容量规划		✓ **功能预览**	✓ **功能预览**	✓ **功能预览**
Cisco IMC 管理引擎和 Cisco UCS Central 授权		✓	✓	✓
Cisco HyperFlex SD-WAN			✓ **功能预览**	✓ **功能预览**
启动隧道 vKVM			✓	✓
Cisco UCS Director 授权				✓

作为新 Intersight 用户，您可以选择以下其中一个选项:

- **试用（评估）**。您可以在没有注册许可证的情况下对 Intersight 进行 90 天的评估。在此**试用**期将提供 Intersight 的高级功能，无需注册许可证。您可以在**许可证**页面**设置**下查看评估期的详细信息。在试用期结束并进入**试用到期**状态之前，您必须激活有效的许可证。当试用到期时，功能将恢复为 Base 级别，所有高级功能都不可用。
- **激活 Intersight 许可证**。根据以下说明注册 Intersight Essentials、Advantage 或 Premier 许可证:
  1. 依次选择**设置** > **许可证**，点击**注册**。
  2. 点击**思科智能软件管理器**，获取您的 Intersight 注册令牌。如果您没有智能账户，请在此处创建一个。您可以从同一智能账户购买订用，并为所选订用持续时间选择所需的 Cisco UCS 服务器卷层。
  3. 将对话框中的**产品实例注册令牌**粘贴到 “智能软件许可产品注册” 对话框中，然后点击**注册**以激活您的许可证。

  观看激活 Cisco Intersight Essentials，了解如何从 “思科智能许可” 账户激活许可证。

根据您的订用状态，Intersight 账户许可证可能是以下一种状态:

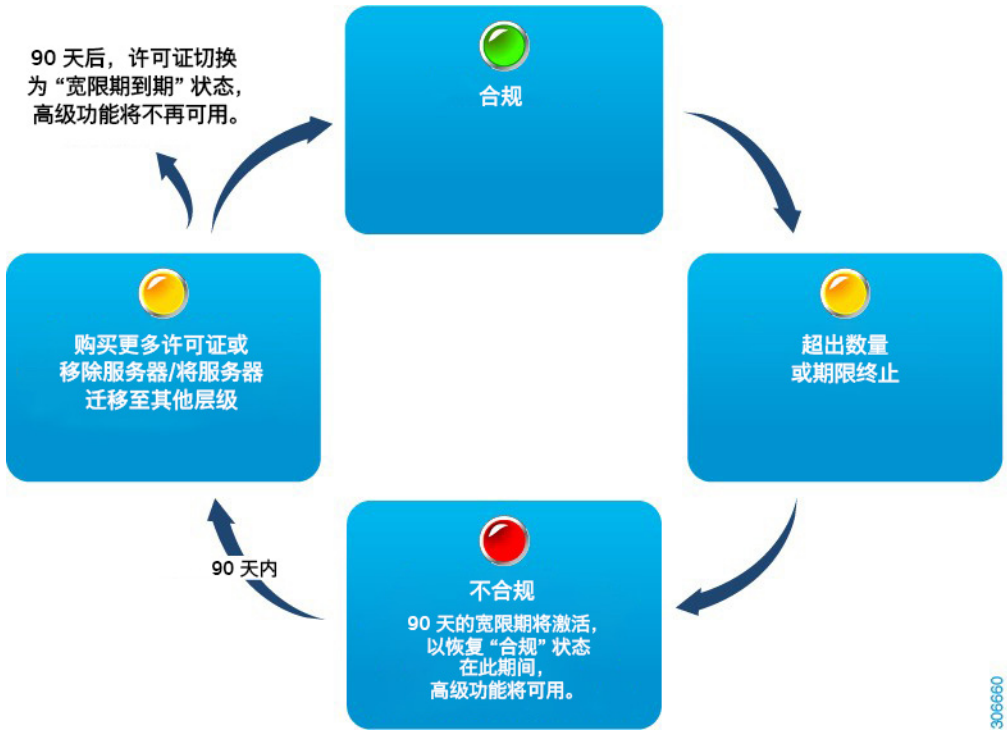
- **未使用。**当许可证级别中的服务器计数为 0 时，系统将显示此状态。
- **合规。**账户许可为 “合规” 状态，所有支持的功能均可供用户使用。
- **不合规。**在以下情况下，账户许可证显示 “不合规” 状态:
  - 因为订用已到期而没有足够的有效许可证，或者您的许可证级别中的服务器数量超过了可用许可证数量。
  - 90 天的宽限期激活或到期
  - 服务器已添加到账户，但未在智能许可账户中注册

  账户许可证状态切换到 “不合规” 状态时，系统将触发 **90 天宽限期**。在此期间，您可以继续使用高级功能，但账户许可证保持 “不合规” 状态。要恢复合规状态，您必须购买更多许可证或将服务器从现有级别删除或将其移至较低的级别。如果您未在 90 天内续约许可证，则许可证将进入**宽限期到期**状态，并且许可证将降级至 Base 级功能，而高级功能将不可用。您必须重新注册有效的许可证，才能继续使用该功能。

  例如，如果某个账户拥有 20 台服务器的有效许可证，并且您需要将另一台服务器申领到该账户，则账户将进入 “不合规” 状态，并启动宽限期。但是，您可以继续像以前一样访问这些功能。要恢复 “合规” 状态，您可以从**服务器详细信息**页面中的**操作**菜单或从表视图的**服务器/批量操作**菜单，将其中一台服务器移至更低的级别（根据需要移至 Base/ Essentials/Advantage 级别）。

备注 从思科智能许可门户购买并激活更多许可证后，点击 “订用” 窗格中的 “刷新” 图标，以将许可状态与门户中的许可状态同步。

审阅稿 - 思科机密



注意

- Intersight 许可证独立于 UCS 域，并在服务器级实施。拥有有效许可证的所有服务器都可以使用许可的功能。
- 您可以随时激活任何 Intersight Essentials/ Advantage/Premier 最多 90 天的试用期，而不一定要在创建账户时激活。这种试用是一次性授权。

多个许可级别

Intersight 允许在单个 Intersight 账户中拥有多个活动许可证级别。您可以将服务器分配到首选级别，这样您可以更灵活地将适当级别的功能应用于特定系统。

系统通过以下方式监控许可证级别:

- **许可证状态** - 这是一个控制面板构件，您可以在其中查看许可证状态快照以及每个级别的服务器数量。Intersight 会显示以下许可证状态:
- **许可证设置**（从**设置**菜单访问）- 提供特定许可证级别的服务器状态和数量的详细信息，合规状态、最近更新日期、使用情况以及注册和取消注册的选项。每个许可证级别的功能列表左上角的蓝色标记表示许可证级别是否处于活动状态，右上角的绿色标记表示该许可证级别是否设置为默认级别。

  要将许可证级别设置为默认级别，请点击**设置为默认值**按钮。将某个级别设置为默认级别时，申领到此账户的所有新服务器都将默认属于此许可证级别。

您可以将一个或多个服务器更新为新的许可证级别。可从以下位置访问**设置许可证级别**选项:

- 从**服务器**表视图中，选择一台服务器，然后点击最右列的省略号 (...)。从菜单中选择**设置许可证级别**，打开**设置许可证级别**窗口，然后从下拉列表中选择新的许可证级别。
- 从**服务器详细信息**视图中，点击**操作**菜单并选择**设置许可证级别**。
- 要同时更新多台服务器，请在**服务器**表视图中选择所需服务器，点击表左上角的**批量操作**省略号 (...)，然后选择**设置许可证级别**。

备注 在具有关联服务器配置文件的服务器上不允许更新许可证级别。要将许可证移至其他级别，请从选择的一个或多个服务器中取消分配配置文件，然后重试。

根据当前许可证状态，如果您将服务器从更低级别更新到更高级别，则可能会保持**合规**状态或更改为**不合规**状态。许可证级别磁贴指示为服务器标记的级别。**默认**级别以蓝色突出显示，已经超出宽限期和不合规的以红色突出显示。当您的服务器处于不止一个级别时，所有服务器都以蓝色突出显示。如果许可证状态为处于**试用**阶段，则会在相应的级别磁贴中显示**试用**标签。

多级别许可准则

- 如果您的 Intersight 账户中所有服务器都在同一许可证级别，则账户许可证状态将同样适用于所有服务器。
- 如果某服务器从更高的许可证级别迁移到较低的级别，则与更高级别关联的所有功能都将无法用于该服务器。
- 如果关联服务器当前正在使用更高级别的功能，则不允许将服务器许可证级别更新到较低的级别。
- 例如，如果您已使用 Essentials 许可证级别申领 50 台服务器，但仅为 25 台服务器注册了 Essentials 许可证，则账户**不合规**。借助多级别许可，您可以将 25 台已申领的服务器移至 Base 许可证级别，从而使账户保持**合规**。

有关 Intersight 许可的最常见问题，请参阅 “常见问题解答” 中的许可部分获取答案。

网络连接要求

所有设备连接器都必须解析 svc.intersight.com 并且在端口 443 上允许出站启动的 HTTPS 连接。如果与 svc.intersight.com 的 HTTPS 连接需要代理，可以在 “设备连接器” 用户界面进行配置。

备注 Intersight 设备连接器可以通过解析一个以下 URL 连接至 Intersight:

- svc.intersight.com **（首选）**
- svc.ucs-connect.com **（以后将弃用）**

要与 Intersight 成功建立设备连接，请确保满足以下连接要求：

- 从设备连接器建立与 Intersight 平台的网络连接。
- 确保在设备连接器中启用 **Intersight 管理**（默认情况下已启用）。**Intersight 管理**可以在 Cisco UCS Manager/Cisco UCS Director/Cisco IMC 中的**管理** > **设备连接器** > **Intersight 管理**中找到，在 Cisco HyperFlex 用户界面中则可以在**设置** > **设备连接器**中找到。
- 检查受管设备和 Intersight 之间是否采用了防火墙，或者是否已更改现有防火墙的规则，以免影响连接。如果更改了规则，请确保更改的规则允许流量通过防火墙。
- 确保允许所有适用的物理和虚拟 IP 通过防火墙。
- 如果您使用 HTTP 代理将流量路由到外部，并且您已对 HTTP 代理服务器的配置进行了更改，请确保相应地更改设备连接器的配置。这是必要的，因为 Intersight 不会自动检测 HTTP 代理服务器。
- 确保存在 Intersight 门户提供的有效 CA 签名证书。
- 配置 DNS 并解析 DNS 名称。设备连接器必须能够向 DNS 服务器发送 DNS 请求并解析 DNS 记录。设备连接器必须能够将 svc.intersight.com 解析为 IP 地址。
- 配置 NTP 并验证设备时间是否与时间服务器正确同步。

备注 当设备时间未正确同步时，设备连接器可能无法与 Intersight 建立安全连接，并且 TLS 证书可能被视为无效。

注意 您必须在管理接口 (Cisco UCS Manager/Cisco IMC/Cisco HyperFlex) 上，而不是在设备连接器用户界面上，配置 DNS 和 NTP。

- 您必须启用与 svc.intersight.com 的网络连接来配置网络路径中的安全设备。例如，您必须创建防火墙或 Web 代理规则。有关详细信息，请参阅关于在安全设备中配置网络 ACL 的建议。
- 设备连接器与 https://svc.intersight.com/ 建立 HTTPS 连接，然后将 HTTPS 连接升级到 Web 套接字。确保您的安全规则允许设备连接器建立 Web 套接字连接。
- 任何给定 URL 的 IP 地址都可能发生更改。如果您需要为具有固定 IP 的 URL 指定防火墙配置，请使用一种以下方法：
  - svc-static1.intersight.com（**首选**）。
  - svc-static1.ucs-connect.com（**以后将弃用**）。这两个 URL 均解析为以下 IP 地址：
    - 3.208.204.228
    - 54.165.240.89
    - 3.92.151.78

审阅稿 - 思科机密

- Intersight 设备连接器访问端口 80 上的 amazontrust.com 以验证证书。为确保证书验证成功，您必须在防火墙设置中打开端口 80 和白名单 amazontrust.com。
- 您可以访问 Intersight 门户，并使用 IPv6 地址调用 API。Intersight 管理的设备可以通过 IPv6 地址连接到 Intersight。

关于在安全设备中配置网络 ACL 的建议

安全设备支持基于 DNS 名称或 IP 地址的网络访问控制列表 (ACL)。安全设备支持 DNS 名称时，请使用 **svc.intersight.com** 配置网络 ACL；安全设备不支持 DNS 名称时，请使用 IP 地址。您可以通过检索 svc.intersight.com 的 DNS A 记录（DNS 系统中公开提供）来获取 IP 地址列表。例如，在 Linux 系统上，键入 **dig svc.intersight.com**，然后查看**答案部分**。以下是答案部分的示例。

```
svc.intersight.com. 5           IN          A           aa.aaa.aaa.aaa
svc.intersight.com. 5           IN          A           aa.aaa.aaa.aaa
svc.intersight.com. 5           IN          A           aa.aaa.aaa.aa
```

A 记录不会频繁更改，但在较长时间内也可能会发生变化。因此，需要定期更新配置。

配置 HTTPS 代理

显式 HTTPS 代理充当设备连接器和 svc.intersight.com 之间交换消息的中介。代理必须支持 HTTP CONNECT 方法，以便设置通过这种连接转发任意数据。要与 svc.intersight.com 建立连接，设备连接器应连接到代理并发送 HTTP CONNECT 方法。代理将转发设备连接器和 svc.intersight.com 之间的所有流量，而不修改 TLS 握手，因此不需要执行证书配置。使用以下步骤在设备连接器用户界面中配置显式代理的主机名或 IP 地址:

- 在设备连接器用户界面的**代理配置**选项卡上，将 “HTTPS 代理” 选项滑动至**开**状态。
- 输入代理主机名或 IP 地址。
- 输入代理端口。
- 输入用于身份验证的用户名和密码。

备注 设备连接器不指定用于身份验证的登录凭证格式。该格式将按原样传递到已配置的 HTTP 代理服务器。是否可以使用包含域名的用户名取决于 HTTP 代理服务器的配置。

支持的浏览器

支持运行 Cisco Intersight 的最低浏览器版本如下:

- Google Chrome 62.0.3202.94
- Mozilla Firefox 57.0.1
- Apple Safari 10.1.1
- Microsoft Edge (Chromium) Beta

软件兼容性

本部分包含有关以下软件的受支持版本的详细信息:

组件	支持的最低版本
Cisco UCS Manager	3.2(1)
Cisco HyperFlex 数据平台	2.5(1a)
Cisco HyperFlex Connect	2.6
Cisco IMC	• 3.1(1) • 对于 Cisco UCS C 系列 M4 服务器为 3.0(4) 有关 M4 和 M5 服务器的 Cisco IMC 软件要求的详细信息，请参阅 https://intersight.com/help/supported_systems。
Cisco UCS Director	6.6.0.0

相关文档

- Cisco Intersight 提供基于云的 RESTful API，可跨多个数据中心管理 Cisco UCS 和 Cisco HyperFlex 系统。要了解有关 Intersight API 的更多信息，请参阅 API 文档。