OPC UA 配置管理器

目录

OPC UA 配置管理器

帮助版本 1.042

目录

概述

OPC 统一架构 (UA) 是由 OPC Foundation 在数十个成员组织的协助下共同建立的开放标准。尽管 UA 旨在提供独立于平台的互操作性标准 (以绕开 Microsoft COM)，但它并不取代 OPC Data Access (DA) 技术。对于大多数工业应用程序，UA 将补充或增强现有的 DA 体系结构。它不是系统范围的替代物。OPC UA 以下列方式补充 OPC DA 基础设施：

- 它提供了一种安全的客户端到服务器连接方法，无需依赖 Microsoft DCOM，并且能够通过防火墙和 VPN 连接进行安全连接。如果用户要连接域内公司网络中的远程计算机 (防火墙内)，OPC DA 和 DCOM 连接可能会令人满意。
- UA 提供了另外一种将工厂车间数据共享到业务系统 (车间到顶层) 的方法。OPC UA 可将多个 OPC DA 源中的数据聚合到非工业系统中。

对于大多数用户应用程序而言，UA 标准中最相关的组件如下所示：

- 通过受信任证书在客户端和服务器端点之间建立的安全连接。
- 可靠的 OPC 项订阅模型，可在客户端和服务器之间提供高效的数据更新。
- 从参与通信的 UA 服务器中发现可用信息的增强方法。

OPC UA 配置管理器

OPC UA 配置管理器 帮助用户管理 UA 服务器配置。OPC UA 的安全特性要求所有参与 UA 通信的端点都通过安全连接进行。为符合此安全要求，每个 UA 服务器实例和 UA 客户端实例都必须提供一个受信任证书来标识自身。这些证书可能是自签名的。因此，在尝试建立安全的 UA 客户端/服务器连接之前，必须由具有管理员权限的用户将这些证书同时添加到服务器和客户端节点上的本地受信任证书存储中。OPC UA 配置管理器 是一个用户友好的界面，可用于执行证书交换。

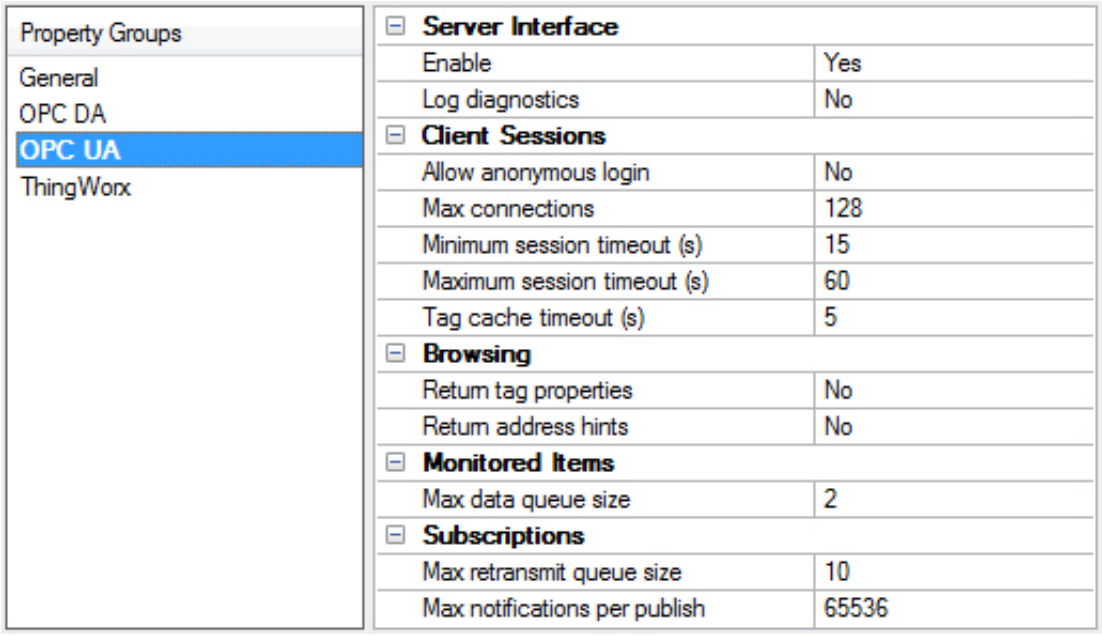
有关特定 OPC UA 配置管理器 属性的详细信息，请从下表中选择一个链接。

服务器端点
受信任的客户端
发现服务器
受信任的服务器
实例证书

项目属性 - OPC UA

OPC 统一架构 (UA) 提供了一个平台无关的互操作性标准。它不是 OPC 数据访问 (DA) 技术的替代品：对于大多数工业应用，UA 补充或增强了现有的 DA 架构。OPC UA 项目属性组显示服务器中当前的 OPC UA 设置。

注意：要更改设置，请单击特定属性的第二列。这将调用显示可用选项的下拉菜单。



服务器接口

“启用”：启用后，UA 服务器接口将初始化，并接受客户端连接。禁用后，此页面上的其余属性将被禁用。

“日志诊断”：启用后，会将 OPC UA 堆栈诊断记录到“OPC 诊断查看器”中。这只能用于故障排除目的。

客户端会话

“允许匿名登录”：此属性指定在建立连接时是否需要用户名和密码。为了安全起见，默认设置为“否”，即不允许匿名访问且需要凭据才能登录。
注意：如果禁用此设置，则用户无法作为 “用户管理器”中的默认用户登录。用户可以以管理员身份登录，前提是 在“用户管理器”中设置了密码 且该密码用于登录。
提示：可将其他用户配置为无需与管理员帐户相关的所有权限即可访问数据。如果客户端在连接时提供密码，服务器将使用由端点的安全策略定义的加密算法来解密密码，并使用该密码登录。

Note: Users can login as the Administrator using the password set during the installation of KEPServerEXOPC 聚合器ThingWorx Kepware ServerThingWorx Kepware Edge to login. Additional users may be configured to access data without all the permissions associated with the administrator account. When the client supplies a password on connect, the server decrypts the password using the encryption algorithm defined by the security policy of the endpoint, then uses it to login.
如果客户端在连接时提供密码，服务器将使用由端点的安全策略定义的加密算法来解密密码。

“最大连接数”: 指定所支持的最大连接数。有效范围为 1 到 128。默认设置为 128。

“最小会话超时”: 指定 UA 客户端建立会话的最小超时限制。可视应用程序需要更改值。默认值为 15 秒。

“最大会话超时”: 指定 UA 客户端建立会话的最大超时限制。可视应用程序需要更改值。默认值为 60 秒。

“标记缓存超时”: 指定标记缓存超时。有效范围为 0 到 60 秒。默认设置为 5 秒。
注意: 此超时控制在使用其完成 UA 客户端操作后，标记被缓存多长时间。在 UA 客户端以设定间隔读取/写入未注册的标记的情况下，用户可以通过增加超时来提高性能。例如，如果客户端每 5 秒读取一个未注册的标记，则标记缓存超时应设置为 6 秒。由于标记不必在每次客户端请求时重新创建，因此可以提高性能。

浏览

“返回标记属性”: 启用以允许 UA 客户端应用程序浏览地址空间中每个标记的标记属性。默认情况下禁用此设置。

“返回地址提示”: 启用以允许 UA 客户端应用程序浏览每个项可用的地址格式化提示。虽然提示不是有效的 UA 标记，但某些 UA 客户端应用程序可能会尝试将其添加到标记数据库。发生此类情况时，客户端将接收到来自服务器的错误。这可能会导致客户端自动报告错误或停止添加标记。为了防止发生这种情况，请确保禁用此属性。默认情况下禁用此设置。

监控的项

“最大数据队列大小”: 指定一个项中将加入队列的数据通知的最大数量。有效范围为 1 到 100。默认设置为 2。
注意: 当监控项的更新速率高于订阅的发布速率时，使用数据队列。例如，如果监控项的更新速率为 1 秒，而订阅每 10 秒发布一次，则每 10 秒就会为该项发布 10 条数据通知。由于队列数据会占用内存，因此当内存出现问题时，应限制此值。

订阅

“最大重新传送队列大小”: 指定每次订阅时加入队列的发布的最大数量。有效范围为 1 到 100。值为零时将禁用重新传输。默认设置为 10。
注意: 订阅发布事件将按照客户端请求加入队列并进行重新传输。由于队列会占用内存，因此当内存出现问题时，应限制此值。

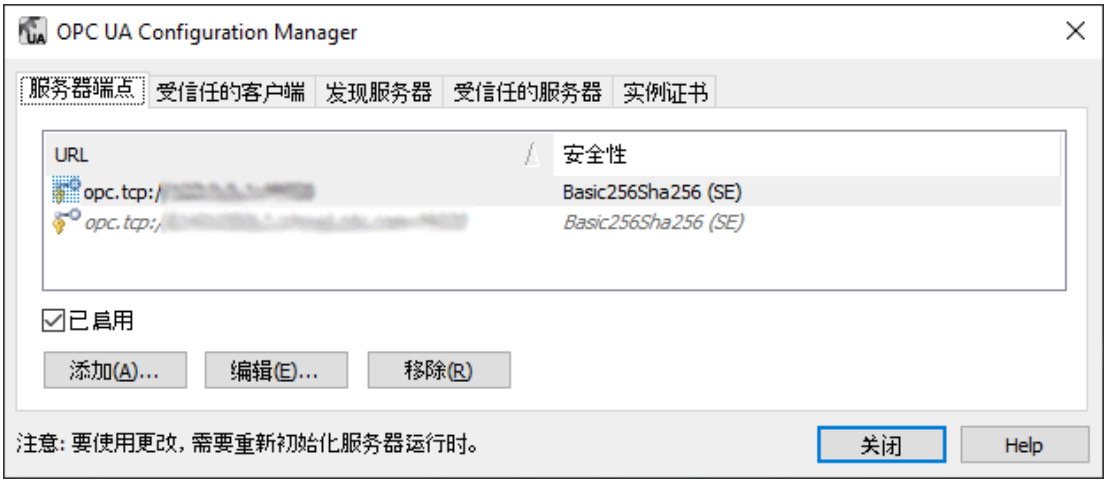
“每次发布的最大通知数”: 指定每次发布的最大通知数。有效范围为 1 到 65536。默认设置为 65536。
注意: 此值可能会通过限制从服务器发送到客户端的数据包大小来影响连接的性能。通常，大值应该用于高带宽连接，而小值应该用于低带宽连接。

“默认值”按钮用于将设置恢复到默认/预设值。

服务器端点

OPC UA 服务器需要服务器端点定义，以创建 UA 客户端可与之通信的 UA 接口。UA 服务器端点定义为通用资源定位器 (URL)，用于标识服务器的特定实例、传输类型以及通信安全性。服务器端点由一个 URL 和一个安全策略类型组成。项目最多允许 100 个服务器端点。“服务器端点”选项卡可在一行中显示多个服务器端点。

注意: 默认情况下会启用每个新定义的端点，但用户可以根据需要禁用它。在服务器运行期间添加、移除或修改端点需要重新初始化 UA 服务器的运行时。

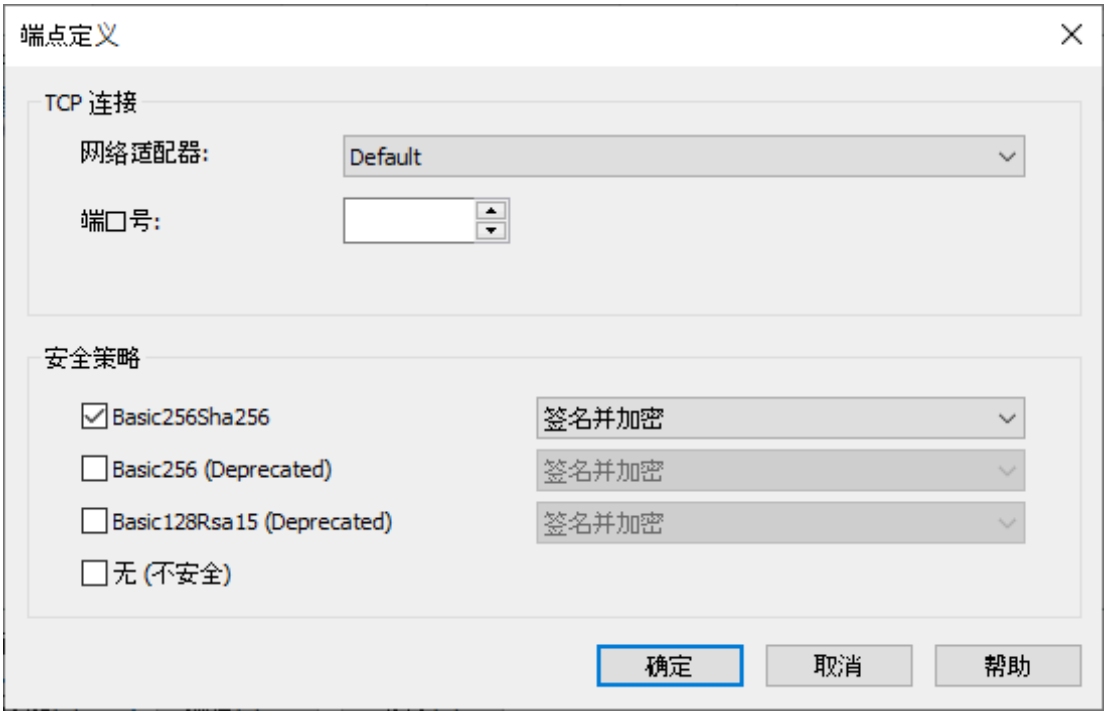


注意：服务器实例中的所有端点都共享相同的实例证书。默认情况下，UA 服务器使用自签名证书，但用户可以在“实例证书”选项卡中导入自定义实例。

重要事项：在符合 OPC UA 要求的情况下，实现标准 UA 服务器配置文件的服务器必须支持用户名/密码登录。此 UA 服务器将支持基于每个服务器实例(而不是每个端点)的用户信息验证。已识别的用户将来自“服务器管理”(位于系统托盘)中的“用户管理器”功能。

端点定义

要访问“端点定义”对话框，请单击“服务器端点”选项卡中的**“添加...”**或**“编辑...”**。



“网络适配器”：此参数用于指定连接所绑定的网络适配器。可将其配置为具有 IP 地址的可用适配器、默认和本地主机。初始选择为默认，即映射到默认网络适配器。

“端口号”：此参数用于指定端口号。这在定义中是必需的，因为 URL 中剩余的用于定义端点的部分已对计算机的主机名和传输协议进行了标准化。此对话框定义的所有端点 URL 的格式均为 *opc.tcp://<hostname>:<port>*。如果无法确定完全限定的主机名，则以本地主机或 IP 地址替代。

“安全策略”：这些安全策略和消息模式参数指定 UA 服务器支持的安全算法。默认情况下选择 Basic256Sha256。选项如下：

- Basic256Sha256
- Basic256 (Deprecated)
- Basic128Rsa15 (Deprecated)
- 无 (不安全)

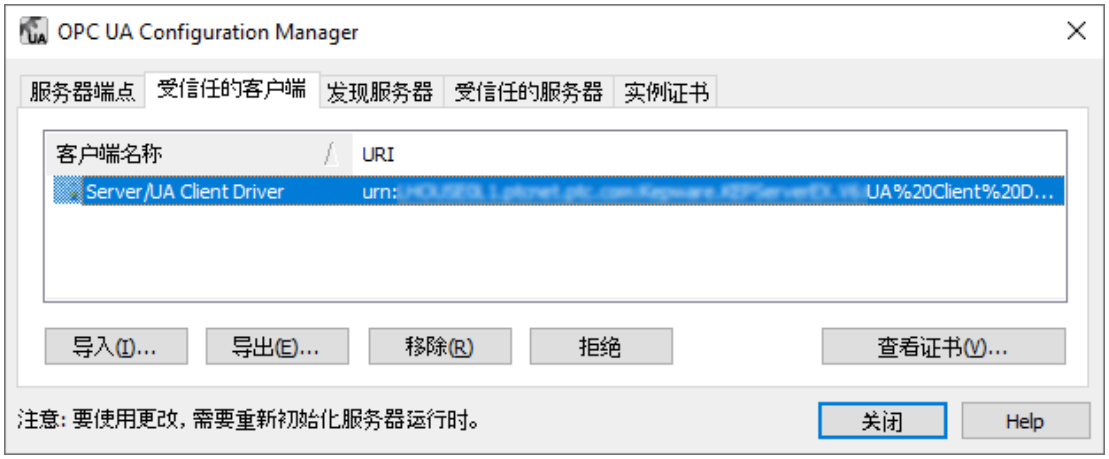
只有选中相应的复选框后，才能访问“安全策略”下拉列表。如果未选中任何安全策略，则假设默认安全策略为“无”，这不会提供保护，我们不建议这样做。每个下拉列表都列出了 UA 服务器支持的消息加密模式，并按安全性由高到低排列。默认选择为“签名并加密”。选项如下：

- 签名并加密
- 签名; 签名并加密
- 签名

警告：安全策略 Basic128Rsa15 和 Basic256 从 OPC UA 规范版本 1.04 开始已被 OPC Foundation 弃用。这些策略提供的加密安全性较低，其使用应限制为提供向后兼容性。

受信任的客户端

UA 服务器需要证书来建立与每个 UA 客户端的受信任连接。为了使服务器接受提供自签名证书的客户端的连接，必须将客户端的证书导入到 OPC UA 服务器接口所使用的受信任客户端证书存储中。为支持此功能，可通过 UA 配置管理器导入、移除和查看受信任的客户端证书。



“导入...”：单击此按钮可导入要信任的客户端证书。

“导出...”：单击此按钮可将受信任的客户端证书导出到所需的位置。

“移除”：单击此按钮可移除对客户端证书的信任。还将从受信任的客户端列表中移除该证书。

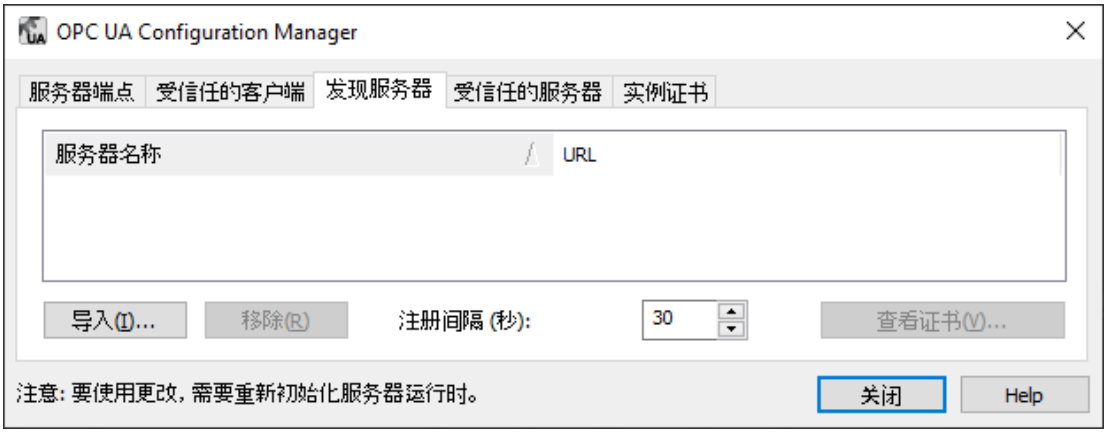
“拒绝”：单击此动态按钮可移除对客户端证书的信任。被拒绝的证书将保留在受信任客户端列表中，并标有红色的 X。

“信任”：单击此动态按钮可信任客户端证书。

“查看证书...”：单击此按钮将调用客户端证书信息的视图。

发现服务器

任何 OPC UA 服务器都可以在 UA 发现服务器中注册，以使具有访问权限的客户端可以使用其端点信息。为了执行此注册，UA 服务器接口必须知道要使用的一个或多个端点。必须具备拥有自签名证书的发现服务器，并将其存储在 UA 服务器的受信任证书存储中。同样，必须具备 UA 服务器的证书并将其存储在 UA 发现服务器的受信任证书存储中。OPC UA 配置管理器 能够导入、移除和查看 UA 服务器接口可识别的受信任发现服务器端点。

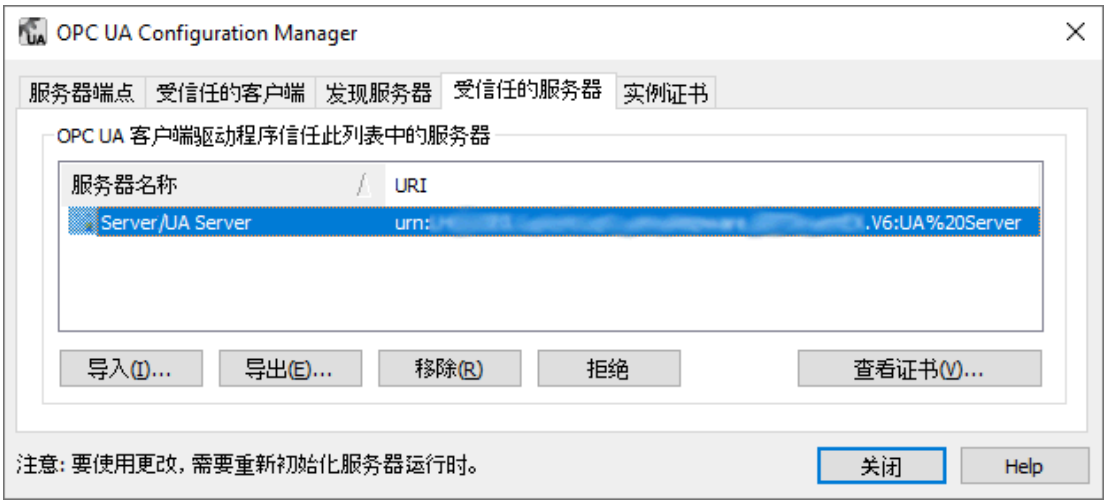


注意：用户可通过**"注册间隔"**参数更改刷新发现服务器的注册间隔时间。默认设置为 30 秒。

受信任的服务器

只有在计算机上安装了 UA 客户端驱动程序时，才会显示"受信任的服务器"选项卡。此对话框用于建立 UA 客户端驱动程序可与之通信的受信任服务器的列表。

注意：对于自签名的客户端，UA 客户端驱动程序需要受信任的证书管理，就像 UA 服务器一样。为了使 UA 客户端驱动程序能够连接到使用自签名证书的服务器，必须由具有管理权限的用户将外部 UA 服务器的证书导入到 UA 客户端驱动程序的受信任证书存储中。因为客户端驱动程序自签名证书，所以必须将该证书导出并存储到服务器的受信任证书存储中。



"导入..."：单击此按钮可导入要信任的服务器证书。

"导出..."：单击此按钮可将受信任的服务器证书导出到所需的位置。

"移除"：单击此按钮可移除对服务器证书的信任。还将从受信任的服务器列表中移除该证书。

"拒绝"：单击此动态按钮可移除对服务器证书的信任。被拒绝的证书将保留在受信任服务器列表中，并标有红色的 X。

"信任"：单击此动态按钮可信任服务器证书。

"查看证书..."：单击此按钮可调用服务器证书信息的视图。

有关在 UA 客户端驱动程序和 UA 服务器之间交换证书的说明，请参阅手动交换。

实例证书

为 UA 服务器和 UA 客户端驱动程序创建自签名的 X.509 实例证书。可通过“实例证书”选项卡访问它们，如下所示。

服务器

“查看证书”: 单击此按钮可调用服务器证书。除了证书路径外，该对话框还包含证书的一般和详细信息。*有关详细信息，请参阅证书显示*。

导出服务器证书: 单击此按钮可将服务器证书导出到所需的位置。

重新颁发证书: 单击此按钮将重新颁发服务器证书。由 OPC UA 配置管理器 生成的证书是自签名证书，采用 rsa-sha256 算法，并在三年后到期。重新颁发证书会使现有的全部信任关系无效。

导入证书: 单击此按钮可导入一个证书。导入的服务器证书必须采用 PKCS12 格式(即 .pfx 扩展名) 。它们必须同时包含实例证书和私钥，并且可能受密码保护。

客户端

查看客户端驱动程序证书: 单击此按钮可调用客户端驱动程序的证书。除了证书路径外，该对话框还包含证书的一般和详细信息。*有关详细信息，请参阅证书显示*。

导出客户端驱动程序证书: 单击此按钮可将客户端驱动程序的证书导出到所需的位置。

重新颁发证书: 单击此按钮将重新颁发客户端驱动程序的证书。由 OPC UA 配置管理器 生成的证书是自签名证书，采用 rsa-sha256 算法，并在三年后到期。重新颁发证书会使现有的全部信任关系无效。

导入证书: 单击此按钮可导入一个证书。导入的客户端证书必须采用 PKCS12 格式(即 .pfx 扩展名) 。它们必须同时包含实例证书和私钥，并且可能受密码保护。

默认自签名证书

文件名:

- <产品名称>_ua_server.der
- <产品名称>_ua_client_driver.der

到期：

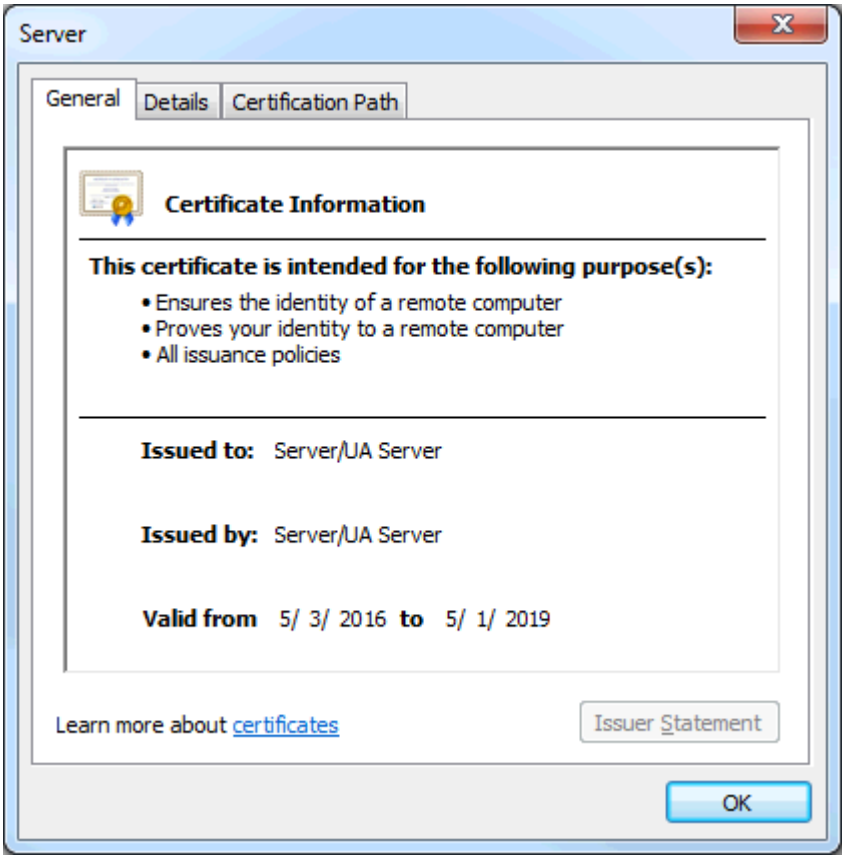
- 自颁发日期起三(3)年

签名算法：

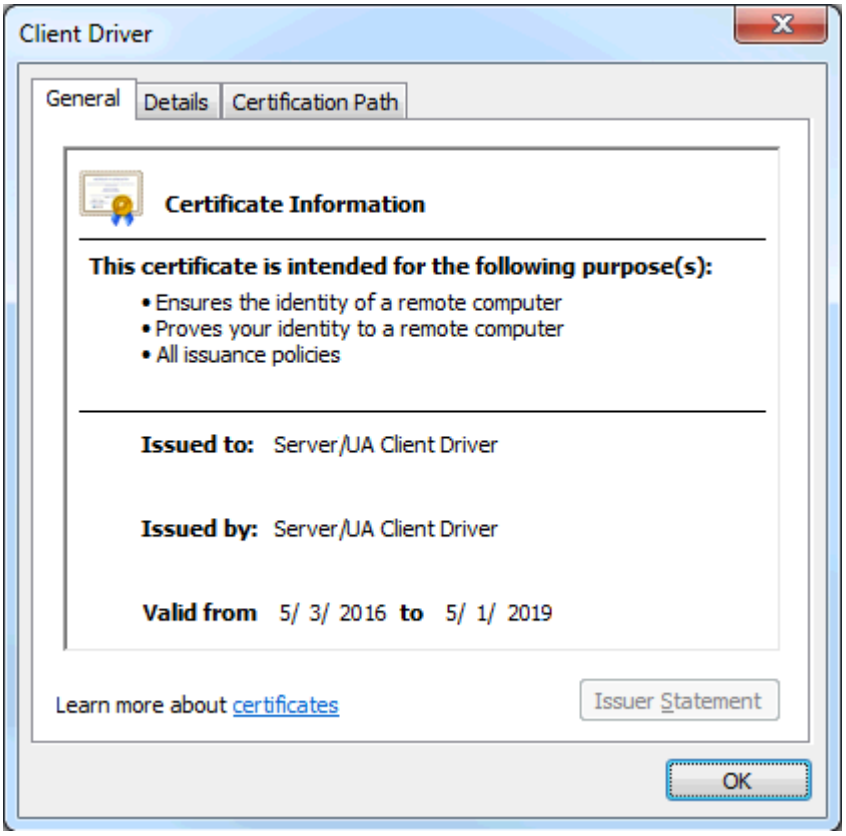
- rsa-sha256

证书显示

查看服务器证书时，对话框应如下所示。

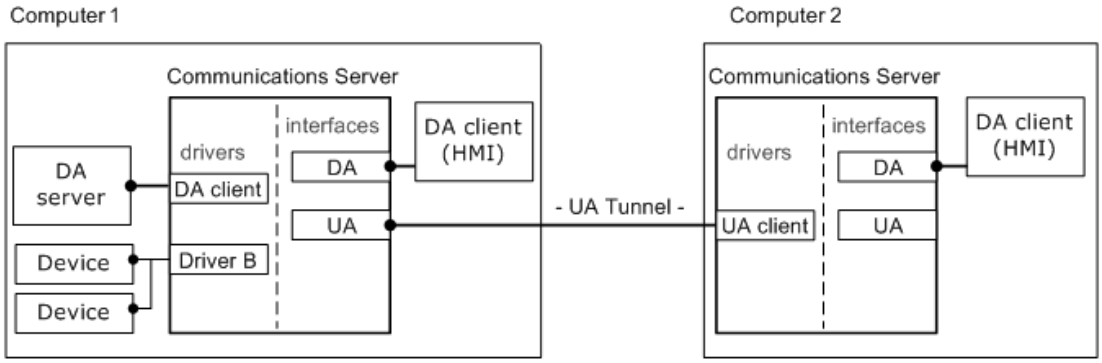


查看客户端驱动程序证书时，对话框应如下所示。


Client Driver
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• All issuance policies
Issued to: Server/UA Client Driver
Issued by: Server/UA Client Driver
Valid from 5/ 3/ 2016 to 5/ 1/ 2019
Learn more about certificates
Issuer Statement
OK

OPC UA 教程

本教程演示如何在运行通信服务器的两台远程计算机之间配置安全的 OPC UA 连接。



需要以下运行时组件：

- 计算机 1 具备带有 UA 服务器接口的通信服务器。
- 计算机 2 具备带有 UA 客户端驱动程序的通信服务器。

注意：OPC DA 客户端驱动程序 (在上图中显示为计算机 1) 是用于连接外部 OPC DA 服务器的可选组件。

先决条件

在继续之前，用户必须执行以下操作：

1. 在客户端计算机上安装服务器应用程序。在“选择功能”对话框中，包括 OPC UA 客户端驱动程序 (位于**“通信驱动程序”**下)。
2. 在服务器计算机上安装服务器应用程序。由于包含 UA 功能，因此在安装过程中不需要选择其他功能。

注意：某些用户应用程序可能需要每台计算机同时充当服务器和客户端。在此情况下，请在需要远程访问 OPC 项的每台计算机上安装 OPC UA 客户端驱动程序。

安全性

OPC UA 不依赖计算机的操作系统来保护应用程序，而是使用 X.509 身份验证技术。此技术需要每个建立信任的实体提供公钥和私钥。公钥放入证书进行分发，私钥则受到保护。客户端和服务器必须交换证书才能建立安全连接。此交换只需在证书的有效期内完成。

手动交换包括在每台计算机上导出和导入证书文件。必须使用可移动介质 (或另一种形式的文件传输) 才能实现交换。手动过程还允许在超出此应用程序范围的客户端和服务器之间交换证书。

如果安全性不是强制的，则可以跳过证书交换。定义服务器端点时，由用户设置安全级别。如果选择了“无”，则不会验证证书。*有关不安全连接的详细信息，请参阅**设置服务器*。

交换

1. 首先，右键单击系统托盘中的**“管理”**图标启动服务器计算机上的 OPC UA 配置管理器。然后，选择**“OPC UA 配置”**。
2. 接下来，选择**“实例证书”**。在**“服务器”**组下，单击**“导出服务器证书”**。为证书文件选择易于访问的位置。用户可能会根据需要更改默认文件名。
3. 从服务器计算机中手动复制服务器证书文件，并将其移动到客户端计算机上。
4. 接下来，在客户端计算机上启动 OPC UA 配置管理器。
5. 选择**“受信任的服务器”**选项卡，然后单击**“导入”**。
6. 找到服务器证书文件，单击**“打开”**。服务器证书应显示在**“受信任的服务器”**窗口中，并可由 URI 进行标识。

7. 接下来，选择**“实例证书”**。在**“客户端驱动程序”**组下，选择**“导出客户端驱动程序证书”**。为证书文件选择易于访问的位置。用户可能会根据需要更改默认文件名。
8. 手动从客户端计算机复制客户端证书文件，并将其回传到服务器计算机。
9. 接下来，在客户端计算机上启动 OPC UA 配置管理器。
10. 选择**“受信任的客户端”**选项卡，然后单击**“导入”**。
11. 找到客户端证书文件，然后单击**“打开”**。客户端证书应显示在**“受信任的客户端”**窗口中，并可由 URI 进行标识。

设置服务器

端点

要使 OPC UA 客户端连接到 OPC UA 服务器，客户端必须知道服务器位置和安全要求。在其复杂形式中，客户端将使用位置和端口号 (称为发现端点) 来发现有关服务器的信息。与之对应，服务器将返回可用于该客户端的所有已配置端点以及安全要求。为简化此过程，发现端点和服务器端点可能位于同一位置 (与此服务器应用程序的情况相同)。

在本地连接的服务器应用程序安装过程中，会创建一个初始端点。需要进行少量配置更改，以允许远程客户端发现和连接到服务器。服务器不需要进行任何更改即可进行本地连接。有关添加和更改现有端点的信息，请按照以下说明进行操作。

1. 首先，右键单击系统托盘中的**“管理”**图标启动 OPC UA 配置管理器。选择**“OPC UA 配置”**。
2. 单击**“服务器端点”**，然后选择安装过程中为非本地连接创建的默认端点。
3. 单击 **“编辑”**。
   注意：请务必记下端口号，以便稍后将其添加到防火墙。
4. 如有必要，请修改**“安全策略”**设置。由于这些是服务器设置，因此这一特定端点将允许所有已启用策略的连接。这意味着默认端点将仅允许使用签名和加密的安全连接。如果不需要安全性，请选择“无”。有此选择的用户可能需要完全禁用安全策略。
5. 对策略进行相应调整后，单击**“确定”**。
6. 要启用端点，请在列表中选择它，然后选中**“启用”**。
7. 右键单击系统托盘中的**“管理”**图标，然后选择**“重新初始化”**，将更改应用到服务器运行时。如果服务器未运行，则右键单击**“管理”**图标，然后选择**“启动运行时”**。

发现服务 (可选)

熟悉 OPC DA 的用户可能会熟悉 OPCEnum，该应用程序在服务计算机上本地运行，并将可用的 OPC DA 服务器呈现给远程连接的客户端。客户端只需要知道服务计算机在网络上的位置。

有一个服务可使 OPC UA 服务器能够在“已知”位置被发现，从而在独立于平台的情况下提供类似的可用性。该服务称为**本地发现服务 (LDS)**，它通常安装在运行 OPC UA 服务器的每台计算机上 (类似于 OPCEnum 随大多数典型的 OPC 服务器一起安装)。由于 LDS 的开发和实施并不像 OPC UA 本身那样深入，因此该服务的实际使用会有所不同。

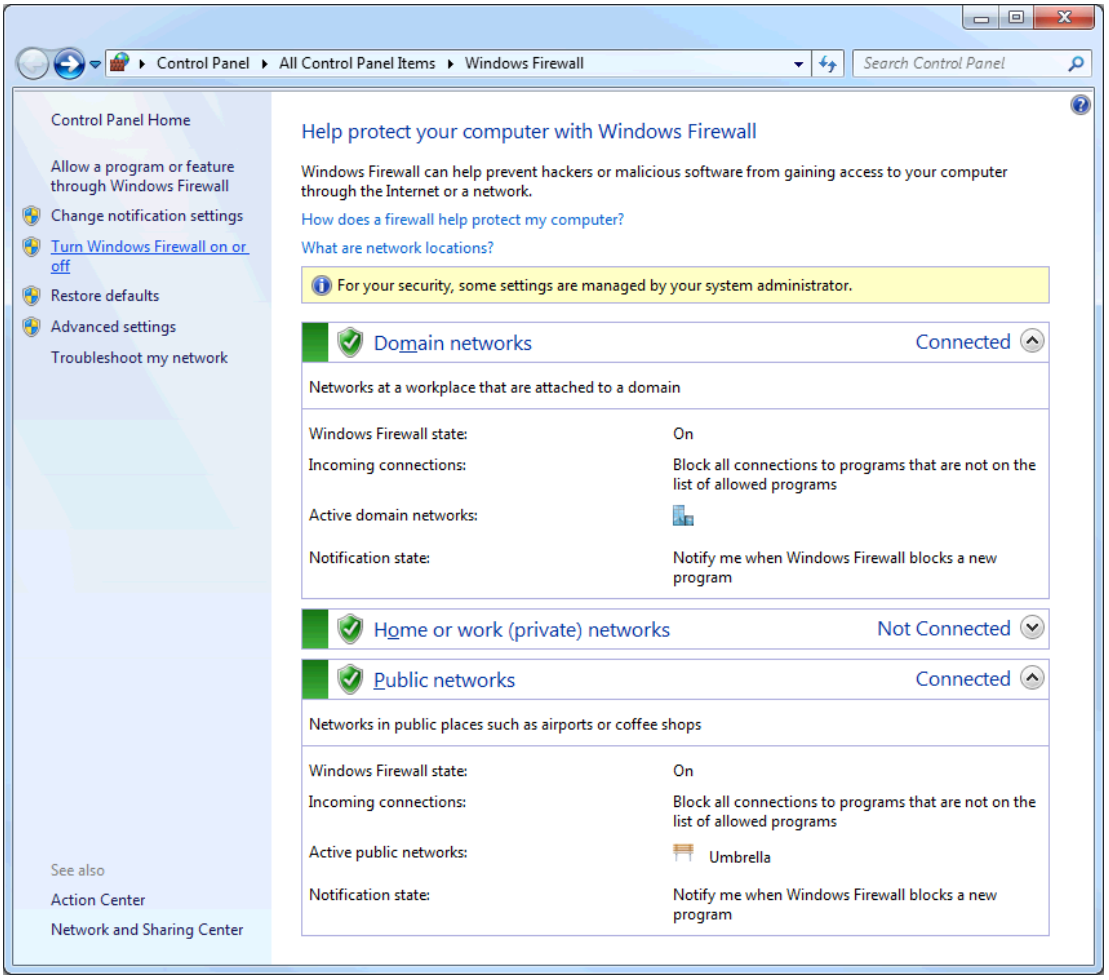
注意：此服务器应用程序不提供 LDS，但可以将其配置为在 LDS 中注册。

防火墙

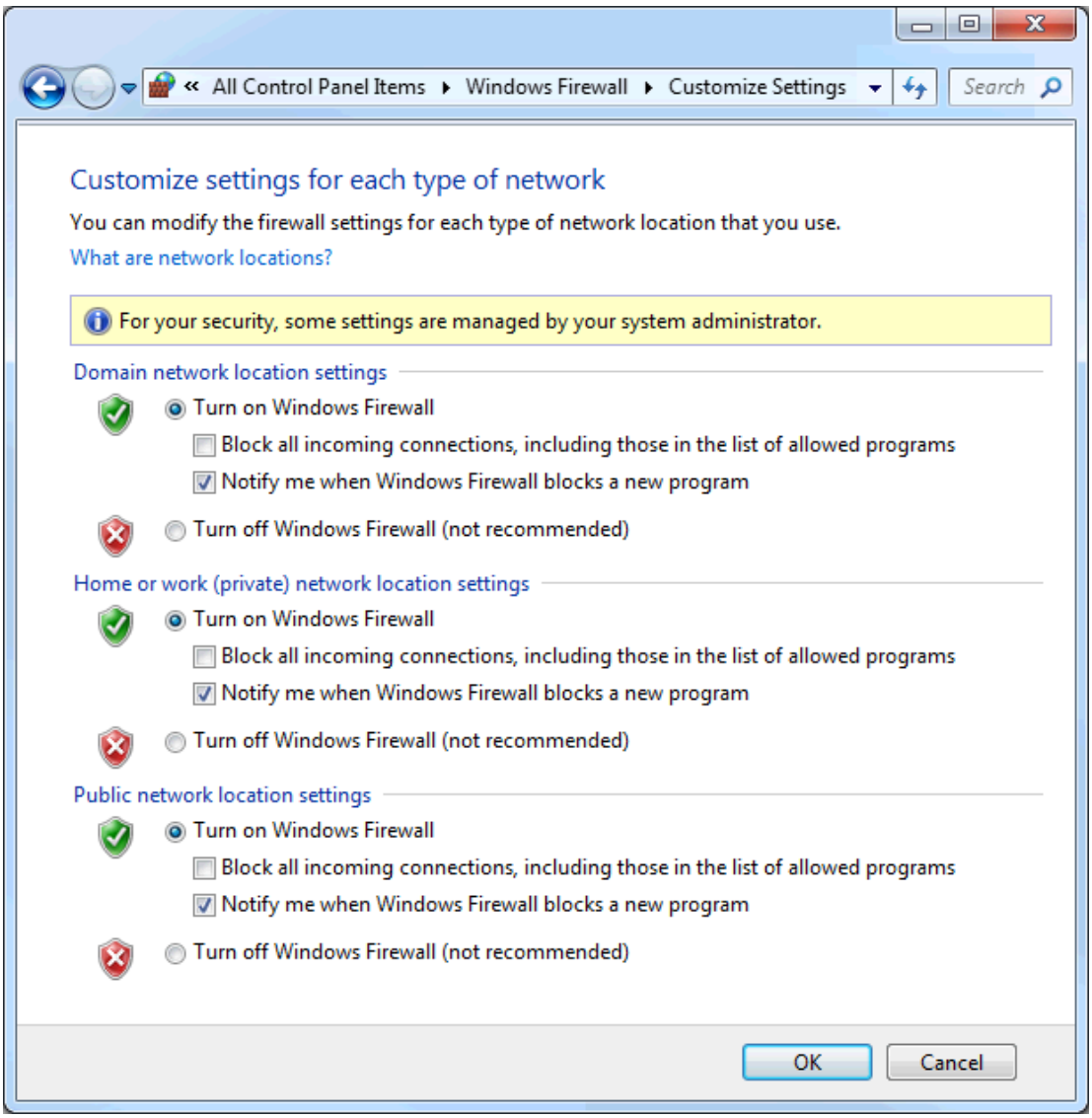
防火墙会丢弃非预期的传入通信流 (称为“未经请求的通信”) 以及与防火墙内设置的例外 (称为“例外通信”) 不对应的传入通信流。由于 OPC UA 不需要回调，因此只有服务器计算机需要有例外。

要添加例外，请在服务器计算机上执行以下操作。

1. 首先，选择**“开始”|“运行”**启动 Windows 防火墙。然后，键入 **firewall.cpl**。

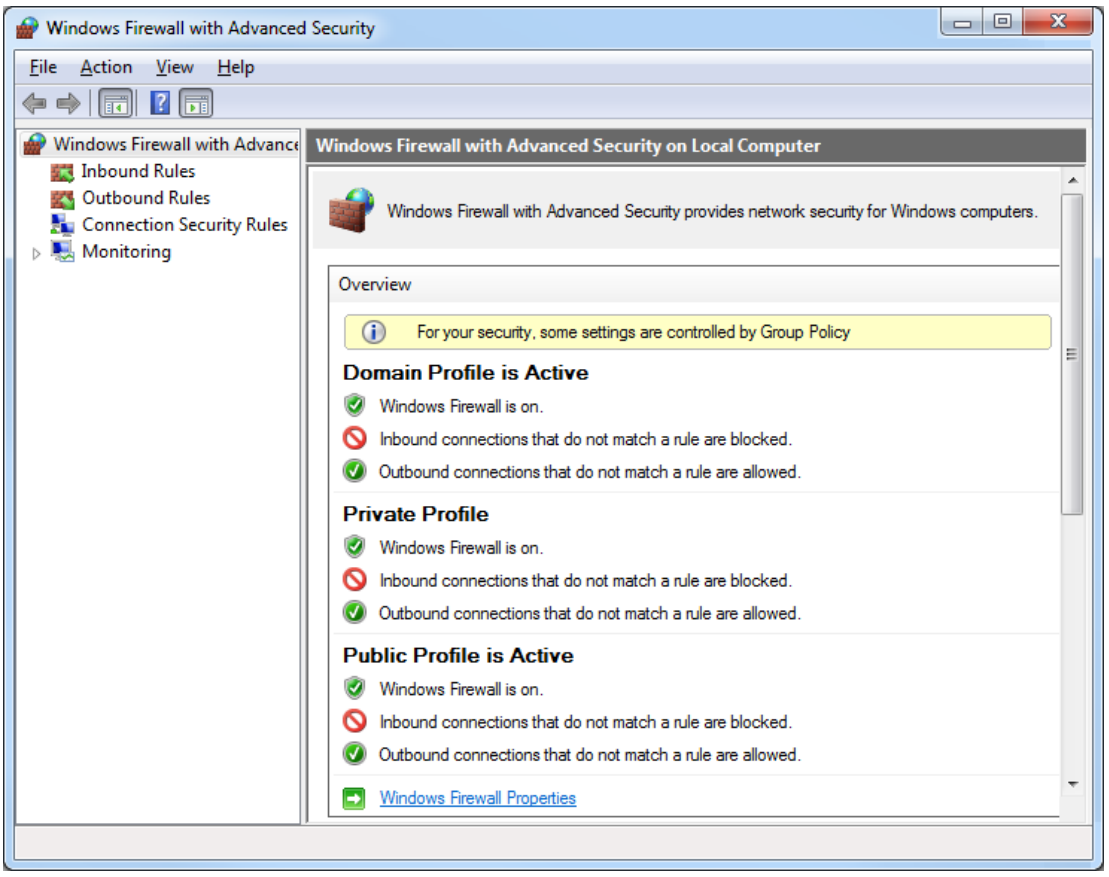

Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
For your security, some settings are managed by your system administrator.
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active domain networks:
Notification state: Notify me when Windows Firewall blocks a new program
Home or work (private) networks
Not Connected
Public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active public networks: Umbrella
Notification state: Notify me when Windows Firewall blocks a new program

2. 单击**“打开或关闭 Windows 防火墙”**。



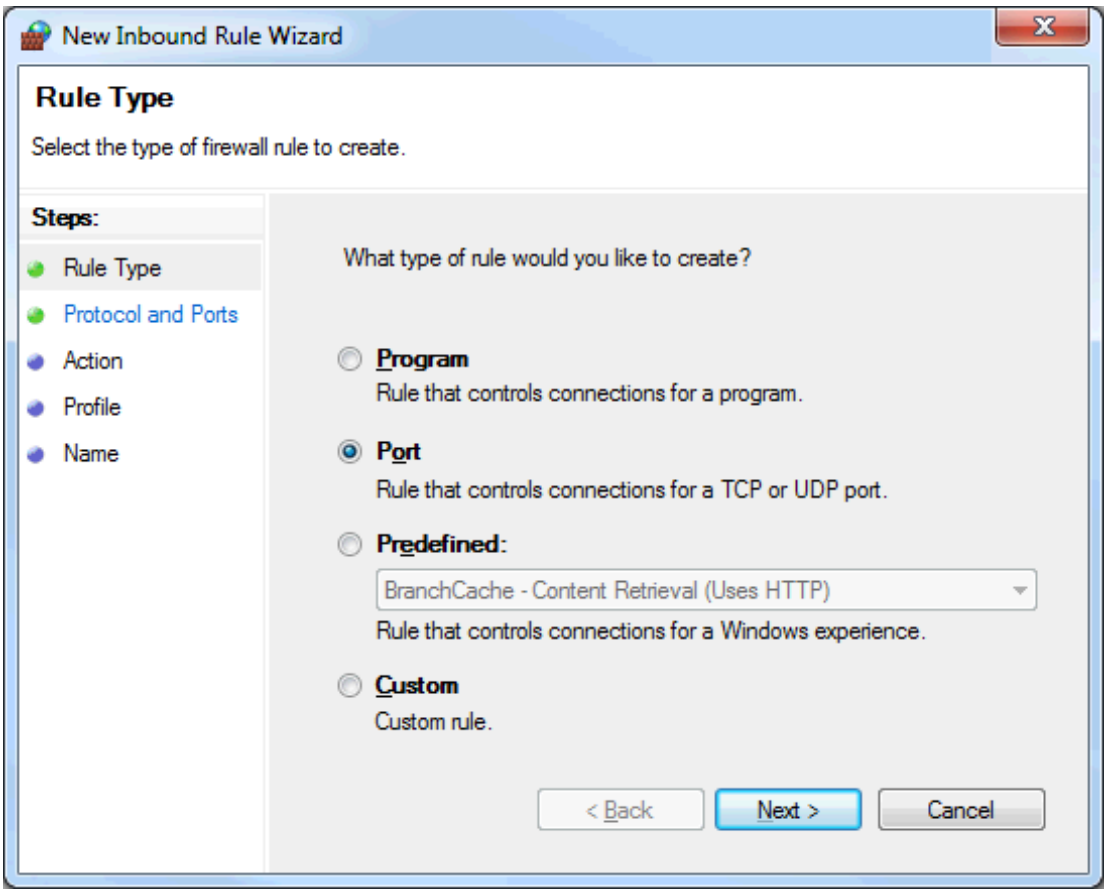
3. 验证防火墙已启用。

4. 单击**"高级设置"**。

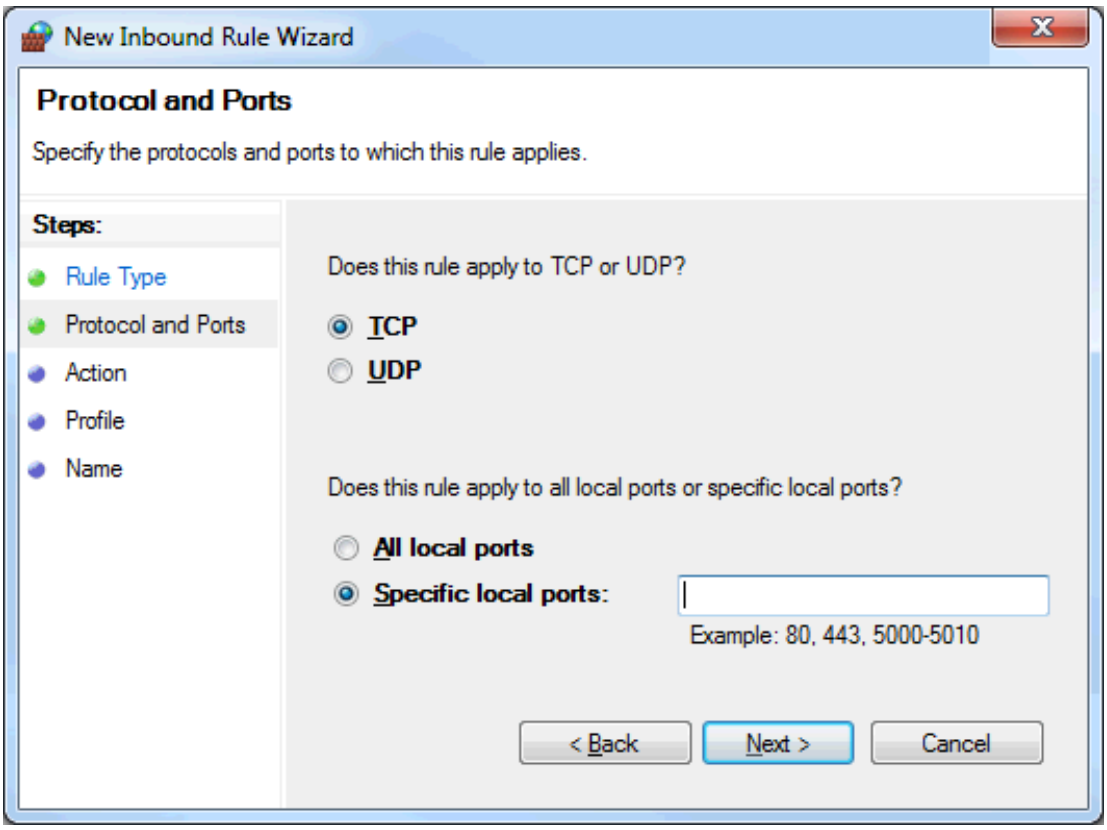


5. 单击**"Windows 防火墙属性"**。
6. 在左侧窗格中选择**"入站规则"**。
7. 在右侧操作窗格中选取**"新建规则..."**。

8. 对于规则类型，选择**"端口"**。



9. 选择**“特定的本地端口”**。



10. 输入分配给端点的 UA 端点。
11. 单击**“下一步”**。
12. 验证已选择了正确的协议。默认设置为 TCP。
13. 单击**“确定”**。
14. 如果已将多个端点分配给服务器，现在可以添加它们。完成后，单击**“确定”**退出。

设置客户端

OPC UA 客户端驱动程序通道

“通道向导”向导用于查找和标识 OPC UA 服务器，配置会话超时，以及在适用时提供用户信息。有关添加 UA 客户端通道的信息，请按照以下说明进行操作。

1. 首先，右键单击系统托盘中的**“管理”**图标启动“配置”。然后，选择**“配置”**。
2. 选择**“编辑”**|**“连接性”**|**“新建通道”**。
3. 在**“选择要创建的通道类型”**下拉列表中，选择**“OPC UA 客户端”**，然后单击**“下一步”**。
4. 在**“指定此对象的标识”**中，键入通道的名称，然后单击**“下一步”**。
5. 单击**“下一步”**即可保留**“写入优化”**中的默认设置。
6. 在**“UA 服务器”**中，将服务器的端点 URL 手动输入到**“端点 URL”**字段中。
7. 或者，用户可以单击**“浏览(...)”**图标，然后在计算机上找到端点。
   a. 验证已禁用**“使用发现 URL”**参数。
   b. 在**“发现端口”**参数中，输入在服务器计算机上创建的端点端口号。默认端口号应已分配，并与默认端点一致。

注意：浏览器将始终扫描端口 4840。因此，如果正在使用发现服务器，则无需在此字段中输入正确的端口号。

c. 如果端口号已更改，请单击**“刷新”**。

d. 定位服务器计算机。分配给 "localhost" 的端点只能在**“本地计算机”**分支下找到。

e. 展开计算机以显示可用服务器的列表，然后展开服务器并选择正确的端点。

f. 要继续使用此端点来发现 UA 服务器，请在对话框顶部的**“发现”**参数中启用**“使用发现 URL”**。这是全局更改，将影响所有其他 UA 客户端驱动程序。

g. 单击**“确定”**。端点信息将出现在 UA 服务器页面中。单击**“下一步”**。

8. 单击**“下一步”**即可保留**“UA 会话”**中的默认设置。如果需要，可在以后对其进行优化。
9. 单击**“下一步”**，使**“身份验证”**中的用户名和密码保留空白。可根据需要对其进行更改。
10. 查看**“汇总”**，然后单击**“完成”**。

OPC UA 客户端设备

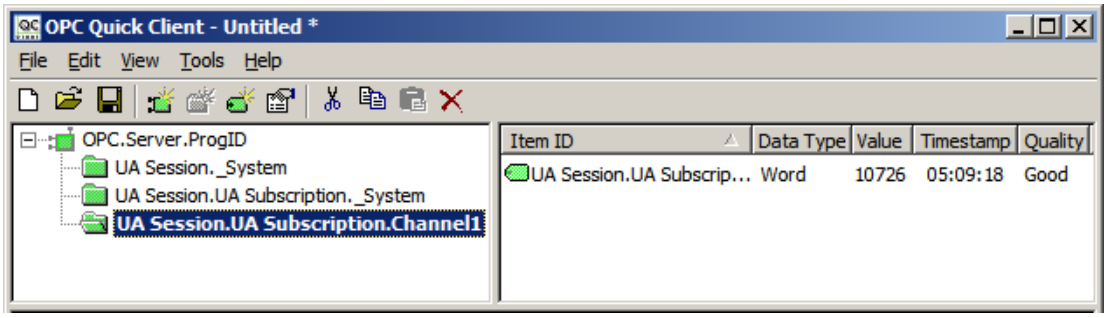
“设备向导”可指引用户设置订阅，并且支持浏览和导入 OPC UA 服务器中的项。设备中的所有项都根据所提供的设置进行更新。可将多个设备添加到同一通道，以提供不同的更新间隔和模式。有关添加 UA 客户端设备的信息，请按照以下说明进行操作。

1. 首先，选择新的通道，然后单击**“编辑”|“连接性”|“新建设备”**。
2. 在**“名称”**中，键入 OPC UA 客户端设备的名称，然后单击**“下一步”**。
3. 保留默认设置，然后单击**“下一步”**继续。如果需要，可在以后对其进行优化。
4. 在**“导入”**中，单击**“选择导入项”**。服务器的可用项应显示在浏览窗口中。如果不是，则安全配置可能不正确。有关详细信息，请参阅故障排除提示。
5. 选择所需的项，然后单击**“添加项”**或**“添加分支”**将其导入到客户端中。导入所有项后，单击**“确定”**，然后单击**“下一步”**。
6. 查看**“汇总”**，然后单击**“完成”**。导入的项将按照服务器的通道和设备名称的分组在设备下进行填充。

验证

在 OPC UA 客户端中添加的项现在可由 OPC DA 客户端浏览。为便于验证，请按以下说明进行操作。

1. 选择**“工具”|“启动 OPC Quick Client”**。将建立与本地 OPC DA 服务器的连接，并且所添加的项将填充视图。



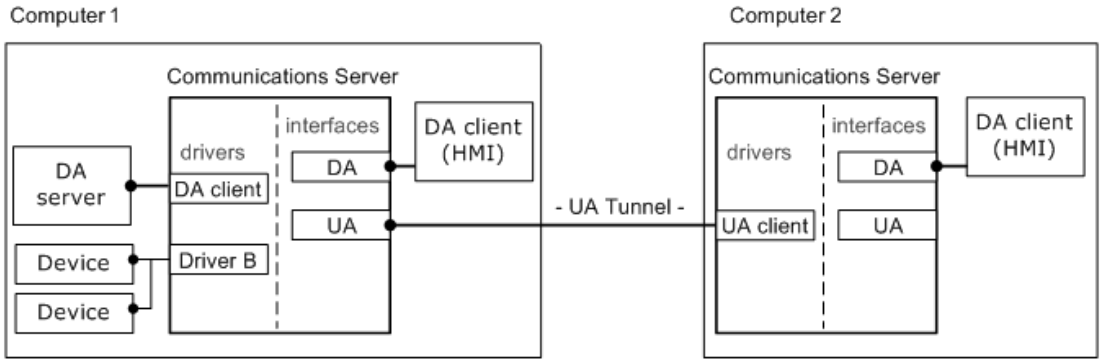
2. 浏览 OPC UA 通道中的项。然后，验证数据质量良好并且值正在更新。

连接示例

OPC UA 隧道本身不是产品，而是从现有的可用组件创建的远程连接解决方案。在隧道的服务器一侧，OPC UA 服务器在整个通信服务器产品中与 OPC DA 并存的封装接口。在隧道的客户端一侧，OPC UA 客户端驱动程序是可随其他设备通道一起添加的驱动程序插件。作为一种工具，OPC UA 配置管理器 可帮助您管理受信任的证书和 UA 服务器端点。DA 客户端驱动程序是一个附加驱动程序插件，可进一步增强 UA 隧道解决方案。由于通信服务器是一个“服务器”，因此该驱动程序提供了与其他 OPC DA 服务器的连接。

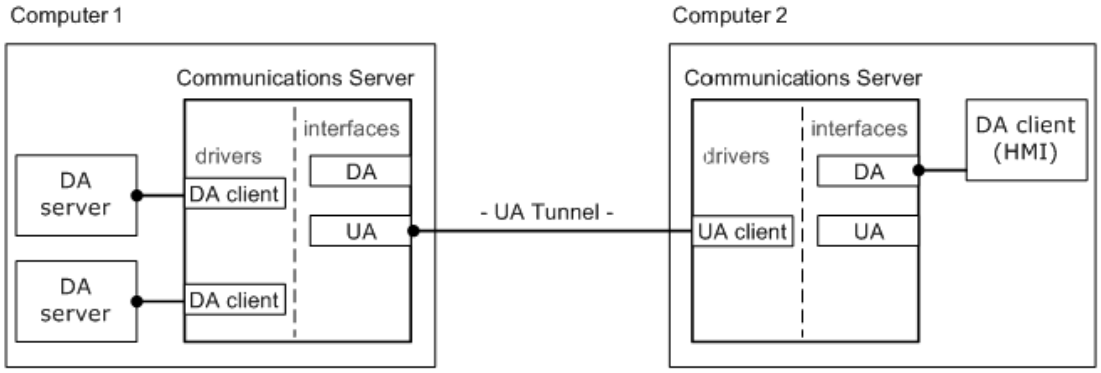
将数据从工厂车间传递到远程客户端

通信服务器为本地和远程 OPC DA 客户端提供数据。UA 隧道解决方案提供安全的远程连接。



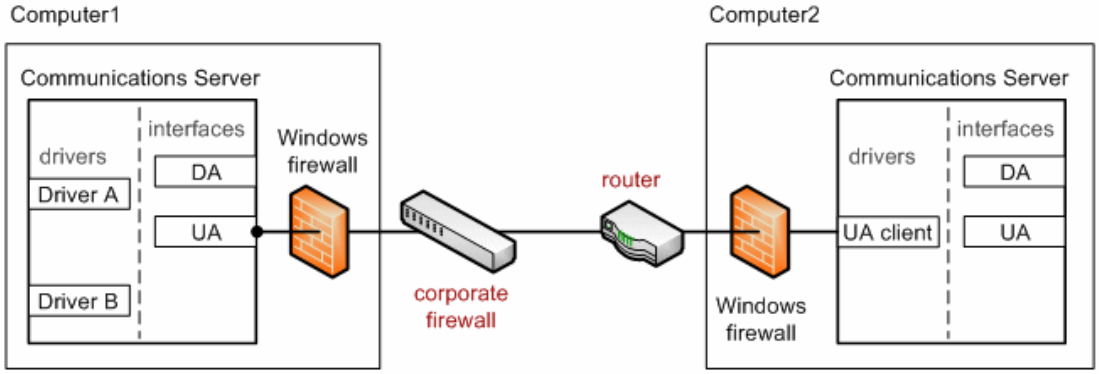
提供来自外部 DA 服务器的安全聚合数据

通信服务器使用 OPC DA 客户端驱动程序来连接 OPC DA 服务器。然后，它会以安全方式为远程 OPC DA 客户端提供聚合的数据。



防火墙和路由架构示例

除了要在公司防火墙中打开端口外，用户可能还需要允许对计算机 1 上的 Windows 防火墙启用端口例外 (如 UA 服务器端点的端口) 。计算机 2 上不应存在对 Windows 防火墙的任何更改。但是，连接中的客户端一侧的路由器可能需要打开端口 (或启用端口转发选项) 。



故障排除提示

单击链接可获取问题说明。

故障排除提示

在“设备属性”对话框中导入项时无法连接 UA 服务器

可能的原因：

1. 选择了不正确的安全配置文件。
2. 证书无效或不存在。
3. UA 服务器和/或 UA 客户端证书的有效期早于当前系统日期。

解决方案：

1. 验证通道 UA 服务器安全配置文件和消息模式配置。
2. 如果不需要安全性，则在“通道属性”对话框中选择“无”作为安全策略。
3. 执行证书交换。
4. 导入未过期的证书。
5. 重新颁发证书以生成新的未过期证书。

从 UA 客户端浏览时无法看到 UA 服务器

可能的原因：

1. “发现端口”字段中列出的端点端口不正确。
2. 端点未在 UA 服务器上启用。
3. UA 服务器接口在“项目属性”中禁用。
4. UA 服务器和端点已启用且正确。但是，尚未将更改保存到服务器运行时。

解决方案：

1. 确认已在 UA 服务器中定义了端点端口，并在“发现端口”字段中输入了正确的端口。然后，刷新视图。
2. 在 UA 服务器计算机上启动 OPC UA 配置管理器，以验证端点已启用。
3. 启动服务器配置。在**“编辑”|“项目属性”**中，检查 **OPC UA** 属性组中的“服务器接口”设置。
4. 确认**“启用”**被设置为**“是”**。
5. 从配置保存项目，并在系统提示保存对运行时所做的更改时单击**“是”**。

运行 UA 服务器的目标计算机不出现在 UA 客户端所浏览的网络中

可能的原因：

目标计算机尚未添加到网络域中。目标计算机可能仅位于工作组中，而不在域中。

解决方案：

确认 UA 服务器计算机上“UA 配置管理器”中的端点 URL。然后，在 UA 客户端驱动程序通道中手动输入端点 URL。

无法通过正确的端点 URL 连接到 UA 服务器

可能的原因：

1. 连接的客户端的企业防火墙可能仅允许通过单个端口(例如 8080) 进行连接。
2. 需要将服务器端路由器/交换机配置为将传入客户端请求转发到 UA 服务器计算机。
3. Windows 防火墙阻止来自 UA 客户端的传入请求。

解决方案：

1. 在企业防火墙中为 UA 隧道连接打开一个端口。或者，重新设置 UA 服务器上的端点端口以与企业防火墙所允许的端口相匹配。
2. 在路由器中配置端口转发。然后，UA 客户端的 URL 将使用路由器 IP 地址以及用于 UA 服务器端点的端口号(路由器中用于端口转发的端口号) 。
3. 将端点端口的例外添加到 Windows 防火墙。

连接 UA 服务器时尝试需要身份验证(用户名和密码)

可能的原因：

UA 服务器的客户端会话参数**“允许匿名登录”**已设置为**“否”**。

解决方案：

启动服务器配置，然后在树状视图中选择项目。在**“编辑”|“属性”**中，检查 OPC UA 属性组中的客户端会话设置，确认**“允许匿名登录”**设置为**“是”**。

注意：

如果需要进行身份验证，请访问“服务器管理”菜单(位于系统托盘中) 中的“用户管理器”，以设置用户名和密码。

对于通过端口转发向 UA 服务器发送请求的路由器，无法对其进行 ping 操作

可能的原因：

路由器中的默认设置可能设置为不响应 ping。

解决方案：

暂时对服务器一端的路由器启用“响应 Ping”。在成功获得 ping 响应后，禁用此设置。

没有特定于 OPC UA 的错误消息发布到事件日志

可能的原因：

OPC UA 服务器诊断未启用。

解决方案：

启动服务器配置，然后在树状视图中选择**“项目”**。选取**“编辑”|“项目属性”**。审阅服务器界面的 UA 选项卡，确认“日志诊断”设置为“是”。

事件日志消息

以下信息涉及发布到主要用户界面中“事件日志”窗格的消息。。关于如何筛选和排序“事件日志”详细信息视图，请参阅 OPC 服务器帮助。服务器帮助包含许多常见的消息，因此也应对其进行搜索。通常，其中会尽可能提供消息的类型 (信息、警告) 和故障排除信息。

帐户 '<名称>' 没有权限运行此应用程序。

错误类型：
错误

可能的原因：
当前登录用户没有足够的权限。

可能的解决方案：

1. 请用管理员帐户登录。
2. 请与系统管理员联系，以进行验证或更新权限。
3. 请验证您具备对此应用程序的应用数据目录的访问权限，或进行更正。

也可以看看：
Application Data (“应用程序数据”，见服务器帮助)，以及 Secure Deployment Guide (《安全的部署指南》) 中的 Application Data User Permissions (“应用程序数据用户权限”) 章节

UA 服务器证书已重新颁发。UA 客户端必须信任新证书才能进行连接。

错误类型：
安全

UA 客户端驱动程序证书已重新颁发。UA 服务器必须信任新证书，客户端驱动程序才能进行连接。

错误类型：
安全

UA 客户端证书 '<客户端名称>' 已被拒绝。服务器无法接受客户端的连接。

错误类型：
安全

UA 客户端证书 '<客户端名称>' 已受信任。服务器可以接受客户端的连接。

错误类型：
安全

UA 服务器证书 '<服务器名称>' 已被拒绝。“UA 客户端驱动程序”无法连接至服务器。

错误类型：
安全

UA 服务器证书 '<服务器名称>' 已受信任。“UA 客户端驱动程序”可连接至服务器。

错误类型：

安全

UA 服务器证书 '<服务器名称>' 已添加至“受信任的服务器”。“UA 客户端驱动程序”现可连接至服务器。

错误类型：
安全

UA 客户端证书 '<客户端名称>' 已添加至“受信任的客户端”。UA 服务器现在可以接受客户端的连接。

错误类型：
安全

UA 客户端证书 '<客户端名称>' 已从“受信任的客户端”中移除。UA 服务器不能接受客户端的连接。

错误类型：
安全

UA 服务器证书 '<服务器名称>' 已从“受信任的服务器”中移除。UA 客户端驱动程序无法连接至服务器。

错误类型：
安全

端点 '<url>' 已添加至 UA 服务器。

错误类型：
安全

端点 '<url>' 已从 UA 服务器中移除。

错误类型：
安全

UA 发现服务器 '<服务器名称>' 已添加。UA 服务器端点现在可以注册到此 UA 发现服务器。

错误类型：
安全

UA 发现服务器 '<服务器名称>' 已移除。UA 服务器端点不能再注册到此 UA 发现服务器。

错误类型：
安全

端点 '<url>' 已禁用。

错误类型：
安全

UA 客户端Driver 证书已导入。UA 服务器必须信任新证书，客户端驱动程序才能进行连接。

错误类型：
安全

UA 服务器证书已导入。UA 客户端必须信任新证书才能进行连接。

错误类型：
安全

端点 '<url>' 已启用。

错误类型：
安全

添加受信任的客户端

UA 客户端证书 '<证书名称>' 已添加到受信任的客户端。UA 服务器现在将接受来自客户端的连接。

移除受信任的客户端

UA 客户端证书 '<证书名称>' 已从受信任的客户端中移除。UA 服务器将不接受客户端的连接。

拒绝受信任的客户端

UA 客户端证书 '<证书名称>' 已被拒绝。服务器将不接受客户端的连接。

信任受信任的客户端

UA 客户端证书 '<证书名称>' 已被信任。服务器将接受客户端的连接。

添加受信任的服务器

UA 服务器证书 '<证书名称>' 已添加到受信任的服务器。UA 客户端驱动程序现在可以连接到服务器。

移除受信任的服务器

UA 服务器证书 '<证书名称>' 已从受信任的服务器中移除。UA 客户端驱动程序无法连接到服务器。

拒绝受信任的服务器

UA 服务器证书 '<证书名称>' 已被拒绝。UA 客户端驱动程序无法连接到服务器。

信任受信任的服务器

UA 服务器证书 '<证书名称>' 已被信任。UA 客户端驱动程序可以连接到服务器。

添加端点

已将端点 '<端点定义>' 添加到 UA 服务器。

启用端点

端点 '<端点定义>' 已启用。

禁用端点

端点 '<端点定义>' 已被禁用。

移除端点

已将端点 '<端点定义>' 从 UA 服务器中移除。

添加发现服务器

已添加发现服务器 '<证书名称>'。UA 服务器端点现在将在此发现服务器中注册。

移除发现服务器

发现服务器 '<证书名称>'已被移除。UA 服务器端点将不再注册到此发现服务器。

重新颁发客户端证书

UA 客户端驱动程序证书已重新颁发。要使客户端驱动程序能够连接，UA 服务器需要信任新证书。

重新颁发服务器证书

UA 服务器证书已重新颁发。UA 客户端需要信任新证书才能进行连接。

索引

O

U

安

帮

本

查

从

导

登

端

对

发

防

匿

启

实

事

受

添

外

网

无

先

项

信

验

移

远

运

在

帐

证

重

注