AXIS Secure Entry for XProtect

用户手册

目录

门禁控制

访问控制是一种物理访问控制与视频监控相结合的解决方案。此集成功能允许您直接通过管理客户端配置安讯士访问控制系统。该系统与XProtect无缝集成，使操作员能够在智能客户端监视访问并执行访问控制响应。

注意

要求

- VMS版本2024 R1或更高版本。
- 有关XProtect访问许可证的信息，请参阅*访问许可证*。
- 在事件服务器和管理客户端上安装AXIS Optimizer。

通过AXIS Secure Entry安装AXIS Optimizer时，端口53459和53461将为传入流量 (TCP) 开放。

访问控制配置

注意

在开始之前，实施以下操作：

- 升级门禁控制器软件。请参阅下表，了解适用于您的VMS版本的最低及推荐AXIS OS版本。
- 日期和时间务必正确。

AXIS Optimizer版本	最低AXIS OS版本	推荐AXIS OS版本
5.6	12.6.94.1	12.6.94.1

将安讯士网络门禁控制器添加到系统中：

1. 转到**Site Navigation（场所导航）** > **AXIS Optimizer** > **Access control（访问控制）**。
2. 在**Configuration（配置）**下，选择**Devices（设备）**。
3. 选择**Discovered devices（已发现设备）**查看可添加至系统的设备列表。
4. 选择您要添加的设备。
5. 在弹出窗口中单击**+ Add（添加）**并提供控制器的凭据。

注意

您应在**Management（管理）**选项卡中看到添加的控制器。

若要将控制器手动添加到系统中，可在**Management（管理）**选项卡中单击**+ Add（添加）**。

在每次添加、删除或编辑门禁控制器名称时将您的更新集成到VMS中：

- 转到**Site Navigation（场所导航）** > **Access control（访问控制）**并单击Access Control integration（访问控制集成）。
- 在**General settings（常规设置）**选项卡中，单击**Refresh Configuration（刷新配置）**。

配置访问控制的工作流

1. 转到**Site Navigation（场所导航）** > **AXIS Optimizer** > **Access control（访问控制）**。
2. 要编辑预定义的识别配置文件或创建新的识别配置文件，请参见 。
3. 要使用卡格式和 PIN 长度的自定义设置，请参见 。
4. 添加门并将识别配置文件应用至门。请参见 。
5. 添加区域并将门添加到区域。请参见 。

门禁控制器的设备软件兼容性

重要

在升级门禁控制器的AXIS OS时，请注意以下事项：

- **支持的AXIS OS版本：** 上述支持的AXIS OS版本仅适用于从其原始推荐VMS版本升级的情况，且系统需配备门禁功能。如果系统不符合这些条件，您必须升级至推荐的适用于特定VMS版本的AXIS OS版本。
- **支持的最低AXIS OS版本** 系统中安装的最旧的AXIS OS版本决定支持的最低AXIS OS版本，但不得早于两个版本。
- **升级至推荐AXIS OS版本以上：** 假设您将AXIS OS升级至高于针对特定VMS版本的推荐版本，那么，只要在为VMS版本设置的支持范围内，您随时可以降级回推荐AXIS OS版本，不会出现问题。
- **未来AXIS OS建议：** 请始终遵循针对相应VMS版本推荐的AXIS OS版本，以保持系统稳定性和完全兼容性。

门禁控制集成

将访问控制集成到VMS：

1. 访问Site Navigation（**场所导航**）> Access control（**访问控制**）。
2. 右键单击Access Control（**访问控制**），然后单击Create new...（**新建...**）。
3. 在Create Access Control System Integration（**创建访问控制系统集成**）对话框中：
   - 为集成输入一个名称。
   - 在Integration plug-in（**集成插件**）的下拉菜单中选择AXIS Secure Entry。
   - 单击Next（**下一步**），直至看到Associate cameras（**关联摄像机**）对话框。将摄像机关联至门禁访问点：
     - 在Cameras（**摄像机**）下单击您的设备，可查看XProtect系统中配置的摄像机列表。
     - 选择并拖动摄像机至您想要关联的访问点。
     - 单击Close（**关闭**）可关闭对话框。

注意

- 有关XProtect中访问控制集成的更多信息，请参阅*在XProtect智能客户端中使用访问控制*。
- 有关访问控制属性（例如常规设置、门禁及关联的摄像机、访问控制事件等）的更多信息，请参阅*访问控制属性*。

门和区域

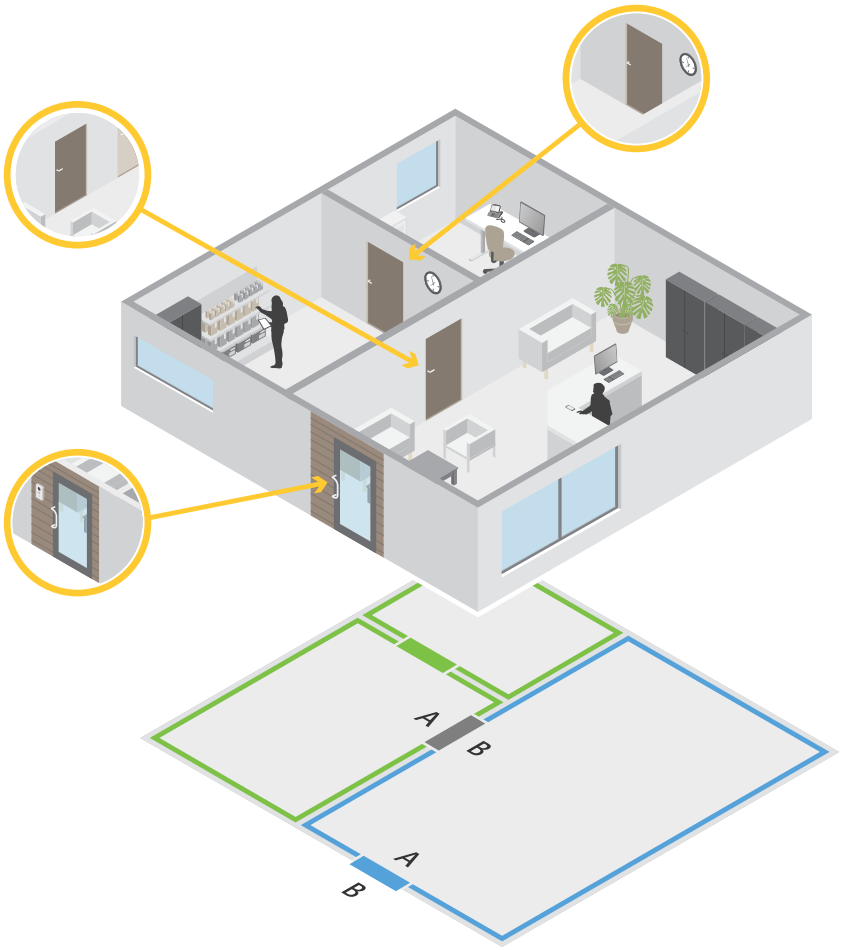
转到Site Navigation（**场所导航**）> Axis Optimizer >Access control（**访问控制**）> Doors and zones（**门禁与区域**）可获取概览并配置门禁和区域。

针图	查看与门相关的控制器针图。如果要打印针图，请单击**打印**。
识别配置文件	更改门上的识别配置文件。
安全通道	打开或关闭特定读卡器的 OSDP 安全通道。

门	
名称	门的名称。
门禁控制器	连接到门的门禁控制器。
A 侧边	门的 A 侧所在的区域。
B 侧	门的 B 侧所在的区域。
识别配置文件	应用于门的识别配置文件。

卡格式和 PIN	显示卡格式的类型或 PIN 长度。
状态	门的状态。 • **在线：** 门联机，工作正常。 • **读卡器离线：** 门配置中的读卡器离线。 • **读卡器错误：** 门配置中的读卡器不支持安全通道，或读卡器的安全通道关闭。
分区	
名称	区域的名称。
门数量	区域中包含的门的数量。

门和区域示例



- 有两个区域：绿色区域和蓝色区域。
- 有三个门禁：绿色门禁、蓝色门禁和棕色门禁。
- 绿色门是绿色区域的内部门。
- 蓝色门是蓝色区域的周界门。
- 棕色门是绿色区域和蓝色区域的周界门。

添加门

注意

- 您可以将门禁控制器配置为一扇具有两道锁的门，或两扇各具有一把锁的门。
- 如果门禁控制器未连接门禁，且您在门禁控制器上使用旧版软件搭配新版AXIS Optimizer，系统将阻止您添加门禁。但是，如果现有门禁已经存在，则系统确实允许在具有较旧软件的系统控制器上安装新门禁。

创建新的门配置来添加门：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）。
2. 单击 + Add door（添加门禁）。
3. 输入门名称。
4. 在**控制器**下拉菜单中，选择门禁控制器名称。当您无法添加另一扇门、脱机或 HTTPS 未处于活动状态时，控制器将呈现灰显。
5. 在**门类型**下拉菜单中，选择要创建的门类型。
6. 单击**下一步**转到门配置页面。
7. 在**主锁**下拉菜单中，选择一个中继端口。
8. 要在门上配置两个锁，请从**第二道锁**下拉菜单中选择一个中继端口。
9. 选择一个识别配置文件。请参见 。
10. 配置门设置。请参见。
11. 设置监视门禁。请参见。
12. 单击 Save（保存）。

复制现有的门配置来添加门：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）。
2. 单击 + Add door（添加门禁）。
3. 输入门名称。
4. 在**控制器**下拉菜单中，选择门禁控制器名称。
5. 单击 Next（下一步）。
6. 从**复制配置**下拉菜单中，选择现有的门配置。它显示连接的门，如果控制器配置了两扇门或一扇门有两个锁，则控制器将呈现灰显。
7. 如果需要，请更改设置。
8. 单击 Save（保存）。

要编辑门：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）> Doors（门禁）。
2. 在列表中选择一道门。
3. 单击 Edit（编辑）。
4. 更改设置，然后单击**保存**。

要移除门：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）> Doors（门禁）。

2. 在列表中选择一道门。
3. 单击 Remove（删除）。
4. 单击 Yes（是）。

在每次添加、删除或编辑门禁名称时将您的更新集成到VMS中：

1. 转到Site Navigation（场所导航）> Access control（访问控制）并单击Access Control integration（访问控制集成）。
2. 在General settings（常规设置）选项卡中，单击Refresh Configuration（刷新配置）。

门设置

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）。
2. 选择要编辑的门。
3. 单击 Edit（编辑）。

访问时间（秒）	设置在授予访问权限后门保持解锁的秒数。门将保持解锁状态，直到门打开或设定的时间结束。即使还有剩余的访问时间，门也会在关闭时锁定。
打开时间太长（秒）	仅在您已配置了门监视器时有效。设置门保持打开状态的秒数。如果在设定时间结束时门开着，则会触发开门时间过长警报。请设置一个操作规则以配置打开时间太长事件的触发操作。
访问时间长（秒）	设置在授予访问权限后门保持解锁的秒数。启用此设置后，长访问时间覆盖已为持卡人设置的访问时间。
打开时间过长（秒）	仅在您已配置了门监视器时有效。设置门保持打开状态的秒数。如果在设定时间结束时门开着，则会触发开门时间过长事件。如果您打开了**长时间访问时间** 设置，则长开放时间将覆盖已为持卡人设置的开放时间过长。
重新锁定延迟时间（毫秒）	设置门在打开或关闭后保持解锁状态的时间（以毫秒为单位）。
重新锁定	• **打开后：** 仅在您添加了门监视器时有效。 • **关闭后：** 仅在您添加了门监视器时有效。

门的安全级别

您可以添加以下安全功能到门：

两人规则 – 两人规则要求两人使用有效凭证才能获得访问权限。

刷卡两次 – 刷卡两次允许持卡人覆盖门的当前状态。例如，他们可以用它来在常规计划之外锁定或解锁门禁，这比进入系统解锁门禁更方便。刷卡两次不会影响现有计划。例如，如果门禁计划为下班时间锁定，而员工离开去吃午饭，门禁仍会按计划锁定。

您可以在添加新门时配置安全级别，也可以在现有门上执行此操作。

为现有门禁添加**两人规则**：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）。
2. 选择要为配置安全级别的门。
3. 单击**编辑**。
4. 单击**安全级别**。
5. 开启Two-person rule（两人规则）。
6. 单击**应用**。

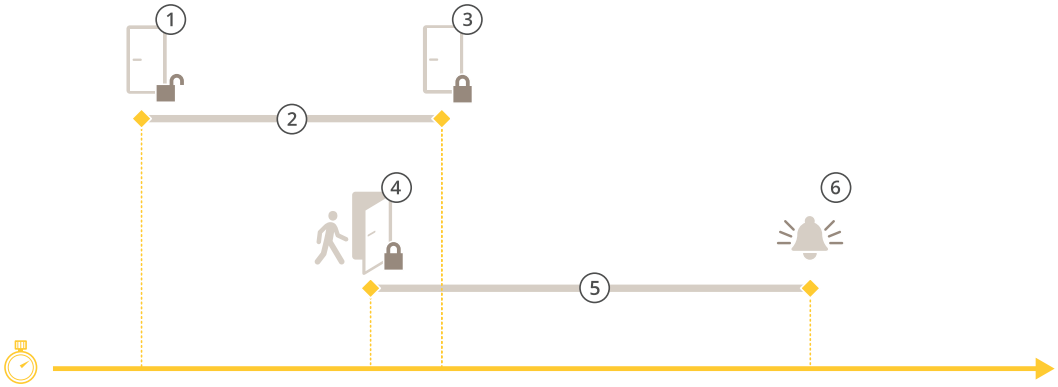
两人规则	
A 侧和 **B 侧**	选择要在门的哪一侧使用该规则。
时间计划表	选择规则处于活动状态的时间。
超时（秒）	超时是指两次刷卡或两次使用其他有效凭证之间允许的最大间隔时间。

将**刷卡两次**添加到现有门禁：

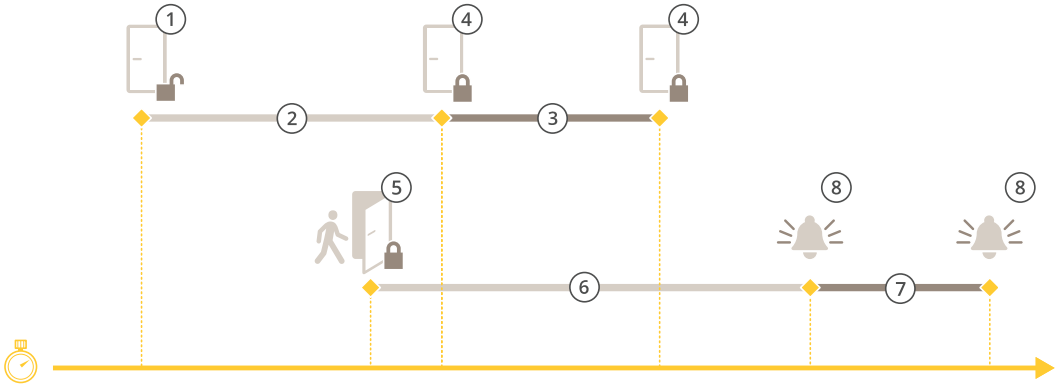
1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）。
2. 选择要为配置安全级别的门。
3. 单击**编辑**。
4. 单击**安全级别**。
5. 开启Double-swipe（刷卡两次）。
6. 单击**应用**。
7. 将Double-swipe（刷卡两次）应用于持卡人。
   7.1. 转到Cardholder management（持卡人管理）。
   7.2. 单击要编辑持卡人的 ⋮，然后单击Edit（编辑）。
   7.3. 单击More（更多）。
   7.4. 选择Allow double-swipe（允许刷卡两次）。
   7.5. 单击**应用**。

刷卡两次	
超时（秒）	超时是指两次刷卡或两次使用其他有效凭证之间允许的最大间隔时间。

时间选项



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 打开时间太长警报响起



1 访问已授权 – 锁解锁
2 访问时间
3 2+3：访问时间长
4 未执行操作 – 锁上锁
5 已执行操作（门已打开）– 锁上锁或保持解锁状态直到门关闭
6 打开时间太长
7 6+7：打开时间太长
8 打开时间太长警报响起

添加门监视器

门监视器是门位置开关，用于监控门的物理状态。您可以添加门监视器到门上，并配置门监视器电路的连接方式。

1. 进入门配置页面。参见
2. 在**传感器**下，单击**添加**。
3. 选择**门监视器传感器**。
4. 选择您要连接门监视器的 I/O 端口。
5. 在**门在以下情况下打开**下，选择门监视器电路的连接方式。

6. 要在数字输入进入新的稳定状态之前忽略其状态变化，请设置**去弹跳时间**。
7. 要在门禁控制器和门监视器之间的连接中断发生时触发事件，请打开**监督输入**。参见。

门在以下情况下打开	
电路打开	门监视器电路为常闭。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。
电路关闭	门监视器电路为常开。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。

添加监视门禁

监视门禁是一种能够显示其开闭状态的门禁类型。例如，您可以在不需要锁具但需要知道门是否打开的防火安全门上使用此门禁。

监视门禁与带门禁监视器的普通门禁不同。带门禁监视器的普通门禁支持锁具和读卡器，但需要使用门禁控制器。监视门禁支持一个门位传感器，但仅需使用连接至门禁控制器的网络输入输出继电器模块。您最多可将五个门位传感器连接到一个网络输入输出继电器模块。

注意

监视门禁需要配备AXIS A9210 Network I/O Relay Module（网络输入输出继电器模块），并安装包含AXIS Monitoring Door ACAP应用在内的最新软件。

设置监视门禁：

1. 安装您的AXIS A9210并将其升级至最新版本的AXIS OS。
2. 安装门位传感器。
3. 在VMS中，转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Doors and zones（**门禁与区域**）。
4. 单击**添加门**。
5. 输入名称。
6. 在Type（**类型**）下，选择Monitoring door（**监视门禁**）。
7. 在Device（**设备**）下，选择您的网络输入输出继电器模块。
8. 单击 Next（**下一步**）。
9. 在Sensors（**传感器**）下，单击+ Add（**添加**）并选择Door position sensor（**门位传感器**）。
10. 选择连接至门位传感器的输入输出。
11. 单击**添加**。

添加读卡器

您可以将门禁控制器配置为使用两个导线连接的读卡器。选择在门的一侧或两侧添加读卡器。

如果将卡格式或 PIN 长度的自定义设置应用于读卡器，您会在**配置 > 访问控制 > 门和区域**下的**卡格式**列中看到该项。参见。

1. 进入门配置页面。请参见。
2. 在门的一侧下，单击**添加**。
3. 选择**读卡器**。
4. 选择**读卡器类型**。
5. 为此读卡器使用自定义 PIN 长度设置。

5.1. 单击**Advanced（高级）**。

5.2. 启用**自定义 PIN 长度**。

5.3. 设置**下限 PIN 长度**、**上限 PIN 长度**和 **PIN 结束字符**。

6. 为此读卡器使用自定义卡格式。

6.1. 单击**Advanced（高级）**。

6.2. 启用**自定义卡格式**。

6.3. 选择要用于读卡器的卡格式。如果具有相同位长的卡格式已在使用中，您必须先停用它。当卡格式设置与配置的系统设置不同时，客户端中将显示警告图标。

7. 单击**添加**。

8. 要将读卡器添加到门的另一侧，请再次执行此过程。

读卡器类型	
OSDP RS485 半双工	对于 RS485 读卡器，请选择 **OSDP RS485 半双工**和读卡器端口。
Wiegand	对于使用 Wiegand 协议的读卡器，请选择 **Wiegand**，然后选择读卡器端口。

Wiegand	
LED 控制	选择**单线**或**双线 (R/G)**。具有双 LED 控制的读卡器其红色和绿色 LED 使用不同的电线。
篡改警报	当读卡器防篡改输入处于激活状态时选择。 • **开路**：当电路打开时，读卡器向门发出篡改信号。 • **闭路**：当电路闭合时，读卡器向门发出篡改信号。
防篡改的时间	要在读卡器篡改输入进入新的稳定状态之前忽略其状态变化，请设置**篡改去弹跳时间**。
监控输入	打开当在门禁控制器和读卡器之间的连接中断时触发事件。参见。

添加 REX 设备

您可以选择在门的一侧或两侧添加退出（REX）设备的要求。REX 设备可以是 PIR 传感器、REX 按钮或推杆。

1. 进入门配置页面。请参见。
2. 在门的一侧下，单击**添加**。
3. 选择 **REX 设备**。
4. 选择要在连接 REX 设备的 I/O 端口。如果只有一个端口可用，则会自动选择该端口。
5. 选择门接收到 REX 信号时要触发的**操作**。
6. 在**REX 激活**下，选择门监视器电路连接。
7. 要在数字输入进入新的稳定状态之前忽略其状态变化，请设置**去弹跳时间（毫秒）**。
8. 要在门禁控制器和 REX 设备之间的连接中断发生时触发事件，请打开**监督输入**。参见。

操作	
打开门锁	选择在门接收到 REX 信号时将其解锁。
无	如果您不想在门接收到 REX 信号时触发操作，请选择此选项。

REX 激活	
电路打开	选择 REX 电路是否为常闭。当电路为开路时，REX 装置发出信号。
电路关闭	选择 REX 电路是否为常开。当电路闭合时，REX 装置发出信号。

添加区域

区域是具有一组门的特定物理区域。您可以建立区域，并将门加入区域。有两种门：

- **周界门：** 持卡人通过此门进入或离开该区域。
- **内部门：** 区域内的内部门。

注意

一个周界门可以属于两个区域。一个内部门只能属于一个区域。

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）> Zones（区域）。
2. 单击 + Add zone（添加区域）。
3. 输入区域名称。
4. 单击**添加门**。
5. 选择要添加到区域的门，然后单击**添加**。
6. 默认情况下，门被设置为周界门。要变更，请从下拉菜单中选择**内部门**。
7. 默认情况下，周界门使用门侧 A 作为该区域的入口。要变更，请从下拉菜单中选择**离开**。
8. 要从区域移除门，请将其选中，然后单击**移除**。
9. 单击 Save（保存）。

要编辑区域：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）> Zones（区域）。
2. 在列表中选择一个区域。
3. 单击 Edit（编辑）。
4. 更改设置，然后单击**保存**。

要删除区域：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Doors and zones（门禁与区域）> Zones（区域）。
2. 在列表中选择一个区域。
3. 单击 Remove（删除）。
4. 单击 Yes（是）。

区域的安全级别

您可以向区域添加以下安全功能：

反潜回 – 防止人们使用与之前进入区域的人相同的凭据。它强制要求一个人必须先离开该区域，然后才能再次使用其凭据。

注意

- 启用反潜回功能后，区域内的门禁均需安装门位传感器，以便系统记录用户刷卡后开门的情况。
- 若某个门禁控制器离线，只要该区域内的门禁均隶属于同一门禁控制器，反潜回功能仍可正常工作。然而，如果区域内的门禁属于不同的门禁控制器，而这些控制器离线，则反潜回功能将停止工作。

您可以在添加新区域时配置安全级别，也可以在现有区域上执行此操作。要向现有区域添加安全级别：

1. 转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Doors and zones（**门禁与区域**）。
2. 选择要为配置安全级别的区域。
3. 单击**编辑**。
4. 单击**安全级别**。
5. 打开要添加到门的安全功能。
6. 单击**应用**。

反潜回	
仅日志冲突（软）	如果您想允许第二个人使用与前一个人相同的凭据进门，请使用此选项。此选项仅会导致系统警报。
拒绝访问（硬）	如果要阻止第二个用户进入门（如果他们使用与前一个人相同的凭据），请使用此选项。此选项还会导致系统警报。
超时（秒）	系统允许用户重新进入之前的持续时间。如果不希望超时，输入0，则表示该区域具有反潜回功能，直到用户离开该区域。仅当该区域中的各门两侧都有读卡器时，才将 0 超时与**拒绝访问（硬）**一起使用。

监控输入

当与门禁控制器的连接中断时，受监控输入可以触发事件。

- 门禁控制器和门监视器之间的连接。参见。
- 门禁控制器和读卡器之间的连接使用 Wiegand 协议。请参见。
- 门禁控制器和 REX 设备之间的连接。参见。

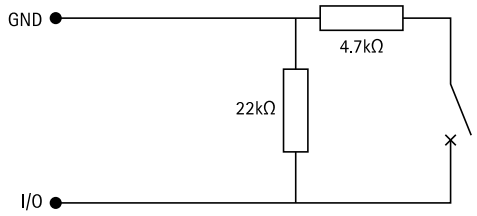
使用监控输入：

1. 根据连接图，尽可能靠近外围设备安装线路末端电阻器。
2. 进入读卡器、门监视器或 REX 设备的配置页面，打开**监督输入**。
3. 如果您按照并联优先连接图进行了操作，请选择**并联优先连接，使用一个 22 KΩ 并联电阻和一个 4.7 KΩ 串联电阻**。
4. 如果您按照串行优先连接图进行了操作，请选择**串行优先连接**，然后从**电阻值**下拉菜单中选择一个电阻值。

连接图

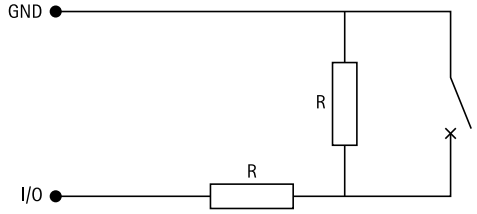
并联优先连接

电阻值要为 4.7 kΩ 和 22 kΩ。



串行首次连接

电阻器值要相同，且在 1–10 kΩ 范围内。



手动操作

您可以对门禁和区域执行以下手动操作：

重设 – 返回至配置的系统规则。

授予访问权限 – 解锁门禁或区域7秒，随后重新锁定。

解锁 – 保持门禁解锁，直至您重置。

锁 – 保持门禁锁定，直至系统授予持卡人访问权限。

封锁区域 – 除非您重置或解锁，否则无人可以进出。

执行手动操作：

1. 转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Doors and zones（**门禁与区域**）。
2. 选择您要对其执行手动操作的门禁或区域。
3. 单击任一手动操作。

卡格式和 PIN

卡格式定义了卡存储数据的方式。它是系统中传入数据和验证数据之间的转换表。每个卡格式都有一组不同的规则，用于确定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。

有预定义的常用卡格式可供您按原样使用或根据需要进行编辑。您还可以创建自定义的卡格式。

转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Card formats and PIN（**卡格式和PIN**）可创建、编辑或激活卡格式。您还可以配置 PIN。

自定义卡格式可以包含以下用于凭证验证的数据字段。

卡号 – 凭证二进制数据的子集编码为十进制或十六进制数字。使用卡号来识别特定的卡或持卡人。

设施代码 – 凭证二进制数据的子集编码为十进制或十六进制数字。使用设施代码来标识特定的终端客户或地点。

要创建卡格式：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Card formats and PIN（卡格式和PIN）。
2. 单击**添加卡格式**。
3. 输入卡格式名称。
4. 在**位长度**字段中，键入介于 1 和 256 之间的位长度。
5. 如果要反转从读卡器接收到的数据的位顺序，请选择**反转位顺序**。
6. 如果要反转从读卡器接收到的数据的字节顺序，请选择**反转字节顺序**。此选项仅在您指定的位长度可以被 8 整除时可用。
7. 选择并配置要在卡格式中激活的数据字段。**卡号**或**设施代码**在卡格式中要有效。
8. 单击**确定**。
9. 要激活卡格式，请选中卡格式名称前面的复选框。

注意

- 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，如果定义了两种 32 位卡格式，则只有其中一种可以处于活动状态。停用卡格式以激活其他卡格式。
- 如果门禁控制器配置了至少一个读卡器，那么您只能激活和停用卡格式。

ⓘ	单击ⓘ可查看反转位顺序后的输出示例。
范围	设置数据字段的数据位范围。该范围要在您为**位长度**指定的范围内。
输出格式	为数据字段选择数据的输出格式。 **十进制**：也称为以 10 为基数的位置数制，由数字 0–9 组成。 **十六进制**：也称十六进位制，由16个唯一符号组成：数字0–9与字母a–f。
子范围的位顺序	选择位顺序。 **小端字节序**：首位是下限（重要性下限）。 **大端字节序**：首位是上限（重要性上限）。

要编辑卡格式：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Card formats and PIN（卡格式和PIN）。
2. 选择卡格式并单击 。
3. 如果编辑预定义的卡格式，则只能编辑**反转位顺序**和**反转字节顺序**。
4. 单击**确定**。

您只能删除自定义卡格式。若要删除自定义卡格式：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Card formats and PIN（卡格式和PIN）。
2. 选择自定义卡格式，单击 ，然后单击Yes（是）。

要重置预定义的存储卡格式：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Card formats and PIN（卡格式和PIN）。

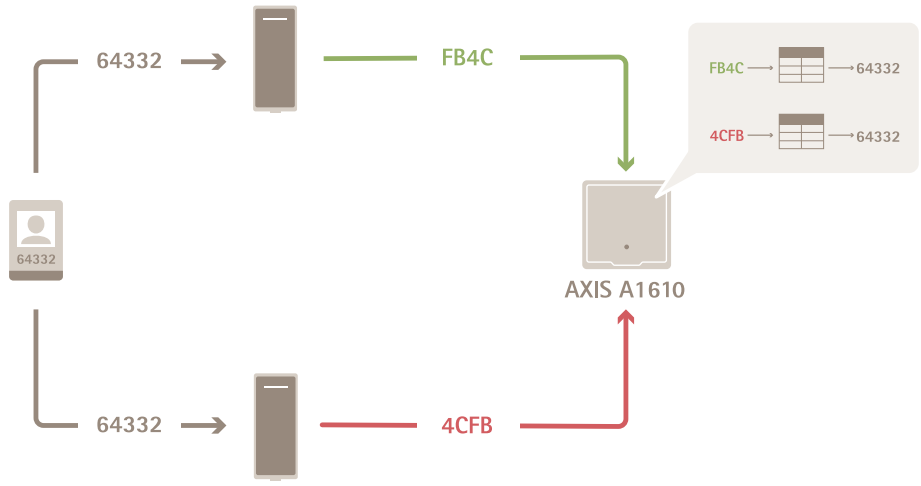
2. 单击 可将卡格式重置为默认字段映射。

要配置 PIN 长度：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Card formats and PIN（卡格式和PIN）。
2. 在PIN configuration（PIN配置）下，单击 。
3. 指定**最小 PIN 长度**、**最大 PIN 长度**和 **PIN 结束字符**。
4. 单击**确定**。

卡格式设置

概述



- 十进制卡号为64332。
- 一个读卡器将卡号转换为十六进制数FB4C。另一个读卡器将其转换为十六进制数4CFB。
- AXIS A1610 Network Door Controller接收FB4C，并根据读卡器的卡格式设置将其转换为十进制数64332。
- AXIS A1610 Network Door Controller接收4CFB，通过反转位顺序将其变更为FB4C，然后根据读卡器的卡格式设置将其转换为十进制数64332。

反转位顺序

在反转比特顺序之后，从读卡器接收的卡数据被从右到左逐比特地读取。

反转字节顺序

一组八比特是一个字节。在反转字节顺序之后，从读卡器接收的卡数据被从右到左逐字节地读取。

26 位标准 Wiegand 卡格式

1 前导奇偶校验
2 设施代码
3 卡号
4 尾部奇偶校验

识别配置文件

识别配置文件是识别类型和计划的组合。您可以将识别配置文件应用于一扇或多扇门，以设置持卡人可以进门的方式和时间。

识别类型是进门所需的凭证信息的载体。常见的标识类型包括令牌、个人标识号（PIN）、指纹、面部图和 REX 设备。标识类型可以携带一种或多种类型的信息。

计划（也称为**时间配置文件**）在管理客户端中创建。若要设置时间配置文件，请参阅*时间配置文件（详解）*。

支持的识别类型：卡、PIN和REX。

转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Identification profiles（**识别配置文件**）。

有五个默认识别配置文件可供您按原样使用或根据需要进行编辑。

卡 – 持卡人必须刷卡才能进入大门。

卡和 PIN – 持卡人必须刷卡并输入 PIN 才能进入该门。

PIN – 持卡人必须输入 PIN 才能进入该门。

卡或 PIN – 持卡人必须刷卡或输入 PIN 才能进入该门。

车ÅÆ – 持卡人必须驾驶带有经批准车牌的车辆朝向摄像机驶去。

要创建识别配置文件：

1. 转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Identification profiles（**识别配置文件**）。
2. 单击**创建识别配置文件**。
3. 输入识别配置文件名称。
4. 选择**包括卡验证的设施代码**以使用设施代码作为凭证验证字段之一。仅当您打开**访问管理 > 设置**下的**设施代码**时，此字段才可用。
5. 为门的一侧配置识别配置文件。
6. 在门的另一侧，重复前面的步骤。
7. 单击**确定**。

要编辑识别配置文件：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Identification profiles（识别配置文件）。
2. 选择一个识别配置文件并单击 。
3. 要更改识别配置文件名称，请输入新名称。
4. 对门的一侧进行编辑。
5. 若要编辑门另一侧的识别配置文件，请重复上述步骤。
6. 单击**确定**。

要删除识别配置文件：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Identification profiles（识别配置文件）。
2. 选择一个识别配置文件并单击 。
3. 如果识别配置文件应用已用于门，请为门选择其他识别配置文件。
4. 单击**确定**。

编辑标识配置文件	
×	要删除识别类型和相关计划。
识别类型	若要变更识别类型，请从**识别类型**下拉菜单中选择一或多个类型。
Schedule（时间表）	若要变更计划，请从**计划**下拉菜单中选择一或多个计划。
+ **添加**	添加识别类型和相关计划，请单击**添加**并设置识别类型和计划。

加密通信

OSDP 安全通道

Secure Entry支持OSDP（开放式监控设备协议）安全通道，可在控制器和安讯士读卡器之间启用线路加密。

要为整个系统打开 OSDP 安全通道，请执行以下操作：

1. 转到Site Navigation（场所导航）> AXIS Optimizer > Access control（访问控制）> Encrypted communication（加密通信）。
2. 输入您的主加密密钥，然后单击**确定**。
3. 打开 **OSDP 安全通道**。在您输入了主加密密钥之后，此选项才可用。
4. 默认情况下，主加密密钥生成 OSDP 安全通道密钥。手动设置 OSDP 安全通道密钥：
   4.1. 在OSDP Secure Channel（OSDP 安全通道）下，单击 。
   4.2. 清除**使用主加密密钥生成 OSDP 安全通道密钥**。
   4.3. 键入 OSDP 安全通道密钥，然后单击**确定**。

要打开或关闭特定读卡器的 OSDP 安全通道，请参见*门和区域*。

多服务器 BETA

在多服务器的情况下，连接的子服务器可使用主服务器上的全局持卡人和持卡人组。

注意

- 一个系统可支持多达 64 个子服务器。
- 它要求主服务器和子服务器位于同一网络上。
- 在主服务器和子服务器上，确保将 Windows 防火墙配置为允许安全入口端口上的传入 TCP 连接。默认端口为 53461。

工作流程

1. 将服务器配置为子服务器并生成配置文件。参见。
2. 将服务器配置为主服务器，并导入子服务器的配置文件。参见。
3. 在主服务器上配置全局持卡人和持卡人组。参见和。
4. 从子服务器查看和监控全局持卡人和持卡人组。请参见。

从子服务器生成配置文件

1. 在子服务器上，转到AXIS Optimizer > Access control（访问控制）> Multi server（多服务器）。
2. 单击**子服务器**。
3. 单击**产生**。它将生成 .json 格式的配置文件。
4. 单击**下载**并选择保存文件的位置。

将配置文件导入主服务器

1. 在主服务器上，转到AXIS Optimizer > Access control（访问控制）> Multi server（多服务器）。
2. 单击**主服务器**。
3. 单击 + Add（添加），然后转到从子服务器生成的配置文件。
4. 输入子服务器的服务器名称、IP 地址和端口号。
5. 单击**导入**以添加子服务器。
6. 子服务器的状态显示`Connected`。

撤销子服务器

您只能在将子服务器的配置文件导入主服务器之前撤销子服务器。

1. 在主服务器上，转到AXIS Optimizer > Access control（访问控制）> Multi server（多服务器）。
2. 单击**子服务器**，然后单击**撤销服务器**。
   现在，您可以将此服务器配置为主服务器或子服务器。

删除子服务器

导入子服务器的配置文件后，其将连接到主服务器。

要删除子服务器：

1. 从主服务器：
   1.1. 转到Access management（访问管理）> Dashboard（仪表板）。
   1.2. 将全球持卡人和团体更改为本地持卡人和团体。
   1.3. 转到AXIS Optimizer > Access control（访问控制）> Multi server（多服务器）。
   1.4. 单击**主服务器**以显示子服务器列表。

1.5. 选择子服务器，然后单击**删除**。

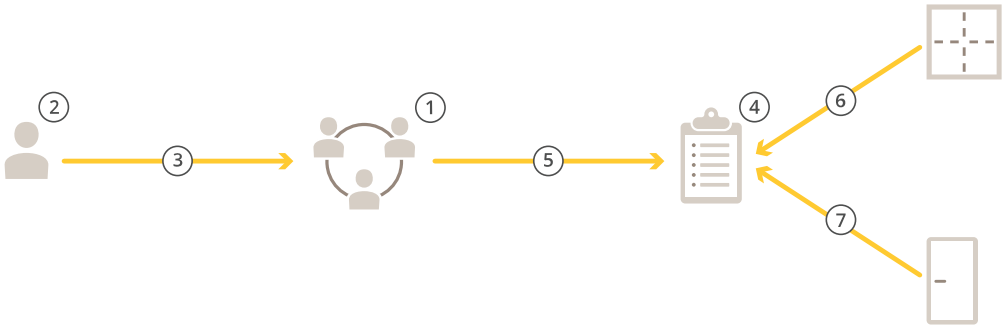
2. 从子服务器：
   - 转到AXIS Optimizer > Access control（**访问控制**）> Multi server（**多服务器**）。
   - 单击**子服务器**和**撤销服务器**。

访问管理

门禁管理选项卡允许您配置和管理系统的持卡人、组和访问规则。

访问管理工作流

门禁管理结构是灵活的，可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. 添加组。请参见 。
2. 新增持卡人。请参见 。
3. 将持卡人添加到组。
4. 添加访问规则。请参见 。
5. 将组应用于访问规则。
6. 将区域应用于访问规则。
7. 将门应用于访问规则。

添加持卡人

持卡人是在系统中注册了单独 ID 的人。为持卡人配置用于识别人员以及何时以及如何授予该人员进门权限的凭据。

1. 转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Cardholder management（**持卡人管理**）。
2. 转到Cardholders（**持卡人**）并单击+ Add（**添加**）。
3. 输入持卡人的姓名，然后单击Next（**下一步**）。
4. 也可以单击Advanced（**高级**）并选择任意选项。
5. 为持卡人添加凭证。请参见
6. 单击 Save（**保存**）。
7. 将持卡人添加到组中。
   7.1. 在Groups（**组**）中，选择您要添加持卡人的组，然后单击Edit（**编辑**）。
   7.2. 单击+ Add（**添加**），然后选择要添加到该组的持卡人。您可以选择多个持卡人。
   7.3. 单击**添加**。

7.4. 单击 Save（保存）。

高级	
访问时间长	选择让持卡人在安装了门监视器时拥有较长的访问时间和较长的打开时间。
暂停持卡人	选择暂停持卡人。
允许刷卡两次	选择此选项可允许持卡人覆盖当前门禁状态。例如，他们可以用它来解锁常规计划之外的门。
从锁定中排除	选择允许持卡人在锁定期间访问。
免于反折返	选择此选项可使持卡人免除反折返规则。反折返可防止人们使用与之前进入区域的人相同的凭据。首位人人士必须先退出该区域，然后才能再次使用其凭据。
全局持卡人	选择此项可以查看和监视子服务器上的持卡人。此选项仅适用于在主服务器上创建的持卡人。请参见 。

添加凭据

您可以为持卡人添加以下类型的凭证：

- PIN
- 卡
- 车ÅÆ
- 手机

为持卡人添加车牌凭证：

1. 在Credentials（凭证）下，单击+ Add（添加）并选择License plate（车牌）。
2. 输入用于描述车辆的凭证名称。
3. 输入车辆的许可证编号。
4. 设置凭证的起始日期和结束日期。
5. 单击**添加**。

请参阅中的示例。

为持卡人添加PIN凭证：

1. 在Credentials（凭证）下，单击+ Add（添加）并选择PIN。
2. 输入 PIN 码。
3. 若要使用强制 PIN 码来触发静音警报，请打开**强制 PIN 码** 并输入强制 PIN 码。
4. 单击**添加**。

PIN 凭据始终有效。您还可以配置强制 PIN，以打开门并在系统中触发无声警报。

为持卡人添加卡凭证：

1. 在Credentials（凭证）下，单击+ Add（添加）并选择Card（卡）。
2. 若要手动输入卡数据，请输入卡名称、卡号和位长。

注意

仅当您使用系统中没有的特定位长创建卡格式时，才可配置位长。

3. 自动获取上一次刷卡的卡数据：

3.1. 从**选择读卡器**下拉菜单中选择一个门。
3.2. 在与该门相连的读卡器上刷卡。
3.3. 单击**从门读卡器获取上次刷卡数据**。
4. 输入设施代码。仅当您启用了**访问管理 > 设置**下的**设施代码**时，此字段才可用。
5. 设置凭证的起始日期和结束日期。
6. 单击**添加**。

有效期限截止日期	
生效日期	设置凭据应有效的日期和时间。
有效期至	从下拉菜单中选择一个选项。

有效期至	
没有结束日期	凭据永不过期。
日期	设置凭据到期的日期和时间。
从首次使用	选择凭据在首次使用后的到期时段。选择首次使用后的若干天、月、年或一段时间。
从上次使用	选择凭据在上次使用后的到期时段。选择上次使用后的天数、月或年。

使用车牌号作为凭证

此示例说明如何使用门禁控制器、带 AXIS License Plate Verifier 的摄像机和车辆的牌照号作为授予访问权限的凭据。

1. 将门禁控制器和摄像机添加到 AXIS Secure Entry for XProtect。
2. 使用**与服务器计算机时间同步设置**新设备的日期和时间。
3. 将新设备上的软件升级到新的可用版本。
4. 添加一个连接到您的门禁控制器的新门。请参见 。
   4.1. 在**Side A（侧面A）**上添加读卡器。参见。
   4.2. 在 **门设置**下，选择 **AXIS License Plate Verifier**作为 **Reader 类型**，然后输入读卡器的名称。
   4.3. （可选）在**侧面 B** 上添加读卡器或 REX 设备。
   4.4. 单击**确定**。
5. 安装并激活摄像机上的 AXIS License Plate Verifier。请参见 *AXIS License Plate Verifier* 用户手册。
6. 启动 AXIS License Plate Verifier。
7. 配置 AXIS License Plate Verifier。
   7.1. 转到**配置 > 访问控制 > 加密通信**。
   7.2. 在**外部外围身份验证密钥**下, 点击**显示身份验证密钥**并**复制秘钥**。
   7.3. 从摄像机的网页界面打开 AXIS License Plate Verifier。
   7.4. 不要进行设置。
   7.5. 前往**设置**。
   7.6. 在 **访问控制**下，选择 **安全输入**作为**类型**。
   7.7. 在 **IP address**，输入门禁控制器的 IP 地址和凭证。

7.8. 在**身份验证密钥**中，粘贴您在前面复制的身份验证密钥。
7.9. 单击 Connect（**连接**）。
7.10. 在**门禁控制器名称**下，选择您的门禁控制器。
7.11. 在**读卡器名称**下，选择您之前添加的读卡器。
7.12. 打开集成。
8. 添加您要授予访问权限的持卡者。请参见 。
9. 将车牌凭据添加到新持卡人。请参见 。
10. 添加访问规则。请参见 。
10.1. 新增计划。
10.2. 添加您想向其授予许可证分配访问权限的持卡者。
10.3. 使用 AXIS License Plate Verifier 读卡器添加门。

添加组

组允许您集中有效地管理持卡人及其访问规则。

1. 转到Site Navigation（**场所导航**）> AXIS Optimizer > Access control（**访问控制**）> Cardholder management（**持卡人管理**）。
2. 转到Groups（**组**）并单击+ Add（**添加**）。
3. 输入组名，可选输入首字母缩写。
4. 选择**全局组**，可在子服务器上查看和监控持卡人。此选项仅适用于在主服务器上创建的持卡人。请参见。
5. 将持卡人添加到组中：
5.1. 单击 **+ 添加**。
5.2. 选择要添加的持卡人，然后单击Add（**添加**）。
6. 单击 Save（**保存**）。

添加访问规则

访问规则定义了授予访问权限必须满足的条件。

访问规则包括：

持卡人和持卡人组 – 谁被授予访问权限。

门和区域 – 访问权限所适用的位置。

时间计划表 – 何时授予访问权限。

要添加访问规则：

1. 转到Access control（**访问控制**）> Cardholder management（**持卡人管理**）。
2. 在Access rules（**访问规则**）下，单击+ Add（**添加**）。
3. 为访问规则输入名称，然后单击Next（**下一步**）。
4. 配置持卡人和组：
4.1. 在Cardholders（**持卡人**）或Groups（**组**）下，单击+ Add（**添加**）。
4.2. 选择持卡人或组并单击Add（**添加**）。
5. 配置门和区域：
5.1. 在Doors（**门禁**）或Zones（**区域**）下，单击+ Add（**添加**）。
5.2. 选择门禁或区域并单击Add（**添加**）。

6. 配置计划：
   6.1. 在Schedules（计划）下，单击+ Add（添加）。
   6.2. 选择一个或多个计划，然后单击Add（添加）。
7. 单击 Save（保存）。

缺少上述一个或多个组件的访问规则为未完成。您可以在Incomplete（未完成）选项卡中查看未完成的访问规则。

手动解锁门禁和区域

有关手动操作的信息（例如手动解锁门禁），请参阅。

有关手动操作的信息（例如手动解锁区域），请参阅。

导出系统配置报告

您可以导出包含系统各类信息的报告。AXIS Secure Entry for XProtect将报告导出为逗号分隔值 (CSV) 文件，并将其保存至默认下载文件夹。导出报告：

1. 转到Reports（报告）> System configuration（系统配置）。
2. 选择要导出的报告，然后单击Download（下载）。

持卡人详细信息	包括有关持卡人、凭证、卡验证和上次事务的信息。
持卡人访问权限	包括持卡人信息以及持卡人相关的持卡人组、访问规则、门和区域的信息。
持卡人组访问权限	包括持卡人组名称以及与持卡人组相关的持卡人、访问规则、门和区域的信息。
访问规则	包括访问规则名称以及与访问规则相关的持卡人、持卡人组、门和区域的信息。
门禁访问权限	包括门的名称和与门相关的持卡人、持卡人组、门禁规则和区域等信息。
区域访问权限	包括区域名称以及与该区域相关的持卡人、持卡人组、门禁规则和门的信息。

创建持卡人活动报告

点名报告列出了特定区域内的持卡人，有助于识别特定时刻的在场人员。

集合报告列出了特定区域内的持卡人，有助于在紧急情况下确认人员安全状况及失踪情况。它可辅助大楼管理者在疏散后定位员工和访客。集合点是指定的读卡器，人员在紧急情况下在此报到，从而生成场所及非场所人员报告。系统将持卡人标记为失踪，直至其在集合点报到或有人手动将其标记为安全。

点名报告和集合报告均需设置区域以追踪持卡人。

创建并运行点名或集合报告：

1. 转到Reports（报告）> Cardholder activity（持卡人活动）。
2. 单击+ Add（添加）并选择Roll call / Mustering（点名/集合）。
3. 为报告输入一个名称。
4. 选择要包含在报告中的区域。
5. 选择您希望包含在报告中的组。
6. 若需生成集合报告，请选择Mustering point（集合点）及该集合点的读卡器。

7. 选择报告的时间范围。
8. 单击 Save（保存）。
9. 选择报告并单击Run（运行）。

点名报告状态	说明
在场	持卡人进入指定区域且在您运行报告前未离开该区域。
不在场	持卡人离开指定区域且在您运行报告前未再次进入该区域。

集合报告状态	说明
安全	持卡人已在集合点刷卡。
丢失	持卡人未在集合点刷卡。

访问管理设置

自定义访问管理仪表板中使用的持卡人字段：

1. 在Access management（访问管理）选项卡中，单击Settings（设置）> Custom cardholder fields（自定义持卡人字段）。
2. 单击+ Add（添加）并输入名称。最多可添加6个自定义字段。
3. 单击**添加**。

要使用设施代码来验证访问控制系统，请执行以下操作：

1. 在Access management（访问管理）选项卡中，单击Settings（设置）> Facility code（设施代码）。
2. 选择Facility code on（开启设施代码）。

注意

配置标识配置文件时，还必须选择**包括用于卡验证的设施代码**。请参见 。

导入和导出

导入持卡人

此选项可从 CSV 文件导入持卡人、持卡人组、凭据和持卡人照片。要导入持卡人照片，请确保服务器可以访问这些照片。

导入持卡人，访问管理系统将自动保存系统配置，包括各硬件配置，并删除先前保存的配置。

导入选项	
新增	此选项删除现有持卡人并添加新持卡人。
更新	此选项更新现有持卡人并添加新持卡人。
添加	保留现有持卡人，增加新持卡人。卡号和持卡人 ID 是单独的，只能使用一次。

1. 在Access management（访问管理）选项卡中，单击Import and export（导入和导出）。
2. 单击Import cardholders（导入持卡人）。
3. 选择**新建**，**更新**，或**添加**。

4. 单击 Next（下一步）。
5. 单击Choose a file（选择文件）并转到CSV文件。单击打开。
6. 输入列分隔符，选择唯一标识符，然后单击Next（下一步）。
7. 为每列分配一个标题。
8. 单击 Import（导入）。

导入设置	
首行是标题	选择 CSV 文件是否包含列标题。
列分隔符	输入 CSV 文件的列分隔符格式。
单独标识符	默认情况下，系统使用**持卡人 ID** 来识别持卡人。您也可使用名字和姓氏或电子邮件地址。单独标识符可防止导入重复的人员记录。
卡号格式	**默认情况下，允许十六进制和数字**选定。

导出持卡人

此选项将系统中的持卡人数据导出为 CSV 文件。

1. 在Access management（访问管理）选项卡中，单击Import and export（导入和导出）。
2. 单击Export cardholders导出持卡人。
3. 选择下载位置，单击Save（保存）。

在配置发生变更时， AXIS Secure Entry for XProtect更新`C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`中的持卡人照片。

撤消导入

导入持卡人时，系统会自动保存其配置。Undo import（撤消导入）选项会将持卡人数据和各硬件配置重置为上次导入持卡人之前的状态。

1. 在Access management（访问管理）选项卡中，单击Import and export（导入和导出）。
2. 单击Undo import（撤销导入）。
3. 单击 Yes（是）。

备份和恢复

自动备份每晚执行一次。最近三个备份文件存储在以下路径：C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup。若要还原这些文件：

1. 将备份文件移动至：C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore。
2. 通过以下任一方法重新启动AXIS Secure Entry：
   - 启动MSC（服务）程序，找到“AXIS Optimizer Secure Entry Service”，然后重新启动。
   - 重新启动计算机。

T10234037_zh

2025-10 (M3.2)