AXIS A1001 & AXIS Entry Manager

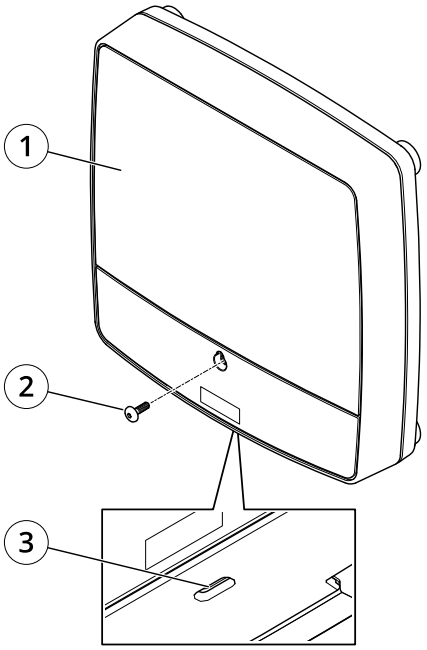
用户手册

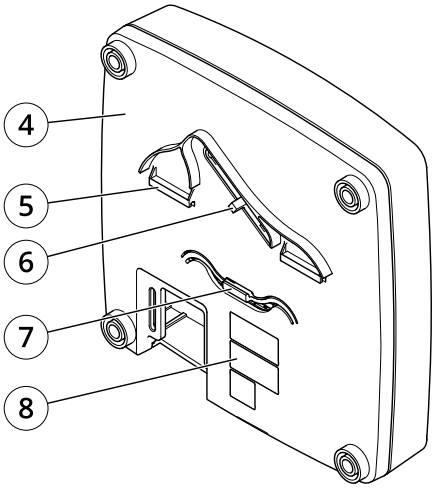
目录

目录

产品概述

产品概述

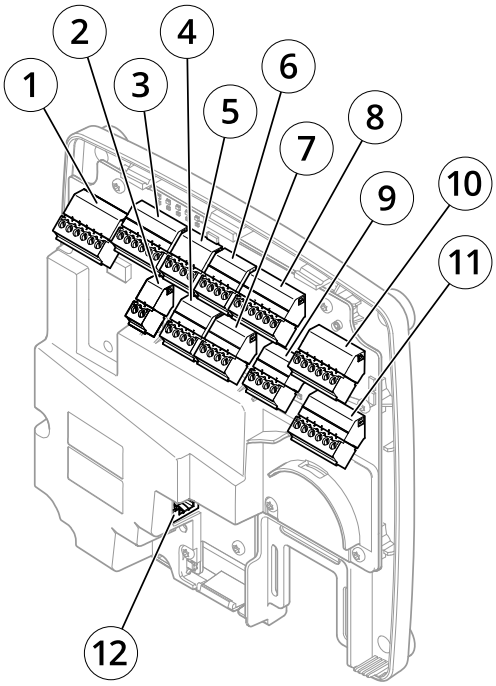




正面和背面：

1 机盖
2 机盖螺丝
3 机盖移除槽
4 底座
5 DIN 轨道 – 上
6 篡改报警开关 – 背面
7 DIN 轨道安装夹 – 下
8 部件号 (P/N) 和序列号 (S/N)

产品概述

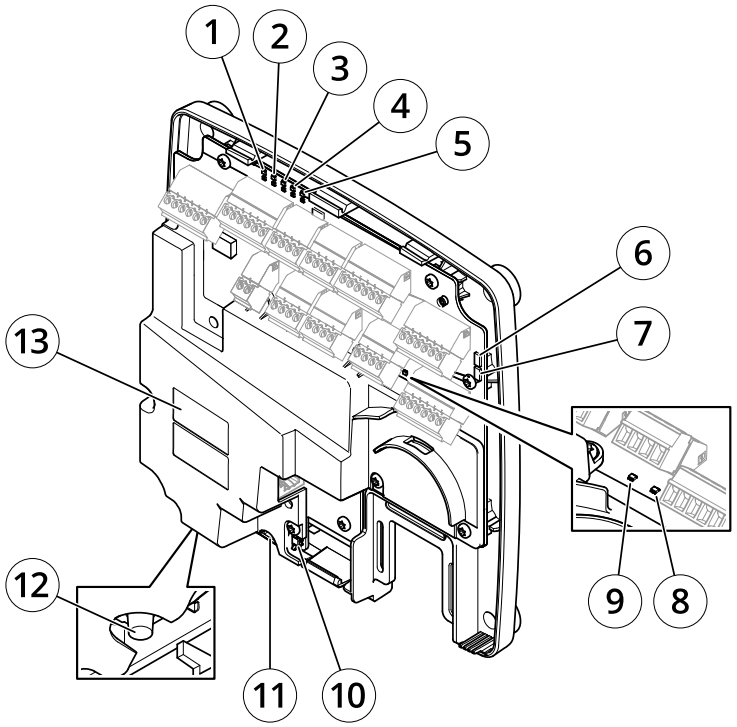


I/O 接口：
1 读卡器数据连接器 (READER DATA 1)
10 读卡器数据连接器 (READER DATA 2)
3 读卡器 I/O 连接器 (READER I/O 1)
8 读卡器 I/O 连接器 (READER I/O 2)
4 门连接器 (DOOR IN 1)
7 门连接器 (DOOR IN 2)
6 辅助连接器 (AUX)
5 音频连接器 (AUDIO)（未使用）

外部电源输入：
2 电源连接器 (DC IN)
12 网络连接器 (PoE)

电源输出：
9 电源锁连接器 (LOCK)
11 电源和中继连接器（PWR、RELAY）

产品概述



LED 指示灯、按钮和其他硬件：

1 *LED 电源指示灯*
2 *LED 状态指示灯*
3 *网络 LED 指示灯*
4 *读卡器 2 LED 指示灯（未使用）*
5 *读卡器 1 LED 指示灯（未使用）*
6 *篡改报警接头 – 前 (TF)*
7 *篡改报警接头 – 后 (TB)*
8 *LED 锁指示灯*
9 *LED 锁指示灯*
10 *篡改报警传感器 – 前*
11 *SD 卡槽 (microSDHC)（未使用）*
12 *控制按钮*
13 *部件号 (P/N) 和序列号 (S/N)*

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。
	橙色	稳定表示连接到 10 MBit/s 网络。闪烁表示网络活动。
	不亮	没有网络连接。
状态	绿色	绿色常亮表示正常工作。
	橙色	在启动期间和还原设置时稳定。
	红色	缓慢闪烁表示升级失败。

电源	绿色	工作正常。
	橙色	在固件升级过程中呈绿色/橙色闪烁。
锁定	绿色	未通电时常亮。
	红色	通电后常亮。
	不亮	浮动状态。

注

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

连接器和按钮

I/O 接口

读卡器数据连接器
支持 RS485 的两个 6 针接线端子和用于与读卡器通信的 Wiegand 协议。具体规格请参见*63*。

读卡器 I/O 连接器
用于读卡器输入和输出的两个 6 针接线端子。除 0 V DC 参考点和电源（DC 输出）外，读卡器 I/O 连接器还提供连接至以下模块的接口：

- 数字输入 – 用于连接，例如，连接读卡器篡改报警。
- 数字输出 – 用于连接，例如，连接读卡器蜂鸣器和读卡器 LED。

具体规格请参见*63*。

门连接器
两个用于连接门禁监控设备和请求退出 (REX) 设备的 4 针接线端子。具体规格请参见*64*。

辅助连接器
4 针可配置 I/O 接线端子。用于外部设备，例如与篡改报警、事件触发和警报通知结合使用。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的报警输入，例如 PIR 传感器或玻璃破碎侦测器。
- 数字输出 – 用于连接防窃报警器、警报器或灯等外部设备。已连接的设备可通过 VAPIX® 应用程序编程接口或由操作规则激活。

具体规格请参见*65*。

外部电源输入

注意

该产品应使用屏蔽网络电缆 (STP) 进行连接。将产品连接到网络的电缆应用于其特定用途。确保根据制造商的说明安装网络设备。有关法规要求的信息，请参见。

电源连接器
2 针接线端子，用于 DC 电源输入。使用一个额定输出功率限制在 ≤ 100 W 或额定输出电流限制在 ≤ 5 A 的安全超低电压 (SELV) 兼容式限功率电源 (LPS)。具体规格请参见*65*。

网络连接器
RJ45 以太网连接器。支持以太网供电 (PoE)。具体规格请参见*66*。

电源输出

电源锁连接器

用于连接一到两个锁的 4 针接线端子。锁连接器还可以用于为外部设备供电。具体规格请参见*66*。

电源和中继连接器

用于将电源和门禁控制器的继电器连接到外部设备（如锁和传感器）的 6 针接线端子。具体规格请参见*66*。

按钮与其他硬件

篡改报警接头
两个双引脚接头用于断开前后篡改报警的连接。具体规格请参见 *67*。

控制按钮
控制按钮用于：

- 将产品重置为出厂默认设置。请参见*59*。
- 连接至 Axis 视频托管系统服务。请参见*53*。若要连接，请按住该按钮约 1 秒，直到状态 LED 呈绿色闪烁。
- 连接到 Axis 互联网动态 DNS 服务。请参见*54*。若要连接，请按住该按钮约 3 秒。

安装

安装

要观看此视频，请转到本文档的网页版本。

www.axis.com/products/online-manual/19467#t10170589_zh

产品的安装视频。

如何访问产品

如何访问产品

要安装该 Axis 产品，请参见产品随附的安装指南。

访问设备

1. 打开浏览器并输入 Axis 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。请参见。
3. AXIS Entry Manager 将在您的浏览器中打开。如果您使用的是计算机，您将到达“概览”页面。如果您使用的是移动设备，您将到达移动登录页面。

关于移动登录页面

移动登录页面显示连接到门禁控制器的门和锁的状态。您可以进行锁定和解锁测试。刷新页面查看结果。

一个链接会将您转到 Axis Entry Manager。

注

- Axis Entry Manager 不支持移动设备。
- 如果您继续进入 Axis Entry Manager，没有返回移动登录页面的链接。

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

- 转到设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 高级。
- 单击启用。
- 手动配置 NAT 路由器以允许从互联网访问。

另请参见 *www.axiscam.net* 上的 AXIS Internet Dynamic DNS Service

注

- 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。路由器还必须支持 UPnP®。

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。请参见 *HTTPS 50*。

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。请参见*重置为出厂默认设置 59*。

若要设置密码，请直接在对话框中输入。

概览页面

AXIS Entry Manager 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或系统中的门禁控制器。

初次访问 Axis 产品时，“概览”页面将提示配置硬件、设置日期和时间、配置网络设置，并将门禁控制器配置为系统的一部分或独立式设备。有关配置系统的详细信息，请参见 *配置 – 分步 12*。

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详细信息，请参见*30*、*38* 和*50*。

配置 – 分步

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 AXIS Entry Manager 使用其他语言。请参见*选择语言 12*。
2. 设置日期和时间。请参见*12*。
3. 配置网络设置。请参见*14*。
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。请参见*配置硬件 14*。
5. 验证硬件连接。请参见*20*。
6. 配置卡和格式。请参见*21*。
7. 配置门禁控制器系统。请参见*管理网络门禁控制器 26*。

有关如何配置和管理系统的门、时间表、用户和组的信息，请参见*门禁管理 30*。

有关维护建议的信息，请参见*维护说明 29*。

注

若要添加或移除门禁控制器，添加、删除或编辑用户，或配置硬件，系统中一半以上的门禁控制器必须在线。若要检查门禁控制器状态，请转到设置 > 管理系统中的网络门禁控制器。

选择语言

AXIS Entry Manager 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

- 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，AXIS Entry Manager 将切换回英语。
- 如果您恢复产品，AXIS Entry Manager 将继续使用所选语言。
- 如果您重启产品，AXIS Entry Manager 将继续使用所选语言。
- 如果您升级固件，AXIS Entry Manager 将继续使用所选语言。

设置日期和时间

如果门控制器属于系统的一部分，那么日期和时间设置将会分配到门控制器中。这意味着，不论您是否与 NTP 服务器同步，设置都将被推送到系统中的其他控制器，请手动设置日期和时间，或从计算机上获取日期和时间。如果您看不到更改，请尝试刷新浏览器中的页面。有关管理门禁控制器的系统的详细信息，请参见*管理网络门禁控制器 26*。

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。请参见 *13*。
- 手动设置日期和时间。请参见 *13*。
- 从计算机上获取日期和时间。请参见 *13*。

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。转到设置 > 其他控制器配置 > 系统选项 > 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 54*。

如果为 NTP 服务器使用主机名称，必须配置 DNS 服务器。请参见 *DNS 配置 54*。

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。

有关网络设置的详细信息，请参见*网络 52*。

配置硬件

您必须在硬件配置页面配置硬件，然后才能够管理门和楼层。

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针图。硬件针图指导如何将设备连接到引脚，可以用作维护参考表。维护说明请参见*29*。

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。请参见*14*。
- 创建新硬件配置。请参见*15*。

注

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 14*。

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

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 15*
- *如何为无线锁创建新硬件配置 18*
- *如何使用升降机控制创建新硬件配置 (AXIS A9188) 19*

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. 为 Axis 产品输入名称。
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。有关可用选项的详细信息，请参见*如何配置门监视器和锁 15*。
5. 配置将使用的读卡器和 REX 设备并单击完成。有关可用选项的详细信息，请参见*如何配置读卡器和 REX 设备 17*。
6. 单击关闭或单击链接查看硬件针图。

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 18*。

注

- 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。
- 电动锁必须配置为辅助锁。

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。

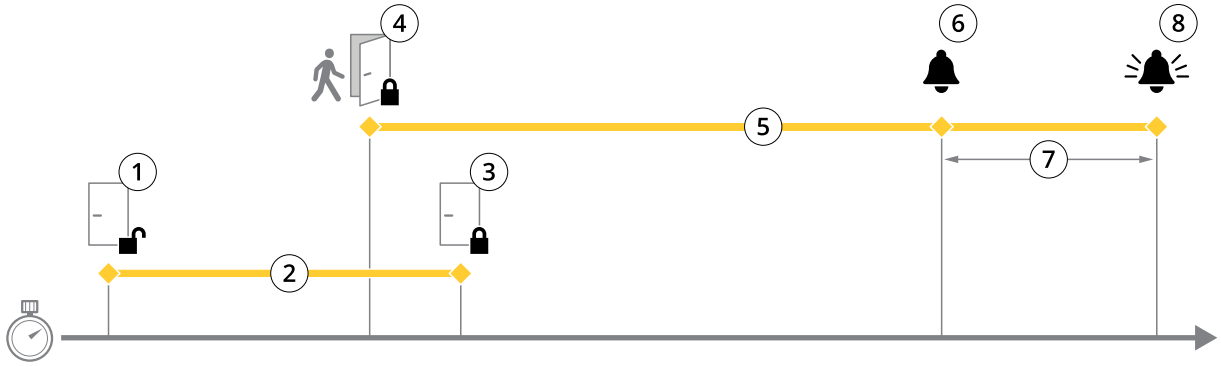
  - 开路 = 关闭门 – 如果门监视器电路常开则选择此项。当电路关闭时，门监视器向门发出打开信号。当电路打开时，门监视器向门发出关闭信号。
  - 开路 = 打开门 – 如果门监视器电路常闭则选择此项。当电路打开时，门监视器向门发出打开信号。当电路关闭时，门监视器向门发出关闭信号。
- 门打开后立即取消访问时间 – 选择此选项可防止尾随。门监视器一指示门已打开，锁便会被锁定。

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，请参见*用户凭据 38*

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

有关如何设置操作规则的信息，请参见*如何设置操作规则 44*。

关于锁选项

提供以下锁电路选项：

- 12 V
  - 断电闭门 – 为在停电期间保持保定的锁选择此项。当通上电流时，锁将解锁。
  - 自动防故障 – 为在停电期间解锁的锁选择此项。当通上电流时，锁将锁定。

- 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。
  - 继电器打开 = 锁定 – 为在继电器打开时保持锁定（断电闭门）的锁选择此项。当继电器关闭时，锁将解锁。
  - 继电器打开 = 解锁 – 为在停电期间解锁（自动防故障）的锁选择此项。当继电器关闭时，锁将锁定。
- 无 – 仅适用于锁 2。如果只使用一个锁则选择此项。

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

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

有关门禁控制器和读卡器、REX 设备以及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*68*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

以下连接器支持监控输入：

- 读卡器 I/O 连接器 – 篡改信号。请参见*63*。
- 门连接器。请参见*64*。

可与监控输入结合使用的读卡器和交换机包括：

- 内部 1 kΩ 上拉到 5 V 的 HID 读卡器。
- 内部 1 kΩ 上拉到 5 V 的读卡器和交换机。
- 无内部上拉的读卡器和交换机。

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. 为 Axis 产品输入名称。
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：单击链接查看硬件针图，或单击关闭并转到设置 > 硬件重新配置完成配置，请参见*添加 Assa Aperio™ 门和设备 18*
   - SmartIntego：单击链接查看硬件针图，或单击单击此处选择无线网关并配置门来完成配置，请参见*如何配置 SmartIntego 25*。

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

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

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

1. 在 A1001 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. 单击网络外围设备完成配置，请参见*如何添加并设置网络外围设备 19*或单击链接转到硬件针图。

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. 单击添加。

注

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. 单击添加。

目前，楼层在访问管理下的楼层选项卡中可见。

注

在 AXIS Entry Manager 中，最多可以添加 16 个楼层。

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*阅读器反馈 48*。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阅读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。
- 升降机读卡器：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*阅读器反馈 48*。另请参见制造商的说明。
- 升降机读卡器：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。
- 升降机读卡器：刷卡 – 获取有关末次刷卡或阅读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。请参见*卡格式说明 21*。
4. 单击添加字段映射，在字段中输入所需信息。请参见*字段映射 21*。
5. 若要添加多个字段映射，请重复上述步骤。

若要展开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 ，根据需要更改卡格式说明和字段映射。然后单击保存。

若要删除编辑卡格式或添加卡格式对话框中的字段映射，请单击

若要删除卡格式，请单击 。

重要

- 卡格式变更适用于整个门控制器系统。
- 如果系统中至少有一个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 14*和*如何配置读卡器和 REX 设备 17*。
- 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。

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。如果计数已经是偶数，校验位值被设置为 0。如果计数为奇数，偶数校验位值设置为 1，确保总计数是偶数。
  - 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，奇数校验位值被设置为 0。如果计数为偶数，校验位值设置为 1，确保总计数是奇数。
  - FacilityCode – 设施代码有时用于验证令牌是否与有序的终端用户凭据批次相匹配。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。十六进制系统也称以 16 为底的数字系统，由 16 个独特符号组成：数字 0–9 和字母 a–f。按从小到大的位顺序意味着第一个位最小（最不重要）。
  - 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。十六进制系统也称以 16 为底的数字系统，由 16 个独特符号组成：数字 0–9 和字母 a–f。按从大到小的位顺序意味着第一个位更大（更重要）。
  - 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。

预设设施代码

设施代码有时用于验证令牌是否与设施的门禁控制系统匹配。通常情况下，针对单个设备签发的不同令牌都具有相同的设备代码。输入预设设施代码可以更轻松地手动注册一批卡。预设设施代码会在添加用户时自动填写，请参见*用户凭据 38*

设置预设设施代码：

1. 转到设置 > 配置卡和格式。
2. 在预设设施代码下：输入设施代码。
3. 单击设置设施代码。

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。

HID Mobile Access

HID Mobile Access 通过将移动设备用作凭据来扩展访问控制。

HID Mobile Access 前提条件

您需要先满足下列前提条件，然后再为您的门禁控制器设置 HID Mobile Access：

- HID 帐户。请联系您的 HID 合作伙伴进行设置。
- 与您的 HID 帐户关联的部件号（用于移动凭据）。
- 产品需要使用传出 HTTPS 加密通信访问 HID Mobile Access 云服务器。请相应更新您的 IT 基础设施。这包括 DNS 服务器连接。

配置 HID Mobile Access

1. 单击顶部菜单中的设置。
2. 单击配置服务 > 设置。
3. 输入您的 HID 客户端 ID 和密码。
4. 如果需要，进入代理设置，然后单击连接。
5. 单击设置为当前选择要用于此安装的部件号。
6. 通过以下方法将 HID Mobile Access 添加到用户：
   - 手动创建和编辑用户（参见页面*38*上的*创建和编辑用户 38*）
   - 导入用户（参见页面*39*上的*导入用户 39*）

注

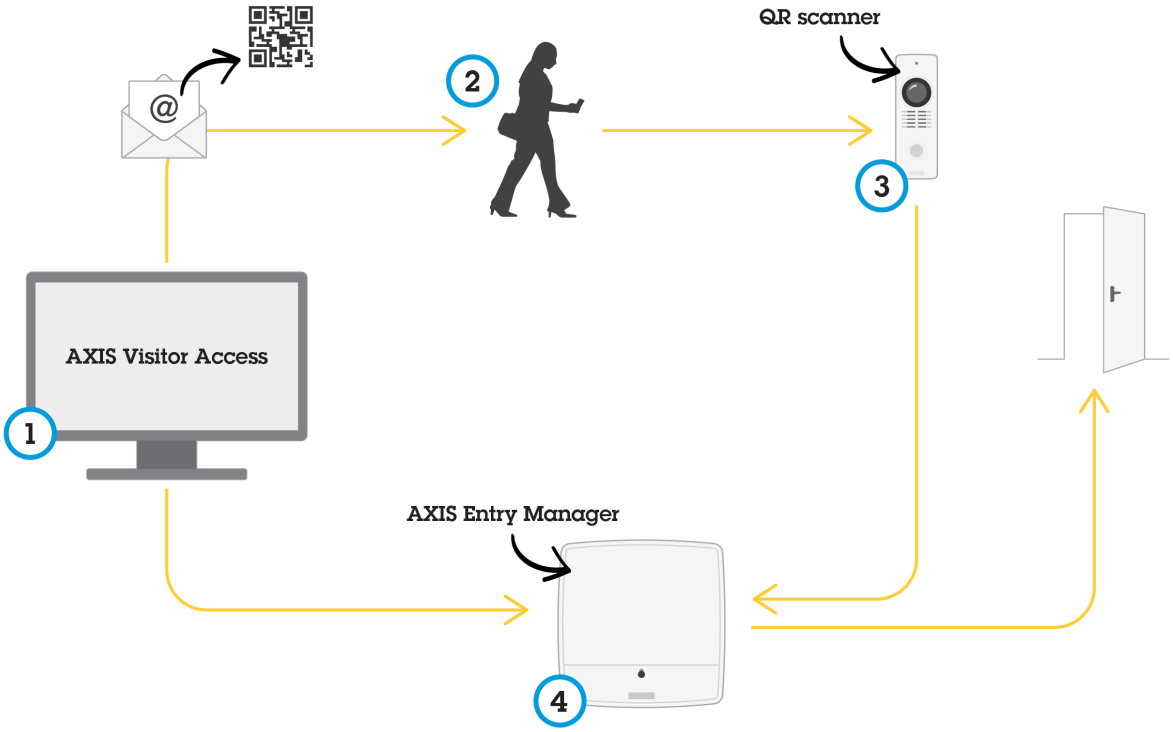
每个被授予 HID Mobile Access 访问权限的用户将收到一封电子邮件，其中包含用于继续在设备上进行安装的应用链接。

AXIS Visitor Access

借助 AXIS Visitor Access，可以二维码的形式创建临时凭证。连接到门禁控制系统的 Axis 网络摄像机或门站扫描二维码。

此服务包含：

- 一个带 AXIS Entry Manager 和 1.65.2 版或更高版固件的 Axis 门控制器。
- 一个已安装二维码扫描仪应用的 Axis 网络摄像机或门站
- 一个已安装 AXIS Visitor Access 应用的 Windows® 个人电脑



AXIS Visitor Access 服务的使用

用户在 AXIS Visitor Access (1) 中创建一个邀请，并将该邀请发送至访问者的电子邮件地址。同时，创建解锁门的凭证，并将其保存在已连接的 Axis 门控制器 (4) 中。访问者出示网络摄像机或门站 (3) 邀请中所包含的二维码，该二维码要求门控制器 (4) 为访问者开门。

QR Code 是 Denso Wave, inc 的注册商标。

AXIS Visitor Access 的先决条件

在你可以使用 AXIS Visitor Access 服务之前，你需要：

- 配置门控制器硬件
- 一个与门控制器连接的网络相同且放在门口使访问者可触及的 Axis 网络摄像机或门站
- AXIS Visitor Access 安装包。你可以在 *axis.com* 上找到它
- 两个额外的门控制器用户帐号，仅由 AXIS Visitor Access 服务使用。你需要将一个用于 AXIS Visitor Access 应用，另一个用于 QR 扫描仪应用。要了解如何创建用户帐号，请参见 *用户 50*

重要

- 你只能将 AXIS Visitor Access 服务连接至整个系统中的单一门控制器。
- 通过 AXIS Visitor Access 服务，你只能访问受已连接门控制器控制的门。你无法访问系统中的其他门。
- 使用 AXIS Visitor Access 应用修改和删除访问者。请勿使用 AXIS Entry Manager。
- 如果你更改了用于 AXIS Visitor Access 的用户帐号的密码，那么你还需要在 AXIS Visitor Access 中更新此密码。
- 如果你更改了用于二维码扫描仪应用的用户帐号的密码，那么你需要再次设置二维码扫描仪。

设置 AXIS Visitor Access

当你设置 AXIS Visitor Access 服务时，你在 Axis 网络摄像机或门站上安装 QR 扫描仪应用。你无需进行单独的安装。

1. 在门禁控制器的网页中，转到设置 > 配置服务 > 设置。
2. 单击开始新设置。
3. 按照说明完成设置。

重要

如果您想要强制使用 HTTPS，请确保门禁控制器通过 HTTPS 通信。否则，应用程序将不会与门禁控制器通信。

4. 在将用于创建临时凭证的电脑上，安装并设置 AXIS Visitor Access 应用。

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 18*。

注

- 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

- 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

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。

管理网络门禁控制器

“管理系统中的网络门禁控制器”页面显示有关门禁控制器、其系统状态以及系统中还有哪些其他门禁控制器的信息。它还让管理员可以通过添加和移除门禁控制器来更改系统设置。

重要

系统中的门控制器必须连接至相同的网络，并设置为在单一站点使用。

若要管理门禁控制器，请转到设置 > 管理系统中的网络门禁控制器。

“管理系统中的网络门禁控制器”页面包括下列面板：

- 此控制器的系统状态 – 显示门禁控制器的系统状态，支持在系统与独立模式之间切换。有关详细信息，请参见*门禁控制器系统状态 26*。
- 系统中的网络门禁控制器 – 显示有关系统中的门禁控制器的信息，包含在系统中添加和移除控制器的控制功能。有关详细信息，请参见*系统中连接的门禁控制器 27*。

门禁控制器系统状态

门禁控制器能否成为门禁控制器系统的一部分取决于其系统的状态。门禁控制器的系统状态显示在此控制器的系统状态面板中。

如果门禁控制器不是独立模式，并且您想要防止门禁控制器被添加到系统中，单击启用独立模式进入独立模式。

如果门禁控制器是独立模式，但您想要将门禁控制器添加到系统，单击停用独立模式离开独立模式。

系统模式

- 此控制器不是系统的一部分且不是独立模式 – 门禁控制器不配置为系统的一部分，并且不处于独立模式。这意味着门禁控制器处于打开状态，可由同一网络内的其他门禁控制器添加至系统。若要防止门禁控制器被添加到系统，请启用独立模式。
- 此控制器设置为独立模式 – 门禁控制器不是系统的一部分。它不能由网络中的其他门禁控制器添加到系统或添加其他门禁控制器。独立模式通常用于一个门禁控制器和一两个门的小型安装。若要允许门禁控制器被添加到系统，请停用独立模式。
- 此控制器是系统的一部分 – 门禁控制器是分布式系统的一部分。在分布式系统中，用户、组、门和时间表在连接的控制器之间共享。

系统中连接的门禁控制器

系统中的网络门禁控制器面板为下列系统更改提供控制：

- 将门禁控制器添加到系统中，请参见*向系统添加门禁控制器 27*。
- 从系统中移除门禁控制器，请参见*从系统中移除门禁控制器 28*。

连接的门禁控制器列表

系统中的网络门禁控制器面板还包括显示有关系统中已连接的门禁控制器的以下 ID 和状态信息的列表：

- 名称 – 用户定义的门禁控制器的名称。如果管理员在配置硬件时未设置名称，将显示默认名称。
- IP 地址
- MAC 地址
- 状态 – 您从其访问系统的门禁控制器将显示状态此控制器。系统中的另一个门禁控制器将显示状态在线。
- 固件版本

若要打开另一个门禁控制器的网页，请单击该控制器的 IP 地址。

若要更新列表，请单击刷新控制器列表。

注

系统中的控制器始终需要具有相同的固件版本。使用 Axis Device Manager 对整个系统中的控制器进行一次并行固件升级。

向系统添加门禁控制器

重要

配对门控制器时，添加的门控制器上的访问管理设置都将被删除且被系统的访问管理设置覆盖。

从门禁控制器列表向系统添加门禁控制器：

1. 转到设置 > 管理系统中的网络门禁控制器。
2. 单击从列表向系统添加控制器。
3. 选择您想要添加的门禁控制器。
4. 单击添加。
5. 要添加更多门禁控制器，请重复上述步骤。

通过已知的 IP 地址或 MAC 地址向系统添加门禁控制器：

1. 转到管理设备。
2. 单击通过 IP 或 MAC 地址向系统添加控制器。
3. 输入 IP 地址或 MAC 地址。
4. 单击添加。
5. 要添加更多门禁控制器，请重复上述步骤。

配对完成后，系统中的门控制器将共享用户、门、时间表和群组。

若要更新列表，请单击刷新控制器列表。

从系统中移除门禁控制器

重要

- 在从系统中移除门禁控制器之前，应重置其硬件配置。如果你跳过此步骤，则与已移除门控制器相关的门将仍然存在于系统中且无法被删除。
- 当从双控制器系统中移除门禁控制器时，两个门禁控制器都将自动切换到独立模式。

从系统中移除门禁控制器：

1. 通过您要移除的门禁控制器访问系统，然后转到设置 > 硬件配置。
2. 单击重置硬件配置。
3. 硬件配置重置后，转到设置 > 管理系统中的网络门禁控制器。
4. 在系统中的网络门禁控制器列表中，找到您想要移除的门禁控制器，然后单击从系统中移除。
5. 一个对话框将打开，提醒您重置门禁控制器的硬件配置。单击移除控制器确认。
6. 一个对话框将打开，提示您确认您想要移除该门禁控制器。单击确定确认。移除的门禁控制器现在处于独立模式。

注

- 当从系统中移除某个门控制器时，其访问管理设置也会被删除。
- 仅在线的门禁控制器可以移除。

配置模式

当你首次访问设备时，配置模式即标准模式。禁用配置模式时，设备的大部分配置功能会隐藏。

重要

禁用配置模式不应被视为一种安全功能。它的用途是停止配置错误，而不能停止更改重要设置的恶意用户。

如何禁用配置模式

1. 转到设置 > 禁用配置模式。
2. 输入 PIN，然后选择确定。

注

PIN 不是强制的。

如何启用配置模式

1. 转到设置 > 启用配置模式。
2. 输入 PIN，并选择确定。

注

如果您忘记了您的 PIN，您可以通过输入 `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode` 来启用配置模式。

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。请参见*验证控制门 20*。
- 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。请参见*验证控制门 20*。
- 请确保访问时间表、门、群组和用户均是更新的。
- 如果门禁控制器未正常工作，请参见*故障排查 60*和*维护 57*了解更多信息。

门禁管理

关于用户

在 AXIS Entry Manager 中，用户是已注册为一个或多个令牌（识别类型）的所有者的人员。每个人都必须拥有一个单一的用户配置文件，以获得访问控制系统中门的访问权限。用户配置文件由告知系统有哪些用户以及用户在何时如何被授予门访问权限的凭据组成。有关详细信息，请参见*创建和编辑用户 38*。

此上下文中的用户不应与管理员混淆。管理员可不受限制地访问设置。在管理门禁控制系统的环境中，即产品网页 (AXIS Entry Manager) 上，管理员有时也称为用户。有关详细信息，请参见*用户 50*。

门禁管理页面

“门禁管理”页面允许您配置和管理系统的用户、组、门和时间表。若要打开“门禁管理”页面，请单击门禁管理。

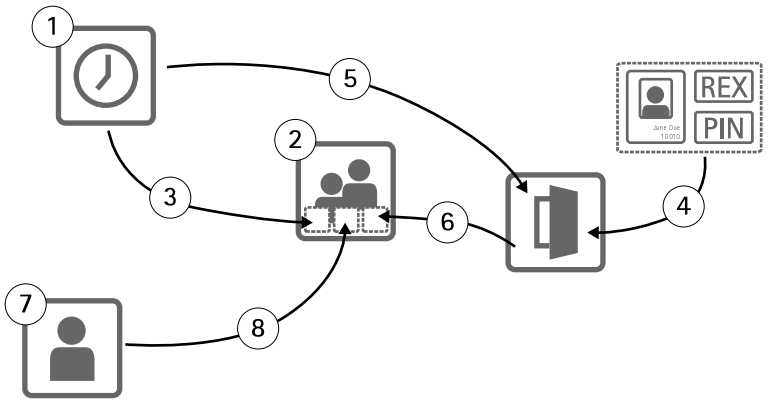
若要将用户添加到组，并应用访问时间表和门，请将项目分别拖到组和门列表中的目标位置。

注

需要执行操作的消息显示为红色文本。

选择工作流

门禁管理结构是灵活的，让您能够建立符合您需求的工作流。下面是一个工作流示例：



1. 创建访问时间表。请参见*31*。
2. 创建组。请参见*32*。
3. 对组应用访问时间表。
4. 向门或楼层添加识别类型。请参见*33*和*34*。
5. 对每个识别类型应用访问时间表。
6. 对组应用门或楼层。
7. 创建用户。请参见*38*。
8. 将用户添加到组。

要查看应用的此工作流的示例，请参见*访问时间表组合示例 40*。

创建和编辑访问时间表

访问时间表用于定义何时可以访问或不可以访问门的一般规则。它们还用于定义组何时可以访问或不可以访问系统中的门的一般规则。有关详细信息，请参见*访问时间表类型 31*。

创建新访问时间表：

1. 转到访问管理。
2. 在访问时间表选项卡中，单击添加新时间表。
3. 在添加访问时间表对话框中，输入时间表名称。
4. 若要创建常规访问日程表，请选择增加时间表。

   或要创建减少时间表，请选择减少时间表。

   有关详细信息，请参见*访问时间表类型 31*。
5. 单击保存。

若要展开访问时间表列表中的项目，单击 。增加时间表以绿色文本显示，减少时间表以深红色文本显示。

若要查看访问时间表的日历，请单击 。

若要编辑访问时间表的名称或时间表项目，请单击 进行更改。然后单击保存。

若要删除访问时间表，请单击 。

注

门禁控制器具有几个预定义的常用访问时间表，可用作示例或根据需要进行修改。不过，预定义的访问时间表始终无法修改或删除。

访问时间表类型

有两种类型的访问时间表：

- 增加时间表 – 定义何时可以访问门的常规访问时间表。典型的增加时间表有办公时间、营业时间、几小时后或夜间时间。
- 减少时间表 – 常规访问时间表的例外情况。通常用来限制常规时间表（增加时间表）的时间段内发生的特定时间期间的访问。例如，减少时间表可以用来拒绝用户在与周末重合的公共假期期间访问建筑物。

这两种类型的访问时间表可以在两个级别使用：

- 识别类型时间表 – 确定读卡器何时以及如何授予用户门访问权限。每个识别类型必须连接到一个访问计划，该计划告诉系统何时使用特定的标识类型授予用户访问权限。可以向每个识别类型添加多个增加时间表和减少时间表。有关识别类型的信息，请参见*34*。
- 组时间表 – 确定何时（不包括方式）向组成员授予门访问权限。每个组必须连接到一个或多个告知系统何时授予其成员访问权限的访问时间表。可以向每个组添加多个增加时间表和减少时间表。有关组的信息，请参见*32*。

组时间表可以限制进入访问权限，但不能将进出访问权限延长到识别类型时间表允许的时间以外。换言之，如果识别类型时间表限制某些时间的进出访问，组时间表将无法覆盖该识别类型时间表。但是，如果组时间表比识别类型时间表对访问的限制更严格，组时间表将覆盖识别类型时间表。

识别类型时间表和组时间表可以通过多个方式组合在一起，从而获得不同结果。有关访问时间表组合的示例，请参见*40*。

添加时间表项目

增加时间表和减少时间表可以是一次性（单个）事件或重复事件。

向访问时间表添加时间表项目：

1. 在访问时间表列表中展开访问时间表。
2. 单击添加时间表项目。
3. 输入计划项目的名称。
4. 选择一次或重复。
5. 在时间字段中设置持续时间。请参见*时间选项 32*。
6. 对于重复时间表事件，请选择重复模式和重复范围参数。请参见*重复模式选项 32*和*重复范围选项 32*。
7. 单击保存。

时间选项

提供以下时间选项：

- 全天 – 为全天 24 小时持续的事件选择。然后输入所需的开始日期。
- 开始 – 单击时间字段，然后选择所需时间。如果需要，单击日期字段，选择所需的月、日和年。您也可以直接在字段中键入日期。
- 结束 – 单击时间字段，然后选择所需时间。如果需要，单击日期字段，选择所需的月、日和年。您也可以直接在字段中键入日期。

重复模式选项

提供以下重复模式选项：

- 每年 – 选择此选项可以每年重复。
- 每周 – 选择此选项可以每周重复。
- 每周于星期一、星期二、星期三、星期四、星期五、星期六、星期日重复 – 选择要重复的日期。

重复范围选项

提供以下重复范围选项：

- 首次发生 – 单击日期字段并选择所需年份、月份和日期。您也可以直接在字段中键入日期。
- 无结束日期 – 选择此选项可以无限次重复发生。
- 结束时间 – 单击日期字段，选择所需的月、日和年。您也可以直接在字段中键入日期。

创建和编辑组

组允许您集中有效地管理用户及其访问权限。组由凭证组成，这些凭证告诉系统组由哪些用户组成，何时以及如何授予组成员访问门禁的权限。

每个用户必须属于一个或多个组。若要将用户添加至组，将用户拖放到组列表中的所需组。有关详细信息，请参见*创建和编辑用户 38*。

创建新组：

1. 转到访问管理。
2. 在组选项卡中，单击添加新组。
3. 在添加组对话框中，输入组的凭据。请参见*组凭据 33*。
4. 单击保存。

若要展开组列表中的项目并查看其成员、门访问权限和时间表，单击 ▶ 。

若要编辑组名称或有效日期，单击 进行更改。然后单击保存。

若要验证组可以在何时如何访问某些门，单击 。

要删除组或组成员、门或时间表，单击 。

组凭据

为组提供了以下凭据：

- 名称（必需）
- 有效起始日期和有效截止日期 – 输入组凭据在其间有效的日期。单击日期字段，选择所需的月、日和年。您也可以直接在字段中键入日期。
- 白名单 – 白名单组中的用户可以始终访问组中的门，即使网络或电源发生故障。由于组中的用户始终有权访问门，因此时间表或有效起始日期和有效截止日期不适用。白名单组中打开门的用户不支持长访问时间。仅支持白名单功能的具有无线锁的门可被添加到组。

注

- 为了能够保存组，您必须输入组的名称。
- 将用户添加到白名单组时，用户的有效截止日期和有效起始日期不适用。
- 将加入白名单的无线凭据与无线锁同步需要一些时间，而且会干扰正常的开门过程。应避免在高峰时间在系统中添加或移除大量凭据。完成更新的凭据与锁的同步时，事件日志中该锁将显示 `SyncOngoing:  false`。

管理门

每个门的一般规则在门选项卡中管理。规则包括添加确定用户如何被授予门访问权限的识别类型，以及确定每个识别类型何时有效的访问时间表。有关详细信息，请参见*识别类型 34*和*创建和编辑访问时间表 31*。

您必须先通过完成硬件配置将门添加到门禁控制系统，然后才能够管理门，请参见*配置硬件 14*。

管理门：

1. 转到门禁管理，选择门选项卡。
2. 在门列表中，单击您要编辑的门旁边的 ▶ 。
3. 将门至少拖到一个组。如果组列表为空，请创建新组。请参见*创建和编辑组 32*。
4. 单击添加识别类型，选择用户要被授予门访问权限需要向读卡器出示的凭据。请参见*识别类型 34*。

   向每个门添加至少一个识别类型。
5. 要添加多个识别类型，请重复上述步骤。

   如果两种识别类型仅卡号和仅 PIN 全部添加，用户则可以选择刷卡或输入 PIN 来访问门。但是，如果只添加了识别类型卡号和 PIN，用户则必须同时刷卡并输入 PIN 才能访问门。

6. 若要定义凭据何时有效，将时间表拖动到每个识别类型。

若要手动解锁门、锁定门或授予临时访问权限，请根据需要单击手动门操作之一。请参见*使用手动门操作 35*。

注

手动解锁门、锁定门或授予临时访问权限的控制不能用于无线门/设备。

若要展开门列表中的项目，单击 。

若要编辑门或读卡器名称，单击 进行更改。然后单击保存。

若要验证读卡器、识别类型和访问时间表组合，请单击 。

若要验证连接到门的锁的功能，请单击验证控制。请参见*验证控制门 20*。

若要删除识别类型或访问时间表，请单击 。

识别类型

识别类型是确定如何向用户授予门访问权限的便携凭据存储设备、若干记住的信息或这两者的不同组合。常见的识别类型包括令牌（如卡或电子钥匙链）、个人识别码 (PIN) 以及请求退出 (REX) 设备。

有关凭据的详细信息，请参见*用户凭据 38*。

提供了以下识别类型：

- 仅设施代码 – 用户可以使用含有读卡器接受的设施代码的卡或其他令牌访问门。
- 仅卡号 – 用户可以只使用读卡器接受的卡或其他令牌访问门。卡号是通常在卡上打印的仅有的编号。请参见有关卡号位置的卡制造商的信息。卡号也可以由系统检索。在连接的读卡器上刷卡，在列表中选择读卡器，然后单击检索。
- 仅原始卡 – 用户可以只使用读卡器接受的卡或其他令牌访问门。此信息在卡上存储为原始数据。卡原始数据可以由系统检索。在连接的读卡器上刷卡，在列表中选择读卡器，然后单击检索。如果无法找到卡号，只能使用此识别类型。
- 仅 PIN – 用户可以只使用四位数的个人识别码 (PIN) 访问门。
- 设施代码和 PIN – 用户同时需要有读卡器接受的包含设施代码的卡或其他令牌以及 PIN 才能访问门。用户必须以指定的顺序出示凭据（先出示卡，然后出示 PIN）。
- 卡号和 PIN – 用户同时需要有读卡器接受的卡或其他令牌以及 PIN 才能访问门。用户必须以指定的顺序出示凭据（先出示卡，然后出示 PIN）。
- 原始卡和 PIN – 用户同时需要有读卡器接受的卡或其他令牌以及 PIN 才能访问门。如果无法找到卡号，只能使用此识别类型。用户必须以指定的顺序出示凭据（先出示卡，然后出示 PIN）。
- REX – 用户可以通过激活请求退出 (REX) 设备（如按钮、传感器或推杆）访问门。
- 仅车牌 – 用户可以仅使用车辆的车牌号访问门。
- HID Mobile Access – 用户可以使用装有 HID Mobile Access 应用的手机访问门。

添加计划解锁状态

若要自动让门在特定时间段内保持解锁状态，您可以向门添加计划解锁状态，并对其应用访问时间表。

例如，若要让门在办公时间保持解锁状态：

1. 转到门禁管理，选择门选项卡。

2. 单击您想要编辑的门列表项目旁边的 ▶ 。
3. 单击添加计划解锁。
4. 选择解锁状态（是已解锁还是解锁两个锁具体取决于门是有一个锁还是两个锁）。
5. 单击确定。
6. 将预定义的办公时间访问时间表应用到计划解锁状态。

若要验证门何时解锁，请单击  。

若要删除计划解锁状态或访问时间表，请单击 ⊖ 。

使用手动门操作

门可以锁定或解锁，可以在门选项卡上通过手动门操作授予临时访问权限。哪种手动门操作可以用于特定门取决于门是如何配置的。

使用手动门操作：

1. 转到门禁管理，选择门选项卡。
2. 在门列表中，单击您要控制的门旁边的 ▶ 。
3. 单击所需的门操作。请参见*手动门操作 35*。

注

若要使用手动门操作，您需要通过特定门连接到的门禁控制器打开“门禁管理”页面。如果您通过其他门禁控制器打开“门禁管理”页面，而不是通过手动门操作，将会有特定门所连接到的门禁控制器的“概览”页面的链接。单击此链接，转到门禁管理，选择门选项卡。

手动门操作

提供以下手动门操作：

- 获取门状态 – 验证门监视器、门警报和锁的当前状态。
- 访问 – 向用户授予门访问权限。适用指定的访问时间。请参见*如何配置门监视器和锁 15*。
- 解锁（一个锁）或解锁两个锁（两个锁）– 打开门锁。门将保持解锁状态，直至您按下锁定或锁定两个锁、激活计划的门状态或重启门禁控制器。
- 锁定（一个锁）或锁定两个锁（两个锁）– 锁定门。
- 解锁第二个锁并锁定主锁 – 此选项只在门配置了辅助锁时可用。打开门锁。辅助锁将保持解锁状态，直至您按下双锁或激活计划的门状态。

管理楼层

如果您在系统中安装了 AXIS 9188 Network I/O Relay Module，则可以采用与门管理相同的方式来管理楼层。

注

如果您使用 A1001 群集模式下支持全局事件已启用，请确保您使用的每个地板有仅有的指定描述性名称。例如，*“Elevator A, Floor 1”*。

注

每个 A1001 Network Door Controller 可以配置 2 个 AXIS 9188 Network I/O Relay Module。

楼层的一般规则在楼层选项卡中管理。规则包括添加确定用户如何被授予楼层访问权限的识别类型，以及确定每个识别类型何时有效的访问时间表。有关详细信息，请参见*识别类型楼层 36*和*创建和编辑访问时间表 31*。

您必须先通过完成硬件配置将楼层添加到门禁控制系统，然后才能够管理楼层，请参见*配置硬件 14*。

管理楼层：

1. 转到门禁管理，选择楼层选项卡。
2. 在楼层列表中，单击您要编辑的楼层旁边的 ▶ 。
3. 将楼层至少拖到一个组。如果组列表为空，请创建新组。请参见*创建和编辑组 32*。
4. 单击添加识别类型，选择用户要被授予楼层访问权限需要向读卡器出示的凭据。请参见*识别类型楼层 36*。

   向每个楼层添加至少一个识别类型。
5. 要添加多个识别类型，请重复上述步骤。

   如果两种识别类型仅卡号和仅 PIN 全部添加，用户则可以选择刷卡或输入 PIN 来访问门。但是，如果只添加了识别类型卡号和 PIN，用户则必须同时刷卡并输入 PIN 才能访问门。
6. 若要定义凭据何时有效，将时间表拖动到每个识别类型。

若要手动解锁楼层、锁定楼层或授予临时访问权限，请根据需要单击手动门操作之一。请参见*使用手动楼层操作 37*。

注

手动解锁楼层、锁定楼层或授予临时访问权限的控制不能用于无线门/设备。

若要展开楼层列表中的项目，单击 ▶ 。

若要编辑楼层或读卡器名称，单击 进行更改。然后单击保存。

若要验证读卡器、识别类型和访问时间表组合，请单击 。

若要验证连接到楼层的锁的功能，请单击验证控制。请参见*验证控制楼层 20*。

若要删除识别类型或访问时间表，请单击 ⊖ 。

识别类型楼层

识别类型是确定如何向用户授予楼层访问权限的便携凭据存储设备、若干记住的信息或这两者的不同组合。常见的识别类型包括令牌（如卡或电子钥匙链）、个人识别码 (PIN) 以及请求退出 (REX) 设备。

有关凭据的详细信息，请参见*用户凭据 38*。

提供了以下识别类型：

- 仅设施代码 – 用户可以使用含有读卡器接受的设施代码的卡或其他令牌访问楼层。
- 仅卡号 – 用户可以只使用读卡器接受的卡或其他令牌访问楼层。卡号是通常在卡上打印的仅有的编号。请参见有关卡号位置的卡制造商的信息。卡号也可以由系统检索。在连接的读卡器上刷卡，在列表中选择读卡器，然后单击检索。
- 仅原始卡 – 用户可以只使用读卡器接受的卡或其他令牌访问楼层。此信息在卡上存储为原始数据。卡原始数据可以由系统检索。在连接的读卡器上刷卡，在列表中选择读卡器，然后单击检索。如果无法找到卡号，只能使用此识别类型。
- 仅 PIN – 用户可以只使用四位数的个人识别码 (PIN) 访问楼层。

- 设施代码和 PIN – 用户同时需要有读卡器接受的包含设施代码的卡或其他令牌以及 PIN 才能访问楼层。用户必须以指定的顺序出示凭据（先出示卡，然后出示 PIN）。
- 卡号和 PIN – 用户同时需要有读卡器接受的卡或其他令牌以及 PIN 才能访问楼层。用户必须以指定的顺序出示凭据（先出示卡，然后出示 PIN）。
- 原始卡和 PIN – 用户同时需要有读卡器接受的卡或其他令牌以及 PIN 才能访问楼层。如果无法找到卡号，只能使用此识别类型。用户必须以指定的顺序出示凭据（先出示卡，然后出示 PIN）。
- REX – 用户可以通过激活请求退出 (REX) 设备（如按钮、传感器或推杆）访问楼层。

添加计划解锁状态

若要让楼层自动保持在特定持续时间内对不同人都可以访问，您可以向楼层添加计划解锁状态并对其应用访问时间表。

例如，让楼层保持在办公时间内对不同人都可以访问：

1. 转到门禁管理，选择楼层选项卡。
2. 单击您想要编辑的楼层列表项目旁边的  。
3. 单击添加计划解锁。
4. 选择解锁状态（是已解锁还是解锁两个锁具体取决于楼层是有一个锁还是两个锁）。
5. 单击确定。
6. 将预定义的办公时间访问时间表应用到计划解锁状态。

若要验证楼层何时可以访问，请单击  。

若要删除计划解锁状态或访问时间表，请单击  。

使用手动楼层操作

楼层可以有不同的可访问性，针对每个人限制或允许访问。可以在楼层选项卡中通过手动楼层操作授予临时访问权限。哪种手动楼层操作可以用于特定楼层取决于楼层是如何配置的。

使用手动楼层操作：

1. 转到门禁管理，选择楼层选项卡。
2. 在楼层列表中，单击您要控制的楼层旁边的  。
3. 单击所需的楼层操作。请参见*手动楼层操作 37*。

注

若要使用手动楼层操作，您需要通过特定门连接到的楼层控制器打开“门禁管理”页面。如果您通过其他楼层控制器打开“门禁管理”页面，而不是通过手动楼层操作，将会有特定楼层所连接到的楼层控制器的“概览”页面的链接。单击此链接，转到门禁管理，选择楼层选项卡。

手动楼层操作

提供以下手动楼层操作：

- 获取楼层状态 – 验证与楼层连接的继电器的当前状态。
- 访问 – 向用户授予楼层访问权限。适用指定的访问时间。请参见*如何配置门监视器和锁 15*。
- 解锁 – 楼层对每个人均可访问，直到按下锁定、激活计划的楼层状态或重启门禁控制器。

- 锁定 – 楼层对每个人均不可访问，直到按下解锁、激活计划的楼层状态或重启门禁控制器。

创建和编辑用户

每个人都必须拥有一个单一的用户配置文件，以获得访问控制系统中门的访问权限。用户配置文件由告知系统有哪些用户以及用户在何时如何被授予门访问权限的凭据组成。

若要高效地管理用户访问权限，每个用户必须属于一个或多个组。有关详细信息，请参见*创建和编辑组*。

创建新用户配置文件：

1. 转到访问管理。
2. 选择用户选项卡，然后单击添加新用户。
3. 在添加用户对话框中，输入用户的凭据。请参见*用户凭据 38*。
4. 单击保存。
5. 将用户拖动到组列表中的一个或多个组。如果组列表为空，请创建新组。请参见*创建和编辑组 32*。

若要展开用户列表中的项目并查看用户的凭据，单击 ▶ 。

要查找特定用户，请在筛选用户字段中输入筛选条件。若要强制匹配，用双引号括住筛选文本，例如，“John”或“potter, virginia”。

要编辑用户的凭据，单击 ✎ ，根据需要更改凭据。然后单击保存。

要删除用户，单击 ⊖ 。

重要

如果用户是通过 AXIS Visitor Manager 创建的，请勿在 AXIS Entry Manager 中编辑或删除该用户。有关 AXIS Visitor Manager 和 QR 代码阅读器服务的详细信息，请参见*AXIS Visitor Access 23*。

用户凭据

为用户提供了以下凭据：

- 名字（必需）
- 姓氏
- 有效起始日期和有效截止日期 – 输入用户凭据在其间有效的日期。单击日期字段，选择所需的月、日和年。您也可以直接在字段中键入日期。
- 暂停凭据 – 选择此选项可以暂停凭据。暂停时，用户无法通过此凭据访问系统中的门。取消选择可以再次给予用户访问权限。暂停一般用于临时用途。如果用户被永久拒绝访问，则删除用户配置文件。
- PIN（在没有卡号或原始卡时需要）– 输入用户选择或分配给用户的四位数的个人识别码 (PIN)。
- 设施代码 – 输入用于验证设施的门禁控制系统的代码。如果输入了预设的设施代码，此字段将自动填写，请参见*预设设施代码 22*
- 卡号（没有 PIN 或原始卡时需要）– 输入卡号。请参见有关卡号位置的卡制造商的信息。卡号也可以由系统检索。在连接的读卡器上刷卡，在列表中选择读卡器，然后单击检索。
- 原始卡（没有 PIN 或卡号时需要）– 输入卡原始数据。此数据可通过系统检索。在连接的读卡器上刷卡，在列表中选择读卡器，然后单击检索。如果无法找到卡号，只能使用此识别类型。

- 长访问时间 – 选择此选项可以覆盖现有的访问时间，并允许门为用户打开较长的访问时间，请参见*关于门监视器和时间选项 15*
- 车 E 米（此凭据在默认的门禁控制器安装中不可用）– 在合作伙伴软件激活此凭据时，输入用户车辆的车牌号。
  此凭据只能与 Axis 合作伙伴软件以及安装了车 E 米识别软件的摄像机一起使用。有关详细信息，请联系您的 Axis 合作伙伴或您当地的 Axis 销售代表。
- HID Mobile Access – 用户可以使用装有 HID Mobile Access 应用的手机访问门。

注

仅当完成了硬件配置并且有一个或多个读卡器连接到控制器时检索按钮才可用。

导入用户

用户可以通过导入逗号分隔值 (CSV) 格式的文本文件添加到系统中。建议在需要一次添加多个用户时导入用户。

您必须先创建并保存正确的 CSV 格式的文件（*.csv 或 *.txt），然后才能够导入用户。使用逗号分隔值，不留空格，并使用换行符分隔每个用户。

示例

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

导入用户：

1. 转到设置 > 导入用户。
2. 找到并选择保存用户列表的 *.csv 或 *.txt 文件。
3. 为每一列选择正确的凭据选项。
4. 若要将用户导入到系统，请单击导入用户。
5. 验证每一列是否包含正确的凭据类型。
6. 如果列正确，请单击开始导入用户。如果列不正确，请单击取消并重新开始。
7. 导入完成时，请单击确定。

提供以下凭据选项：

- 名字
- 姓氏
- PIN 码
- 卡号
- 车 E 米
- HID Mobile Access
- 未分配 – 不会导入的值。选择此选项可以跳过特定列。

有关凭据的详细信息，请参见*创建和编辑用户*。

导出用户

导出页面显示系统中用户的逗号分隔值 (CSV) 列表。此列表可用于将用户导入到其他系统。

导出用户列表：

1. 打开纯文本编辑器并创建一个新文档。
2. 转到设置 > 导出用户
3. 选择页面上的值并复制它们。
4. 将值粘贴到文本文档中。
5. 将此文档另存为逗号分隔值文件 (*csv) 或文本 (*.txt) 文件。

访问时间表组合示例

识别类型时间表和组时间表可以通过多个方式组合在一起，从而获得不同结果。下方示例遵循*30*中所述的工作流。

示例
创建以下时间表组合

- 始终向守卫授予门访问权限，
  - 白班期间使用卡（星期一 – 星期五，上午 6 点至下午 4 点），
  - 白班之前和之后时段使用卡和 PIN，
- 授予白班人员访问同一个门的权限，
  - 白班期间只使用卡：

1. 创建名为白班的增加时间表。请参见*31*。
2. 创建在星期一 – 星期五 06:00–16:00 时段重复的白班时间表项目。
3. 创建两个组，一个名为守卫的组和一个名为白班人员的组。请参见*32*。
4. 将预定义的始终访问时间表拖动至守卫组。
5. 将白班访问时间表拖动至白班人员组。
6. 向门的读卡器添加卡号和 PIN 和仅卡号识别类型。
7. 将预定义的始终拖动至卡号和 PIN 识别类型。
8. 将白班访问时间表拖动至仅卡号识别类型。
9. 将门拖到两个组。然后根据需要向组添加用户。请参见*38*。

示例
创建以下时间表组合

- 始终向守卫授予门访问权限，
  - 白班期间使用卡（星期一 – 星期五，上午 6 点至下午 4 点），
  - 白班之前和之后时段使用卡和 PIN，
- 向白班人员授予每天从早晨 6 点到下午 4 点访问同一个门的权限，
  - 白班期间使用卡，
  - 夜间或周末使用卡和 PIN：

1. 创建名为白班的增加时间表。请参见*31*。

2. 创建在星期一 – 星期五 06:00–16:00 时段重复的白班时间表项目。
3. 创建名为夜间和周末的减少时间表。
4. 创建在星期日 – 星期六 16:00–06:00 时段重复的夜间和周末时间表项目。
5. 将预定义的始终时间表与夜间和周末访问时间表拖动到白班人员组。
6. 创建两个组，一个名为守卫的组和一个名为白班人员的组。请参见*32*。
7. 将预定义的始终访问时间表拖动到守卫组和白班人员组。
8. 将夜间和周末访问时间表拖动到白班人员组。
9. 向门的读卡器添加卡号和 PIN 和仅卡号识别类型。
10. 将预定义的始终拖动至卡号和 PIN 识别类型。
11. 将白班访问时间表拖动至仅卡号识别类型。
12. 将门拖到两个组。然后根据需要向组添加用户。请参见*38*。

警报和事件配置

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。记录的事件可以配置为触发警报，此类警报会记录在警报日志中。

- 查看事件日志。请参见*42*。
- 导出事件日志。请参见*42*
- 查看警报日志。请参见*43*。
- 配置事件和警报日志。请参见*43*。

也可以将警报配置为触发电子邮件通知等操作。有关详细信息，请参见*如何设置操作规则 44*。

查看事件日志

若要查看记录的事件，请转到事件日志。

如果启用了全局事件，您可以从系统中的一个门禁控制器打开事件日志。有关全局事件的详细信息，请参见 *配置事件和警报日志 43*。

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 42*。

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、为哪些控制器记录。有关详细信息，请参见*事件日志选项 43*。

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。
- 源 – 筛选所选控制器中的事件。仅在控制器集群中并且启用了全局事件时可用。
- 日期和时间 – 按日期和时间范围筛选事件日志。

导出事件日志

若要导出记录的事件，请转到事件日志：

1. 单击 ⬇ 。
2. 从弹出菜单中选择导出格式以开始导出。

注

浏览器支持 CSV 格式，Chrome™ 和 Internet Explorer® 支持 XLSX 格式。

注

完成导出后，导出按钮会从  变为  。若要开始另一次导出，请刷新网页。导出按钮将变回  。

查看警报日志

若要查看触发的警报，请转到警报日志。如果启用了全局事件，您可以从系统中的一个门禁控制器打开警报日志。有关全局事件的详细信息，请参见*配置事件和警报日志 43*。

若要展开警报日志中的项目并查看警报详细信息（例如，门识别和状态），请单击  。

若要在验证警报原因后从列表中删除警报，请单击确认。要移除警报，请单击确认警报。

作为管理员，您可能需要某些事件触发警报。因此，您可以选择哪些事件、为哪些控制器触发警报。有关详细信息，请参见*警报日志选项 43*。

配置事件和警报日志

“配置事件和警报日志”页面允许您定义应该记录并触发警报的事件。

要共享已连接控制器之间的事件和警报，请选择全局事件。当全局事件已启用时，你仅需打开一个事件日志页和一个警报日志页，即可同时管理系统中门控制器的事件和警报。默认启用全局事件。

如果禁用全局事件，您必须为每个单独的门禁控制器打开一个“事件日志”页和一个“警报日志”页，然后分别管理其事件和警报。

重要

每次启用或禁用全局事件，事件日志将被清除。这意味着在此之前的事件都会被删除，且事件日志会重头开始。

也可以将警报配置为触发电子邮件通知等操作。有关详细信息，请参见*如何设置操作规则 44*。

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 > 配置事件和警报日志。

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 – 启用门控制器中的事件日志记录。将登记控制器的事件，并将其包含在事件日志中。
- 为所选源记录 – 在所选的门禁控制器中启用事件记录。将登记选定控制器的事件，并将其包含在事件日志中。为将与警报日志选项无警报或记录所选控制器的警报合并的事件选择此选项。

  在配置事件记录列表中，单击您要启用的事件日志项下的选择控制器。设备特定事件记录对话框将打开。在记录事件下，选择应启用警报记录的控制器并单击保存。

警报日志选项

若要定义哪些事件应触发警报，请转到设置 > 配置事件和警报日志。

提供以下触发和记录警报选项：

- 无警报 – 禁用警报记录。此事件不会触发警报或包含在警报日志中。
- 源的日志警报 – 启用门控制器中的警报日志记录。此事件会触发报警并包含在警报日志中。

- 记录所选源的警报 – 在所选的门禁控制器中启用警报记录。此事件会触发报警并包含在警报日志中。

  在配置警报记录列表中，单击您要启用的警报日志项下的选择源。设备特定警报触发对话框将打开。在触发警报下，选择应启用警报记录的门禁控制器并单击保存。

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。例如，产品可以在触发警报时发送电子邮件通知或激活输出端口。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操作。

有关可用触发器和操作的详细信息，请参见 *触发事件 45* 和 *操作 46*。

此示例描述如何设置操作规则以在触发不同警报时均发送电子邮件通知。

1. 配置警报。请参见 *配置事件和警报日志 43*。
2. 转到设置 > 其他控制器配置 > 事件 > 操作规则，然后单击添加。
3. 选择启用规则，然后为规则输入一个描述性名称。
4. 从触发器下拉列表中选择事件记录器。
5. 视情况，可选择时间表和附加条件。参见下方。
6. 在操作下，从类型下拉列表中选择发送通知。
7. 从下拉列表中选择电子邮件收件人。请参见 *如何添加接受者 47*。

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 > 操作规则，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。

触发事件

提供的操作规则触发事件和条件包括：

- 访问点
  - 门禁点已启用 – 当配置读卡器或 REX 设备等门禁点设备时（例如，当完成硬件配置或添加识别类型时），将触发操作规则。
- 配置
  - 门禁点已更改 – 当更改读卡器或 REX 设备等门禁点设备的配置时（例如，当配置硬件或编辑识别类型时），将触发该操作，从而更改门禁方式。
  - 门禁点已移除 – 当重置读卡器或 REX 设备等门禁点设备的硬件配置时，将触发操作规则。
  - 区域已更改 – 此版本的 AXIS Entry Manager 不支持。必须由客户端（如门禁管理系统）通过支持此功能的 VAPIX® 应用程序编程接口进行配置，并使用可提供所需信号的设备。当门禁区域更改时，将触发操作规则。
  - 区域已移除 – 此版本的 AXIS Entry Manager 不支持。必须由客户端（如门禁管理系统）通过支持此功能的 VAPIX® 应用程序编程接口进行配置，并使用可提供所需信号的设备。当从系统中移除门禁区域时，将触发操作规则。
  - 门已更改 – 当门配置设置（如门名称）发生更改或将门添加到系统时，将触发操作规则。例如，该触发器可用于在安装和配置门时发送通知。
  - 门已移除 – 当从系统中移除门时，将触发操作规则。例如，该触发器可用于在从系统中移除门时发送通知。
- 门
  - 电池报警 – 当无线门电池电量低及电量不足时，将触发操作规则。
  - 门报警 – 当门监视器指示门被强行打开、门打开时间过长或门发生故障时，将触发操作规则。例如，该触发器可用于在有人强行进入时发送通知。
  - 门双锁监视器 – 仅当辅助锁状态更改为锁定或解锁时，才会触发操作规则。
  - 门锁监视器 – 当正常锁状态更改为锁定或解锁时，才会触发操作规则。例如，当门监视器侦测到门已打开但锁却是锁定状态时，将触发故障。
  - 门模式 – 当门更改状态时（例如，当门已允许或阻止访问或处于锁定模式时），将触发操作规则。有些这些模式的详细信息，请参见联机帮助。
  - 门监视器 – 当门监视器状态更改时，将触发操作规则。例如，该触发器可用于在门监视器指示门已打开或关闭时发送通知。
  - 门篡改 – 当门监视器侦测到连接中断（例如，有人切断了门监视器的电线）时，将触发操作规则。要使用此触发器，请确保已选择启用受监控输入，并且线电阻器末端安装在相应的门连接器输入端口上。有关详细信息，请参见 *如何使用监控输入 18*。
  - 门警告 – 在门打开时间过长且并未触发警报之前，将触发操作规则。例如，如果并未在指定的时间内关门，可以使用该触发器发送警告信号，指示门禁控制器将发送真实警报，即，过长时间开门警报。有关过长时间开门的详细信息，请参见 *如何配置门监视器和锁 15*。
  - 锁卡住 – 当无线门锁被阻挡时，将触发操作规则。
- 事件记录器 – 保持追踪门控制器中的事件，例如当用户刷卡或开门时。如果全局事件已启用，则事件记录器将保持追踪系统中每个控制器的事件。 要设置哪些警报和事件可以触发操作规则，

请转到设置 > 配置事件和警报日志。 事件记录器由系统共享，并且可存储多达 30000 个事件。达到限制时，事件记录器会使用先进先出 (FIFO) 规则。这意味着第一个事件将第一个被覆盖。

- 警报 – 当触发其中一个指定的警报时，将触发操作规则。系统管理员可配置哪些事件比其他事件重要，并选择特定事件是否应触发警报。
- 丢弃的警报 – 当新的警报记录无法写入警报日志时，将触发操作规则。例如，如果同时出现许多警报，则事件记录器无法跟上步调。当丢弃某个警报时，可向操作员发送通知。
- 丢弃的事件 – 当新的事件记录无法写入事件日志时，将触发操作规则。例如，如果同时出现许多事件，则事件记录器无法跟上步调。当丢弃某个事件时，可向操作员发送通知。

• 硬件

- 网络 – 当网络连接丢失时触发操作规则。选择是将在网络连接丢失时触发操作规则。选择否将在网络连接恢复时触发操作规则。选择 IPv4/v6 地址已移除或新 IPv4/v6 地址在 IP 地址改变时触发操作。
- 对等连接 – 如果设备之间的网络连接丢失，或者如果门禁控制器配对失败，当 Axis 产品建立了与另一个门禁控制器的连接时触发操作规则。例如，这可以用于发送门禁控制器丢失网络连接的通知。

• 输入信号

- 数字输入端口 – 当 I/O 端口从连接的设备收到信号时触发操作规则。请参见 *I/O 端口 57*。
- 手动触发器 – 当手动触发器被激活时触发操作规则。该触发器可由客户端（如门禁管理系统）用于通过 VAPIX® 应用程序编程接口来手动启动或停止操作规则。
- 虚拟输入 – 当任一虚拟输入更改状态时，将触发操作规则。该触发器可由客户端（如门禁管理系统）用于通过 VAPIX® 应用程序编程接口来触发操作。例如，虚拟输入可连接到管理系统的用户界面中的按钮。

• 时间表

- 间隔 – 在计划的开始时间触发操作规则，并在到达计划的结束时间之前保持其活动状态。
- 脉冲 – 当发生一次性事件时，将触发操作规则。也就是，在特定时间发生且没有持续时间的事件。

• 系统

- 系统就绪 – 当系统处于就绪状态时，将触发操作规则。例如，Axis 产品可在系统启动后侦测系统状态并发送通知。

  选择是可在产品处于就绪状态时触发操作规则。请注意，仅在已启动必要服务（如事件系统）时规则才会触发。

• 时间

- 重复 – 通过监视已创建的重复来触发操作规则。您可以使用此触发器来发起重复操作，如每小时发送通知。选择一个重复模式或创建新的重复模式。有关设置重复模式的详细信息，请参见 *如何设置重复 48*。
- 使用时间表 – 根据所选的时间表触发操作规则。请参见 *如何创建时间表 48*。

操作

你可以配置以下几种操作：

- 输出端口 – 激活 I/O 端口来控制外部设备。
- 发送通知 – 向接受者发送通知消息。

- LED 状态指示灯 – LED 状态指示灯可设置为在操作规则激活期间闪烁或在设定秒数内闪烁。LED 状态指示灯可在安装和配置期间用于目视确认触发器设置是否正常工作，例如，门打开时间过长触发器。若要设置 LED 状态指示灯的闪烁颜色，从下拉列表中选择 LED 颜色。

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*接收者类型 47*.

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. 单击确定。

接收者类型

提供了以下接收者类型：

HTTP

HTTPS

电子邮件

TCP

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

某些电子邮件提供商拥有安全过滤器，可防止用户接收或查看较大附件、接收计划的电子邮件及类似内容。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*证书 51*。

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。

创建新时间表：

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。

阅读器反馈

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 LED	OSDP	蜂鸣器模式	状态
空闲[1]	关闭	红色	红色	无声	正常
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	哔哔声	授权访问
拒绝访问	红色	红色	红色	哔哔声	拒绝访问

1. 当门关闭并且锁已锁定时进入空闲状态。

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。

报告

“报告”页面允许您查看、打印和导出包含不同类型的系统信息的报告。有关哪些报告可用的详细信息，请参见*报告类型 49*。

查看、打印和导出报告

若要打开“报告”页面，请单击报告。

若要查看报告，请单击查看和打印。

打印报告：

1. 单击查看和打印。
2. 选择应在报告中包含的列。默认情况下，将选择各列。
3. 如果要缩小报告范围，在相关的筛选器字段中输入筛选器。例如，您可以按用户所属的组筛选用户，按时间表筛选门，或按组有权访问的门筛选组。

   若要强制匹配，用双引号括住筛选文本，例如，“John”。
4. 如果您想要按不同顺序排序报告项，请单击相关列中的 。若要在标准和反向顺序之间更改，切换排序按钮。

   ▲ 按标准顺序（升序）显示项目。

   ▼ 按反向顺序（降序）显示项目。
5. 单击打印所选列。

若要导出报告，请单击导出 CSV 文件。

报告被导出为一个逗号分隔值 (CSV) 文件，并且包括针对该报告类型的可能列和项目。除非另外指定，否则导出的文件 (*.csv) 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。

注

仅具有凭据的用户会显示在报告中。

报告类型

提供以下报告类型：

- 访问时间表。有关访问时间表类型和选项的详细信息，请参见*31*和*32*。
- 组。有关组凭据的详细信息，请参见*33*。
- 门。有关门和识别类型的详细信息，请参见*33*和*34*。
- 用户。有关用户凭据的详细信息，请参见*38*。
- 门禁控制器。有关连接的控制器及其 ID 类型的详细信息，请参见*27*。有关门监视器时间选项的详细信息，请参见*16*。

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）：

- 管理员可不受限制地访问全部设置。管理员可以添加、修改和删除其他用户。

注

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 地址过滤在设置 > 其他控制器配置 > 系统选项 > 安全 > 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。转到设置 > 其他控制器配置 > 系统选项 > 安全 > 证书安装和管理证书。请参见*证书 51*。

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. 单击保存启用这些设置。

若要通过所需协议访问 Axis 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，请转到设置 > 其他控制器配置 > 系统选项 > 安全 > 证书。请参见*证书 51*。

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

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。请参见*日期和时间 52*。

证书

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）。Axis 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。

CA 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

- 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. 转到设置 > 其他控制器配置 > 系统选项 > 安全 > 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。
2. 转到设置 > 其他控制器配置 > 系统选项 > 安全 > 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. 转到设置 > 其他控制器配置 > 系统选项 > 安全 > 证书。
2. 单击安装证书上载证书。

日期和时间

Axis 产品的日期和时间设置在设置 > 其他控制器配置 > 系统选项 > 日期和时间下配置。

当前服务器时间显示当前的日期和时间（24 小时制）。

若要更改日期和时间设置，在新服务器时间下选择首选的时间模式：

- 与计算机时间同步 – 根据计算机时钟设置日期和时间。通过此选项，日期和时间设置一次，不会自动更新。
- 与 NTP 服务器同步 – 从 NTP 服务器获取日期和时间。通过此选项，日期和时间设置会不断更新。有关 NTP 设置的信息，请参见 *NTP 配置 54*。

  如果为 NTP 服务器使用主机名称，必须配置 DNS 服务器。请参见 *DNS 配置 54*。
- 手动设置 – 您可以手动设置日期和时间。

如果使用 NTP 服务器，请从下拉列表中选择您的时区。如果需要，选中随夏令时变化自动调整。

网络

基本 TCP/IP 设置

Axis 产品支持 IP 版本 4 (IPv4)。

Axis 产品可以通过以下方式获得 IPv4 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*59*。

ARP/Ping

产品的 IP 地址可以使用 ARP 和 Ping 分配。有关说明，请参见*使用 ARP/Ping 分配 IP 地址 53*。

ARP/Ping 服务默认启用，但会在产品启动后两分钟自动禁用，或在 IP 地址分配后即自动禁用。若要使用 ARP/Ping 重新分配 IP 地址，产品必须重启以再启用两个分钟的 ARP/Ping 服务。

若要禁用此服务，请转到设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 基本，然后清除选项启用 IP 地址的 ARP/Ping 设置。

禁用此服务后，仍可以对产品执行 Ping 命令。

使用 ARP/Ping 分配 IP 地址

设备的 IP 地址可以使用 ARP/Ping 分配。必须在连接电源后两分钟内发出该命令。

1. 在与计算机相同的网络段上获取自由的静态 IP 地址。
2. 在设备标签上找到序列号 (S/N)。
3. 打开命令提示符，输入以下命令：

   Linux/Unix 语法

   ```
   arp -s <IP 地址> <序列号> temp
   ping -s 408 <IP 地址>
   ```

   Linux/Unix 示例

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Windows 语法（可能需要您以管理员身份运行命令提示符）

   ```
   arp -s <IP 地址> <序列号>
   ping -l 408 -t <IP 地址>
   ```

   Windows 示例（可能需要您以管理员身份运行命令提示符）

   ```
   arp -s 192.168.0.125 00-40-8c-18-10-00
   ping -l 408 -t 192.168.0.125
   ```

4. 通过断开并重新连接网络连接器重启设备。
5. 当设备使用 `Reply from 192.168.0.125:...` 或类似命令响应时关闭命令提示符。
6. 打开浏览器并在地址字段中键入 `http://<IP 地址>`。

若要了解其他 IP 地址分配方法，请参见文档*如何分配 IP 地址和访问设备*（位于 *www.axis.com/support*）

注

- 若要在 Windows 中打开命令提示符，打开开始菜单，搜索 `cmd`。
- 若要在 Windows 8/Windows 7/Windows Vista 中使用 ARP 命令，右键单击命令提示符图标，选择以管理员身份运行。
- 若要在 Mac OS X 中打开命令提示符，从应用程序 > 实用程序打开终端实用程序。

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 设置在设置 > 其他控制器配置 > 系统选项 > 网络 > TCP IP > 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*产品概述 4*），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。

始终 – 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

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 Axis 产品注册 AXIS Internet Dynamic DNS Service，请转到设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 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

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 设置在设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 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 设置在设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 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。主机名在设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 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，请参见联机帮助。

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。

此功能可以在设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 高级下禁用。

HTTP

Axis 产品使用的 HTTP 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 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，请转到设置 > 其他控制器配置 > 系统选项 > 安全 > HTTPS。有关详细信息，请参见 *HTTPS 50*。

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 遍历在设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 高级下配置。

注

- 为使 NAT 遍历正常工作，其必须受路由器支持。路由器还必须支持 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，Axis 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（请参见设置 > 其他控制器配置 > 系统选项 > 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

- 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

Axis 产品中运行的 FTP 服务器支持上传新的固件、用户应用程序，等等。FTP 服务器可以在设置 > 其他控制器配置 > 系统选项 > 网络 > TCP/IP > 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

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 在设置 > 其他控制器配置 > 系统选项 > 网络 > SOCKS 下配置。有关详细信息，请参见联机帮助。

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 设置在设置 > 其他控制器配置 > 系统选项 > 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 Axis 产品中启用和配置 SNMP，请转到设置 > 其他控制器配置 > 系统选项 > 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

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 50*。若要启用 SNMP v3，选中此框，并提供初始用户密码。

注

初始密码只能设置一次。如果密码丢失，Axis 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 59*。

UPnP

Axis 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 可以在设置 > 其他控制器配置 > 系统选项 > 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 可以在设置 > 其他控制器配置 > 系统选项 > 网络 > Bonjour 下禁用。

端口和设备

I/O 端口

Axis 产品上的辅助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。有关如何连接外部设备的信息，请参见《安装指南》，位于 *www.axis.com*

I/O 端口在设置 > 其他控制器配置 > 系统选项 > 端口和设备 > I/O 端口下配置。选择端口方向（输入或输出）。可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。这些功能位于设置 > 其他控制器配置 > 系统选项 > 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

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。Axis 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 59*。

有关固件升级的信息，请参见*如何升级固件 60*。

备份应用数据

转到设置 > 创建一个备份以创建一个应用数据备份。要备份的数据包括用户、凭证、群组和时间表。当你创建一个备份时，含这些数据的文件会本地存储在你的电脑上。

重要

如果应用数据包含 HID 移动凭证，则你无法创建该数据的备份。

转到设置 > 上传一个备份以使用先前创建的备份文件恢复应用数据。在你可以上传备份文件前，你必须先将设备重置为出厂默认设置。有关说明，请参见 *重置为出厂默认设置 59*。

支持

支持概览

如果您需要技术帮助，设置 > 其他控制器配置 > 系统选项 > 支持 > 支持概览页面提供了有关故障排查和联系人信息的信息。

另请参见*故障排查 60*。

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

设置 > 其他控制器配置 > 系统选项 > 支持 > 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设置 > 其他控制器配置 > 系统选项 > 支持 > 日志和报告 > 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，请转到设置 > 其他控制器配置 > 系统选项 > 高级 > 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*59*。

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，请转到设置 > 其他控制器配置 > 系统选项 > 高级 > 文件上传。

已上传的文件通过 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）。

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。请参见*产品概述 4*。
3. 按住控制按钮 25 秒，直到 LED 状态指示灯再次变成橙色。
4. 松开控制按钮。当 LED 状态指示灯变绿时，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。转到 设置 > 其他控制器配置 > 设置 > 系统选项 > 维护，然后单击默认。

故障排查

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你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

- 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、凭据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。

独立的门禁控制器：

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。

系统中的门禁控制器：

你可以使用 AXIS Device Manager 或 AXIS Camera Station 升级系统中的门控制器。更多信息请参见 *www.axis.com*。

重要

- 请勿选择顺序升级。

注

- 系统中的控制器都必须始终具有相同的固件版本。
- 使用 AXIS Device Manager 或 AXIS Camera Station 中的并行选项同时升级系统中的控制器。

紧急恢复过程

如果电源或网络连接在升级过程中丢失，升级过程将失败，产品可能会没有响应。闪烁红色的状态指示灯指示升级失败。若要恢复产品，请按照以下步骤操作。序列号在产品标签上。

1. 在 UNIX/Linux 中，从命令行键入以下内容：

   ```
   arp -s <IP 地址> <序列号> temp
   ping -l 408 <IP 地址>
   ```

   在 Windows 中，从 command/DOS 提示符键入以下内容（这可能需要以管理员身份运行命令提示符）：

   ```
   arp -s <IP 地址> <序列号>
   ping -l 408 -t <IP 地址>
   ```

2. 如果产品未在 30 秒内响应，重启产品，然后等待响应。按 CTRL+C 停止 Ping。
3. 打开浏览器，键入产品的 IP 地址。在打开的页面上，使用浏览按钮选择要使用的升级文件。然后单击加载重新启动升级过程。
4. 升级完成（1–10 分钟）后，产品将自动将重启，状态指示灯显示稳定的绿色。
5. 参照《安装指南》重新安装产品。

如果紧急恢复过程没有让产品恢复正常并重新运行，请在 *www.axis.com/support* 上联系 Axis 支持部门

征兆、可能的原因和补救措施

升级固件时出现问题	
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。请确保 Ping 长度设置为 408。有关说明，请参见位于 *axis.com* 的产品页面的《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 Axis 摄像机。运行 Ping 命令（在 Command/DOS 窗口中，键入 `ping` 和产品的 IP 地址）： • 如果收到消息：`Reply from <IP 地址>: bytes=32; time=10...`，这意味着网络上其他设备可能已使用该 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。 • 如果收到消息：`Request timed out`，这意味着该 IP 地址可用于此 Axis 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。

故障排查

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栏中手动键入 `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。请参见*重置为出厂默认设置 59*。
DHCP 尚未更改 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。请参见*日期和时间 52*。

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 Axis 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 Axis 产品，请参见 *为 IPv4 使用 NAT 遍历（端口映射）55*。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。

状态和网络 LED 指示灯快速闪烁红色

硬件故障	请联系您的 Axis 经销商。

产品不启动

产品不启动	如果产品不启动，保持网络电缆连接并将电源线重新插入中跨。

规格

连接器

有关连接器位置的信息，请参见。

要获取连接图以及有关通过硬件配置生成的硬件针图的信息，请参见*连接图 67*和*配置硬件 14*。

以下部分介绍连接器的技术规格。

读卡器数据连接器

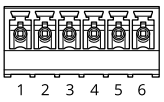
支持用于与读卡器通信的 RS485 和 Wiegand 协议的 6 针接线端子。

RS485 端口支持：

- 两线 RS485 半双工
- 四线 RS485 全双工

Wiegand 端口支持：

- 两线 Wiegand



功能		引脚	备注
RS485	A–	1	用于全双工 RS485 用于半双工 RS485
	B+	2	
RS485	A–	3	用于全双工 RS485 用于半双工 RS485
	B+	4	
Wiegand	D0（数据 0）	5	用于 Wiegand
	D1（数据 1）	6	

重要

RS485 端口具有 9600 Bit/s 固定波特率。

重要

推荐最大电缆长度为 30 米（98.4 英尺）。

重要

本部分的输出电路为 2 类限制电源。

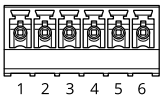
读卡器 I/O 连接器

6 针接线端子，用于：

- 辅助电源（DC 输出）

- 数字输入
- 数字输出
- 0 V DC (–)

读卡器 I/O 连接器上的针 3 可以被监控。如果连接中断，将激活事件。要使用监控输入，则安装线尾电阻器。使用连接图来安装监控输入。请参见*68*。



功能	引脚	备注	规格
0 V DC (–)	1		0 V DC
DC 输出	2	用于为辅助设备供电。 注意：此引脚只能用作电源输出。	12 V DC 最大载荷电流 = 300 mA
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 40 V DC
		数字输出 — 连接到针 1 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，二极管必须与负载并联连接，以防止电压瞬变。	0 至最大 40 V DC，开漏，100 mA

重要

推荐最大电缆长度为 30 米（98.4 英尺）。

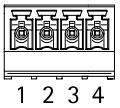
重要

本部分的输出电路为 2 类限制电源。

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）。

可监控门输入引脚。如果连接中断，将触发报警。要使用监控输入，则安装线尾电阻器。使用连接图来安装监控输入。请参见*68*。



功能	引脚	备注	规格
0 V DC (–)	1, 3		0 V DC
输入	2, 4	用于与门监视器通信。 数字输入 — 分别连接至针 1 或针 3 以启用，或保留浮动状态（断开连接）以停用。 注意：此引脚只能用于输入。	0 至最大 40 V DC

重要

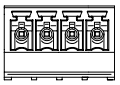
推荐最大电缆长度为 30 米（98.4 英尺）。

辅助连接器

4 针可配置 I/O 接线端子用于：

- 辅助电源（DC 输出）
- 数字输入
- 数字输出
- 0 V DC (–)

示例连接图请参见*连接图 67*。



功能	引脚	备注	规格
0 V DC (–)	1		0 V DC
DC 输出	2	用于为辅助设备供电。 注意：此引脚只能用作电源输出。	3.3 V DC 最大载荷电流 = 100 mA
可配置（输入或输出）	3–4	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 40 V DC
		数字输出 — 连接到针 1 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，二极管必须与负载并联连接，以防止电压瞬变。	0 至最大 40 V DC，开漏，100 mA

重要

推荐最大电缆长度为 30 米（98.4 英尺）。

重要

本部分的输出电路为 2 类限制电源。

电源连接器

用于 DC 电源输入的双引脚接线盒。使用一个额定输出功率限制在 ≤ 100 W 或额定输出电流限制在 ≤ 5 A 的安全超低电压 (SELV) 兼容式限功率电源 (LPS)。

功能	针脚	备注	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。 注释：此引脚只能用作电源输入。	10–28 V DC，最大 36 W 输出最大负载 = 14 W

网络连接器

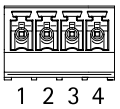
RJ45 以太网连接器。使用类别 5e 或更高级别的电缆。

功能	规格
电源和以太网	以太网供电 IEEE 802.3af/802.3at 1 型 3 类，44–57 V DC 输出上的最大负载 = 7.5 W

电源锁连接器

用于为一到两个锁供电的 4 针接线端子（DC 输出）。锁连接器还可以用于为外部设备供电。

请根据通过硬件配置生成的硬件针图将锁和负荷连接到引脚。



功能	引脚	备注	规格
0 V DC (–)	1, 3		0 V DC
0 V DC，浮动，或 12 V DC	2, 4	用于控制多达两个 12 V 锁定。使用硬件针图。请参见*配置硬件 14*。	12 V DC 最大总负载 = 500 mA

注意

如果锁无极性，建议您增加外部续流二极管。

重要

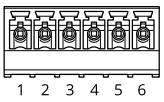
本部分的输出电路为 2 类限制电源。

电源和中继连接器

具有内置继电器的 6 针接线端子用于：

- 外部设备
- 辅助电源（DC 输出）
- 0 V DC (–)

请根据通过硬件配置生成的硬件针图将锁和负荷连接到引脚。



功能	引脚	备注	规格
0 V DC (–)	1, 4		0 V DC
继电器	2–3	用于连接中继设备。使用硬件针图。请参见*配置硬件 14*。 两个继电器引脚与电路的其余部分电位隔离。	最大电流 = 700mA 最大电压 = +30 V DC
12 V DC	5	用于为辅助设备供电。 注意：此引脚只能用作电源输出。	最大电压 = + 12 V DC 最大负载 = 500 mA
24 V DC	6	未用	

注意

如果锁无极性，建议您增加外部续流二极管。

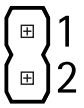
重要

本部分的输出电路为 2 类限制电源。

篡改报警接头

两个 2 针针头用于绕过：

- 后篡改报警 (TB)
- 前篡改报警 (TF)



功能	引脚	备注
后篡改报警	1–2	若要同时绕过前后篡改报警，请分别在 TB 1、TB 2 和 TF 1、TF 2连接跳线。绕过篡改报警意味着系统不会识别篡改尝试。
前篡改报警	1–2	

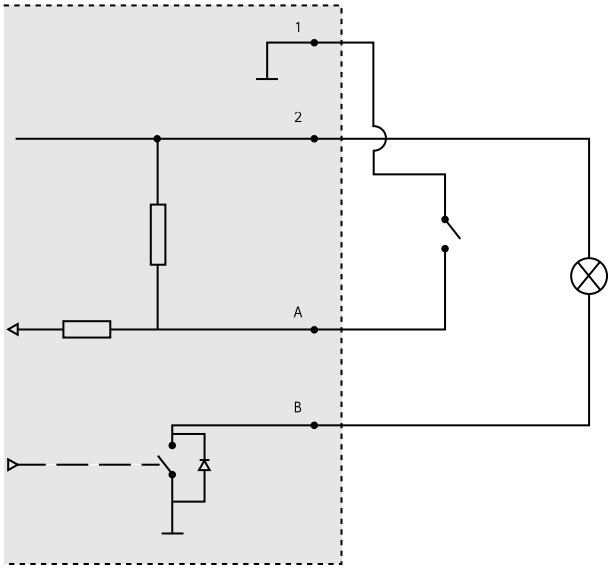
注

前后篡改报警均默认连接。外壳打开触发器可以配置为在门禁控制器被打开或门禁控制器被从墙壁或天花板上取下时执行操作。有关如何配置报警和事件的信息，请参见*警报和事件配置 42*。

连接图

请根据通过硬件配置生成的硬件针图连接设备。有关硬件配置的详细信息和硬件针图，请参见*配置硬件 14*。

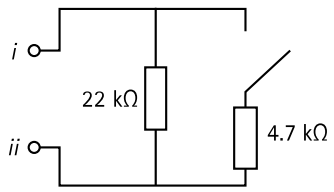
辅助连接器



1 0 V DC (–)
2 DC 输出：3.3 V，最大 100 mA
A I/O 配置为输入
B I/O 配置为输出

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 (–)

注

建议使用绞合屏蔽电缆。将屏蔽件连接至 0 V DC。

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

表示有助于充分利用产品的有用信息。

用户手册
AXIS A1001 & AXIS Entry Manager

版本 M23.3
日期： 五月 2021
零件号 T10010336