SIEMENS

SIMATIC

TIA Portal Cloud Connector 的操作指南

操作手册

07/2016
A5E37384256-AA

法律资讯

警告提示系统

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

⚠ 危险
表示如果不采取相应的小心措施，**将会**导致死亡或者严重的人身伤害。

⚠ 警告
表示如果不采取相应的小心措施，**可能**导致死亡或者严重的人身伤害。

⚠ 小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。 由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

按规定使用 Siemens 产品

请注意下列说明：

⚠ 警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

商标

所有带有标记符号 ® 的都是西门子股份有限公司的注册商标。本印刷品中的其他符号可能是一些其他商标。若第三方出于自身目的使用这些商标，将侵害其所有者的权利。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
德国

A5E37384256-AA
℗ 07/2016 本公司保留更改的权利

目录

TIA Portal Cloud Connector 简介

1

1.1 长版

Siemens 为其产品及解决方案提供了工业安全功能，以支持工厂、系统、机器和网络的安全运行。

为了防止工厂、系统、机器和网络受到网络攻击，需要实施并持续维护先进且全面的工业安全保护机制。Siemens 的产品和解决方案仅构成此类概念的其中一个要素。

客户负责防止其工厂、系统、机器和网络受到未经授权的访问。只有在必要时并采取适当安全措施（例如，使用防火墙和网络分段）的情况下，才能将系统、机器和组件连接到企业网络或 Internet。

此外，应考虑遵循 Siemens 有关相应安全措施的指南。更多有关工业安全的信息，请访问 http://www.siemens.com/industrialsecurity (http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx)。

Siemens 不断对产品和解决方案进行开发和完善以提高安全性。Siemens 强烈建议您及时更新产品并始终使用最新产品版本。如果使用的产品版本不再受支持，或者未能应用最新的更新程序，客户遭受网络攻击的风险会增加。

要及时了解有关产品更新的信息，请订阅 Siemens 工业安全 RSS 源，网址为 http://www.siemens.com/industrialsecurity (http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx)。

1.2 有关使用 TIA Portal Cloud Connector 的基本知识

TIA Portal Cloud Connector 的功能

TIA Portal 支持在虚拟系统中运行。TIA Portal Cloud Connector 选件适用于各种产品，可快速访问本地 PG/PC 接口以及 TIA Portal 工程组态系统中所连接的 SIMATIC 硬件设备，即使通过远程桌面连接方式在私有云中进行工程组态也同样支持。

使用插件“TIA Portal Cloud Connector”，可通过虚拟机访问 PG/PC 上本地连接的 SIMATIC 硬件设备。这要求，在虚拟机和硬件设备所连接的 PG/PC 上都安装有 TIA Portal Cloud Connector。此外，TIA Portal Cloud Connector 还支持通过远程桌面从所连接的虚拟机上远程访问其它 PG/PC 的硬件设备，即使这些硬件设备位于在私有网络中也同样可以。进行此类远程访问时，必须安装 TIA Portal Cloud Connector。

虚拟机与 TIA Portal Cloud Connector 紧密协作，具有以下优势：

- 支持先进的私有云系统架构：
  - 具有绝佳的可扩展性
  - 无需安装在每一个工作站上
  - 可在虚拟机中对 TIA Portal 进行统一维护和管理
  - 项目和库数据进行集中存储
- 支持跨网络在线访问 PLC 和 HMI 设备
- 通过 HTTPS 进行安全连接（Windows 8.1 和更高版本）
- 支持工作站的所有本地接口
- 可快速访问不同版本的 TIA Portal
- 显著提高可用许可证的应用效率
- 远程轻松实现设备维护

用户可基于预组态的虚拟机快速创建一个模板，并基于该模板，创建新的虚拟机，进而显著降低安装与组态工作量。

TIA Portal Cloud Connector 的获取

TIA Portal Cloud Connector 软件随 TIA Portal V14.0 及以上版本的 SIMATIC 软件包一同提供：

- STEP 7 Basic
- STEP 7 Professional
- WinCC Basic
- WinCC Professional
- WinCC Comfort/Advanced

要在 PG/PC 上使用 TIA Portal Cloud Connector，需购买单独的许可证。

说明

TIA Portal Cloud Connector

TIA Portal Cloud Connector 仅适用于在 TIA Portal 中完成工程组态任务。因而，不允许在产品操作过程中进行在线访问（如，SCADA）。对于安全程序，更是如此。

组态 TIA Portal Cloud Connector

在使用 TIA Portal Cloud Connector 建立连接之前，必须对 TIA Portal Cloud Connector 进行组态。具体的组态设置取决于设备的通信角色。TIA Portal Cloud Connector 可具备以下两种通信角色：

- 通信角色“用户设备”：
  用户设备是指连接硬件设备的 PG/PC。在此设备上，无需安装 TIA Portal。单独安装 TIA Portal Cloud Connector 时（即，不随 TIA Portal 一同安装），系统将自动预设该通信角色。
  另请参见“在 PG/PC 上组态 TIA Portal Cloud Connector (页 38)”
- 通信角色“远程设备”：
  远程设备是指安装有 TIA Portal 的虚拟机。TIA Portal Cloud Connector 与 TIA Portal 一同安装时，系统将自动预置该通信角色。
  另请参见“在虚拟机中组态 TIA Portal Cloud Connector (页 40)”

参见

TIA Portal Cloud Connector 的用户界面 (页 7)

TIA Portal Cloud Connector 的应用示例 (页 17)

使用虚拟机时的特别注意事项 (页 20)

使用证书 (页 21)

系统要求 (页 23)

使用虚拟机 (VM) (页 29)

使用虚拟机 (VM) (页 37)

1.3 TIA Portal Cloud Connector 的用户界面

TIA Portal Cloud Connector 的用户界面中包含以下元素：

- Windows 任务栏信息区中的条目
- TIA Portal Cloud Connector - 设置
- TIA Portal Cloud Connector - 状态显示
- TIA Portal Cloud Connector - 信息窗口
- TIA Portal - 状态栏中的显示信息

Windows 任务栏信息区中的 TIA Portal Cloud Connector

启动 TIA Portal Cloud Connector 之后，Windows 任务栏的信息区中将显示一个 Cloud Connector 图标。右键单击该图标，可打开 TIA Portal Cloud Connector 菜单。

下图显示了禁用通信端点时，Windows 任务栏信息区中的 TIA Portal Cloud Connector 图标：

该图标的颜色取决于通信端点的状态。

下图显示了组态的通信角色为“远程设备”时，信息区中的菜单：

通过该菜单，可执行以下操作：

- 启用通信：通过该命令，可启用远程设备和用户设备上的通信功能。
- 组态（远程设备/用户设备）：以指定的通信角色打开 TIA Portal Cloud Configurator。
- 状态显示：打开状态显示，指示所有操作的状态。
- 关于：打开 TIA Portal Cloud Connector 的“关于”(About) 窗口。在该窗口中，将显示诸如软件版本等信息。
- 帮助：打开 TIA Portal Cloud Connector 的在线帮助。
- 退出：关闭 TIA Portal Cloud Connector。

TIA Portal Cloud Connector - 设置

根据所选的通信角色，TIA Portal Cloud Connector 的用户界面可能有所不同。下图显示了通信角色为“远程设备”时，TIA Portal Cloud Connector 中的各种设置选项卡：


TIA Portal Cloud Connector - 远程设备
常规
协议
设置
通信协议
TCP 设置
用户设备地址：
pg.automation.dom
端口：
9022
HTTPS 设置
用户设备地址：
特征码：
导入
选择...
需要进行用户认证
组态的通信协议
Cloud Connector 将建立与以下地址的数据连接：
tcp://pg.automation.dom:9022
检查连接
确定
取消
应用
该设置已成功保存。

在这些选项卡中，可进行各种必需的所有设置。

下表简要列出了通信角色为“远程设备”时的各种设置与按钮：

选项卡	区域	设置/按钮	说明
常规	通信角色	用户设备	与 SIMATIC 硬件设备建立物理连接的 PG/PC。
		远程设备	安装有 TIA Portal 的私有云服务器中的虚拟机。可通过远程桌面连接，从用户设备中对其进行操作控制。
	Cloud Connector 通信	启用通信 禁用通信	启用或禁止与 PG/PC 端点的数据通信

选项卡	区域	设置/按钮	说明
协议	通信协议		定义通信端点间的传输机制可选择 TCP 或 HTTPS（Windows 8.1 和更高版本）。
	TCP 设置	用户设备地址	用户设备的 IP 地址或名称
		端口	进行数据传输的端口号
	HTTPS 设置	用户设备地址	用户设备的 IP 地址或名称
		特征码	用于确保证书的完整性。
		导入	将现有证书导入到 Windows 证书中心。基于导入的证书，可对数据进行加密并通过 HTTPS 发送。
		选择	选择先前导入的证书进行数据加密。
	组态的通信协议	检查连接	检查连接是否建立且无任何错误。
设置	自动启动	启用 Cloud Connector 的自动启动功能	在系统启动过程中，允许或者禁止 TIA Portal Cloud Connector 的自动启动功能。
	语言	选择语言	指定 TIA Portal Cloud Connector 的用户界面语言。
	用户认证	用户证书的名称。	显示当前使用的用户证书。
		特征码	证书的校验和，用于确保数据的完整性
		创建	创建新证书进行用户认证。
		选择	从 Windows 证书中心中选择一个现有的证书。
		导出	导出当前所使用的证书

下表简要列出了通信角色为“用户设备”时的各种设置和按钮：

选项卡	区域	设置/按钮	说明
常规	通信角色	用户设备	与 SIMATIC 硬件设备建立物理连接的 PG/PC。
		远程设备	安装有 TIA Portal 的私有云服务器中的虚拟机。可通过远程桌面连接，从用户设备中对其进行操作控制。
	Cloud Connector 通信	启用通信 禁用通信	启用或禁止与 PG/PC 端点的数据通信

选项卡	区域	设置/按钮	说明
协议	TCP 端点	端口	进行数据通信的端口号用户设备的端口号必须与远程设备的端口号相匹配。
	HTTPS 端点	用户设备地址	用户设备的 IP 地址或名称
		特征码	用于确保证书的完整性。
		创建	创建新证书进行数据加密。
		导出	导出当前所使用的证书
		选择	用户可选择一个现有证书。
设置	自动启动	启用 Cloud Connector 的自动启动功能	在系统启动过程中，允许或者禁止 TIA Portal Cloud Connector 的自动启动功能。
	语言	选择语言	指定 TIA Portal Cloud Connector 的用户界面语言。
	用户认证	可信任的用户证书	显示所有可用的用户证书和可信任的用户证书。
		导入	可将在远程设备上创建的用户证书导入到 Windows 证书中心。
		添加	可将 Windows 证书中心的证书添加到可信任的证书列表中。
		删除	从可信任的证书列表中删除选定的证书。但该证书仍保留在 Windows 的证书中心。

TIA Portal Cloud Connector - 状态显示

状态显示用于显示 TIA Portal Cloud Connector 应用过程中的相关信息、警告和错误消息。下图显示了通信角色为“远程设备”时的状态显示：

下图显示了通信角色为“用户设备”时的状态显示：


TIA Portal Cloud Connector - 用户设备
通信端
TCP:
00.00:00:00
HTTPS:
00.00:00:00
通知
类型
报警
时间戳
该设置已成功保存。
1:12:55 PM
该设置已成功保存。

TIA Portal Cloud Connector - 信息窗口

在信息窗口中，将显示有关所安装的 TIA Portal Cloud Connector 版本信息。

TIA Portal - 状态栏中的显示信息

在 TIA Portal 中，状态栏用于显示当前通过 TIA Portal Cloud Connector 在线连接的 SIMATIC 硬件设备。除了在线显示之外，对于 TIA Portal Cloud Connector 建立连接，状态栏中还将显示以下图标：

参见

有关使用 TIA Portal Cloud Connector 的基本知识 (页 5)

TIA Portal Cloud Connector 的应用示例 (页 17)

使用虚拟机时的特别注意事项 (页 20)

使用证书 (页 21)

系统要求 (页 23)

使用虚拟机 (VM) (页 29)

使用虚拟机 (VM) (页 37)

1.4 TIA Portal Cloud Connector 的应用示例

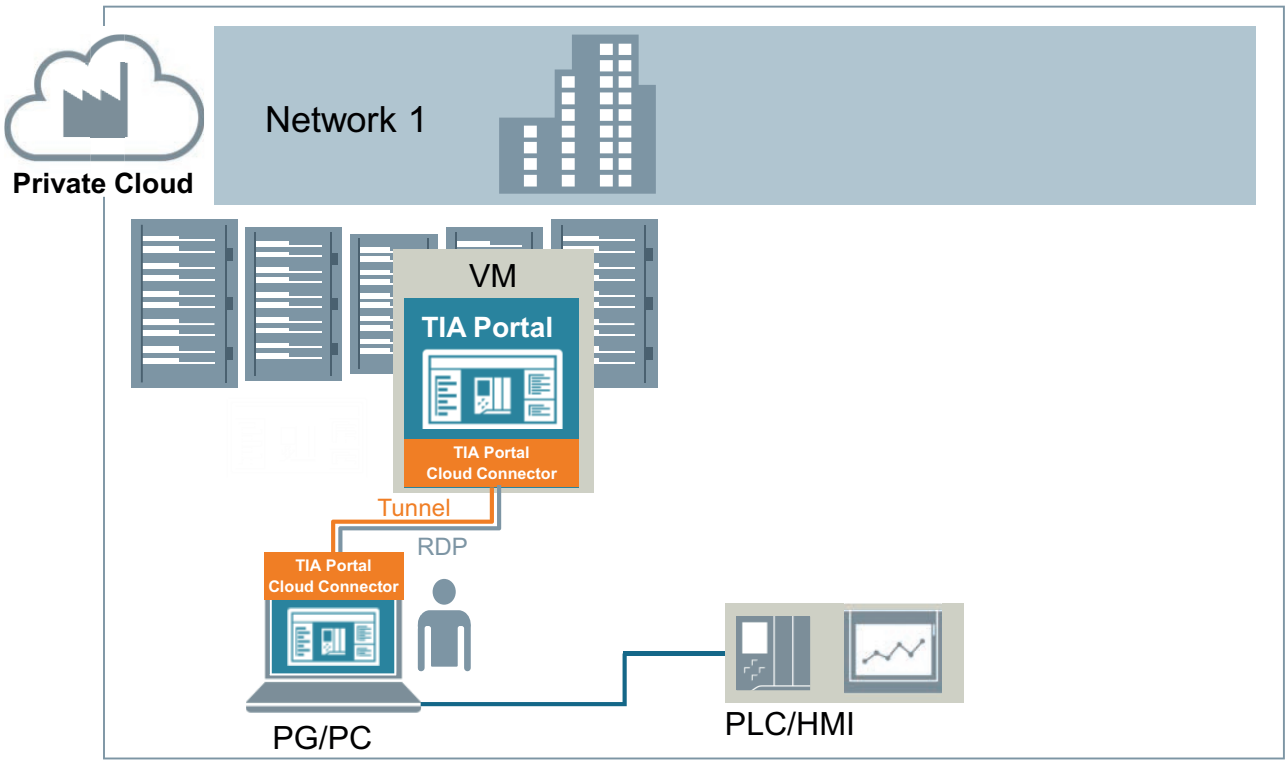
通过 TIA Portal Cloud Connector，可实现以下功能：

- 访问本地 PG/PC 上连接的硬件设备
- 访问其它 PG/PC 上所连接的硬件设备。该 PG/PC 可位于用户当前所在网络中，也不在该网络中。

访问本地 PG/PC 上所连接的硬件设备

TIA Portal 安装在公司的私有云中，但用户的 PG/PC 上并未安装 TIA Portal。该 PG/PC 上连接有自动化硬件设备 (PLC/HMI)。虚拟机和本地 PG/PC 上均安装有 TIA Portal Cloud Connector。该 PG/PC 上需要一个 TIA Portal Cloud Connector 许可证。用户可通过远程桌面连接登录该虚拟机并正常使用 TIA Portal。通过 TIA Portal Cloud Connector，用户可访问该 PG/PC 上本地连接的硬件设备。

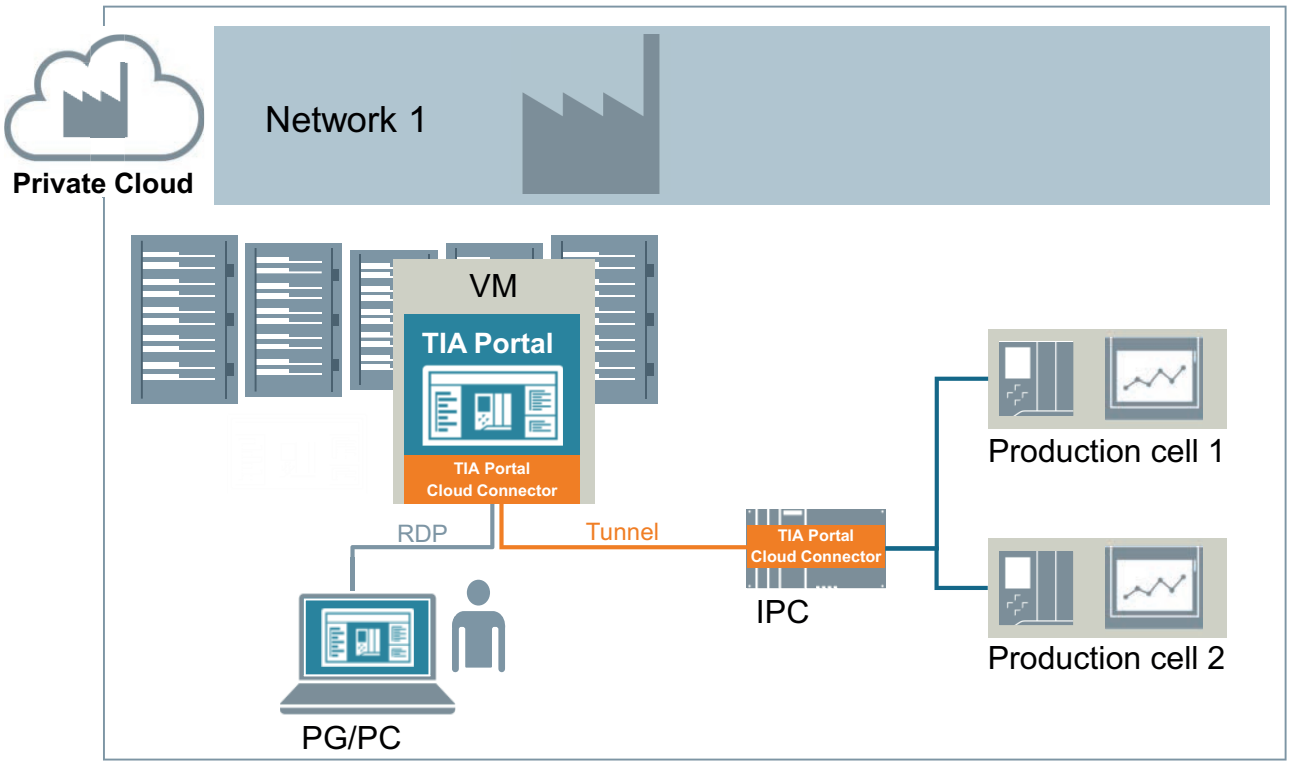
下图显示了本地 PG/PC 连接硬件设备时，虚拟环境中 TIA Portal Cloud Connector 的应用。

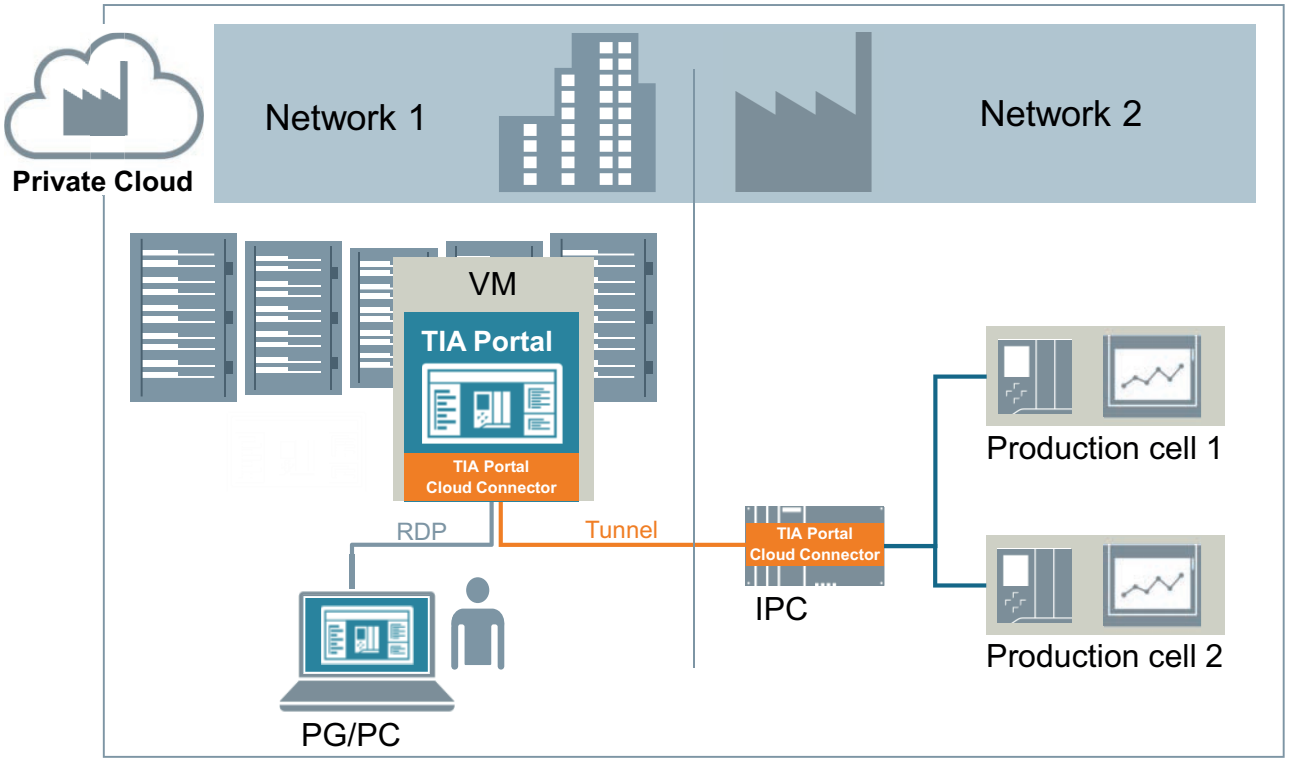


访问其它 PG/PC 上所连接的硬件设备

TIA Portal 安装在虚拟机中。但本地 PG/PC 上并未安装 TIA Portal。自动化硬件（如，IPC）连接某个 PG/PC 中。该设备可与 PG/PC 位于同一个网络中（如上图所示）；也可以位于不同的网络中（如下图所示）。TIA Portal Cloud Connector 安装在其它 PG/PC 和虚拟机中。首先，需通过远程桌面连接登录该虚拟机，之后即可正常使用 TIA Portal。通过 TIA Portal Cloud Connector，可在虚拟机与另一台 PG/PC 之间建立连接并访问连接的自动化硬件设备。

下图显示了硬件设备连接另一台 PG/PC 时，虚拟环境中 TIA Portal Cloud Connector 的应用。


Private Cloud
Network 1
VM
TIA Portal
TIA Portal
Cloud Connector
RDP
Tunnel
TIA Portal
Cloud Connector
IPC
Production cell 1
Production cell 2
PG/PC


Private Cloud
Network 1
Network 2
VM
TIA Portal
TIA Portal
Cloud Connector
RDP
Tunnel
TIA Portal
Cloud Connector
IPC
Production cell 1
Production cell 2
PG/PC

参见

有关使用 TIA Portal Cloud Connector 的基本知识 (页 5)

TIA Portal Cloud Connector 的用户界面 (页 7)

使用虚拟机时的特别注意事项 (页 20)

使用证书 (页 21)

系统要求 (页 23)

使用虚拟机 (VM) (页 29)

使用虚拟机 (VM) (页 37)

1.5 使用虚拟机时的特别注意事项

仿真

要仿真一个 PLC 程序，则需先禁用 TIA Portal Cloud Connector。而仿真 HMI 设备时无需如此。

运行更新包和支持包

更新包和支持包可先安装在 VM 模板中，也可以在以后安装在各个虚拟机中。为此，需要使用 TIA Portal 的更新机制。

更多信息，请参见 TIA Portal 的信息系统。

参见

有关使用 TIA Portal Cloud Connector 的基本知识 (页 5)

TIA Portal Cloud Connector 的用户界面 (页 7)

TIA Portal Cloud Connector 的应用示例 (页 17)

使用证书 (页 21)

系统要求 (页 23)

使用虚拟机 (VM) (页 29)

使用虚拟机 (VM) (页 37)

1.6 使用证书

在 TIA Portal Cloud Connector 中使用证书

在 Windows 8.1 及更高版本中，可使用 HTTPS 连接进行数据通信。TIA Portal Cloud Connector 通过证书确保 HTTPS 连接的信息安全。在建立用户设备与远程设备间的数据连接时，需要以下证书：

- 数据加密证书
- 用户认证证书

如果证书不可用或用户设备的证书与远程设备的不匹配，则无法建立连接。

数据加密证书

首先，在用户设备上生成数据加密证书。之后，需要将该证书复制到远程设备的本地硬盘上，然后导入 TIA Portal Cloud Connector 之中。如果证书匹配，则在交换用户认证证书后立即建立设备间的连接。

用户认证证书

首先，在远程设备上生成数据加密证书。之后，需要将该证书复制到用户设备中并导入 TIA Portal Cloud Connector 之中。如果证书匹配，则在交换数据加密证书时建立设备间的连接。

参见

有关使用 TIA Portal Cloud Connector 的基本知识 (页 5)

TIA Portal Cloud Connector 的用户界面 (页 7)

TIA Portal Cloud Connector 的应用示例 (页 17)

使用虚拟机时的特别注意事项 (页 20)

创建数据加密证书 (页 41)

导出数据加密证书 (页 42)

导入数据加密证书 (页 43)

选择数据加密证书 (页 44)

创建用户认证证书 (页 45)

导出用户认证证书 (页 47)

系统要求

2

2.1 PG/PC 的系统要求

支持的操作系统

要使用 TIA Portal Cloud Connector，用户 PG/PC 上需安装以下某个操作系统：

- Windows 7（64 位）
- Windows 8.1（64 位）
- Windows 10（64 位）

说明

请注意以下事项：

- TIA Portal Cloud Connector 不支持 32 位操作系统。
- 请确保操作系统的状态始终最新。为此，应及时执行所有的 Windows 重要更新。
- 如果安装有 SIMATIC NET，则 TIA Portal Cloud Connector 将无法启动。

TIA Portal Cloud Connector 的许可证

要使用 TIA Portal Cloud Connector，TIA Portal Cloud Connector 中指定为“用户设备”的每台设备上都需要具有有效的 License Key。而对于那些作为“远程设备”的设备而言，无需安装 License Key。

License Key 可包含在安装中，也可在安装后通过 Automation License Manager 进行传送。

参见

VM 的系统要求 (页 24)

许可证 (页 26)

2.2 VM 的系统要求

支持的访客 (guest) 操作系统和虚拟机系统

TIA Portal 可与虚拟机 (VM) 一同使用。为此，请选择使用以下指定版本或更新版本的虚拟机系统：

- VMware vSphere Hypervisor (ESXi) V6.0
- Microsoft Windows Server 2012 R2 Hyper-V
- Microsoft Windows Azure Pack V1.0

在虚拟机中，可安装一个或多个以下软件包：

- SIMATIC STEP 7 Basic
- SIMATIC STEP 7 Professional
- SIMATIC WinCC Basic
- SIMATIC WinCC Comfort/Advanced
- SIMATIC WinCC Professional

除了这些软件包之外，还可以额外安装 STEP 7 选件包和 WinCC 选件包。

说明

在安装有 SIMATIC NET 系统时，运行 TIA Portal Cloud Connector

如果虚拟机中安装有 SIMATIC NET，则 TIA Portal Cloud Connector 将无法启动。

虚拟机可支持各种不同的访客操作系统，具体取决于选定的软件包：

访客操作系统	SIMATIC STEP 7 Basic	SIMATIC STEP 7 Professional	SIMATIC WinCC Basic	SIMATIC WinCC Professional	SIMATIC WinCC Advanced
Windows Server 2008 R2 StdE SP1（完全安装）（64 位）	-	√	-	√	√
Windows Server 2012 R2 StdE（完全安装）（64 位）	√	√	√	√	√

访客操作系统	SIMATIC STEP 7 Basic	SIMATIC STEP 7 Professional	SIMATIC WinCC Basic	SIMATIC WinCC Professional	SIMATIC WinCC Advanced
Windows 7 Home Premium SP1（64 位）	√	-	√	-	-
Windows 7 Professional SP1（64 位）	√	√	√	√	√
Windows 7 Enterprise SP1（64 位）	√	√	√	√	√
Windows 7 Ultimate SP1（64 位）	√	√	√	√	√
Windows 8.1（64 位）	√	-	√	-	-
Windows 8.1 Professional（64 位）	√	√	√	√	√
Windows 8.1 Enterprise（64 位）	√	√	√	√	√
-：不支持该操作系统 X：支持该操作系统					

说明

请注意以下事项：

- 不支持 32 位操作系统。
- 对于各种 TIA 产品而言，访客操作系统的硬件要求都相同。
- 不支持 SIMATIC USB 编程器。
- 如果要在虚拟机中使用 SD 卡，则需先将 SD 卡作为可移动式介质连接到虚拟机中。具体操作步骤，请参见虚拟机系统的帮助信息。
- 请确保操作系统的状态始终最新。为此，应及时执行所有的 Windows 重要更新。

TIA Portal Cloud Connector 的安装

可通过以下两种方式安装 TIA Portal Cloud Connector：

- 在安装上述 SIMATIC 软件包时，将 TIA Portal Cloud Connector 作为选件激活。之后，即可与该软件包一同安装。
- 也可以不随 SIMATIC 软件包安装，而独立安装 TIA Portal Cloud Connector。相应的安装文件位于安装介质中的“Support”文件夹中。也可以将该安装文件放置在网络中。这样，即可在虚拟机中以管理员身份创建相应脚本，对 TIA Portal Cloud Connector 进行自动更新。但请注意，每个 PG/PC 上都需要具有一个有效的 TIA Portal Cloud Connector 许可证。

TIA Portal Cloud Connector 的许可证

在虚拟机中运行 TIA Portal Cloud Connector 时，如果将通信角色组态为“远程设备”，则无需具有 TIA Portal Cloud Connector 许可证。

参见

PG/PC 的系统要求 (页 23)

许可证 (页 26)

2.3 许可证

SIMATIC 软件包的许可授权

如果要在虚拟系统中安装 TIA Portal (STEP 7、WinCC) 各种 SIMATIC 软件包，则每个安装都需要具有一个单独的许可证。对 VM 模板的复制或克隆将同样视为一次单独安装。而对访问虚拟机的 PG/PC 而言，如果未在本地安装 TIA Portal，则无需具有许可证。

使用浮动许可密钥时，将由许可密钥服务器提供许可证。

TIA Portal Cloud Connector 的许可授权

要使用 TIA Portal Cloud Connector，TIA Portal Cloud Connector 中指定为“用户设备”的每台设备上都需要具有有效的 License Key。而对于那些作为“远程设备”的设备而言，无需安装 License Key。

License Key 可包含在安装中，也可在安装后通过 Automation License Manager 进行传送。

参见

PG/PC 的系统要求 (页 23)

VM 的系统要求 (页 24)

使用虚拟机 (VM) 3

3.1 创建 VM 新模板

可使用以下虚拟机系统：

- VMware vSphere Hypervisor (ESXi) V6.0
- Microsoft Windows Server 2012 R2 Hyper-V
- Microsoft Windows Azure Pack V1.0

根据所用的虚拟机系统，基于当前的虚拟机 (VM) 创建模板时，具体的操作步骤可能有所不同。更多信息，请参见所用虚拟机系统的帮助信息。

在 VM 中搭建 SIMATIC 开发环境的方式与 PG/PC 中的相同。

创建新虚拟机模板的基本步骤

要创建新的虚拟机模板，按以下步骤操作：

1. 创建一个虚拟机。
2. 安装所需的 SIMATIC 软件，如指定版本的 SIMATIC STEP 7（TIA Portal V14 及更高版本）或 SIMATIC WinCC（TIA Portal V14 及更高版本）（Basic、Professional、Comfort/Advanced）。

   说明

   在虚拟机 (VM) 中安装 TIA Portal 的操作步骤与 PG/PC 中的相同。有关安装的详细信息，请参见 TIA Portal 的安装指南。

3. 必要时，可安装相应的选件包，如 SIMATIC STEP 7 Safety Advanced。
4. 如果需要，还可额外安装适用于所有用户的兼容软件包。
5. 根据需要，组态虚拟机。
6. 遵循相应的虚拟机系统操作步骤，基于该虚拟机创建一个模板。

结果

创建了一个 VM 模板，并且可以进行复制和分发。请注意，在使用该模板的副本时，必须具有相应的许可证。此时，可通过一个单独的许可证服务器 (VM) 对这些许可证进行管理。

参见

统一保存用户设置和项目设置 (页 30)

使用许可密钥服务器 (页 32)

在虚拟机中安装 TIA Portal Cloud Connector (页 33)

3.2 统一保存用户设置和项目设置

如果虚拟机用户将设置和项目保存在虚拟机中，则在删除虚拟机后这些信息将丢失。如果要在其它虚拟机中访问设置信息和项目信息，则需将这些信息保存在虚拟机之外的其它位置处。在虚拟机中，可设置各种环境变量指定用户特定设置和项目的存储位置。在首次启动 TIA Portal 之前，需完成相应环境变量的设置。如果首次启动 TIA Portal 时这些环境变量不存在，则 TIA Portal 将设置文件存储在默认的目录并在此之后始终使用该文件。如果文件存在，则 TIA Portal 将忽略在以之后设置的所有环境变量。

通过环境变量，可指定以下路径：

- 用户特定设置：该设置将保存在指定目录中。
- 项目：创建新项目时，该位置将作为默认位置，但项目的存储目录可随时更改。

用户可手动设置环境变量，也可通过脚本进行设置。可通过不同的脚本分别设置环境变量（设置和项目），也可通过一个脚本对这两种环境变量进行统一设置。

所有用户的设置文件名称相同。此外，每位用户都需要指定一个单独的文件目录，确保所有用户仅访问自己的设置信息。否则，用户设置可能会不断的被其他用户所覆盖。已登录用户可通过一个变量对该路径进行相应调整。

统一存储设置信息的目录结构示例

设置信息将存储在一个网络共享的“用户设置”(User Settings) 目录中。“用户设置” (UserSettings) 的结构如下所示：

```
UserSettings
            User1
            User2
            User3
```

其中，“User1”、“User2”和“User3”为 VM 用户的用户名。此时，该路径环境变量为“\\MyServer\UserSettings\%USERNAME%”。

在本示例中，“MyServer”为网络中可用的计算机。“%USERNAME%”为用户名变量。用户登录后，系统将对该变量进行解析并对环境变量进行相应更改。在多用户系统中，建议将脚本保存在 Autostart 文件夹中。每次登录时，都会对该环境变量进行复位，并根据登录的用户对设置的存储位置进行相应变更。

要求

- 所有用户对作为新存储位置的服务器区域具有写访问权限。
- 相应的用户自定目录已创建。

通过脚本设置环境变量

要通过脚本设置环境变量，请按以下步骤操作：

1. 创建并打开一个新脚本进行编辑。或者，也修改现有脚本。
2. 在脚本中添加以下命令行：
   `setx TiaUserSettingsPath \\<Server>\<Settings>\%USERNAME%`
   `setx TiaDefaultProjectPath \\<Server>\<Projects>\%USERNAME%`
   将“`<Server>\<Settings>`”和“`<Server>\<Projects>`”替换为网络中设置和项目的存储目录。
3. 保存该脚本。
4. 将该脚本复制到 Windows 的 Autostart 文件夹中，以便其他用户访问。
   下一次登录 PG/PC 时，系统将对“%USERNAME%”变量进行解析。并根据该变量置调整所登录用户设置的存储位置。

如果要使用两个脚本而非一个脚本，则需对每个脚本分别执行步骤 1 到 4，并在每个脚本中添加其中一个“`setx`”命令。

手动设置环境变量

要手动设置环境变量，请按以下步骤操作：

1. 启动将作为模板分发的虚拟机。
2. 在 Windows 系统中，打开对话框设置环境变量。
3. 新建一个名为“TiaUserSettingsPath”的系统变量。
4. 输入网络中用户设置存储目录的访问路径，并作为该变量的值。此时，需确保将该用户名指定为一个“%USERNAME%”变量。
5. 单击“确定”(OK) 进行确认。
6. 创建另一个名为“TiaDefaultProjectPath”的系统变量。

7. 输入网络中用作项目默认存储位置的目录路径，并作为该变量的值。在此，可将用户名指定为一个“%USERNAME%”变量，将该项目保存在子目录中。如果忽略“%USERNAME%”，则所有项目都将保存在同一个目录中。
8. 单击“确定”(OK) 进行确认。
   下一次登录 PG/PC 时，系统将对“%USERNAME%”变量进行解析。并根据该变量置调整所登录用户设置的存储位置。

参见

创建 VM 新模板 (页 29)

使用许可密钥服务器 (页 32)

在虚拟机中安装 TIA Portal Cloud Connector (页 33)

3.3 使用许可密钥服务器

简介

在安装 TIA Portal 或 TIA Portal Cloud Connector 的过程中，将同时安装 Automation License Manager (ALM)。该软件可用于对许可证进行传送和处理。

有关 Automation License Manager 和许可证服务设置的更多信息，请参见 Automation License Manager 的用户文档。

参见

创建 VM 新模板 (页 29)

统一保存用户设置和项目设置 (页 30)

在虚拟机中安装 TIA Portal Cloud Connector (页 33)

3.4 在虚拟机中安装 TIA Portal Cloud Connector

在虚拟中中，可通过以下两种方式安装 TIA Portal Cloud Connector：

- TIA Portal Cloud Connector 随 TIA Portal 一同安装
  TIA Portal Cloud Connector 可与 TIA Portal 一同安装。在安装过程中，只需激活“TIA Portal Cloud Connector”选项即可。
- 独立于 TIA Portal，单独安装 TIA Portal Cloud Connector
  运行安装介质上的安装程序，可独立于 TIA Portal 单独安装 TIA Portal Cloud Connector。为此，需要确保其他用户可通过网络驱动器访问该安装文件。

TIA Portal Cloud Connector 随 TIA Portal 一同安装

要将 TIA Portal Cloud Connector 与 TIA Portal 一同安装，请按以下步骤操作：

1. 在相应的驱动器中插入安装介质。
   安装程序将自动启动，除非 PG/PC 上禁用了自动启动功能。
2. 如果安装程序未自动启动，则双击“Start.exe”文件手动运行。
   将打开一个对话框选择安装语言。
3. 选择将在安装程序对话框中显示的语言。
4. 有关产品和安装信息，可单击“阅读说明”(Read Notes) 或“安装说明”(Installation Notes) 按钮。
   包含相关说明的帮助文件随即打开。
5. 阅读说明信息后，关闭该帮助文件并单击“下一步”(Next) 按钮。
   将打开一个对话框选择产品语言。
6. 选择产品用户界面的显示语言，然后单击“下一步”(Next) 。

   说明

   系统通常将“英语”(English) 安装为基本的产品语言。

   将打开一个对话框选择具体的产品组态。
7. 单击“用户自定义”(User-defined)。
8. 选择“TIA Portal Cloud Connector”复选框。必要时，还可选择要安装的其它产品复选框。
9. 如果要在桌面上创建 TIA Porta 快捷方式，可选择“创建桌面快捷方式”(Create desktop shortcut) 复选框。
10. 如果要更改安装的目标目录，则可单击“浏览”(Browse) 按钮。请注意，安装路径的长度不能超过 89 个字符。
11. 单击“下一步”(Next) 按钮。
    许可条款对话框随即打开。
12. 要继续安装，请阅读并接受所有的许可协议，并单击“下一步”(Next)。
    如果在安装 TIA Portal 时需要更改安全和权限设置，则将打开安全设置对话框。
13. 要继续安装，则需接受对安全和权限设置的更改，并单击“下一步” (Next)。
    在下一个对话框中，将显示安装设置的概览信息。

14. 检查选择的安装设置。如果要进行更改，可单击“上一步”(Back)，直至到达需更改的对话框处。完成更改后，可单击“下一步”(Next) 返回概述窗口。
15. 单击“安装”(Install)。
    安装随即启动。

说明

如果在安装过程中未找到相应的许可密钥，则可在此将其传送到 PC 中。如果跳过许可密钥的传送步骤，也可以在稍后通过 Automation License Manager 进行传送。

完成安装后，系统将显示一则消息，指示安装是否成功。

16. 此时，可能需要重新启动计算机。此时，可选择“是，立即重新启动计算机”(Yes, restart my computer now.) 单选按钮，然后单击“重启”(Restart)。
17. 如果计算机未重启，则可单击“退出”(Exit)。

独立于 TIA Portal，单独安装 Cloud Connector

要独立于 TIA Portal 独立安装 TIA Portal Cloud Connector，请按以下步骤操作：

1. 在指定驱动器中插入安装介质，或浏览到计算机操作系统中该安装文件的位置所在处。
   该安装文件位于安装介质的“支持”(Support) 目录中。
2. 双击安装文件“TIA Portal Cloud Connector_<版本>.exe”。
   此时，将显示 Windows 的用户帐户控制窗口。
3. 单击“是”(Yes)，确认用户帐户控制信息。
   安装对话框随即打开。
4. 单击“下一步”(Next)。
   将显示一个可用的安装语言选择列表。
5. 选择所需的安装语言，并单击“下一步”(Next)。
   解压缩该文件，下一个安装对话框随即打开。
6. 关闭所有当前正在运行的程序，并单击“下一步”(Next)。
   许可证条款对话框随即打开。
7. 接受许可证条款，并单击“下一步”(Next)。
   此时，将显示可安装的程序和相应的存储要求。
8. 单击“下一步”(Next)。
   在打开的对话框中，将显示安装过程中可能会更改的系统设置概览信息。
9. 选择该复选框，应用更改。
10. 单击“下一步”(Next)。
    系统将显示待安装程序的概览信息。
11. 单击“安装”(Install)。
    安装随即启动。
12. 此时，可能需要重新启动计算机。此时，可选择“是，立即重新启动计算机”(Yes, restart my computer now.) 单选按钮，单击“完成”(Finish)。

参见

创建 VM 新模板 (页 29)
统一保存用户设置和项目设置 (页 30)
使用许可密钥服务器 (页 32)

使用虚拟机 (VM)

4

4.1 在 PG/PC 上安装 TIA Portal Cloud Connector

说明

请注意以下事项：

- 为此，需要具有有效的 TIA Portal Cloud Connector 许可证。
- 在 Windows 防火墙中进行设置：允许接入连接的先决条件为：在防火墙的“例外”(Exceptions) 选项卡中，为“西门子 SCP 远程连接”(Siemens SCP Remote Connection) 服务设置 TIA Portal Cloud Connector 中所用的端口。默认值为“Any”。

操作步骤

要安装 TIA Portal Cloud Connector，请按以下步骤操作：

1. 在指定驱动器中插入安装介质，或浏览到计算机操作系统中该安装文件的位置所在处。
   该安装文件位于安装介质的“支持”(Support) 目录中。
2. 双击安装文件“TIA Portal Cloud Connector_<版本>.exe”。
   此时，将显示 Windows 的用户帐户控制窗口。
3. 单击“是”(Yes)，确认用户帐户控制信息。
   安装对话框随即打开。
4. 单击“下一步”(Next)。
   将显示一个可用的安装语言选择列表。
5. 选择所需的安装语言，并单击“下一步”(Next)。
   解压缩该文件，下一个安装对话框随即打开。
6. 关闭所有当前正在运行的程序，并单击“下一步”(Next)。
   许可证条款对话框随即打开。
7. 接受许可证条款，并单击“下一步”(Next)。
   此时，将显示可安装的程序和相应的存储要求。
8. 单击“下一步”(Next)。
   在打开的对话框中，将显示安装过程中可能会更改的系统设置概览信息。
9. 选择该复选框，应用更改。
10. 单击“下一步”(Next)。
    系统将显示待安装程序的概览信息。
11. 单击“安装”(Install)。
    安装随即启动。
12. 此时，可能需要重新启动计算机。此时，可选择“是，立即重新启动计算机”(Yes, restart my computer now.) 单选按钮，单击“完成”(Finish)。

参见

在 PG/PC 上组态 TIA Portal Cloud Connector (页 38)

在虚拟机中组态 TIA Portal Cloud Connector (页 40)

通过 TIA Portal Cloud Connector 进行在线连接 (页 52)

离线使用虚拟机 (VM) (页 53)

4.2 在 PG/PC 上组态 TIA Portal Cloud Connector

说明

通信协议

要连接 PG/PC 和虚拟机，必须指定一个通信协议。出于安全考虑，Windows 8.1 及以上版本通常使用 HTTPS 协议。

组态 TCP 连接

要组态 PG/PC 的 TCP 连接，请按以下步骤操作：

1. 右键单击任务栏信息区中 TIA Portal Cloud Connector 图标，并选择“组态”(Configuration) 命令。
   TIA Portal Cloud Connector 随即打开。
2. 打开“设置”(Settings) 选项卡并根据需要，更改 TIA Portal Cloud Connector 的用户界面语言。
3. 转至“常规”(General) 选项卡，并检查通信角色。如果需要，可将设置更改为“用户设备” (User device)。
4. 切换到“协议”(Protocol) 选项卡。
5. 选择“TCP 端点”(TCP endpoint) 复选框。
6. 输入数据通信的端口。该端口必须与远程设备上指定的端口相同。
7. 再次打开“常规”(General) 选项卡。
8. 在“Cloud Connector 通信”(Cloud Connector Communication) 区域中，单击“启用通信” (Enable communication)。

组态 HTTPS 连接

要组态 PG/PC 的 HTTPS 连接，请按以下步骤操作：

1. 右键单击任务栏信息区中 TIA Portal Cloud Connector 图标，并选择“组态”(Configuration) 命令。
   TIA Portal Cloud Connector 随即打开。
2. 打开“设置”(Settings) 选项卡并根据需要，更改 TIA Portal Cloud Connector 的用户界面语言。
3. 转至“常规”(General) 选项卡，并检查通信角色。如果需要，可将设置更改为“用户设备” (User device)。
4. 切换到“协议”(Protocol) 选项卡。
5. 选择“HTTPS 端点”(HTTPS endpoint) 复选框。
6. 对于数据加密，可创建一个新的证书，也可从 Windows 证书中心选择一个现有证书。
   另请参见
   “创建数据加密证书 (页 41)”
   “选择数据加密证书 (页 44)”
7. 如果在用户设备不包含用户认证证书，则可在远程设备上创建一个并复制到用户设备的本地硬盘中。
   另请参见
   “创建用户认证证书 (页 45)”
8. 切换至“设置”(Settings) 选项卡。
9. 导入用户认证的新证书，或将 Windows 证书中心的现有证书添加到可信任证书列表中。
   另请参见
   “导入用户认证证书 (页 48)”
   “添加用户认证证书 (页 49)”
10. 再次打开“常规”(General) 选项卡。
11. 在“Cloud Connector 通信”(Cloud Connector Communication) 区域中，单击“启用通信” (Enable communication)。

结果

PG/PC 现已就绪，可与虚拟机进行数据通信。之后，即可在虚拟机中组态 TIA Portal Cloud Connector。

参见

在 PG/PC 上安装 TIA Portal Cloud Connector (页 37)

在虚拟机中组态 TIA Portal Cloud Connector (页 40)

通过 TIA Portal Cloud Connector 进行在线连接 (页 52)

离线使用虚拟机 (VM) (页 53)

4.3 在虚拟机中组态 TIA Portal Cloud Connector

说明

通信协议

要连接 PG/PC 和虚拟机，需指定要使用的通信协议。出于安全考虑，Windows 8.1 及以上版本通常使用 HTTPS 协议。接受连接之前，还需检查连接请求伙伴的身份。

组态 TCP 连接

要组态虚拟机的 TCP 连接，请按以下步骤操作：

1. 建立与虚拟机的远程桌面连接。
2. 右键单击任务栏信息区中 TIA Portal Cloud Connector 图标，并选择“组态”(Configuration) 命令。
   TIA Portal Cloud Connector 随即打开。
3. 打开“设置”(Settings) 选项卡并根据需要，更改 TIA Portal Cloud Connector 的用户界面语言。
4. 转至“常规”(General) 选项卡，并检查通信角色。如果需要，可将设置更改为“远程设备” (Remote device)。
5. 打开“协议”(Protocol) 选项卡。
6. 在“通信协议”(Communication protocol) 区域中，选择“TCP 设置”(TCP Settings) 复选框。
7. 输入用户设备的 IP 地址或选择“自动组态”(Automatic configuration) 条目，自动检测该地址。
8. 输入数据通信的端口。该端口必须与用户设备上指定的端口相同。
9. 再次打开“常规”(General) 选项卡。
10. 在“Cloud Connector 通信”(Cloud Connector Communication) 区域中，单击“启用通信” (Enable communication)。

组态 HTTPS 连接

要组态虚拟机的 HTTPS 连接，请按以下步骤操作：

1. 建立与虚拟机的远程桌面连接。
2. 右键单击任务栏信息区中 TIA Portal Cloud Connector 图标，并选择“组态”(Configuration) 命令。
   TIA Portal Cloud Connector 随即打开。
3. 打开“设置”(Settings) 选项卡并根据需要，更改 TIA Portal Cloud Connector 的用户界面语言。
4. 打开“常规”(General) 选项卡，检查通信角色。如果需要，可将设置更改为“远程设备” (Remote device)。
5. 打开“协议”(Protocol) 选项卡。

6. 在“通信协议”(Communication protocol) 区域中，选择“HTTPS 设置”(HTTPS settings) 复选框。
7. 输入用户设备的 IP 地址或选择“自动组态”(Automatic configuration) 条目，自动检测该地址。
8. 对于数据加密，可导入在用户设备上创建证书，也可从 Windows 证书中心选择一个现有证书。
   另请参见
   “导入数据加密证书 (页 43)”
   “选择数据加密证书 (页 44)”
9. 切换至“设置”(Settings) 选项卡。
10. 对于用户认证，可创建一个新的证书，也可从 Windows 证书中心选择一个现有证书。
    另请参见
    “创建用户认证证书 (页 45)”
    “选择用户认证证书 (页 50)”
11. 再次打开“常规”(General) 选项卡。
12. 在“Cloud Connector 通信”(Cloud Connector Communication) 区域中，单击“启用通信”(Enable communication)。

结果

TIA Portal Cloud Connector 现已就绪，可进行数据通信。激活双方通信伙伴之后，即可从用户设备中访问本地连接的 SIMATIC 硬件设备 (PLC/HMI)。

参见

在 PG/PC 上安装 TIA Portal Cloud Connector (页 37)

在 PG/PC 上组态 TIA Portal Cloud Connector (页 38)

通过 TIA Portal Cloud Connector 进行在线连接 (页 52)

离线使用虚拟机 (VM) (页 53)

4.4 使用证书（仅适用 HTTPS 连接）

4.4.1 创建数据加密证书

在 Windows 8.1 及更高版本中，可使用 HTTPS 连接进行数据通信。为了提高信息安全性，需要通过证书进行数据加密；该证书在用户设备上创建并在远程设备中使用。

操作步骤

要创建数据加密证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在用户设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（用户设备）”(Configuration (user device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 端点”(HTTPS endpoint) 复选框。
   “创建”(Create) 和“选择”(Select) 按钮将激活。
5. 单击“创建”(Create)。
   “另存为”(Save as) 对话框随即打开。
6. 选择存储位置并输入证书名称。
7. 单击“保存”(Save)。

结果

在用户设备上，创建了证书并可用于 HTTPS 端点。此外，该证书还将以“.cer”扩展名的文件保存在指定存储位置处，并且可复制到远程设备中。该证书也将添加到 Windows 的证书中心。

参见

使用证书 (页 21)

导出数据加密证书 (页 42)

导入数据加密证书 (页 43)

选择数据加密证书 (页 44)

4.4.2 导出数据加密证书

用户可随时导出当前使用的数据加密证书。

要求

数据加密证书已创建并显示在用户设备的 HTTPS 端点下方。

操作步骤

要导出数据加密证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在用户设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（用户设备）”(Configuration (user device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 端点”(HTTPS endpoint) 复选框。
   “创建”(Create)、“选择”(Select) 和“导出”(Export) 按钮将激活。
5. 单击“导出”(Export)。
   “另存为”(Save as) 对话框随即打开。
6. 选择存储位置并输入证书名称。
7. 单击“保存”(Save)。

结果

当前使用的数据加密证书将以“.cer”扩展名的文件保存在指定存储位置处。

参见

使用证书 (页 21)

创建数据加密证书 (页 41)

导入数据加密证书 (页 43)

选择数据加密证书 (页 44)

4.4.3 导入数据加密证书

要建立用户设备与远程设备间的 HTTPS 连接，必须将用户设备上创建的数据加密证书导入到远程设备的 TIA Portal Cloud Connector 中。

要求

- 用户设备上创建有数据加密证书。
- 数据加密证书已复制到远程设备的本地硬盘中。

操作步骤

要将数据加密证书导入到远程设备的 TIA Portal Cloud Connector 中，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在远程设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（远程设备）”(Configuration (remote device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 设置”(HTTPS settings) 复选框。
   “导入”(Import) 和“选择”(Select) 按钮将激活。
5. 单击“导入”(Import)。
   “打开”(Open) 对话框随即打开。
6. 在文件系统中选择该证书文件。证书文件的文件扩展名为“.cer”。
7. 单击“打开”(Open)。

结果

证书导入并立即应用于数据通信中。该证书也将添加到 Windows 的证书中心。

参见

使用证书 (页 21)

创建数据加密证书 (页 41)

导出数据加密证书 (页 42)

选择数据加密证书 (页 44)

4.4.4 选择数据加密证书

用户可从 Windows 证书中心选择现有的数据加密证书。可在用户设备进行选择，也可从远程设备进行选择。

要求

事先已创建（用户设备）或导入（远程设备）了数据加密证书，并保存在 Windows 证书中心内。

操作步骤

要在 Windows 证书中心选择并使用现有的数据加密证书，请按以下操作步骤：

1. 要打开 TIA Portal Cloud Connector，可在 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择命令“组态（用户设备）”(Configuration (user device)) 或“组态（远程设备）(Configuration (remote device))。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 端点”(HTTPS endpoint) 复选框（用户设备），或“HTTPS 设置”(HTTPS settings) 复选框（远程设备）。
   “选择”(Select) 按钮随即激活。
5. 单击“选择”(Select)。
   “Windows 信息安全”(Windows Security) 对话框随即打开，并显示可用的证书。
6. 选择一个证书。必要时，还可显示该证书的其它附加属性。
7. 单击“确定”(OK)。

结果

选择相应的数据通信证书。为了确保通信，用户设备上设置的证书应与远程设备上的相同。

参见

使用证书 (页 21)

创建数据加密证书 (页 41)

导出数据加密证书 (页 42)

导入数据加密证书 (页 43)

4.4.5 创建用户认证证书

在 Windows 8.1 及更高版本中，可使用 HTTPS 连接进行数据通信。为了提高信息安全性，需要通过证书进行用户认证；该证书在远程设备上创建并在用户设备中使用。

操作步骤

要创建用户认证证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在远程设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（远程设备）”(Configuration (remote device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 设置”(HTTPS settings) 复选框。
   在“设置”(Settings) 选项卡中，用户认证区域激活。
5. 切换至“设置”(Settings) 选项卡。
6. 在“用户认证” (User authentication) 区域，单击“创建”(Create)。
   “TIA Portal Cloud Connector - 用户认证”(TIA Portal Cloud Connector - User authentication) 对话框随即打开。
7. 在“证书名称”(Certificate name) 字段中，输入新证书的名称。
8. 单击“浏览”(Browse)。
   “另存为”(Save as) 对话框随即打开。
9. 选择存储位置并输入证书名称。
10. 单击“保存”(Save)。
11. 选择证书的生效日期。
12. 选择证书的失效日期。
13. 单击“确定”(OK)。

结果

证书已创建并且可在远程设备上使用。此外，该证书还将以“.cer”扩展名的文件保存在指定存储位置处，并且可复制到用户设备中。该证书也将添加到 Windows 的证书中心。

参见

使用证书 (页 21)

导出用户认证证书 (页 47)

导入用户认证证书 (页 48)

添加用户认证证书 (页 49)

选择用户认证证书 (页 50)

删除用户认证证书 (页 51)

4.4.6 导出用户认证证书

创建用户认证证书后，必须导出该证书以便用户设备使用。用户可随时导出当前使用的证书。

要求

在远程设备上事先创建有用户认证证书，并显示在“设置”(Settings) 选项卡的“用户认证” (User authentication) 下方。

操作步骤

要导出用户认证证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在远程设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（远程设备）”(Configuration (remote device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 设置”(HTTPS settings) 复选框。
   在“设置”(Settings) 选项卡中，用户认证区域激活。
5. 切换至“设置”(Settings) 选项卡。
6. 在“用户认证”(User authentication) 区域，单击“导出”(Export)。
   “另存为”(Save as) 对话框随即打开。
7. 选择存储位置并输入证书名称。
8. 单击“保存”(Save)。

结果

当前使用的用户认证证书将以“.cer”扩展名的文件保存在指定存储位置处。

参见

使用证书 (页 21)

创建用户认证证书 (页 45)

导入用户认证证书 (页 48)

添加用户认证证书 (页 49)

选择用户认证证书 (页 50)

删除用户认证证书 (页 51)

4.4.7 导入用户认证证书

要建立用户设备与远程设备之间的 HTTPS 连接，必须将在远程设备上创建的用户认证证书导入到用户设备的 TIA Portal Cloud Connector 中。

要求

- 在远程设备上，创建有用户认证证书。
- 用户认证证书已复制到远程设备的本地硬盘中。

操作步骤

要导入用户认证证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在用户设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（用户设备）”(Configuration (user device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 端点”(HTTPS endpoint) 复选框。
   在“设置”(Settings) 选项卡中，用户认证区域激活。
5. 切换至“设置”(Settings) 选项卡。
6. 在“用户认证”(User authentication) 区域，单击“导入”(Import)。
   “打开”(Open) 对话框随即打开。
7. 在文件系统中选择该证书文件。证书文件的文件扩展名为“.cer”。
8. 单击“打开”(Open)。

结果

证书已导入并添加到可信任证书列表中。通过该列表，可指定与用户设备进行通信的远程设备。指定的远程设备上安装的用户认证证书必须与用户设备上的相同。

参见

使用证书 (页 21)

创建用户认证证书 (页 45)

导出用户认证证书 (页 47)

添加用户认证证书 (页 49)

选择用户认证证书 (页 50)

删除用户认证证书 (页 51)

4.4.8 添加用户认证证书

除了从文件系统中导入证书，还可以将该证书从 Windows 证书中心添加到可信认证证书列表中。

要求

指定的证书包含在 Windows 证书中心内。

操作步骤

要从 Windows 证书中心添加用户认证证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在用户设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（用户设备）”(Configuration (user device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 端点”(HTTPS endpoint) 复选框。
   在“设置”(Settings) 选项卡中，用户认证区域激活。
5. 切换至“设置”(Settings) 选项卡。
6. 在“用户认证”(User authentication) 区域，单击“添加”(Add)。
   “选择证书”(Select certificate) 对话框随即打开，并显示可用的证书。
7. 选择一个证书。必要时，可显示该证书。
8. 单击“确定”(OK)。

结果

该证书从 Windows 证书中心添加到可信任的证书列表中。通过该列表，可指定与用户设备进行通信的远程设备。指定的远程设备上安装的用户认证证书必须与用户设备上的相同。

参见

使用证书 (页 21)

创建用户认证证书 (页 45)

导出用户认证证书 (页 47)

导入用户认证证书 (页 48)

选择用户认证证书 (页 50)

删除用户认证证书 (页 51)

4.4.9 选择用户认证证书

除了在远程设备上创建新证书，还可以从 Windows 证书中心选择并使用一个现有的证书。

要求

事先已创建了用户认证证书，并保存在 Windows 证书中心内。

操作步骤

要从 Windows 证书中心选择一个用户认证证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在远程设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（远程设备）”(Configuration (remote device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 设置”(HTTPS settings) 复选框。
   在“设置”(Settings) 选项卡中，用户认证区域激活。
5. 切换至“设置”(Settings) 选项卡。
6. 在“用户认证”(User authentication) 区域，单击“选择”(Select)。
   “Windows 信息安全”(Windows Security) 对话框随即打开，并显示可用的证书。
7. 选择一个证书。必要时，还可显示该证书的其它附加属性。
8. 单击“确定”(OK)。

结果

该证书已在远程设备上用于用户认证。必要时，也可导出该证书并与用户设备进行交换。

参见

使用证书 (页 21)

创建用户认证证书 (页 45)

导出用户认证证书 (页 47)

导入用户认证证书 (页 48)

添加用户认证证书 (页 49)

删除用户认证证书 (页 51)

4.4.10 删除用户认证证书

用户可随时从用户设备的可信任证书列表中删除某个用户认证证书。

操作步骤

要从可信任的证书列表中删除某个用户认证证书，请按以下步骤操作：

1. 要打开 TIA Portal Cloud Connector，可在用户设备的 Windows 任务栏信息区中右键单击 TIA Portal Cloud Connector 图标。
2. 在快捷菜单中，选择“组态（用户设备）”(Configuration (user device)) 命令。
   此时，TIA Portal Cloud Connector 组态窗口随即打开。
3. 切换到“协议”(Protocol) 选项卡。
4. 选择“HTTPS 端点”(HTTPS endpoint) 复选框。
   在“设置”(Settings) 选项卡中，用户认证区域激活。
5. 切换至“设置”(Settings) 选项卡。
6. 在可信任的证书列表中，选择要删除的证书。
7. 在“用户认证” (User authentication) 区域，单击“删除”(Remove)。

结果

在可信任的证书列表中，删除了该证书。此时，将无法再连接使用该证书进行用户认证的远程设备。

参见

使用证书 (页 21)

创建用户认证证书 (页 45)

导出用户认证证书 (页 47)

导入用户认证证书 (页 48)

添加用户认证证书 (页 49)

选择用户认证证书 (页 50)

4.5 通过 TIA Portal Cloud Connector 进行在线连接

简介

如果使用 TIA Portal Cloud Connector 连接硬件设备，则 TIA Portal 中的操作与普通的硬件设备在线连接完全相同。如果启用了隧道通信，则可按之前的操作方式进行数据编译、加载或监控。

有关建立在线连接和在线模式下操作的更多信息，请参见 TIA Portal 在线帮助。

状态符号概览

如果通过 TIA Portal Cloud Connector 建立一个在线连接，则 Windows 任务栏的信息区中将显示一个状态符号，指示连接的状态。下表简要列出了各种状态符号及其含义：

状态符号	含义
	通信已禁用
	通信已启用，但 TIA Portal 和 SIMATIC 自动化硬件间没有数据交换。
	通信已启用，且 TIA Portal 和 SIMATIC 自动化硬件间正在进行数据交换。
	TIA Portal 与 SIMATIC 自动化硬件间的数据交换操作已中断。显示的状态符号可指示相关原因的更多详细信息。

状态显示

在 Windows 任务栏的信息区中，远程设备和用户设备上都将显示一个状态符号。单击该符号，可打开“TIA Portal Cloud Connector - 远程设备”(TIA Portal Cloud Connector - Remote device) 或“TIA Portal Cloud Connector - 用户设备” (TIA Portal Cloud Connector - User device) 窗口。在该窗口中，将显示有关 TIA Portal Cloud Connector 的所有信息、警告和错误消息。此外，还会显示 TCP 或 HTTPS 的连接时间。

用户可随时隐藏该状态栏。

参见

在 PG/PC 上安装 TIA Portal Cloud Connector (页 37)

在 PG/PC 上组态 TIA Portal Cloud Connector (页 38)

在虚拟机中组态 TIA Portal Cloud Connector (页 40)

离线使用虚拟机 (VM) (页 53)

4.6 离线使用虚拟机 (VM)

用户可离线使用虚拟机。为此，需要将虚拟机从远程设备复制到本地 PG/PC 中。之后，即可在 PG/PC 上启动虚拟机并使用 TIA Portal 以及连接该 PG/PC 的硬件设备或网络中的硬件设备。

可通过以下几种方式使用虚拟机：

- 通过以太网连接硬件设备和本地 PG/PC，并硬件设备与 PG/PC 位于相同子网中。
- 通过以太网或 PROFIBUS 连接硬件设备和本地 PG/PC，但硬件设备与 PG/PC 位于不同的子网中。

不使用 TIA Portal Cloud Connector 进行连接。可能会发生以下情景：

- 如果硬件设备通过以太网或 USB 适配器直接连接 PG/PC，则可设置“Bridged”网络连接。
  虚拟机中必须禁用该连接类型的 TIA Portal Cloud Connector。
- 如果硬件设备通过自带的 USB 或网络适配器连接到网络中，则可使用“Host-only”选项。此时，必须在虚拟机中启用 TIA Portal Cloud Connector，才能使用 PROFIBUS 接口。

在本地使用该虚拟机时，可将其复制到远程设备中。

要求

- PG/PC 上安装有启动虚拟机的相应软件，如 VMware Workstation。
- PG/PC 上安装有 Automation License Manager 。

将虚拟机 (VM) 从远程设备传送到 PG/PC 上。

要离线使用虚拟机，请按以下步骤操作：

1. 将虚拟机复制到本地的 PG/PC 中。具体的操作步骤取决于所用的虚拟机系统。如需帮助，请参见相关文档。
2. 打开 Automation License Manager，将 TIA Portal 中 SIMATIC 软件所需的许可证传送到本地驱动器中。
3. 将所有需要的项目数据从服务器复制到本地驱动器中。
4. 启动虚拟机并组态网络连接。请仔细阅读页面顶部显示的提示信息。

将虚拟机 (VM) 从 PG/PC 传送到远程设备

要将虚拟机 (VM) 传送回远程设备，请按以下步骤操作：

- 将虚拟机从本地 PG/PC 复制到远程设备中。具体的操作步骤取决于所用的虚拟机系统。如需帮助，请参见相关文档。
- 打开 Automation License Manager，将许可证从本地驱动器传送回 ALM Server。
- 将所有需要的项目数据从本地驱动器复制回服务器中。

参见

在 PG/PC 上安装 TIA Portal Cloud Connector (页 37)

在 PG/PC 上组态 TIA Portal Cloud Connector (页 38)

在虚拟机中组态 TIA Portal Cloud Connector (页 40)

通过 TIA Portal Cloud Connector 进行在线连接 (页 52)

索引