AXIS A1601 Network Door Controller

用户手册

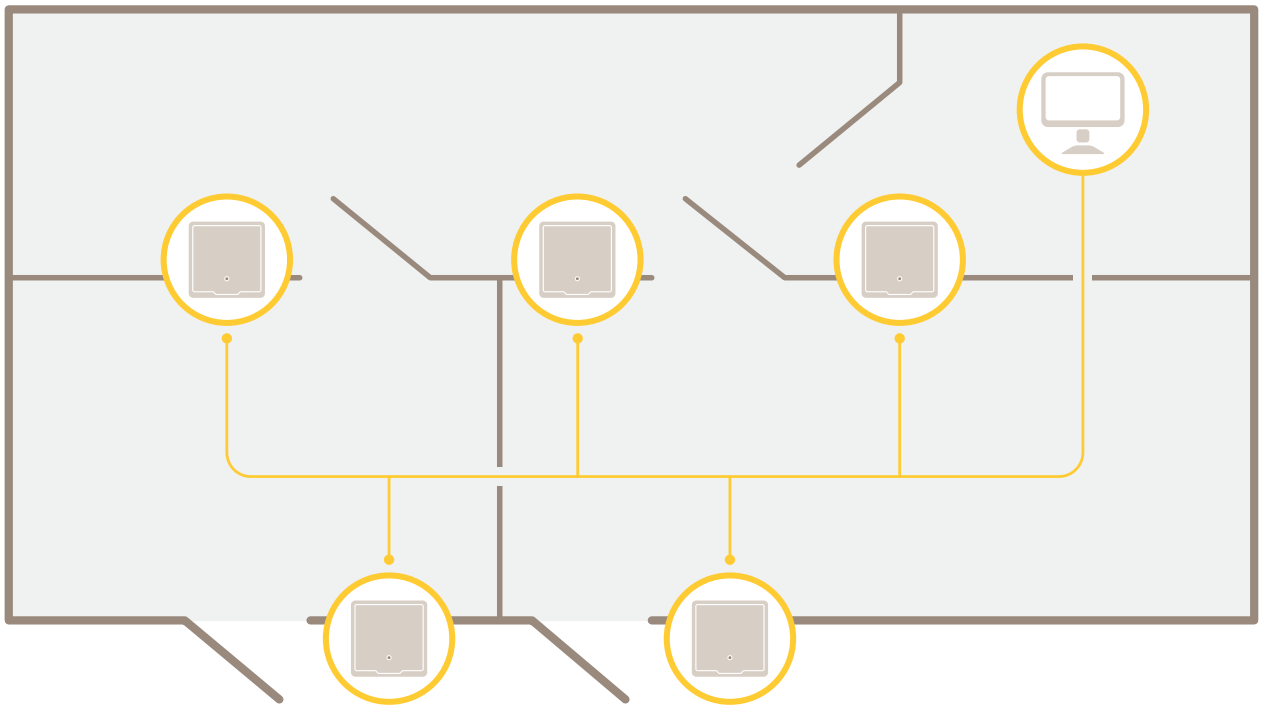
目录

解决方案概述 5
产品概览 6
在网络上查找设备 7
访问设备 7
如何通过互联网访问产品 7
安全密码 7
如何设置根密码 7
概览页面 8
系统配置 9
配置 – 分步说明 9
选择语言 9
设置日期和时间。 9
从网络时间协议 (NTP) 服务器获取日期和时间 9
手动设置日期和时间 10
从计算机上获取日期和时间 10
配置网络设置。 10
配置硬件 10
如何导入硬件配置文件 10
创建新硬件配置。 11
如何不使用外围设备创建新硬件配置 11
如何为无线锁创建新硬件配置 14
如何使用升降机控制创建新硬件配置 (AXIS A9188) 14
如何添加并设置网络外围设备 15
验证硬件连接。 15
验证控制门 15
验证控制楼层 16
配置卡和格式。 16
卡格式说明 17
卡格式： 17
字段映射 17
配置服务 18
SmartIntego 18
OSDP LED 配置文件 19
维护说明 20
事件配置 21
查看事件日志。 21
事件日志筛选器 21
配置事件日志。 21
事件日志选项 21
如何设置操作规则 21
如何添加接受者 22
如何创建时间表 23
如何设置重复 23
读卡器反馈 23
系统选项 24
安全： 24
用户 24
ONVIF 24
IP 地址过滤器 24
HTTPS 24
IEEE 802.1X 25
认证 25
网络： 26

基本 TCP/IP 设置 26
高级 TCP/IP 设置 27
SOCKS 28
QoS（服务质量） 29
SNMP 29
UPnP 29
Bonjour 29
端口和设备 30
I/O 端口 30
端口状态 30
维护 30
支持页面 30
支持概览 30
系统概览 30
日志和报告 31
高级 31
脚本 31
文件上传 31
故障排查 32
重置为出厂默认设置。 32
如何检查当前固件 32
如何升级固件 32
征兆、可能的原因和补救措施 33
规格 34
..... 34
LED 指示灯 34
按钮 34
控制按钮 34
连接器 34
网络连接器： 34
读卡器连接器 34
门连接器 36
中继连接器 36
辅助连接器 37
外部连接器 38
电源连接器 38
备份电池输入连接器 39
安全信息 40
危险等级 40
其他消息等级 40
网页界面 41
..... 41
状态： 41
设备 42
警报 42
联网 43
读卡器 43
无线锁 43
升级 44
系统 44
时间和位置 44
网络： 45
安全： 49
帐户 54
MQTT： 55
附件 57

日志 58
维护 60

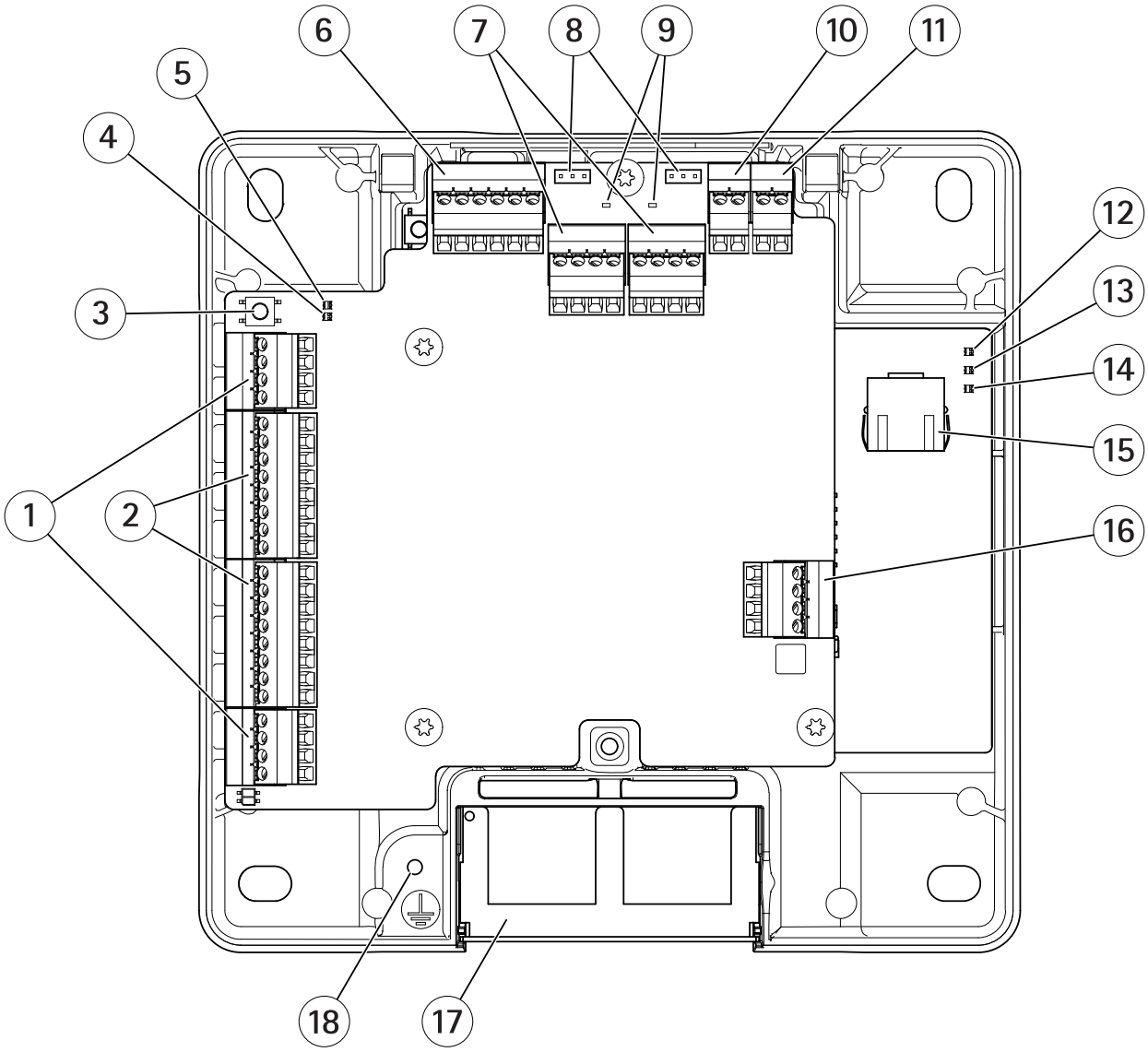
解决方案概述



网络门禁控制器可以轻松地连接到您现有的 IP 网络并由其供电，无需专用电缆。

每个网络门禁控制器都是一个智能设备，可以轻松安装在靠近门的位置。它可以供电和控制高达四个读卡器。

产品概览



1 门连接器, on page 36 (2x)
2 读卡器连接器, on page 34 (2x)
3 控制按钮, on page 34
4 读卡器过流 LED
5 继电器过流 LED
6 辅助连接器, on page 37
7 中继连接器, on page 36 (2x)
8 继电器跳线（2 个）
9 继电器 LED（2 个）
10 备份电池输入连接器, on page 39
11 电源连接器, on page 38
12 LED 电源指示灯
13 状态 LED
14 LED 网络指示灯
15 网络连接器：, on page 34
16 外部连接器, on page 38
17 双面电缆盖板
18 接地位置

在网络上查找设备

若要在网络中查找安讯士设备并为它们分配 Windows® 中的 IP 地址，请使用 AXIS IP Utility 或 AXIS Device Manager。这两种应用程序都是免费的，可以从*axis.com/support* 上下载。

有关如何查找和分配 IP 地址的更多信息，前往*如何分配一个 IP 地址和访问您的设备*。

访问设备

1. 打开浏览器并输入安讯士设备的 IP 地址或主机名。
   如果您不知道 IP 地址，请使用AXIS IP Utility 或AXIS Device Manager 在网络上查找设备。
2. 输入用户名和密码。如果您是首次访问设备，则必须设置 root 用户密码。参见.
3. 设备网页将在您的浏览器中打开。开始页面称为“概览”页。

如何通过互联网访问产品

网络路由器允许私有网络 (LAN) 上的产品共享与互联网的单一连接。这通过将网络通信从私有网络转至互联网来实现。

多数路由器被预配置为阻止从公共网络（互联网）访问私有网络 (LAN) 的尝试。

如果 Axis 产品位于内联网 (LAN) 上，并且您希望它可以从 NAT（网络地址转换器）路由器的另一端 (WAN) 使用，则打开 **NAT 遍历**。在正确配置 NAT 穿越的情况下，NAT 路由器中流向外部 HTTP 端口的 HTTP 流量都会转发给产品。

如何打开 NAT 遍历功能

- 转到**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Network（网络）** > **TCP/IP** > **Advanced（高级）**。
- 单击**启用**。
- 手动配置 NAT 路由器以允许从互联网访问。

注意

- 在此上下文中，“路由器”指任意网络路由设备（如 NAT 路由器、网络路由器、互联网网关、宽带路由器、宽带共享设备）或软件（如防火墙）。
- 为使 NAT 遍历正常工作，其必须受路由器支持。该路由器还要支持 UPnP®。

安全密码

重要

请使用安全超文本传输协议 (HTTPS)（默认已启用）通过网络设置密码或其他敏感配置。安全超文本传输协议 (HTTPS) 可启用安全且经过加密的网络连接，从而保护密码等敏感数据。

设备密码是对数据和服务的主要保护。安讯士设备不会强加密码策略，因为它们可能会在不同类型的安装中使用。

为保护您的数据，我们强烈建议您：

- 使用至少包含 8 个字符的密码，而且密码建议由密码生成器生成。
- 不要泄露密码。
- 定期更改密码，至少一年一次。

如何设置根密码

要访问 Axis 产品，您必须为默认管理员用户 **root** 设置密码。此操作在**配置根密码**对话框中完成，首次访问产品时会打开该对话框。

为防止发生网络窃听，可通过加密的 HTTPS 连接设置根密码，这需要 HTTPS 证书。HTTPS (Hypertext Transfer Protocol over SSL) 是一种用于为 Web 浏览器和服务器之间的通信加密的协议。HTTPS 证书确保信息交换经过加密处理。参见 *HTTPS, on page 24*.

默认管理员用户名 **root** 是永久性的，无法删除。如果 root 的密码丢失，则产品必须重置为出厂默认设置。参见 *重置为出厂默认设置。, on page 32*.

若要设置密码，请直接在对话框中输入。

概览页面

产品网页中的“概览”页面显示有关门禁控制器名称、MAC 地址、IP 地址和固件版本的信息。您还能够在此页面上确定网络上的门禁控制器。

初次访问 Axis 产品时，“概览”页面将提示您配置硬件、设置日期和时间、配置网络设置。有关配置系统的详细信息，请参见 *配置 – 分步说明, on page 9*。

若要从产品的其他网页返回“概览”页面，请单击菜单栏中的**概览**。

系统配置

若要打开产品的设置页面，单击概览页面右上角的**设置**。

Axis 产品可以由管理员配置。关于用户和管理员的更多信息，请参见 *page 24*。

配置 – 分步说明

在开始使用门禁控制系统之前，您应该完成以下设置步骤：

1. 如果英语不是您的母语，您可能希望产品网页使用其他语言。参见 *选择语言, on page 9*.
2. 设置日期和时间。参见*page 9*.
3. 配置网络设置。参见*page 10*.
4. 配置门禁控制器和连接的设备，如读卡器、锁和请求退出 (REX) 设备。参见 *配置硬件, on page 10*.
5. 验证硬件连接。参见*page 15*.
6. 配置卡和格式。参见*page 16*.

有关维护建议的信息，请参见 *维护说明, on page 20*。

选择语言

产品网页的默认语言是英语，但可以切换到产品固件中包含的不同语言。有关新可用固件的信息，请访问 *www.axis.com*

您可以在一个产品网页中切换语言。

若要切换语言，请单击语言下拉列表 并选择一种语言。产品网页和帮助页都以所选的语言显示。

注意

- 当您切换语言时，日期格式也将更改为所选语言的常用格式。正确的格式显示在数据字段中。
- 如果您将产品重置为出厂默认设置，产品网页将切换回英语。
- 如果您恢复或重启产品，或升级固件，产品网页将继续使用所选语言。

设置日期和时间。

若要设置 Axis 产品的日期和时间，请转到**设置 > 日期和时间**。

您可以通过以下方式设置日期和时间：

- 从网络时间协议 (NTP) 服务器获取日期和时间。参见*page 9*.
- 手动设置日期和时间。参见*page 10*.
- 从计算机上获取日期和时间。参见*page 10*.

当前的控制器时间显示门禁控制器当前的日期和时间（24 小时制）。

相同的日期和时间选项也会在“系统选项”页面提供。转到Setup（**设置**）> Additional Controller Configuration（**其他控制器配置**）> System Options（**系统选项**）> Date & Time（**日期和时间**）。

从网络时间协议 (NTP) 服务器获取日期和时间

1. 转到**设置 > 日期和时间**。
2. 从下拉列表中选择您的**时区**。
3. 如果您所在的地区使用夏令时，请选择**随夏令时调整**。
4. 选择**与 NTP 同步**。

5. 选择默认的 DHCP 地址，或输入 NTP 服务器的地址。
6. 单击**Save（保存）**。

在与 NTP 服务器同步时，日期和时间会不断更新，因为数据从 NTP 服务器推送。有关 NTP 设置的信息，请参见 *NTP 配置, on page 27*。
如果为 NTP 服务器使用主机名称，必须配置 DNS 服务器。参见 *DNS 配置, on page 27*.

手动设置日期和时间

1. 转到**设置 > 日期和时间**。
2. 如果您所在的地区使用夏令时，请选择**随夏令时调整**。
3. 选择**手动设置日期和时间**。
4. 输入所需的日期和时间。
5. 单击**Save（保存）**。

在手动设置日期和时间时，日期和时间设置一次，且不会自动更新。这意味着，如果需要更新日期和时间，更改必须手动进行，因为没有与外部 NTP 服务器的连接。

从计算机上获取日期和时间

1. 转到**设置 > 日期和时间**。
2. 如果您所在的地区使用夏令时，请选择**随夏令时调整**。
3. 选择**手动设置日期和时间**。
4. 单击**立即同步并保存**。

在使用计算机时间时，日期和时间与计算机时间同步一次，且不会自动更新。这意味着，如果您更改了管理系统的日期或时间，则应该再次同步。

配置网络设置。

若要配置基本网络设置，请转到**设置 > 网络设置**或转到**设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 基本**。

有关侦网络设置的更多信息，请参见 *网络：, on page 26*。

配置硬件

在完成硬件配置前，您可以将读卡器、锁及其他设备连接到 Axis 产品。不过，如果首先完成硬件配置，连接设备会更轻松。这是因为配置完成时会提供硬件引脚图。硬件引脚图指导如何将设备连接到引脚，可以用作维护参考表。有关维护说明，请参见 *page 20*。

如果是首次配置硬件，请选择以下方法之一：
- 导入硬件配置文件。参见*page 10*.
- 创建新硬件配置。参见*page 11*.

注意

如果产品的硬件以前未配置或者已被删除，**硬件配置**将在“概览”页的通知面板中显示。

如何导入硬件配置文件

通过导入硬件配置文件，可以更快地完成 Axis 产品的硬件配置。

将文件从一个产品导出然后再导入到其他产品，可以为相同的硬件设置建立多个副本，而无需不断重复相同步骤。您还可以将导出的文件存储为备份，使用它们来还原之前的硬件配置。有关详细信息，请参见 *如何导出硬件配置文件, on page 11*。

导入硬件配置文件：
1. 转到**设置 > 硬件配置**。

2. 单击**导入硬件配置**，或者，如果硬件配置已存在，单击**重置并导入硬件配置**。
3. 在显示的文件浏览器对话框中，找到并选择您的计算机上的硬件配置文件 (*.json)。
4. 单击 OK（**确定**）。

如何导出硬件配置文件

Axis 产品的硬件配置可以导出，用于为同一个硬件设置建立多个副本。您还可以将导出的文件存储为备份，使用它们来还原之前的硬件配置。

注意

楼层的硬件配置不能导出。

硬件配置导出中不包括无线锁设置。

导出硬件配置文件：

1. 转到**设置 > 硬件配置**。
2. 单击**导出硬件配置**。
3. 根据浏览器，您可能需要完成一个对话框流程来完成导出。
   除非另外指定，否则导出的文件 (*.json) 将保存在默认下载文件夹中。您可以在 Web 浏览器的用户设置中选择下载文件夹。

创建新硬件配置。

请根据您的要求按照说明操作：

- *如何不使用外围设备创建新硬件配置, on page 11*
- *如何为无线锁创建新硬件配置, on page 14*
- *如何使用升降机控制创建新硬件配置 (AXIS A9188), on page 14*

如何不使用外围设备创建新硬件配置

1. 转到**设置 > 硬件配置**，单击**开始新硬件配置**。
2. 输入 Axis 产品名称。
3. 选择连接的门数量，然后单击**下一步**。
4. 根据您的要求配置门监视器（门位置传感器）和锁，然后单击**下一步**。有关可用选项的更多信息，请参见 *如何配置门监视器和锁, on page 11*。
5. 配置将使用的读卡器和 REX 设备并单击**完成**。有关可用选项的更多信息，请参见 *如何配置读卡器和 REX 设备, on page 13*。
6. 单击 Close（**关闭**）或单击链接查看硬件引脚图。

如何配置门监视器和锁

在新硬件配置中选择了门选项后，您可以配置门监视器和锁。

1. 如果要使用门监视器，选择**门监视器**，然后选择与门监视器的电路连接方式匹配的选项。
2. 如果门锁应在门打开后立即锁定，请选择**门打开后立即取消访问时间**。
   如果您想要延迟重新锁定，在**重新锁定时间**中以毫秒为单位设置延迟时间。
3. 指定门监视器时间选项，如果不使用门监视器，则指定锁时间选项。
4. 选择与锁的电路连接方式匹配的选项。
5. 如果要使用锁监视器，选择**门监视器**，然后选择与锁监视器的电路连接方式匹配的选项。
6. 如果应监控读卡器、REX 设备和门监视器的输入连接，请选择**启用监控输入**。
   有关详细信息，请参见 *如何使用监控输入, on page 13*。

注意

- 大多数锁、门监视器和读卡器选项都可以更改，无需重置和开始新硬件配置。转到**设置 > 硬件重新配置**。
- 每个门禁控制器可以连接一个锁监视器。所以，如果您使用双锁门，只有一个锁可以有锁监视器。如果两个门连接到同一个门禁控制器，则无法使用锁监视器。

关于门监视器和时间选项

提供以下门监视器选项：

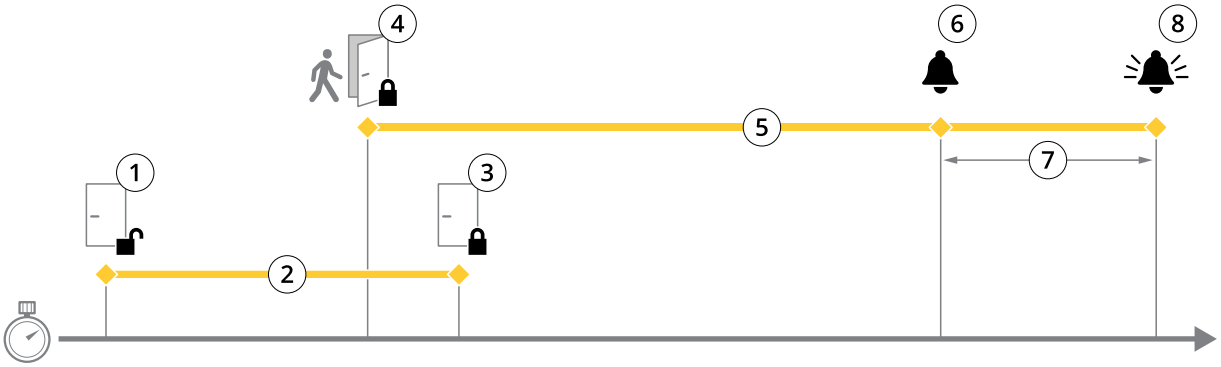
- **门监视器** – 默认选择。每个门有其自己的门监视器，将在门被强制打开或打开时间过长时（举例）发出信号。如果不使用门监视器，则取消选择。
- **开路 = 关闭门** – 如果门监视器电路常开则选择此项。当电路关闭时，门监视器向门发出打开信号。当电路打开时，门监视器向门发出关闭信号。
- **开路 = 打开门** – 如果门监视器电路常闭则选择此项。当电路打开时，门监视器向门发出打开信号。当电路关闭时，门监视器向门发出关闭信号。
- **门打开后立即取消访问时间** – 选择此选项可防止尾随。门监视器一指示门已打开，锁便会被锁定。

始终提供以下门时间选项：

- **访问时间** – 设置在授予访问权限后门应保持解锁的秒数。在门已打开或达到设定时间前门会一直保持解锁状态。门将在关闭时锁定，无论访问时间是否过期。
- **长访问时间** – 设置在授予访问权限后门应保持解锁的秒数。长访问时间覆盖已设置的访问时间，并为选择了长访问时间的用户启用。

选择**门监视器**后以下门时间选项将可用：

- **打开时间太长** – 设置允许门保持打开状态的秒数。如果门在达到设定时间时仍处于打开状态，将触发门打开时间太长警报。请设置一个操作规则以配置打开时间太长应触发的操作。
- **预报警时间** – 预报警是在达到过长打开时间前触发的警告信号。它将通知管理员，并根据操作规则的设置方式提醒进入门的人员门需要关闭以避免发起门打开时间太长警报。请设置系统应在触发门打开时间太长警报之前多少秒发出预报警警告信号。若要禁用预报警，将预报警时间设置为 0。



1 *访问已授权 – 锁解锁*
2 *访问时间*
3 *未执行操作 – 锁上锁*
4 *已执行操作（门已打开）– 锁上锁或保持解锁状态直到门关闭*
5 *打开时间太长*
6 *预报警停止*
7 *预报警时间*
8 *打开时间太长 – 报警停止*

有关如何设置响应规则的更多信息，请参见 *如何设置操作规则, on page 21*。

关于锁选项

提供以下锁电路选项：

- **继电器** – 只能在每个门禁控制器的一个锁上使用。如果有两个门连接至门禁控制器，继电器只能用于第二个门的锁。
- **无** – 仅适用于 Lock 2。选择此项可仅使用一把锁。

以下锁监视器选项可用于单门配置：

- **锁监视器** – 选择此选项让锁监视器控制可用。然后选择应被监视的锁。锁监视器只能用于双锁门，如果两个门已连接到门禁控制器则无法使用。

– **开路 = 锁定** – 如果锁监视器电路常闭则选择此项。当电路关闭时，锁监视器向门发出解锁信号。当电路打开时，锁监视器向门发出锁定信号。

– **开路 = 解锁** – 如果锁监视器电路常开则选择此项。当电路打开时，锁监视器向门发出解锁信号。当电路关闭时，锁监视器向门发出锁定信号。

如何配置读卡器和 REX 设备

在新硬件配置中配置了门监视器和锁后，您可以配置读卡器和请求退出 (REX) 设备。

1. 如果要使用读卡器，选择复选框，然后选择与读卡器的通信协议匹配的选项。
2. 如果要使用按钮、传感器或推杆等 REX 设备，选择复选框，然后选择与 REX 设备的电路连接方式匹配的选项。
   如果 REX 信号不影响开门（例如，对于具有机械手柄或推杆的门），选择 **REX 不解锁门**。
3. 如果将多个读卡器或 REX 设备连接至门禁控制器，再次执行上述两个步骤，直至每个读卡器或 REX 设备具有正确的设置。

关于读卡器和 REX 设备选项

提供以下读卡器选项：

- **Wiegand** – 为使用 Wiegand 协议的读卡器选择此项。然后选择读卡器支持的 LED 控制。具有单 LED 控制的读卡器通常在红色和绿色之间切换。具有双 LED 控制的读卡器其红色和绿色 LED 使用不同的电线。这意味着对 LED 进行相互独立的控制。两个 LED 都打开时，灯光看上去呈琥珀色。请参见制造商的信息了解读卡器支持哪种 LED 控制。
- **OSDP，RS485 半双工** – 为具有半双工支持的 RS485 读卡器选择此项。请参见制造商的信息了解读卡器支持哪种协议。

提供以下 REX 设备选项：

- **低电平有效** – 如果激活 REX 设备将关闭电路则选择此项。
- **高电平有效** – 如果激活 REX 设备将打开电路则选择此项。
- **REX 不解锁门** – 如果 REX 信号不影响开门（例如，对于具有机械手柄或推杆的门），则选择此项。只要用户在访问时间内打开门，便不会触发门强制打开警报。如果当用户激活 REX 设备时门应自动解锁，则取消选择此项。

注意

大多数锁、门监视器和读卡器选项都可以更改，无需重置和开始新硬件配置。转到**设置 > 硬件重新配置**。

如何使用监控输入

有关门禁控制器和门监视器之间的连接状态的监控输入报告。如果连接中断，将激活事件。

使用监控输入：

1. 在使用的监控输入端安装线尾电阻。请参见 *page 36* 上的连接图。
2. 转到**设置 > 硬件重新配置**，然后选择**启用监控输入**。您还可以在硬件配置过程中启用监控输入。

关于监控输入的兼容性

以下功能支持监控输入：

- 门监视器。参见 *门连接器, on page 36*.

如何为无线锁创建新硬件配置

1. 转到**设置 > 硬件配置**，单击**开始新硬件配置**。
2. 输入 Axis 产品名称。
3. 在外围设备列表中，选择无线网关的制造商。
4. 如果您希望连接有线门，选择 **1 个门**复选框并单击**下一步**。如果未加入门，单击**完成**。
5. 根据所显示的锁制造商，按照下列选项之一继续操作：
   - ASSA Aperio：单击链接查看硬件引脚图，或单击“Close（关闭）”并转到“Setup（设置）> Hardware Reconfiguration（硬件重新配置）”完成配置，请参见 *添加 Assa Aperio™ 门和设备, on page 14*。
   - SmartIntego：单击链接查看硬件引脚图，或单击“Click here to select wireless gateway and configure doors（单击此处选择无线网关并配置门）””，完成配置，请参见 *如何配置 SmartIntego, on page 18*。

添加 Assa Aperio™ 门和设备

在向系统添加无线门前，需要先使用 Aperio PAP（Aperio 编程应用程序工具）将其与连接的 Assa Aperio 通讯集线器配对。

添加无线门：

1. 转到**设置 > 硬件重新配置**。
2. 在“无线门和设备”下，单击**添加门**。
3. 在**门名称**字段中：输入一个描述性名称。
4. 在**锁定**下的 ID 字段中：输入您要添加的设备的六位字符长的地址。设备地址打印在产品标签上。
5. 或者，在**门位置传感器**下：选择**内置门位置传感器**或**外部门位置传感器**。

注意

如果使用外部门位置传感器 (DPS)，请在配置前确保 Aperio 锁定设备支持门处理状态检测。

6. 或者，在**门位置传感器**下的 ID 字段中：输入您要添加的设备的六位字符长的地址。设备地址打印在产品标签上。
7. 单击 **Add（添加）**。

如何使用升降机控制创建新硬件配置 (AXIS A9188)

重要

在创建 HW 配置前，您需要在 AXIS A9188 Network I/O Relay Module 中添加用户。转到 A9188 网页界面 > **首选项 > 其他设备配置 > 基本设置 > 用户 > 添加 > 用户设置**。

注意

每个 Axis Network Door Controller 最多可以配置 2 个 AXIS 9188 Network I/O Relay Module

1. 在门禁控制器的网页中，转到**设置 > 硬件配置**，单击**开始新硬件配置**。
2. 输入 Axis 产品名称。
3. 在外围设备列表中，选择**升降机控制**来加入 AXIS A9188 Network I/O Relay Module 并单击**下一步**。
4. 为连接的读卡器输入一个名称。
5. 选择使用的读卡器协议并单击**完成**。
6. 单击“Network Peripherals（网络外设）”完成配置，请参见 *如何添加并设置网络外围设备, on page 15*；或单击链接跳转至硬件引脚图。

如何添加并设置网络外围设备

重要

- 在设置网络外围设备前，需要在 AXIS A9188 Network I/O Relay Module 中添加一位用户。转到 AXIS A9188 网页界面 > **首选项 > 其他设备配置 > 基本设置 > 用户 > 添加 > 用户设置**。
- 请勿添加另一个 AXIS A1001 Network Door Controller 作为网络外围设备。

1. 转到**设置 > 网络外围设备**以添加一个设备
2. 在**已发现设备**下找到你的设备。
3. 单击**添加此设备**
4. 为设备输入一个名称
5. 输入 AXIS A9188 用户名和密码
6. 单击 **Add（添加）**。

注意

你可以通过在**手动添加设备**对话框中输入 MAC 地址或 IP 地址来手动添加网络外围设备。

重要

如果你想要删除某个时间表，首先请确保网络 I/O 继电器模块未使用此时间表。

如何设置网络外围设备中的 I/O 和继电器

重要

在设置网络外围设备前，你需要在 AXIS A9188 Network I/O Relay Module 中添加一位用户。转到 AXIS A9188 网页界面 > **首选项 > 其他设备配置 > 基本设置 > 用户 > 添加 > 用户设置**。

1. 转到**设置 > 网络外围设备**并单击**添加设备**行。
2. 选择将哪些 I/O 和继电器设置为楼层。
3. 单击**设置为楼层**并输入一个名称。
4. 单击 **Add（添加）**。

验证硬件连接。

硬件安装和配置完成后，在门禁控制器生命周期内的不同时间，您都可以验证连接的门监视器、网络 I/O 继电器模块、锁和读卡器的功能。

若要验证配置、访问验证控制，请转到**设置 > 硬件连接验证**。

验证控制门

- **门状态** – 验证门监视器、门警报和锁的当前状态。单击**获取当前状态**。
- **锁** – 手动触发锁。主锁和辅助锁（如果有）都将受到影响。单击**锁定**或**解锁**。
- **锁定** – 手动触发锁以授予访问权限。仅主锁将受到影响。单击**访问**.
- **读卡器：反馈** – 验证不同命令的读卡器反馈，例如，声音和 LED 信号。选择命令，然后单击**测试**。哪些反馈类型可用取决于读卡器。有关详细信息，请参见 *读卡器反馈, on page 23*。另请参见制造商的说明。
- **读卡器：篡改** – 获取有关末次篡改尝试的信息。在阅读器已安装的情况下，会登记首次篡改尝试。单击**获取末次篡改**。
- **读卡器：刷卡** – 获取有关末次所刷卡或读卡器接受的其他用户令牌类型的信息。单击**获取最后一个凭据**。
- **REX** – 获取有关末次提出设备退出请求 (REX) 的信息。单击**获取末次 REX**。

验证控制楼层

- **楼层状态** – 验证楼层访问的当前状态。单击**获取当前状态**。
- **楼层锁定和解锁** – 手动触发楼层访问。主锁和辅助锁（如果有）都将受到影响。单击**锁定**或**解锁**。
- **楼层访问** – 手动授予对楼层的临时访问权限。仅主锁将受到影响。单击**访问**.
- **电梯读卡器：反馈** – 验证不同命令的读卡器反馈，例如，声音和 LED 信号。选择命令，然后单击**测试**。哪些反馈类型可用取决于读卡器。有关详细信息，请参见 *读卡器反馈, on page 23*。另请参见制造商的说明。
- **电梯读卡器：篡改** – 获取有关末次篡改尝试的信息。在阅读器已安装的情况下，会登记首次篡改尝试。单击**获取末次篡改**。
- **电梯读卡器：刷卡** – 获取有关末次所刷卡或读卡器接受的其他用户令牌类型的信息。单击**获取最后一个凭据**。
- REX – 获取有关末次提出设备退出请求 (REX) 的信息。单击**获取末次 REX**。

配置卡和格式。

门禁控制器有几个预定义的常用卡格式，您可以直接使用，也可以根据需要进行修改。您还可以创建自定义的卡格式。每个卡格式都有一组不同的规则——字段映射，用于确定卡上存储的信息如何安排。通过定义卡格式，您告知系统如何解释控制器从读卡器获取的信息。有关读卡器支持哪些卡格式的信息，请参见制造商的说明。

启用卡格式：

1. 转到**设置 > 配置卡和格式**。
2. 选择一个或多个与连接的读卡器使用的卡格式匹配的卡格式。

创建新的卡格式：

1. 转到**设置 > 配置卡和格式**。
2. 单击**添加卡格式**。
3. 在**添加卡格式**对话框中，输入卡格式的名称、说明和位长度。参见 *卡格式说明, on page 17*.
4. 单击**添加字段映射**，在字段中输入所需信息。参见 *字段映射, on page 17*.
5. 若要添加多个字段映射，请重复上述步骤。

若要展开Card formats（卡格式）列表中的项目并查看卡格式说明和字段映射，请单击 ▶。

若要编辑卡格式，请单击 ,255mm,sfx)=″graphics:graphic22C8DF706A81C282C5E770119D01267C″，根据需要更改卡格式说明和字段映射。然后单击**保存**。

若要删除Edit card format（编辑卡格式）或Add card format（添加卡格式）对话框中的字段映射，请单击 ,255mm,sfx)=″graphics:graphicB4C819F24CDC47C362364056DF7FE71C″

若要删除卡格式，请单击 ,255mm,sfx)=″graphics:graphicB4C819F24CDC47C362364056DF7FE71C″。

重要

- 如果门禁控制器配置了至少一个读卡器，那么您只能启用和禁用卡格式。请参见 *配置硬件, on page 10*和 *如何配置读卡器和 REX 设备, on page 13*。
- 具有相同位长度的两个卡格式不能同时处于活动状态。例如，如果您定义了两个 32 位的卡格式，“格式 A”和“格式 B”，并且启用了“格式 A”，那么如果不先禁用“格式 A”则无法启用“格式 B”。
- 如果未启用卡格式，您可以使用**仅原始卡**和**原始卡和 PIN** 识别类型来识别卡并授予用户访问权限。不过，我们不建议使用此方法，因为不同的读卡器制造商或读卡器设置可能生成不同的卡原始数据。

卡格式说明

- **名称**（必需）– 输入一个描述性名称。
- **说明** – 根据需要输入其他信息。此信息仅在**编辑卡格式**和**添加卡格式**对话框中可见。
- **位长度**（必需）– 输入卡格式的位长度。必须是从 1 到 1000000000 的数字。

卡格式：

此功能仅供专家使用。一旦开启 Card format（卡片格式）：

- 如果您使用 37 位凭证，则最后 5 位将被移除。
- 如果您使用 64 位凭证（QR 码），则前 24 位序列将被移除。

您可以使用示例数据或读卡器来查看凭证。

1. 转到 Advanced（高级）> Card format（卡格式）。
2. 阅读警告并单击 I understand（我理解）以启用 Card format（卡格式）。
3. 在 Reader data visualization（读卡器数据可视化）下拉菜单中选择您的读卡器。
4. 单击 Get reader data（获取读卡器数据）或 Use sample data（使用示例数据）以生成卡片输出。该设置将应用于设备上的所有持卡人。
5. 开启 Trim reader data（修剪读卡器数据）以移除卡片凭证的末端位。
6. 单击**启用**。

字段映射

- **名称**（必需）– 输入无间隙的字段映射名称，例如，`OddParity`。
  常见的字段映射的示例包括：
  - `Parity` – 校验位用于错误侦测。校验位通常被添加到二进制代码字符串的开头或结尾，指示位数是偶数还是奇数。
  - `EvenParity` – 偶数校验位确保字符串中的位数是偶数。值为 1 的位会计算在内。如果计数已为偶数，则奇偶校验位值设为 0。如果计数为奇数，则偶校验位值设为 1，使总计数变为偶数。
  - `OddParity` – 奇数校验位确保字符串中的位数是奇数。值为 1 的位会计算在内。如果计数已经是奇数，则将奇偶校验位的值设为 0。如果计数为偶数，则校验位设为 1，使总计数变为奇数。
  - `FacilityCode` – 设施代码有时用于验证令牌是否与有序的终端用户凭证批次相匹配。在传统门禁系统中，设备代码用于降级验证，允许使用凭证批次的员工进入，且站点代码编码相匹配。此字段映射名称区分大小写，对于要对设施代码进行验证的产品是必需的。
  - `CardNr` – 卡号或用户 ID 是门禁系统中常验证的内容。此字段映射名称区分大小写，对于要对卡号进行验证的产品是必需的。
  - `CardNrHex` – 卡号二进制数据在产品中被编码为十六进制小写数字。其主要用于对您为何没有从读卡器收到预期的卡号进行故障排查。
- Range（必需）– 输入字段映射的位范围，例如，1、2–17、18–33、34。
- Encoding（必需）– 选择每个字段映射的编码类型。
  - BinLE2Int – 二进制数据按从小到大的位顺序编码为整数。整数意味着需要是一个完整数（无小数）。按从小到大的位顺序意味着第一个位最小（最不重要）。
  - BinBE2Int – 二进制数据按从大到小的位顺序编码为整数。整数意味着需要是一个完整数（无小数）。按从大到小的位顺序意味着第一个位更大（更重要）。
  - BinLE2Hex – 二进制数据按从小到大的位顺序编码为十六进制小写数字。十六进制也称为基数 16 记数制，包含 16 个唯一符号：数字 0–9 和字母 a–f。小端位序指第一位为最小（最低有效）位。

- BinBE2Hex – 二进制数据按从大到小的位顺序编码为十六进制小写数字。十六进制也称为基数 16 记数制，包含 16 个唯一符号：数字 0–9 和字母 a–f。大端位序表示第一位是最高（最重要）位。
- BinLEIBO2Int – 二进制数据的编码方式与 BinLE2Int 相同，但卡原始数据在字段映射被取出编码前，使用多字节序列按相反的字节顺序读取。
- BinBEIBO2Int – 二进制数据的编码方式与 BinBE2Int 相同，但卡原始数据在字段映射被取出编码前，使用多字节序列按相反的字节顺序读取。

有关您的卡格式使用哪些字段映射的信息，请参见制造商的说明。

配置服务

“设置”页面中的“配置服务”用于访问可与门禁控制器结合使用的外部服务的设置。

SmartIntego

SmartIntego 是一种无线解决方案，提高了门禁控制器可以处理的门的数量。

SmartIntego 前提条件

在继续进行 SmartIntego 配置前需要满足以下前提条件：

- 需要创建一个 csv 文件。此 csv 文件包含有关 SmartIntego 解决方案中使用的 GatewayNode 和门的信息。此文件在 SimonsVoss 合作伙伴提供的独立软件中创建。
- SmartIntego 的硬件配置已完成，请参见 *如何为无线锁创建新硬件配置, on page 14*。

注意

- SmartIntego 配置工具必须是版本 2.1.6452.23485，
  内部版本 2.1.6452.23485 (8/31/2017 1:02:50 PM) 或更高版本。
- SmartIntego 不支持高级加密标准 (AES)，因此必须在 SmartIntego 配置工具中禁用。

如何配置 SmartIntego

注意

- 请确保已满足列出的前提条件。
- 若要进一步了解电池状态，请转到**设置** > **配置事件与报警日志**，将**门 — 电池报警**或 **IdPoint — 电池报警**添加为报警。
- 门监视器设置从导入的 CSV 文件提供。正常安装时应该不需要更改此设置。

1. 单击**浏览...**，选择此 csv 文件并单击**上传文件**。
2. 选择 GatewayNode，然后单击**下一步**。
3. 新配置的预览将显示。如果需要，可以禁用门监视器。
4. 单击**配置**。
5. 配置中包含的门概览将显示。单击**设置**单独配置每个门。

如何重新配置 SmartIntego

1. 单击顶部菜单中的**设置**。
2. 单击**配置服务** > **设置**。
3. 单击**重新配置**。
4. 单击**浏览...**，选择此 csv 文件并单击**上传文件**。
5. 选择 GatewayNode，然后单击**下一步**。
6. 新配置的预览将显示。如果需要，可以禁用门监视器。

注意

门监视器设置从导入的 CSV 文件提供。正常安装时应该不需要更改此设置。

7. 单击**配置**。
8. 配置中包含的门概览将显示。单击**设置**单独配置每个门。

OSDP LED 配置文件

您可以自定义 OSDP 读卡器的 LED 配置文件，以定义不同事件所使用的灯光和声音。有关配置文件的完整列表，请参见 *LED profiles（LED 配置文件）*。

设置灯光和音频级别

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 展开 Light and audio levels（灯光和音频级别）下拉菜单。
3. 使用滑块调节 LED 灯条、LED 背光和声音的强度。
4. 单击Save（保存）。

注意

当您更改灯光和音频级别时，设置将更新到连接到控制器的所有读卡器。

测试 OSDP LED 设置：

您可以使用 OSDP LED **测试**菜单查看任意读卡器配置文件的音频和灯光设置。

要测试 OSDP LED 配置文件的设置：

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 展开 OSDP LED test（OSDP LED 测试）下拉菜单。
3. 选择一种 LED 反馈。
4. 选择您要测试的读卡器。
5. 单击**开始**。
6. 单击 Edit feedback（编辑反馈）以更改配置文件的灯光和音频设置。
   - 从 Color（颜色）下拉菜单中选择一种新颜色。
   - 如适用，从 Audio（音频）下拉菜单中选择一种音频频率。
   - 您还可以单击 Reset to default values（重置为默认值）来重置配置文件的设置。
   - 单击Save（保存）。

更改 OSDP LED 配置文件设置：

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 导航至 OSDP LED profile（OSDP LED 配置文件）。
3. 单击要编辑的配置文件旁边的 。
4. 编辑适用的设置：
   - 从 Behavior（行为）下拉菜单中选择 LED 将遵循的行为。
   - 从 Color（颜色）下拉菜单中选择 LED 的颜色。
   - 设置 LED 的 Duration on（点亮持续时间）和 Duration off（熄灭持续时间）。
   - 设置 LED 响应的 Recurrence（重复次数）。

- 从 Audio（音频）下拉菜单中选择 Beep duration, on（蜂鸣持续时间，开启）和 Beep duration, off（蜂鸣持续时间，关闭），并设置蜂鸣器响应的 Recurrence（重复次数）。确保 Beep duration, on（蜂鸣持续时间，开启）和 Beep duration, off（蜂鸣持续时间，关闭）时长相同。

5. 单击Save（保存）。

从另一台控制器导入现有设置

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 单击 Import（导入）。
3. 选择您要上传的文件。
4. 单击 ↦ Import（导入）。

导出当前设置

1. 转到 Peripherals（外设）> Readers（读卡器）> OSDP LED profile（OSDP LED 配置文件）。
2. 单击 ↦ Export（导出）。
3. 选择要保存 json 文件的位置，单击 Save（保存）。

维护说明

若要保持访问控制系统平衡运行，Axis 建议定期维护访问控制系统，包括门禁控制器和连接设备。

每年至少进行一次维护。建议的维护过程包括（但不限于）以下步骤：

- 请确保门控制器和外部设备之间的连接都安全。
- 验证硬件连接。参见 *验证控制门, on page 15*.
- 检查系统是否正确工作，包括连接的外部设备。

– 刷卡并测试读卡器、门和锁。

– 如果系统包含 REX 设备、传感器或其他设备，也一并测试。

– 如果已经激活，还应测试篡改报警。

如果上述步骤的结果指示存在故障或异常行为：

– 使用适合的设备测试电线信号，检查电线或电缆是否有损坏。

– 更换被损坏或有故障的电缆和电线。

– 更换电缆和电线后，再次验证硬件连接。参见 *验证控制门, on page 15*.

- 如果门禁控制器未正常工作，请参见 *故障排查, on page 32* 和 *维护, on page 30* 了解更多信息。

事件配置

系统中发生的事件记录会记录在事件日志中，例如，用户刷卡或 REX 设备激活。

- 查看事件日志。参见*page 21*.
- 导出事件日志。参见.
- 配置事件日志。参见 *配置事件日志。, on page 21*.

查看事件日志。

若要查看记录的事件，请转到**事件日志**。

若要展开事件日志中的项目并查看事件详细信息，请单击 ▶。

为事件日志应用筛选器可以更轻松地查找特定事件。若要筛选列表，请选择一个或多个事件日志筛选器，然后单击**应用筛选器**。有关详细信息，请参见 *事件日志筛选器, on page 21*。

作为管理员，您可能对某些事件的关注比其他人更多。因此，您可以选择哪些事件应该记录。有关详细信息，请参见 *事件日志选项, on page 21*。

事件日志筛选器

您可以通过选择以下一个或多个筛选器来缩小事件日志的范围：

- 用户 – 筛选与选定用户相关的事件。
- 门和楼层 – 筛选与特定门或楼层相关的事件。
- 主题 – 筛选事件类型。
- 日期和时间 – 按日期和时间范围筛选事件日志。

配置事件日志。

通过“配置事件日志”页面，您可以定义应记录的事件。

事件日志选项

若要定义哪些事件应包含在事件日志中，请转到**设置 > 配置事件日志**。

提供以下记录事件选项：

- **不记录** – 禁用事件记录。此事件不会登记或包含在事件日志中。
- **源的日志** – 启用事件日志记录。此事件会登记并包含在事件日志中。

如何设置操作规则

通过事件页面，您可以配置 Axis 产品在不同事件发生时执行操作。定义何时以及如何触发操作的一组规则被称为操作规则。如果定义了多个条件，则必须满足全部条件才能触发响应。

有关可用触发器和操作的详细信息，请参见产品的内置帮助。

此示例描述如何设置操作规则以在门被强行打开时激活输出端口。

1. 转到**设置 > 其他控制器配置 > 系统选项 > 端口和设备 > I/O 端口**。
2. 从所需的 **I/O 端口类型**下拉列表中选择**输出**，然后输入**名称**。
3. 选择 I/O 端口的**正常状态**，然后单击**保存**。
4. 转到**事件 > 响应规则**，然后单击**添加**。
5. 从**触发器**下拉列表中选择**门**。
6. 从下拉列表中选择**门报警**。

7. 从下拉列表中选择所需的门。
8. 从下拉列表中选择 DoorForcedOpen。
9. 视情况，可选择**时间表**和**附加条件**。参见下方。
10. 在**操作**下，从**类型**下拉列表中选择**输出端口**。
11. 从**端口**下拉列表中选择所需的输出端口。
12. 设置状态**主动**。
13. 选择**持续时间**和**之后转入相反状态**。然后输入所需的操作持续时间。
14. 单击 OK（**确定**）。

若要为操作规则使用多个触发器，选择**附加条件**，然后单击**添加**添加附加触发器。当使用其他条件时，必须满足全部条件才能触发操作。

为防止重复触发操作，可设置**至少等待**时间。输入以小时、分钟和秒为单位的时间，这段时间内，在可以再次触发操作规则前触发器应被忽略。

有关详细信息，请参见产品的内置帮助。

如何添加接受者

产品可以发送消息来通知接受者发生的事件和警报。但是，必须先定义一个或多个接受者，然后产品才能够发送通知消息。有关可用选项的信息，请参见。

添加接受者：

1. 转到**设置 > 其他控制器配置 > 事件 > 接受者**，然后单击**添加**。
2. 输入一个描述性名称。
3. 选择**接受者**类型。
4. 输入接受者类型所需的信息。
5. 单击**测试**测试与接收者的连接。
6. 单击 OK（**确定**）。

如何设置电子邮件接受者

可以通过选择其中一个列出的电子邮件提供商，或指定公司电子邮件服务器（举例）使用的 SMTP 服务器、端口和身份验证来配置电子邮件接受者。

注意

某些电子邮件提供商拥有可防止用户接收或查看大型附件、接收预定电子邮件及类似内容的安全过滤器。检查电子邮件提供商的安全策略，以避免出现投递问题，防止电子邮件帐户被锁定。

使用其中一个列出的提供商设置电子邮件接受者：

1. 转到**事件 > 接受者**，然后单击**添加**。
2. 输入**名称**，然后从**类型**列表中选择**电子邮件**。
3. 在**收件人**字段中输入要向其发送电子邮件的电子邮件地址。使用逗号分隔多个地址。
4. 从**提供商**列表中选择电子邮件提供商。
5. 输入电子邮件帐户的用户 ID 和密码。
6. 单击**测试**发送测试电子邮件。

例如，若要使用公司电子邮件服务器设置电子邮件接受者，请按照上述说明操作，但选择**用户定义**作为**提供商**。在**发件人**字段中输入要显示为发件人的电子邮件地址。选择**高级设置**，然后指定 SMTP 服务器地址、端口和身份验证方法。或者，选择**使用加密**通过加密连接发送电子邮件。可以使用 Axis 产品中可用的证书验证服务器证书。有关如何上传证书的信息，请参见 *认证, on page 25*。

如何创建时间表

时间表可用作操作规则触发器或附加条件。使用一个预定义时间表或如下所述创建新时间表。

创建一个新的时间表：

1. 转到**设置 > 其他控制器配置 > 事件 > 时间表**，然后单击**添加**。
2. 为每日、每周、每月或每年时间表输入一个描述性名称以及所需信息。
3. 单击 **OK（确定）**。

若要在操作规则中使用时间表，从“操作规则设置”页面上的**时间表**下拉列表中选择时间表。

如何设置重复

“重复”用于重复触发操作规则，例如，每隔 5 分钟或每小时。

设置重复：

1. 转到**设置 > 其他控制器配置 > 事件 > 重复**，然后单击**添加**。
2. 输入一个描述性名称和重复模式。
3. 单击 **OK（确定）**。

要在操作规则中使用重复，请先从“操作规则设置”页面的**触发器**下拉列表中选择**时间**，然后从第二个下拉列表中选择该重复。

若要修改或移除重复，选择**重复列表**中的重复，然后单击**修改**或**移除**。

读卡器反馈

阅读器使用 LED 和蜂鸣器向用户（访问或尝试访问门的人员）发送反馈消息。门禁控制器可以触发若干反馈消息，其中一些已在门禁控制器中预配置，受大多数读卡器支持。

读卡器具有不同的 LED 行为，但通常使用不同的红色、绿色和橙色稳定灯和闪烁灯顺序。

读卡器还可以使用一音蜂鸣器发送消息，利用不同顺序的长、短蜂鸣器信号。

下表显示门禁控制器中预配置的事件如何触发读卡器反馈及其典型的读卡器反馈信号。Axis 读卡器的反馈信号在 Axis 读卡器随附的《安装指南》中加以介绍。

事件	Wiegand **双** LED	Wiegand **单个** LED	OSDP	**蜂鸣器模式**	**状态**
空闲[1]	关	红色	红色	无声	普通镜头
需要 PIN	闪烁红色/绿色	闪烁红色/绿色	闪烁红色/绿色	两次短哔哔声	需要 PIN
授权访问	绿色	绿色	绿色	蜂鸣声	授权访问
拒绝访问	红色	红色	红色	蜂鸣声	拒绝访问

上述外的反馈消息，必须使用访问管理系统等客户端通过支持该功能的 VAPIX® 应用编程接口进行配置，并使用可提供所需信号的阅读器。有关详细信息，请参见门禁管理系统开发人员和读卡器制造商提供的用户信息。

1. 当门关闭并且锁已锁定时进入空闲状态。

系统选项

安全：

用户

用户访问控制默认已启用，可以在**设置 > 其他控制器配置 > 系统选项 > 安全 > 用户**下配置。管理员可以通过为用户提供用户名和密码来设置其他用户。

用户列表显示被授权的用户和用户组（访问级别）：

- **程序管理员**无设置访问限制。管理员可以添加、修改和删除其他用户。

注意

请注意，当选择选项**加密和未加密**时，Web 服务器将为密码加密。这是新单元或重置为出厂默认设置的单元的默认选项。

在 **HTTP/RTSP 密码设置**下，选择要允许的密码类型。如果存在不支持加密的查看客户端，或者如果您升级了固件，而现有客户端支持加密，但需要再次登录并被配置为使用此功能，您则需要允许未加密密码。

ONVIF

ONVIF 是一个开放的行业论坛，为让基于 IP 的物理安全产品达到有效的互操作性提供并推进标准化接口。

创建用户即可自动启用 ONVIF 通信。在与产品的ONVIF 通信中都使用用户名和密码。有关详细信息，请参见 *www.onvif.org*

IP 地址过滤器

IP 地址过滤可在**Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Security（安全）> IP Address Filter（IP 地址过滤器）**页面启用。启用之后，将允许或拒绝列出的 IP 地址访问 Axis 产品。从列表中选择**允许**或**拒绝**，然后单击**应用**启用 IP 地址过滤。

管理员可向列表添加多达 256 个 IP 地址条目（单个条目可包含多个 IP 地址）。

HTTPS

HTTPS（HyperText Transfer Protocol over Secure Socket Layer 或 HTTP over SSL）是一种 Web 协议，提供加密浏览。HTTPS 也可以被用户和客户端用来验证所访问的设备是否正确。HTTPS 提供的安全级别被视为适合大多数商业交换。

Axis 产品可以配置为当管理员登录时需要 HTTPS。

要使用 HTTPS，则必须先安装 HTTPS 证书。转到**Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Security（安全）> Certificates（证书）**安装和管理证书。参见 *认证, on page 25*.

在 Axis 产品上启用 HTTPS：

1. 转到**设置 > 其他控制器配置 > 系统选项 > 安全 > HTTPS**
2. 从已安装的证书列表中选择 HTTPS 证书。
3. 或者，单击**密码**，选择要用于 SSL 的加密算法。
4. 为不同用户组设置 **HTTPS 连接策略**。
5. 单击**Save（保存）**可启用这些设置。

若要通过所需协议访问安讯士产品，在浏览器的地址字段中为 HTTPS 协议输入`https://`，为 HTTP 协议输入`http://`。

HTTPS 端口可以在**系统选项 > 网络 > TCP/IP > 高级**页面更改。

IEEE 802.1X

IEEE 802.1X 是针对基于端口的网络管理控制一种标准，可提供有线和无线网络设备的安全身份验证。IEEE 802.1x 基于 EAP（可扩展身份验证协议）。

若要访问受 IEEE 802.1X 保护的网络，设备必须通过身份验证。该身份验证由身份验证服务器执行，通常是 **RADIUS 服务器**，例如 FreeRADIUS 和 Microsoft Internet 身份验证服务。

在 Axis 的实施中，Axis 产品和身份验证服务器通过使用 EAP–TLS（可扩展身份验证协议 – 传输层安全）的数字证书自我识别。证书由**证书颁发机构** (CA) 提供。您需要：

- 用于验证身份验证服务器的 CA 证书。
- 用于对 Axis 产品进行身份验证的 CA 签发的客户端证书。

若要创建和安装证书，请转到**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Security（安全）** > **Certificates（证书）**。参见 *认证, on page 25*.

允许产品访问受 IEEE 802.1X 保护的网络：

1. 转到**设置 > 其他控制器配置 > 系统选项 > 安全 > IEEE 802.1X**。
2. 从已安装的证书列表中选择 **CA 证书**和**客户端证书**。
3. 在**设置**下，选择 EAPOL 版本，并提供与客户端证书关联的 EAP 身份。
4. 选中此框以启用 IEEE 802.1X，然后单击**保存**。

注意

为了让身份验证正常工作，Axis 产品中的日期和时间设置应该与 NTP 服务器同步。参见.

认证

证书用于对网络上的设备进行身份验证。典型应用包括加密的 Web 浏览 (HTTPS)、通过 IEEE 802.1X 提供网络保护以及通知消息（例如，通过电子邮件）。安讯士产品可使用两种类型的证书：

服务器/客户端证书 – 对 Axis 产品进行身份验证。**服务器/客户端**证书可以是自签名的或由证书颁发机构 (CA) 颁发。自签名证书提供有限的保护，可在获得 CA 颁发的证书之前使用。

证书 – 当 Axis 产品连接到 IEEE 802.1X 受保护网络时验证对等证书，如验证服务器的证书。Axis 产品随附几个预装的 CA 证书。

注意

- 如果产品重置为出厂默认设置，则将删除证书（预装 CA 证书除外）。
- 如果产品重置为出厂默认设置，则将重新安装已删除的预装 CA 证书。

如何创建自签名证书

1. 转到**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Security（安全）** > **Certificates（证书）**。
2. 单击**创建自签名证书**提供请求的信息。

如何创建和安装 CA 签发的证书

1. 创建自签名证书，请参见 *如何创建自签名证书, on page 25*。
2. 转到**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Security（安全）** > **Certificates（证书）**。
3. 单击**创建证书签名请求**提供请求的信息。
4. 复制 PEM 格式的请求并发送到您选择的 CA。

5. 当返回签名的证书时，单击**安装证书**上传证书。

如何安装其他 CA 证书

1. 转到Setup（设置） > Additional Controller Configuration（其他控制器配置） > System Options（系统选项） > Security（安全） > Certificates（证书）。
2. 单击**安装证书**上载证书。

网络：

基本 TCP/IP 设置

Axis 产品支持 IP 版本 4 (IPv4) 和 IP 版本 6 (IPv6)。

Axis 产品可以通过以下方式获得 IP 地址：

- **动态 IP 地址** – 默认选择**通过 DHCP 获取 IP 地址**。这意味着 Axis 产品被设置为通过动态主机配置协议 (DHCP) 自动获取 IP 地址。
  DHCP 允许网络管理员集中管理和自动分配 IP 地址。
- **静态 IP 地址** – 若要使用静态 IP 地址，请选择**使用以下 IP 地址**，然后指定 IP 地址、子网掩码和默认路由器。然后单击**保存**。

仅当使用动态 IP 地址通知，或者 DHCP 能够更新可以实现按名称（主机名）访问 Axis 产品的 DNS 服务器时，DHCP 才应启用。

如果启用了 DHCP 但产品无法访问，则运行 AXIS IP Utility 来为已连接的 Axis 产品搜索网络，或将产品重置为出厂默认设置，然后重新进行安装。有关如何重置为出厂默认设置的信息，请参见 *page 32*。

AXIS 视频托管系统 (AVHS)

AVHS 与 AVHS 服务结合使用，可从不同位置通过互联网方便安全地访问控制器管理和日志。有关如何查找本地 AVHS 服务提供商的更多信息和帮助，请转到 www.axis.com/hosting

AVHS设置在Setup（设置） > Additional Controller Configuration（其他控制器配置） > System Options（系统选项） > Network（网络） > TCP IP > Basic（基本）下配置。默认已启用连接到 AVHS 服务功能。若要禁用，清除**启用 AVHS** 框。

一键启用 – 按住产品的控制按钮保持3秒（请参见 *产品概览, on page 6*），可以通过互联网连接到AVHS服务。注册后将**始终**启用，Axis 产品会一直连接到 AVHS 服务。如果在按下按钮后的 24 小时内未注册产品，产品将断开与 AVHS 服务的连接。

总是 – Axis 产品将不断尝试通过互联网连接到 AVHS 服务。注册之后，产品会一直连接到服务。如果已安装产品并且不方便或无法使用一键式安装时，可以使用此选项。

注意

AVHS 支持取决于服务提供商订阅的可用情况。

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service 分配主机名称以轻松访问产品。有关详细信息，请参见 *www.axiscam.net*

要为安讯士产品注册AXIS Internet Dynamic DNS Service，请转到Setup（设置） > Additional Controller Configuration（其他控制器配置） > System Options（系统选项） > Network（网络） > TCP/IP > Basic（基本）。在**服务**下，单击 AXIS Internet Dynamic DNS Service **设置**按钮（需要接入互联网）。当前在 AXIS Internet Dynamic DNS Service 为产品注册的域名可以随时删除。

注意

AXIS Internet Dynamic DNS Service 需要 IPv4。

高级 TCP/IP 设置

DNS 配置

DNS（域名服务）提供主机名到 IP 地址的转换。DNS设置在**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Network（网络）** > **TCP/IP** > **Advanced（高级）**下配置。

选择**通过 DHCP 获取 DNS 服务器地址**使用 DHCP 服务器提供的 DNS 设置。

若要进行手动设置，请选择**使用以下 DNS 服务器地址**，然后指定以下信息：

域名 – 输入域搜索 Axis 产品使用的主机名。多个域可以用分号隔开。主机名称始终是限定域名的第一部分，例如，`myserver`是限定域名`myserver.mycompany.com`中的主机名，其中`mycompany.com`是域名。

主要/辅助 DNS 服务器 – 输入主要和辅助 DNS 服务器的 IP 地址。辅助 DNS 服务器是可选的，在主要 DNS 服务器不可用时使用。

NTP 配置

NTP（网络定时协议）用于同步网络中设备的时钟时间。NTP设置在**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Network（网络）** > **TCP/IP** > **Advanced（高级）**下配置。

选择**通过 DHCP 获取 NTP 服务器地址**使用 DHCP 服务器提供的 NTP 设置。

若要进行手动设置，请选择**使用以下 NTP 服务器地址**，然后输入主机名或 NTP 服务器的 IP 地址。

主机名配置

Axis 产品可以通过主机名而不是 IP 地址访问。主机名通常与分配的 DNS 名称相同。主机名在**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Network（网络）** > **TCP/IP** > **Advanced（高级）**下配置。

选择**通过 IPv4 DHCP 获取主机名**使用在 IPv4 上运行的 DHCP 服务器提供的主机名。

选择**使用主机名**手动设置主机名。

选择**启用动态 DNS 更新**在 Axis 产品的 IP 地址每次更改时动态更新本地 DNS 服务器。有关详细信息，请参见在线帮助 。

Link–Local IPv4 地址

Link–Local 地址默认启用，其将在 Axis 产品分配到其他 IP 地址，这些地址可用于从本地网络同一个网段上的其他主机访问产品。产品可同时有 Link–Local IP 地址和静态或 DHCP 提供的 IP 地址。

此功能可以在**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Network（网络）** > **TCP/IP** > **Advanced（高级）**下禁用。

HTTP

安讯士产品使用的HTTP端口可以在**Setup（设置）** > **Additional Controller Configuration（其他控制器配置）** > **System Options（系统选项）** > **Network（网络）** > **TCP/IP** > **Advanced（高级）**下更改。除了默认设置（默认为 80）外，范围在 1024–65535 内的不同端口均可使用。

HTTPS

Axis 产品使用的 HTTPS 端口可以在**设置** > **其他控制器配置** > **系统选项** > **网络** > **TCP/IP** > **高级**下更改。除了默认设置（默认为 443）外，范围在 1024–65535 内的不同端口均可使用。

若要启用 HTTPS，请转到 Setup（设置）>Additional Controller Configuration（其他控制器配置）>System Options（系统选项）>Security（安全）> HTTPS。有关详细信息，请参见 *HTTPS, on page 24*。

为 IPv4 使用 NAT 遍历（端口映射）

网络路由器允许专用网络 (LAN) 上的设备共享与互联网的单一连接。这通过将网络通信从私有网络转至“外部”（即互联网）来实现。由于大多数路由器进行了预配置，可以停止从公共网络（互联网）访问专用网络 (LAN) 的尝试，因而专用网络 (LAN) 上的安全性得以提高。

当 Axis 产品位于内联网 (LAN)，并且您希望产品可以从 NAT 路由器的另一 (WAN) 侧使用时，请使用 **NAT 遍历**。在正确配置 NAT 穿越的情况下，NAT 路由器中流向外部 HTTP 端口的 HTTP 流量都会转发给产品。

NAT遍历在Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Network（网络）> TCP/IP > Advanced（高级）下配置。

注意

- 为使 NAT 遍历正常工作，其必须受路由器支持。该路由器还要支持 UPnP®。
- 在此上下文中，路由器指任意网络路由设备（如 NAT 路由器、网络路由器、互联网网关、宽带路由器、宽带共享设备）或软件（如防火墙）。

启用/禁用 – 当启用后，安讯士产品将尝试采用 UPnP 在网络上的 NAT 路由器中配置端口映射。请注意，必须在产品中启用 UPnP（请参见Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Network（网络）> UPnP）。

使用手动选择的 NAT 路由器 – 选择此选项可以手动选择 NAT 路由器并在字段中输入路由器的 IP 地址。如果未指定路由器，产品会自动搜索网络上的 NAT 路由器。如果找到多个路由器，会选中默认路由器。

替代 HTTP 端口 – 选择此选项可以手动定义外部 HTTP 端口。输入范围 1024–65535 中的端口。如果端口字段为空或包含默认设置（即 0），启用 NAT 遍历功能时会自动选择端口号。

注意

- 可以使用替代 HTTP 端口，即使已禁用 NAT 遍历功能，其也可以处于活动状态。如果您的 NAT 路由器不支持 UPnP，您需要在 NAT 路由器中手动配置端口转发，这很有用。
- 如果您尝试手动输入正在使用的端口，将自动选择另一个可用端口。
- 自动选择了端口后，端口将显示在此字段中。要进行更改，输入新的端口号，然后单击**保存**。

FTP

通过安讯士产品中运行的FTP服务器，可以上传新固件、用户应用等。FTP服务器可以在Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Network（网络）> TCP/IP > Advanced（高级）下禁用。

RTSP

Axis 产品中运行的 RTSP 服务器允许连接客户端来开始事件流。RTSP 端口号可以在**设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 高级**下更改。默认端口为 554。

注意

如果 RTSP 服务器被禁用，事件流将不可用。

SOCKS

SOCKS 是一种网络代理协议。Axis 产品可以配置为使用 SOCKS 服务器到达防火墙或代理服务器另一侧的网络。如果 Axis 产品位于防火墙后面的本地网络，并且需要将通知、上传文件、警报等发送到本地网络以外的目的地（例如，互联网），此功能会很有用。

SOCKS 在**Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Network（网络）> SOCKS**下配置。有关详细信息，请参见在线帮助 。

QoS（服务质量）

QoS（服务质量）可保证为网络上所选流量指定的资源具有一定级别。基于 QoS 的网络可以确定流量的优先级，并通过控制应用程序可以使用的带宽量来提高网络可靠性。

QoS 设置在**Setup（设置）>Additional Controller Configuration（其他控制器配置）>System Options（系统选项）>Network（网络）> QoS**下配置。使用 DSCP（差分服务编码）值，Axis 产品可以标记事件/警报流量和管理流量。

SNMP

简单网络管理协议 (SNMP) 允许远程管理网络设备。SNMP 社区是一组运行 SNMP 的设备兼管理站。社区名称可用于识别组群。

要在安讯士产品中启用和配置 SNMP，请转到**Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Network（网络）> SNMP**页面。

根据所需的安全级别，选择要使用的 SNMP 上的版本。

Axis 产品可使用陷阱发送有关重要的事件和状态更改的消息到管理系统。选中**启用陷阱**，然后输入应发送陷阱消息以及**陷阱社区**应收到消息的 IP 地址。

注意

如果启用了 HTTPS，则应禁用 SNMP v1 和 SNMP v2c。

Axis 产品可使用 **SNMP v1/v2 的陷阱**发送有关重要的事件和状态更改的消息到管理系统。选中**启用陷阱**，然后输入应发送陷阱消息以及**陷阱社区**应收到消息的 IP 地址。

可用陷阱如下：

- 冷启动
- 热启动
- 连接
- 身份验证失败

SNMP v3 提供加密和安全密码。若要使用 SNMP v3 的陷阱，需要 SNMP v3 管理应用程序。

若要使用SNMP v3，必须启用HTTPS，请参见 *HTTPS, on page 24*。若要启用 SNMP v3，选中此框，并提供初始用户密码。

注意

初始密码只能设置一次。如果密码丢失，安讯士产品必须重置为出厂默认设置，请参见 *重置为出厂默认设置。, on page 32*。

UPnP

安讯士产品提供 UPnP® 支持。UPnP 默认启用，产品由支持此协议的操作系统和客户端自动检测。

UPnP可以在**Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Network（网络）> UPnP**下禁用。

Bonjour

Axis 产品提供 Bonjour 支持。Bonjour 默认启用，产品由支持此协议的操作系统和客户端自动检测。

Bonjour可以在**Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Network（网络）> Bonjour**下禁用。

端口和设备

I/O 端口

辅助连接器提供四个用于连接外部设备的可配置输入和输出端口。

外部连接器提供两个用于连接外部设备的可配置输入和输出端口。

您可以在**设置 > 其他控制器配置 > 系统选项 > 端口和设备 > I/O 端口**下配置 I/O 端口。选择端口方向（**输入**或**输出**）。您可以为端口指定描述性名称，端口的**正常状态**可以配置为**开路**或**接地电路**。

端口状态

系统选项 > 端口和设备 > 端口状态页面上的列表显示产品输入和输出端口的状态。

维护

Axis 产品提供多项维护功能。这些功能位于Setup（**设置**）> Additional Controller Configuration（**其他控制器配置**）> System Options（**系统选项**）> Maintenance（**维护**）。

如果 Axis 产品无法正常运行，单击**重启**执行正确重启。这将不会影响当前设置。

注意

重启会清除服务器报告中的条目。

单击**恢复**将大多数设置重置为出厂默认值。下列设置不会受影响：

- 引导协议（DHCP 还是静态）
- 静态 IP 地址
- 默认路由器
- 子网掩码
- 系统时间
- IEEE 802.1X 设置

单击**默认值**以将设置（包括 IP 地址）重置为出厂默认值。此按钮应谨慎使用。安讯士产品还可以使用控制按钮重置为出厂默认设置，请参见 *重置为出厂默认设置。, on page 32*。

有关固件升级的信息，请参见 *如何升级固件, on page 32*。

支持页面

支持概览

如果您需要技术帮助，Setup（**设置**）> Additional Controller Configuration（**其他控制器配置**）> System Options（**系统选项**）> Support（**支持**）> Support Overview（**支持概览**）页面提供了有关故障排查和联系人信息的信息。

另请参阅 *故障排查, on page 32*。

系统概览

若要获取 Axis 产品的状态和设置的概览，请转到**设置 > 其他控制器配置 > 系统选项 > 支持 > 系统概览**。此处提供的信息包括固件版本、IP 地址、网络和安全设置、事件设置和近期的日志内容。

日志和报告

Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Support（支持）> Logs & Reports（日志和报告）页面生成对系统分析和故障排查很有用的日志和报告。在与 Axis Support 联系时，请将服务器报告与问题一起提供。

系统日志 – 提供有关系统事件的信息。

访问日志 – 列出产品访问失败尝试。访问日志也可配置为列出与产品的连接（参见下文）。

查看服务器报告 – 在弹出窗口中提供有关产品状态的信息。服务器报告中自动包含访问日志。

下载服务器报告 – 创建一个 .zip 文件，其中包含 UTF–8 格式的完整服务器报告文本文件。选择**包含实景快照**选项以包含产品实景的快照。联系支持时，应始终包含此 .zip 文件。

参数列表 – 显示产品的参数及其当前设置。在排查故障或联系 Axis Support 时，这些信息可能很有用。

连接列表 – 列出当前正在访问媒体流的客户端。

崩溃报告 – 生成包含调试信息的存档文件。需要几分钟时间生成此报告。

系统和访问日志的日志级别在Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Support（支持）> Logs & Reports（日志和报告）> Configuration（配置）下设置。可配置访问日志以列出与产品的连接（选择“重要警告和信息”）。

高级

脚本

脚本允许富有经验的用户自定义和使用自己的脚本。

注意

使用不当可能导致意外行为并丢失与 Axis 产品的连接。

Axis 强烈建议您不要使用此功能，除非您了解后果。Axis Support 不帮助解决自定义脚本相关问题。

若要打开脚本编辑器，请转到Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Advanced（高级）> Scripting（脚本）。如果脚本导致问题，请将产品重置为出厂默认设置，请参见*page 32*。

有关详细信息，请参见 *www.axis.com/developer*

文件上传

可以将文件（例如，网页和图像）上传到 Axis 产品，然后用作自定义设置。若要上传文件，请转到 Setup（设置）> Additional Controller Configuration（其他控制器配置）> System Options（系统选项）> Advanced（高级）> File Upload（文件上传）。

已上传的文件可通过 `http://<ip address>/local/<user>/<file name>` 访问，其中 `<user>` 是为上传的文件选择的用户组（管理员）。

故障排查

重置为出厂默认设置。

重要

重置为出厂默认设置时应谨慎。重置为出厂默认设置会将全部设置（包括 IP 地址）重置为出厂默认值。

将产品重置为出厂默认设置：

1. 断开产品电源。
2. 按住控制按钮，同时重新连接电源。参见 *产品概览, on page 6*.
3. 按住控制按钮 25 秒，直到状态指示灯指示灯再次变成淡黄色。
4. 释放控制按钮。当状态LED指示灯变绿时，此过程完成。产品已重置为出厂默认设置。如果网络上没有可用的 DHCP 服务器，则默认 IP 地址为 `192.168.0.90`.
5. 使用安装和管理软件工具分配 IP 地址、设置密码和访问产品。

也可通过网页界面将参数重置为出厂默认设置。前往 Setup（设置）>Additional Controller Configuration（其他控制器配置）>Setup（设置）>System Options（系统选项）>Maintenance（维护），然后单击 Default（默认）。

如何检查当前固件

固件是决定网络设备功能的软件。进行故障排查时，您首先应检查当前固件版本。新版本可能包含能修复您的某个特定问题的校正。

Axis 产品的当前固件版本显示在“概述”页面。

如何升级固件

重要

- 对于因用户错误升级引起的维修，您的经销商会保留收费权利。
- 升级固件时，将保存预配置和自定义设置（如果这些功能在新固件中可用），但 Axis Communications AB 不对此做保证。
- 如果安装以前的固件版本，您随后需要将产品恢复为出厂默认设置。

注意

- 升级过程完成后，产品将自动重启。如果您在升级后手动重启产品，请等待 5 分钟，即使您怀疑升级失败。
- 由于用户、组、凭证和其他数据的数据库将在固件升级后更新，因此首次启动可能需要几分钟才能完成。所需时间取决于数据量。
- 当你使用新固件升级 Axis 产品时，产品会获得提供的新功能。在升级固件之前，请务必阅读升级说明和每个新版本的发布说明。

1. 将新固件文件下载到你的电脑，文件可在 *www.axis.com/support* 上免费获得
2. 转到产品网页中的**设置 > 其他控制器配置 > 系统选项 > 维护**。
3. 在**升级服务器**下，单击**选择文件**，在您的计算机上找到文件。
4. 如果您希望产品在升级后自动恢复为出厂默认设置，请选中**默认**复选框。
5. 单击**升级**。
6. 产品升级并重启需要等待大约 5 分钟。然后清除 Web 浏览器的缓存。
7. 访问产品。

征兆、可能的原因和补救措施

固件升级问题

固件升级失败	如果固件升级失败，该产品将重新加载以前的固件。检查固件文件，然后重试。

设置 IP 地址时出现问题

使用 ARP/Ping 时	尝试重新安装。必须在产品接通电源后两分钟内设置 IP 地址。确保Ping长度设置为408。有关说明，请参阅*Axis.com*产品页面上的安装指南。
产品位于不同子网掩码上	如果用于产品的 IP 地址和用于访问该产品的计算机 IP 地址位于不同子网上，则无法设置 IP 地址。请联系网络管理员获取 IP 地址。
该 IP 地址已用于其他设备	从网络上断开安讯士摄像机。运行 Ping 命令（在 Command/DOS 窗口中，键入`ping`和产品的 IP 地址）： • 如果收到：`Reply from <IP address>: bytes=32; time=10...`，这意味着网络上的另一个设备可能已使用该 IP 地址。请从网络管理员处获取新的 IP 地址，然后重新安装该产品。 • 如果您收到：`Request timed out`，这意味着该 IP 地址可用于此安讯士产品。检查布线并重新安装产品。
可能的 IP 地址与同一子网上的其他设备发生冲突	在 DHCP 服务器设置动态地址之前，将使用 Axis 产品中的静态 IP 地址。这意味着，如果其他设备也使用同一默认静态 IP 地址，则可能在访问该产品时出现问题。

无法通过浏览器访问该产品

无法登录	启用 HTTPS 时，请确保在尝试登录时使用正确的协议（HTTP 或 HTTPS）。您可能需要在浏览器的地址字段中手动键入 `http` 或 `https`。 如果 root 用户的密码丢失，则产品必须重置为出厂默认设置。参见 *重置为出厂默认设置。, on page 32*.
通过DHCP修改了IP地址。	从 DHCP 服务器获得的 IP 地址是动态的，可能会更改。如果 IP 地址已更改，请使用 AXIS IP Utility 或 AXIS 设备管理器在网络上找到产品。使用产品型号或序列号或根据 DNS 名称（如果已配置该名称）来识别产品。 如果需要，可以手动分配静态 IP 地址。有关说明，请参见产品页面 (axis.com) 的文档*如何分配 IP 地址和访问设备*
使用 IEEE 802.1X 时出现证书错误	为了让身份验证正常工作，Axis 产品中的日期和时间设置应该与 NTP 服务器同步。参见.

该产品可从本地访问但不可从外部访问

路由器配置	若要将路由器配置为允许进入安讯士产品的传入数据流量，启用NAT遍历功能，此功能会尝试将路由器自动配置为允许访问安讯士产品，请参见 *为 IPv4 使用 NAT 遍历（端口映射）, on page 28*。路由器必须支持 UPnP®。
防火墙保护	请与网络管理员确认 Internet 防火墙。
所需的默认路由器	检查您是否需要从**设置** > **网络设置**或**设置** > **其他控制器配置** > **系统选项** > **网络** > TCP/IP > **基本**配置路由器设置。

规格

使用 UL 标记的文本仅对 UL 293 或 UL 294 安装有效。

LED 指示灯

LED	颜色	指示
网络：	绿色	稳定表示连接到 100 MBit/s 网络。闪烁表示网络活动。
	琥珀色	稳定表示连接到 10 MBit/s 网络。闪烁表示网络活动。
	熄灭	无网络连接。
状态：	绿色	稳定绿色表示正常工作。
	琥珀色	在启动期间和还原设置时常亮。
	红色	缓慢闪烁表示升级失败。
电源	绿色	正常工作.
	琥珀色	在固件升级过程中呈绿色/橙色闪烁。
继电器过流	红色	短路或检测到过流时稳定亮起。
	熄灭	正常工作.
读卡器过流	红色	短路或检测到过流时稳定亮起。
	熄灭	正常工作.
继电器 ：	绿色	继电器激活。[2]
	熄灭	继电器不活动。

注意

- LED 状态指示灯可被配置为在事件激活时闪烁。
- LED 状态指示灯可配置为在识别装置时闪烁。前往**设置> 其他控制器配置> 系统选项> 维护**。

按钮

控制按钮

控制按钮用于：

- 将产品重置为出厂默认设置。参见 *重置为出厂默认设置。, on page 32*.

连接器

网络连接器：

采用以太网供电 增强版 (PoE+) 的 RJ45 以太网连接器。

UL：以太网供电 (PoE) 应由通过 UL 294 认证的以太网供电 IEEE 802.3af/802.3at 1 型 3 类或以太网供电增强版 (PoE+) IEEE 802.3at 2 型 4 类限制电源馈电器（提供 44–57 V DC、15.4 W / 30 W）供电。以太网供电 (PoE) 已由 UL 使用 AXIS T8133 中跨 30 W 单端口进行评估。

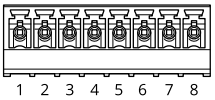
读卡器连接器

支持用于与读卡器通信的 RS485 和 Wiegand 协议的两个 8 针接线端子。

2. 当 *COM* 连接到 *NO* 时继电器处于活动状态。

指定的电源输出值在两个读卡器端口之间共享。这意味着将为连接到门禁控制器的全部读卡器保留 486 mA (12 V DC)。

选择要在产品网页中使用的协议。



针对 RS485 的配置

功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输出 (+12 V)	2	为读卡器供电。	两个读卡器组合 12 V DC，上限486 mA
RX/TX	3–4	全双工:RX.半双工:RX/TX.	
TX	5–6	全双工:TX.	
可配置（输入或输出）	7–8	数字输入 – 连接到针 1 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC
		数字输出 — 如果与电感负载（如继电器）一起使用，则将二极管与负载并联连接，以防止电压瞬变。	0 至最高 30 V DC，开路，100 mA

重要

- 当读卡器由控制器供电时，电缆长度不超 200 米（656 英尺）。
- 当读卡器不是由控制器供电时，则如果满足以下电缆要求，读卡器数据的电缆长度不超 1000 米（(3280,8 英尺）：1 对带屏蔽双绞线，AWG 24，120 欧姆阻抗。

针对 Wiegand 的配置

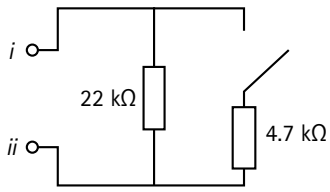
功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
DC 输出 (+12 V)	2	为读卡器供电。	两个读卡器组合 12 V DC，上限486 mA
D0	3		
D1	4		
O	5–6	数字输出，开漏	
可配置（输入或输出）	7–8	数字输入 – 连接到针 1 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC
		数字输出 — 如果与电感负载（如继电器）一起使用，则将二极管与负载并联连接，以防止电压瞬变。	0 至最高 30 V DC，开路，100 mA

重要

- 当读卡器由控制器供电时，电缆长度不超 150 米（500 英尺）。
- 当读卡器不是由控制器供电时，则如果满足以下电缆要求，读卡器数据电缆长度不超150 米（500 英尺）：AWG 22。

监控输入

要使用监控输入，则根据下面的图表安装线尾电阻器。



i 输入

ii 0 V DC(–)

UL：UL 并不评估监控输入是否适用于入室盗窃。仅门监控器和 REX 支持监控，使用线尾电阻器。

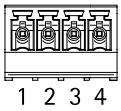
注意

建议使用绞合屏蔽电缆。将屏蔽件连接至 0 V DC。

门连接器

用于门禁监控设备的两个 4 针接线端子（数字输入）。

门监视器支持使用线尾电阻器监控。如果连接中断，将触发报警。要使用监控输入，安装线尾电阻器。使用连接图来安装监控输入。参见。



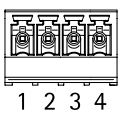
功能	引脚	注意	规格
DC 接地	1, 3		0 V DC
输入	2, 4	用于与门禁监控器通信。 数字输入或监控输入 – 分别连接至 引脚 1 或 3 以启用，或保留浮动状态 （断开连接）以停用。	0 至最大 30 V DC

重要

如果满足以下电缆要求，合格电缆长度可达200 米（656 英尺）：AWG 24。

中继连接器

例如，C 型继电器的两个 4 针接线端子可以用于控制大门的锁或接口。



功能	引脚	注意	规格
DC 接地 (GND)	1		0 V DC
否	2	常开。 用于连接中继设备。在 NO 和 DC 接地之间连接断电闭门锁。 如果不使用跳线，则两个继电器引脚与电路的其余部分电气隔离。	最大电流 = 每个继电器 2 A 最大电压 = 30 V DC
COM	3	公共	
NC	4	常闭。 用于连接中继设备。在 NC 和 DC 接地之间连接自动防故障锁。 如果不使用跳线，则两个继电器引脚与电路的其余部分电气隔离。	

继电器电源跳线

当安装继电器电源跳线时，它将12 V DC 或24 V DC 连接到继电器 COM 针。

它可以用于连接 GND 和 NO 或 GND 和 NC 针之间的锁。

电源	12 V DC 时的上限功率[3]	24 V DC 时的上限功率[3]
DC 输入	1 600 mA	800 mA
PoE	800 mA	400 mA

注意

如果锁无极性，建议您增加外部续流二极管。

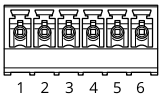
辅助连接器

在外部设备结合了移动侦测、事件触发和报警通知等功能的情况下，使用辅助连接器。除0 V DC 参考点和电源（DC 输出）外，辅助连接器还提供连接至以下模块的接口：

数字输入 – 用于连接可在开路和闭路之间切换的设备，例如 PIR 传感器、门/窗磁和玻璃破碎侦测器。

数字输出 – 用于连接继电器和 LED 等外部设备。已连接的设备可通过 VAPIX® 应用程序编程接口或从产品网页进行激活。

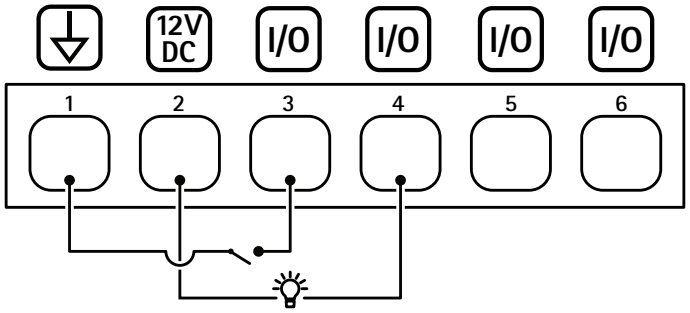
6 针接线端子



功能	引脚	注意	规格
DC 接地	1		0 V DC
DC 输出	2	可用于为辅助设备供电。 注意:此针只能用作电源输出。	12 V DC 最大负载 = 每个 I/O 50 mA

3. 两个继电器和 AUX I/O12 V DC 共享电源。

可配置（输入或输出）	3–6	数字输入 – 连接到针 1 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC
		数字输出 – 启用时内部连接至引脚 1（DC 接地），停用时保留浮动状态（断开连接）。如果与电感负载（如继电器）一起使用，则将二极管与负载并联连接，以防止电压瞬变。如果使用内部 12 V DC 输出（引脚 2），每个 I/O 能够驱动 12 V DC (50 mA)（最大）外部负载。如果结合外部电源使用开漏连接，I/O 则可以管理 0–30 V DC、100 mA 的直流供电。	0 至最大 30 V DC，开漏，100 mA

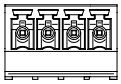


1 *DC 接地*
2 *DC 输出12 V*
3 *I/O 配置为输入*
4 *I/O 配置为输出*
5 *可配置的 I/O*
6 *可配置的 I/O*

外部连接器

外部设备的 4 针接线端子，例如，玻璃破碎或火灾侦测器。

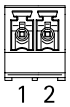
UL：此连接器尚未由 UL 进行防窃/防火报警使用方面的评估。



功能	引脚	注意	规格
DC 接地	1, 3		0 V DC
可配置（输入或输出）	2, 4	数字输入 – 连接至针 1 或 3 以启用，或保留浮动状态（断开连接）以停用。	0 至最大 30 V DC
		数字输出 – 连接到针 1 或 3 以启用，或保留浮动状态（断开连接）以停用。如果与电感负载（如继电器）一起使用，则将二极管与负载并联连接，以防止电压瞬变。	0 至最大 30 V DC，开漏，100 mA

电源连接器

用于 DC 电源输入的双针接线端子。使用额定输出功率限制为 ≤100 W或额定输出电流限制为 ≤5 A 且符合安全超低电压 (SELV) 要求的限制电源 (LPS)。



功能	引脚	注意	规格
0 V DC(–)	1		0 V DC
DC 输入	2	在未使用以太网供电时，可用于给控制器供电。 注意:此引脚只能用作电源输入。	10.5–28 V DC，最大 36 W

UL：使用具有适当额定功率的 UL 294、UL 293 或 UL 603 上市电源供应器提供 DC 电源，具体取决于应用。

备份电池输入连接器

用于使用具有内置充电器的电池的备份解决方案。12 V DC 输入。

UL：此连接器尚未由 UL 评估。

重要

在使用电池输入时，必须串联连接外部 3 A 慢熔保险丝。



功能	引脚	注意	规格
0 V DC(–)	1		0 V DC
电池输入	2	用于在其他电源不可用时为门禁控制器供电。 注意:此引脚只能用作电池电源输入。仅适用于连接到 UPS。	11– 13.7 V DC，最大 36 W

安全信息

危险等级

⚠ 危险
表示如果不避免则会导致死亡或严重伤害的危险情况。

⚠ 警告
表示如果不避免则可能导致死亡或严重伤害的危险情况。

⚠ 警示
表示如果不避免则可能导致轻微或中度伤害的危险情况。

注意
表示如果不避免则可能导致财产损失的情况。

其他消息等级

重要
表示产品正常工作所必需的重要信息。

注意
表示有助于充分利用产品的有用信息。

网页界面

注意

此部分仅适用于具有 AXIS Camera Station Secure Entry 固件的 AXIS A1601 Network Door Controller。

:在 Device settings（**设备设置**）和 Analytics（**分析**）概览之间切换。

:显示或隐藏主菜单。

帮助：访问产品帮助、发行说明和生命周期指南。

信息：

- **关于**：查看设备信息，包括 AXIS OS 版本和序列号。
- **法律**：查看有关 Cookie 和许可证的信息。
- **反馈**：分享反馈，以帮助我们改善您的用户体验。
- **分析数据**：接受共享非个人浏览器数据。
- **设备服务器报告**：下载设备服务器报告。

管理员：

- :有关登录用户的信息。
- :更改语言。
- :设置浅主题或深色主题。
- Change account（**更改账户**）：从当前帐户退出，然后登录新帐户。
- **退出**：从当前帐户退出。

状态：

时间同步状态

显示 NTP 同步信息，包括设备是否与 NTP 服务器同步、下次同步前的剩余时间以及 PTP 状态。

NTP 设置：查看并更新 NTP 设置。转到可更改 NTP 设置的 Time and location（**事件和位置**）页面。

设备信息

显示设备相关信息，包括 AXIS OS 版本和序列号。

Upgrade AXIS OS（**升级 AXIS OS**）：升级设备上的软件。前往在其中进行升级的维护页面。

设备

警报

移动设备：打开当检测到设备移动时在系统中触发警报。

外壳打开：打开当检测到门禁控制器的外壳打开时在系统中触发警报。关闭裸机门禁控制器的此设置。

外部篡改：当检测到外部篡改时，打开以在系统中触发警报。例如，当外部机柜打开或关闭时。

- Relay（**正常状态**：）如果是开路，单击，闭路则单击。
- **监控输入**：打开以监控输入状态，并配置线路上的电阻。
  - 要使用并联首次连接，请选择**带有 22 KΩ 并联电阻器和 4.7 KΩ 串联电阻器的并联首次连接**。
  - 要使用串行首次连接，请选择**串行首次连接**，然后从**电阻值**下拉列表中选择电阻值。

联网

读卡器

添加：单击添加读卡器。

Axis network readers（**安讯士网络读卡器**）：您最多可向控制器添加16个蓝牙读卡器，无需许可证。

- Name（**名称**）：为连接的读卡器输入一个名称。
- Reader（**读卡器**）：从下拉列表中选择读卡器。
- **IP 地址**：手动输入读卡器的 IP 地址。
- **用户名**：输入读卡器用户名。
- **密码**：输入读卡器密码。
- **忽略服务器证书验证**：开启此选项以忽略验证。
- **I/O 端口和继电器**：展开以配置I/O端口和继电器。
  - Port（**端口**）：显示端口的名称。
  - Direction（**方向**）：指示它是一个输入或输出端口。
  - Relay（**正常状态**：）如果是开路，单击 ，闭路则单击 。

安讯士网络对讲机（需在 AXIS Camera Station 中重新配置）

- Name（**名称**）：为连接的读卡器输入一个名称。
- Reader（**读卡器**）：从下拉列表中选择读卡器。
- **IP 地址**：手动输入读卡器的 IP 地址。
- **用户名**：输入读卡器用户名。
- **密码**：输入读卡器密码。
- **忽略服务器证书验证**：开启此选项以忽略验证。

AXIS License Plate Verifier（需在 AXIS Camera Station 中重新配置）

- Name（**名称**）：为连接的读卡器输入一个名称。
- API–key（**API 密钥**）：输入 API 密钥。
- **生成**：单击生成API密钥。
- **复制API–密钥**：单击复制API密钥，将其保存在安全位置。

AXIS Barcode Reader（需在 AXIS Camera Station 中重新配置）

- Name（**名称**）：为连接的读卡器输入一个名称。
- API–key（**API 密钥**）：输入 API 密钥。
- **生成**：单击生成API密钥。
- **复制API–密钥**：单击复制API密钥，将其保存在安全位置。

编辑：选择一个读卡器，然后单击Edit（**编辑**），对所选读卡器进行更改。

删除：选择读卡器，并单击Delete（**删除**），删除所选读卡器。

无线锁

使用AH30通讯集线器，最多可连接16个ASSA ABLOY Aperio无线锁。无线锁需要许可证。

注意

您必须将AH30通讯集线器安装在安全侧。

Connect communication hub（**连接通信中心**）：单击以连接无线锁。

升级

Upgrade readers（**升级读卡器**）：单击升级读卡器软件。只有受支持的读卡器在线时您才能升级它们。

升级转换器：单击升级转换器软件。只有受支持的转换器在线时您才能升级它们。

系统

时间和位置

日期和时间。

时间格式取决于网页浏览器的语言设置。

注意

我们建议您将设备的日期和时间与 NTP 服务器同步。

同步：选择设备日期和时间同步选项。

- Automatic date and time (PTP)（**自动日期和时间 (PTP)**）：使用精确时间协议进行同步。
- Automatic date and time (manual NTS KE servers)（**自动日期和时间（手动 NTS KE 服务器）**）：与安全 NTP 密钥建立连接至 DHCP 服务器的服务器进行同步。
  - **手动 NTS KE 服务器**：输入一个或两个 NTP 服务器的 IP 地址。当您使用两台 NTP 服务器时，设备会根据两者的输入同步并调整其时间。
  - Trusted NTS KE CA certificates（**可信NTS KE CA证书**）：选择想要使用的可信CA证书用于安全NTS KE时间同步的，或保持为无。
  - **上限 NTP 轮询时间**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
  - **NTP 轮询时间下限**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- Automatic date and time (NTP servers using DHCP)（**自动日期和时间（使用 DHCP 的 NTP 服务器）**）：与连接到 DHCP 服务器的 NTP 服务器同步。
  - **备用 NTP 服务器**：输入一个或两个备用服务器的 IP 地址。
  - **上限 NTP 轮询时间**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
  - **NTP 轮询时间下限**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- Automatic date and time (manual NTP servers)（**自动日期和时间（手动 NTP 服务器）**）：与您选择的 NTP 服务器同步。
  - **手动 NTP 服务器**：输入一个或两个 NTP 服务器的 IP 地址。当您使用两台 NTP 服务器时，设备会根据两者的输入同步并调整其时间。
  - **上限 NTP 轮询时间**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间上限。
  - **NTP 轮询时间下限**：选择设备在轮询 NTP 服务器以获取更新时间之前应等待的时间下限。
- **自定义日期和时间**：手动设置日期和时间。单击**从系统获取**以从计算机或移动设备获取日期和时间设置。

时区：选择要使用的时区。时间将自动调整为夏令时和标准时间。

- DHCP：采用 DHCP 服务器的时区。设备必须连接到 DHCP 服务器（v4 或 v6），然后才能选择此选项。如果两种版本都可用，设备优先选择 IANA 时区而非 POSIX 时区，并优先使用 DHCPv4 而非 DHCPv6。
  - DHCPv4 选择选项 100 用于 POSIX 时区，选择选项 101 用于 IANA 时区。
  - DHCPv6 选择选项 41 用于 POSIX，选择选项 42 用于 IANA。
- **手动**：从下拉列表中选择时区。

注意

系统在各录像、日志和系统设置中使用日期和时间设置。

时间同步状态：显示 NTP 同步信息和 PTP 状态。

网络时间同步捕获：打开此功能可允许多台摄像机同时捕捉图像。

网络：

网络：

IPv4

自动分配 IPv4：选择 IPv4 自动获取 IP 地址 (DHCP)，即可由网络自动分配您的 IP 地址、子网掩码和路由器，无需手动配置。我们建议大多数网络采用自动 IP 分配 (DHCP)。

IP 地址：为设备输入唯一的IP地址。在独立的网络中可随机分配静态 IP 地址，只要每个指定地址是唯一的。为避免冲突，建议在分配静态 IP 地址前联系网络管理员。

子网掩码：输入子网掩码，以定义局域网内的地址。局域网之外的地址都通过路由器。

路由器：输入默认路由器（网关）的 IP 地址用于连接已连接至不同的网络和网段的设备。

如果 DHCP 不可用，退回到静态 IP 地址：如果希望在 DHCP 不可用且无法自动分配 IP 地址时，添加要用作备用静态 IP 地址，请选择此项。

注意

如果 DHCP 不可用且设备使用备用静态地址，则静态地址配置范围有限。

IPv6

自动分配 IPv6：选择打开 IPv6 并让网络路由器自动分配设备的 IP 地址。

主机名

自动分配主机名称：选择让网络路由器自动分配设备的主机名称。

主机名称：手动输入主机名称，作为访问设备的另一种方式。服务器报告和系统日志使用主机名。允许的字符是 A–Z, a–z, 0–9 和 –。

启动动态 DNS 更新： 允许设备在 IP 地址更改时自动更新其域名服务器记录。

注册 DNS 名称：输入指向设备IP地址的唯一域名。允许的字符是 A–Z, a–z, 0–9 和 –。

TTL：生存时间 (TTL) 设置 DNS 记录在需要更新之前保持有效的时长。

DNS 服务器

自动分配 (DNS)：选择以让 DHCP 网络路由器自动向设备分配搜索域和 DNS 服务器地址。我们建议大多数网络采用自动 DNS（DHCP）。

搜索域：当您使用不完全合格的主机名时，请单击**添加搜索域**并输入一个域，以在其中搜索设备使用的主机名称。

DNS 服务器：单击**添加 DNS 服务器**并输入 DNS 服务器的 IP 地址。此服务器提供主机名到网络上 IP 地址的转换。

注意

如果禁用 DHCP，依赖自动网络配置的功能（如主机名、DNS 服务器、NTP 等）可能停止工作。

HTTP 和 HTTPS

HTTPS 是一种协议，可为来自用户的页面请求和网络服务器返回的页面提供加密。加密的信息交换使用 HTTPS 证书进行管理，这保证了服务器的真实性。

要在设备上使用 HTTPS，必须安装 HTTPS 证书。转到**系统 > 安全性**以创建和安装证书。

允许访问浏览：选择是否允许用户通过HTTP、HTTPS 或同时通过HTTP 和 HTTPS 协议连接到设备。

注意

如果通过 HTTPS 查看加密的网页，则可能会出现性能下降，尤其是您首次请求页面时。

HTTP port（HTTP 端口）：输入要使用的 HTTP 端口。设备允许端口 80 或范围 1024–65535 中的端口。如果您以管理员身份登录，则您还可以输入 1–1023 范围内的端口。如果您使用此范围内的端口，您将得到一个警告。

HTTPS port（HTTPS 端口）：输入要使用的 HTTPS 端口。设备允许端口 443 或范围 1024–65535 中的端口。如果您以管理员身份登录，则您还可以输入 1–1023 范围内的端口。如果您使用此范围内的端口，您将得到一个警告。

证书：选择要为设备启用 HTTPS 的证书。

网络发现协议

Bonjour®：选中此项，允许在网络上自动发现设备。

Bonjour 名称：键入要在网络中显示的昵称。默认名称为设备名加 MAC 地址。

UPnP®：选中此项，允许在网络上自动发现设备。

UPnP 名称：键入要在网络中显示的昵称。默认名称为设备名加 MAC 地址。

WS–Discovery（WS–Discovery）：选中此项，允许在网络上自动发现设备。

LLDP and CDP（LLDP 和 CDP）：选中此项，允许在网络上自动发现设备。如果不允许使用 LLDP 和 CDP，可能会影响 PoE 电源协商。若要解决 PoE 电源协商问题，请仅为硬件 PoE 电源协商配置 PoE 交换机。

Neighbors（邻近设备）：单击此选项，将显示与连接到同一网络的邻近设备相关的信息。

一键云连接

一键云连接 (O3C) 与 O3C 服务结合使用，可从不同位置通过互联网安全地访问实时视频和录制的视频。有关详细信息，请参见*axis.com/end–to–end–solutions/hosted–services*。

允许 O3C：

- One-click（**一键**）：这是默认选项。按下设备上的控制按钮，即可连接到 O3C。根据设备型号的不同，按下并松开或按住不放，直到状态 LED 指示灯闪烁。在 24 小时内向 O3C 服务注册设备，启用 Always（**总是**）选项并保持连接。如果不注册，设备将断开与 O3C 的连接。
- **总是**：设备将不断尝试通过互联网连接到 O3C 服务。一旦注册设备，就会保持连接。如果无法够到控制按钮，则使用此选项。
- No（**无**）：断开 O3C 服务连接。

代理设置：如果需要，请输入代理设置以连接到代理服务器。

主机：输入代理服务器的地址。

Port（**端口**）：输入用于访问的端口号。

登录和**密码**：如果需要，请输入代理服务器的用户名和密码。

身份验证方法：

- **基本**：此方法是 HTTP 兼容的身份验证方案。它的安全性不如**摘要** 方法，因为它将用户名和密码发送到服务器。
- **摘要**：此方法一直在网络中传输加密的密码，因此更安全。
- Auto（**自动**）：借助此选项，可使设备根据支持的方法自动选择身份验证方法。**摘要**方法优先于**基本**方法。

Owner authentication key (OAK)（**所有者身份验证密钥** (OAK)）：单击Get key（**获取密码**）以获取所有者的身份验证密钥。只有在没有防火墙或代理的情况下设备连接到互联网时，才可能发生这种情况。

SNMP

简单网络管理协议 (SNMP) 允许远程管理网络设备。

SNMP：选择要使用的 SNMP 版本。

- **v1 和 v2c**：
  - **读取团体**：输入可只读访问支持的 SNMP 目标的团体名称。默认值为**公共**。
  - **编写社区**：输入可读取或写入访问支持全部的 SNMP 目标（只读目标除外）的团体名称。默认值为**写入**。
  - **激活陷阱**：打开以激活陷阱报告。该设备使用陷阱发送重要事件或更改状态的消息到管理系统。在网页界面中，您可以设置 SNMP v1 和 v2c 的陷阱。如果您更改为 SNMP v3 或关闭 SNMP，陷阱将自动关闭。如果使用 SNMP v3，则可通过 SNMP v3 管理应用程序设置陷阱。
  - **陷阱地址**：输入管理服务器的 IP 地址或主机名。
  - **陷阱团体**：输入设备发送陷阱消息到管理系统时要使用的团体。
  - **陷阱**：
    - **冷启动**：设备启动时发送陷阱消息。
    - **建立连接**：链接自下而上发生变更时，发送陷阱消息。
    - **断开连接**：链接自上而下发生变更时，发送陷阱消息。
    - **身份验证失败**：验证尝试失败时，发送陷阱消息。

注意

打开SNMP v1和v2c陷阱时，将启用Axis Video MIB陷阱。有关更多信息，请参见 *AXIS OS Portal > SNMP*。

- **v3**：SNMP v3 是一个提供加密和安全密码的更安全版本。若要使用 SNMP v3，我们建议激活 HTTPS，因为密码将通过 HTTPS 发送。这还会防止未授权方访问未加密的 SNMP v1 及 v2c 陷阱。如果使用 SNMP v3，则可通过 SNMP v3 管理应用程序设置陷阱。
  - **隐私**：选择用于保护您的SNMP数据的加密方式。
  - **Password for the account “initial”（账户“initial”的密码）**：输入名为'initial'的帐户的 SNMP 密码。尽管可在不激活 HTTPS 的情况下发送密码，但我们不建议这样做。SNMP v3 密码仅可设置一次，并且推荐仅在 HTTPS 启用时。一旦设置了密码，密码字段将不再显示。要重新设置密码，则设备必须重置为出厂默认设置。请注意，密码必须符合密码策略，请参阅 *帐户, on page 54*。

连接的客户端

显示连接和连接的客户端数量。

查看详细信息：查看和更新已连接客户端列表。该列表显示了每个连接的 IP 地址、协议、端口、状态和 PID/进程。

安全：

认证

证书用于对网络上的设备进行身份验证。该设备支持两种类型的证书：

- **客户端/服务器证书**
  客户端/服务器证书用于验证设备身份，可以是自签名证书，也可以是由证书颁发机构颁发的证书。自签名证书提供有限的保护，可在获得 CA 颁发的证书之前使用。
- **证书**
  您可以使用 CA 证书来验证对等证书，例如，在设备连接到受 IEEE 802.1X 保护的网络时，用于验证身份验证服务器的身份。设备具有几个预装的 CA 证书。

支持以下格式：

- 证书格式：PEM、CER 以及 。PFX
- 私钥格式：PKCS#1 和 PKCS#12

重要

如果将设备重置为出厂默认设置，将删除各证书。预安装的 CA 证书将重新安装。

Add certificate（**添加证书**）：单击添加证书。分步指南打开。

- More（**更多**）：显示更多要填充或选择的栏。
- **安全密钥库**：选择以使用**可信执行环境** (SoC TEE)、**安全元件**或**可信平台模块** 2.0 来安全存储私钥。有关选择哪个安全密钥库的更多信息，请转至 *help.axis.com/axis-os#cryptographic-support*。
- **密钥类型**：从下拉列表中选择默认或其他加密算法以保护证书。

上下文菜单包括：

- **证书信息**：查看已安装证书的属性。
- **删除证书**：删除证书。
- **创建证书签名请求**：创建证书签名请求，发送给注册机构以申请数字身份证书。

安全密钥库：

- Trusted Execution Environment (SoC TEE)（**可信执行环境** (SoC TEE)）：选中此项，使用 SoC TEE 作为安全密钥库。
- Secure element (CC EAL6+, FIPS 140-3 Level 3)（**安全元件**（CC EAL6+、FIPS 140-3 **第 3 级**））：选择使用安全元素来实现安全密钥库。
- Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)（**可信平台模块** 2.0（CC EAL4+、FIPS 140-2 **第 2 级**））：安全密钥库选择使用 TPM 2.0。

网络访问控制和加密

IEEE 802.1x

IEEE 802.1x 是针对基于端口的网络管理控制一种 IEEE 标准，可提供有线和无线网络设备的安全身份验证。IEEE 802.1x 基于 EAP（可扩展身份验证协议）。

要访问受 IEEE 802.1x 保护的网络，网络设备必须对其自身进行身份验证。该身份验证由身份验证服务器执行，通常是 RADIUS 服务器（例如，FreeRADIUS 和 Microsoft Internet Authentication Server）。

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec 是一项针对媒体访问控制（MAC）安全性的 IEEE 标准，它定义了媒体访问独立协议无连接数据的机密性和完整性。

认证

在不配置 CA 证书时，这意味将禁用服务器证书验证，不管网络是否连接，设备都将尝试进行自我身份验证。

在使用证书时，在安讯士的实施中， 设备和身份验证服务器通过使用 EAP–TLS（可扩展身份验证协议 – 传输层安全）的数字证书对其自身进行身份验证。

要允许设备访问通过证书保护的网络，您必须在设备上安装已签名的客户端证书。

身份验证方法：选择用于身份验证的 EAP 类型。

Client certificate（客户端证书）：选择客户端证书以使用 IEEE 802.1 x。使用证书可验证身份验证服务器的身份。

CA Certificates（CA 证书）：选择一个 CA 证书来验证身份验证服务器的身份。未选择证书无时，无论连接到哪个网络，设备都将尝试进行自我身份验证。

EAP 身份：输入与客户端的证书关联的用户标识。

EAPOL 版本：选择网络交换机中使用的 EAPOL 版本。

Use IEEE 802.1x（使用 IEEE 802.1x）：选择以使用 IEEE 802.1 x 协议。

仅当您使用**IEEE 802.1x PEAP–MSCHAPv2** 作为身份验证方法时，这些设置才可用：

- **密码**：输入您的用户标识密码。
- **Peap 版本**：选择网络交换机中使用的 Peap 版本。
- **Label（标签）**：选择 1 使用客户端 EAP 加密；选择 2 使用客户端 PEAP 加密。选择使用 Peap 版本 1 时网络交换机使用的标签。

仅当您使用**IEEE 802.1ae MACsec（静态 CAK/预共享密钥）**作为身份验证方法时，这些设置才可用：

- **密钥协议连接关联密钥名称**：输入连接关联名称 (CKN)。必须为 2 到 64（可被 2 整除）个十六进制字符。必须在连接关联中手动配置 CKN，而且链路两端的 CKN 必须匹配，才能初始启用 MACsec。
- **密钥协议连接关联密钥**：输入连接关联密钥 (CAK)。其长度应为 32 或 64 个十六进制字符。必须在连接关联中手动配置 CAK，而且链路两端的 CAK 必须匹配，才能初始启用 MACsec。

防止蛮力攻击

正在阻止：开启以阻止强力攻击。强力攻击使用试验和错误来猜测登录信息或加密密钥。

阻止期：输入阻止暴力攻击的秒数。

阻止条件：输入在阻止开始之前每秒允许的身份验证失败次数。您可设置页面级和设备级上所允许的失败次数。

防火墙

防火墙：开启以启用防火墙。

默认策略：选择希望防火墙如何处理规则未涵盖的连接请求。

- ACCEPT（**接受**）：允许与设备的所有连接。默认情况下设置此选项。
- DROP（**丢弃**）：阻止与设备的所有连接。

要对默认策略进行例外处理，您可以创建允许或阻止从特定地址、协议和端口连接到设备的规则。

+ New rule（**+ 新规则**）：单击以创建规则。

Rule type（**规则类型**）：

- **过滤器**：选中此项，允许或阻止来自符合规则中定义条件的设备的连接。
  - **策略**：为防火墙规则选择 Accept（**接受**）或 Drop（**丢弃**）。
  - IP range（**IP 范围**）：选择以指定允许或阻止的地址范围。在 Start（**开始**）和 End（**结束**）中使用 IPv4/IPv6。
  - IP **地址**：输入要允许或阻止的地址。使用 IPv4/IPv6 或 CIDR 格式
  - **协议**：选择要允许或阻止的网络协议（TCP、UDP 或两者都是）。如果选择协议，还必须指定端口。
  - MAC：输入要允许或阻止的设备的 MAC 地址。
  - Port range（**端口范围**）：选择以指定允许或阻止的端口范围。将它们添加到Start（**开始**）和 End（**结束**）中。
  - Port（**端口**）：输入要允许或阻止访问的端口号。端口号必须介于 1 和 65535 之间。
  - Traffic type（**通信流类型**）：选择要允许或阻止的通信流类型。
    - UNICAST（**单播**）：流量从单个发送方传输到单个接收方。
    - BROADCAST（**广播**）：流量从单个发送方传输到网络上的所有设备。
    - MULTICAST（**组播**）：流量从一个或多个发送方传输到一个或多个接收方。
- LIMIT（**限制**）：选中此项，接受来自符合规则中定义条件的设备的连接，但应用限制以减少过多流量。
  - IP range（**IP 范围**）：选择以指定允许或阻止的地址范围。在 Start（**开始**）和 End（**结束**）中使用 IPv4/IPv6。
  - IP **地址**：输入要允许或阻止的地址。使用 IPv4/IPv6 或 CIDR 格式
  - **协议**：选择要允许或阻止的网络协议（TCP、UDP 或两者都是）。如果选择协议，还必须指定端口。
  - MAC：输入要允许或阻止的设备的 MAC 地址。
  - Port range（**端口范围**）：选择以指定允许或阻止的端口范围。将它们添加到Start（**开始**）和 End（**结束**）中。
  - Port（**端口**）：输入要允许或阻止访问的端口号。端口号必须介于 1 和 65535 之间。
  - Unit（**单位**）：选择允许或阻止的连接类型。
  - Period（**时段**）：选择与 Amount（**数量**）相关的时间段。
  - Amount（**数量**）：设置设备在设定 Period（**时段**）内的最大允许连接次数。最大数量为 65535。
  - Burst（**突发**）：在设定 Period（**时段**）内，输入允许超过设定 Amount（**数量**）一次的连接次数。一旦达到这个数字，就只允许在设定时段内的设定数量。
  - Traffic type（**通信流类型**）：选择要允许或阻止的通信流类型。
    - UNICAST（**单播**）：流量从单个发送方传输到单个接收方。
    - BROADCAST（**广播**）：流量从单个发送方传输到网络上的所有设备。

- MULTICAST（**组播**）：流量从一个或多个发送方传输到一个或多个接收方。

Test rules（**测试规则**）：单击以测试已定义的规则。

- Test time in seconds（**测试时间（秒）**）：设置测试规则的时间限制。
- **还原**：在测试规则之前，单击可将防火墙回滚到之前的状态。
- Apply rules（**应用规则**）：单击此选项，可激活规则，而不执行测试。我们不建议您这样做。

自定义签名的 AXIS OS 证书

要在设备上安装来自安讯士的测试软件或其他自定义软件，您需要自定义签名的 AXIS OS 证书。证书验证软件是否由设备权利人和安讯士批准。软件只能在由其单一序列号和芯片 ID 标识的特定设备上运行。只有安讯士可以创建自定义签名 AXIS OS 证书，因为安讯士持有对其进行签名的密钥。

安装：单击安装以安装证书。在安装软件之前，您需要安装证书。

上下文菜单包括：

- **删除证书**：删除证书。

帐户

设备账户

帐户

Add account（**添加账户**）：单击以添加新帐户。您可以添加多达 100 个帐户。

账户：输入唯一的帐户名。

新密码：输入帐户的密码。密码长度必须为 1 到 64 个字符。密码仅允许包含可打印的ASCII字符（代码32–126），如字母、数字、标点符号和某些符号。

确认密码：再次输入同一密码.

优先权：

- **管理员**：可完全访问全部设置。管理员也可以添加、更新和删除其他帐户。
- **操作员**：有权访问全部设置，以下各项除外：
  - 全部 System（**系统**）设置。
- **观看者**：没有权限更改设置。

上下文菜单包括：

更新帐户：编辑帐户的属性。

删除帐户：删除帐户。无法删除根帐户。

MQTT：

MQTT（消息队列遥测传输）是用于物联网（IoT）的标准消息协议。它旨在简化IoT集成，并在不同行业中使用，以较小的代码需求量和尽可能小的网络带宽远程连接设备。安讯士设备软件中的MQTT 客户端可使设备中的数据和事件集成至非视频管理软件 (VMS) 系统的流程简化。

将设备设置为 MQTT 客户端。MQTT 通信基于两个实体、客户端和中间件。客户端可以发送和接收消息。代理负责客户端之间路由消息。

您可以在 *AXIS OS Knowledge Base* 中了解有关 MQTT 的更多信息。

ALPN

ALPN 是一种 TLS/SSL 扩展，允许在客户端和服务器之间的连接信号交换阶段中选择应用协议。这用于在使用其他协议（如 HTTP）的同一个端口上启用 MQTT 流量。在某些情况下，可能没有为 MQTT 通信打开专用端口。这种情况下的解决方案是使用 ALPN 来协商将 MQTT 用作标准端口上的应用协议（由防火墙允许）。

MQTT 客户端

连接：打开或关闭 MQTT 客户端。

状态：显示 MQTT 客户端的当前状态。

代理

主机：输入 MQTT 服务器的主机名或 IP 地址。

协议：选择要使用的协议.

Port（端口）：输入端口编号。

- 1883 是 **MQTT over TCP** 的默认值。
- 8883 是**SSL 的 MQTT** 的默认值
- 80 是 **WebSocket 的 MQTT** 的默认值
- 443 是**WebSocket Secure 的 MQTT** 的默认值

ALPN 协议：输入 MQTT 代理提供商提供的 ALPN 协议名称。这仅适用于 SSL 的 MQTT 和 WebSocket Secure 的 MQTT。

用户名：输入客户将用于访问服务器的用户名。

密码：输入用户名的密码。

Client ID（客户端 ID）:输入客户端 ID。客户端连接服务器时，会将客户端标识符发送给服务器。

清理会话：控制连接和断开时间的行为。选定时，状态信息将在连接及断开连接时被丢弃。

Http proxy（HTTP 代理）：最大长度为 255 字节的 URL。如果您不想使用 HTTP 代理，则可以将该字段留空。

Https proxy（HTTPS 代理）：最大长度为 255 字节的 URL。如果您不想使用 HTTPS 代理，则可以将该字段留空。

保持活动状态间隔：让客户端能够在无需等待长 TCP/IP 超时的情况下，侦测服务器何时停用。

超时：允许连接完成的时间间隔（以秒为单位）。默认值：60

设备主题前缀：在**MQTT 客户端**选项卡上的连接消息和 LWT 消息中的主题默认值中使用，以及在**MQTT 发布**选项卡上的发布条件中使用。

自动重新连接：指定客户端是否应在断开连接后自动重新连接。

连接消息

指定在建立连接时是否应发送消息。

发送消息：打开以发送消息。

使用默认设置：关闭以输入您自己的默认消息。

主题：输入默认消息的主题。

有效负载：输入默认消息的内容。

保留：选择以保留此**主题**的客户端状态

QoS：更改数据包流的 QoS 层。

最后证明消息

终了证明（LWT）允许客户端在连接到中介时提供证明及其凭证。如果客户端在某点后仓促断开连接（可能是因为电源失效），它可以让代理向其他客户端发送消息。此终了证明消息与普通消息具有相同的形式，并通过相同的机制进行路由。

发送消息：打开以发送消息。

使用默认设置：关闭以输入您自己的默认消息。

主题：输入默认消息的主题。

有效负载：输入默认消息的内容。

保留：选择以保留此**主题**的客户端状态

QoS：更改数据包流的 QoS 层。

MQTT 出版

使用默认主题前缀：选择以使用默认主题前缀，即在**MQTT 客户端**选项卡中的设备主题前缀的定义。

Include condition（**包含条件**）：选择以包含描述 MQTT 主题中的条件的主题。

Include namespaces（**包含命名空间**）：选择以将 ONVIF 主题命名空间包含在 MQTT 主题中。

包含序列号：选择以将设备的序列号包含在 MQTT 有效负载中。

＋ Add condition（**添加条件**）：单击以添加条件。

保留：定义将哪些 MQTT 消息作为保留发送。

- None（**无**）：全部消息均以不保留状态发送。
- **性能**：仅将有状态消息发送为保留。
- All（**全部**）：将有状态和无状态消息作为保留发送。

QoS：选择 MQTT 发布所需的级别。

MQTT 订阅

＋ Add subscription（**添加订阅**）：单击以添加一个新的 MQTT 订阅。

订阅筛选器：输入要订阅的 MQTT 主题。

注意

如果编辑订阅筛选器，请确保更新连接的事件。

使用设备主题前缀：将订阅筛选器添加为 MQTT 主题的前缀。

订阅类型：

- **无状态**：选择以将 MQTT 消息转换为无状态消息。
- **有状态**：选择将 MQTT 消息转换为条件。负载用作状态。

QoS：选择 MQTT 订阅所需的级别。

附件

I/O 端口

数字输入用于连接可在开路和闭路之间切换的外部设备，例如 PIR 传感器、门或窗传感器和玻璃破碎探测器。

数字输出用于连接继电器和 LED 等外部设备。您可通过 VAPIX® 应用程序编程接口或网页界面激活已连接的设备。

端口

Name（**名称**）：编辑文本来重命名端口。

Direction（**方向**）：表示端口是输入端口。表示端口是输出端口。如果端口可配置，则您可以单击这些图标以在输入和输出之间进行切换。

Relay（**正常状态**：）如果是开路，单击，闭路则单击。

Current state（**当前状态**）：显示端口的当前状态。在当前状态并非正常状态时，将激活输入或输出。当断开连接或电压高于 1 VDC 时，设备上的输入为开路。

注意

在重启过程中，输出电路为开路。当重启完成时，电路将恢复为正常位置。如果更改此页面上设置，无论是否存在活动的触发器，输出电路都将返回其正常位置。

监控：如果有人篡改连接到数字 I/O 设备，请打开，以侦测并触发响应。除了侦测某个输入是否打开或关闭外，您还可以侦测是否有人篡改了该输入（即，剪切或短路）。监控连接功能要求外部 I/O 回路中存在其他硬件（线尾电阻器）。

日志

报告和日志

报告

- **查看设备服务器报告**：在弹出窗口中查看有关产品状态的信息。服务器报告中自动包含访问日志。
- **下载设备服务器报告**：它创建一个 .zip 文件，其中包含一个 UTF–8 格式的完整服务器报告文本文件。要包含当前实时浏览图像的抓拍，请选择**包含图像**。当您与支持部门联系时，请始终提供服务器报告 .zip 文件。
- **下载崩溃报告**：下载和存档有关服务器状态的详细信息。崩溃报告中包含服务器报告中的信息和详细的调试信息。此报告中可能包含网络追踪之类敏感信息。可能需要几分钟时间才生成此报告。

日志

- **查看系统日志**：单击以查看有关系统事件（如设备启动、警告和重要消息）的信息。
- **查看访问日志**：单击以查看访问设备的全部失败尝试，例如，使用了错误的登录密码。
- View the audit log（**查看审计日志**）：单击可显示有关用户和系统活动的信息，例如身份验证和配置成功的或失败。

网络追踪

重要

网络跟踪文件可能包含敏感信息，例如证书或密码。

通过录制网络上的活动，网络追踪文件可帮助您排除问题。

追踪时间：选择以秒或分钟为单位的跟踪持续时间，并单击**下载**。

远程系统日志

系统日志是消息日志记录的标准。它允许分离生成消息的软件、存储消息的系统以及报告和分析这些消息的软件。每个消息都标有设施代码，指示生成消息的软件类型，并为其分配一个严重性等级。

+ Server（服务器）：单击以添加新服务器。

主机：输入服务器的主机名或 IP 地址。

格式化：选择要使用的 syslog 消息格式。

- Axis
- RFC 3164
- RFC 5424

协议：选择要使用的协议：

- UDP（默认端口为 514）
- TCP（默认端口为 601）
- TLS（默认端口为 6514）

Port（端口）：编辑端口号以使用其他端口。

严重程度：选择触发时要发送哪些消息。

类型：选择要发送的日志类型。

Test server setup（测试服务器设置）：保存设置前，向所有服务器发送测试消息。

CA 证书已设置：查看当前设置或添加证书。

维护

重启：重启设备。这不会影响当前设置。正在运行的应用程序将自动重启。

恢复：将大部分设置恢复为出厂默认值。之后，您必须重新配置设备和应用，重新安装未预安装的应用，并重新创建事件和预置。

重要

重置后保存的仅有设置是：

- 引导协议（DHCP 或静态）
- 静态 IP 地址
- 默认路由器
- 子网掩码
- 802.1X 设置
- O3C 设置
- DNS 服务器 IP 地址

出厂默认设置：将全部恢复为出厂缺省值。之后，您必须重置 IP 地址，以便访问设备。

注意

安讯士设备软件均经过数字签名以确保仅在设备上安装经过验证的软件。这会进一步提高安讯士设备的总体网络安全级别门槛。有关详细信息，请参见*axis.com* 上的白皮书“Axis Edge Vault”。

AXIS OS 升级：升级到新的 AXIS OS 版本。新版本中可能包含改进的功能、补丁和全新功能。建议您始终使用新 AXIS OS 版本。要下载更新版本，前往 *axis.com/support*。

升级时，您可以在三个选项之间进行选择：

- **标准升级**：升级到新的 AXIS OS 版本。
- **出厂默认设置**：升级并将设置都恢复为出厂默认值。当您选择此选项时，无法在升级后恢复到以前的 AXIS OS 版本。
- **自动回滚**：在规定时间内升级并确认升级。如果您没有确认，设备将恢复到以前的 AXIS OS 版本。

AXIS OS 回滚：恢复为先前安装的 AXIS OS 版本。

T10125657_zh

2026-09 (M15.3)

© 2018 – 2026 Axis Communications AB