MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2023 R3

管理员手册

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

目录

Copyright、商标和免责声明

商标

XProtect 是 Milestone Systems A/S 的注册商标。

Microsoft 和 Windows 是 Microsoft Corporation 的注册商标。App Store 是 Apple Inc. 的服务标记。Android 是 Google Inc.

的商标。本文涉及的所有其他商标均为其各自所有者的商标。

免责声明

本文仅可用作一般信息，在制作时已做到力求准确。

因使用该信息而引发的任何风险均由使用者承担，系统中的任何信息均不应解释为任何类型的担保。

Milestone Systems A/S 保留进行修改的权利，恕不另行通知。

本文的示例中使用的所有人名和组织名称均为虚构。如有雷同，纯属巧合。

本产品可能会使用第三方软件，第三方软件可能会应用特定条款和条件。出现这种情况时，您可在 Milestone 系统安装文件夹中的 `3rd_party_software_terms_and_conditions.txt` 文件里找到详细信息。

总览

新功能

在 Management Client 2023R3 中

XProtect Management Client

Azure Active Directory 现在可用于执行身份验证。在安装过程中，您可以选择 **Windows 身份验证**或 **Azure Active Directory Integrated**，以实现集成安全。

有关如何使用 Azure 集成安全功能安装 XProtect 的详细信息，请参阅 第 134 页上的安装本系统 - 自定义选项。

XProtect Management Client

Windows 身份验证和 Azure Active Directory Integrated 现在提供了一个(不信任服务器证书)选项。对于 Azure Active Directory Integrated，此选项必选。(不信任服务器证书)选项可确保在安装之前验证服务器证书。

XProtect Management Client:

警报中引入了新的**编辑警报设置**用户权限，允许管理员编辑警报定义、警报状态、警报类别、警报声音、警报保留和事件保留。警报定义的相应编辑权限已从现有的**管理**用户权限中删除，管理员需要同时拥有**编辑警报设置**和**管理**用户权限才能管理警报设置。

新的**编辑警报设置**用户权限不适用于现有用户，必须手动分配给需要管理员级别访问权限才能在安装或升级后配置警报的用户。

有关自定义安装的信息，请参阅 第 431 页上的角色(“安全性”节点)

在 Management Client 2023 R2 中

XProtect Management Client:

现在可以配置自适应流，在播放模式下使用。这种方法称为自适应播放。有关详细信息，请参阅 第 201 页上的自适应播放(已说明)。

XProtect Management Client:

在安装 XProtect 组件时，现在可以选择使用预先创建的数据库作为自定义安装的一部分。有关自定义安装的信息，请参阅 第 134 页上的安装本系统 - 自定义选项

XProtect Management Client:

引入了新的视频限制用户权限，允许管理员为用户配置和分配创建、查看、编辑和删除权限。有关详细信息，请参阅 第 431 页上的角色(“安全性”节点)。

在 Management Client 2023 R1 中

XProtect Incident Manager:

- 为了遵守 GDPR 或其他有关个人数据的适用法律，XProtect Management Client 的管理员现在可以为事件项目定义一个保留时间。

在 Management Client 2022 R3 中

XProtect Incident Manager:

- XProtect Incident Manager 扩展现在还与 XProtect Expert、XProtect Professional+ 和 XProtect Express+ 2022 R3 或更高版本兼容。
- XProtect Incident Manager 现在可以显示超过 10,000 个事件项目。

在 Management Client 2022 R2 中

XProtect Incident Manager:

- 该扩展的第一个版本。
- XProtect Incident Manager 扩展兼容 XProtect Corporate 版本 2022 R2 和更高版本，以及 XProtect Smart Client 版本 2022 R2 和更高版本。

XProtect LPR:

- 作为国家/地区模块一部分的牌照样式现在列在一处。
- 为了使牌照样式更易于管理，您可以根据牌照识别需要将它们分组为别名。
- 匹配列表现在支持别名。

在 Management Client 2022 R1 中

事件服务器加密：

- 您可以对事件服务器和与事件服务器 通信的组件之间的双向连接进行加密，包括 LPR Server。

  有关详细信息，请参阅 第 263 页上的启用事件服务器加密。

通过外部 IDP 登录：

- 您现在能够使用外部 IDP 登录 Milestone XProtect VMS。通过外部 IDP 登录是以 Active Directory 用户或基本用户登录的一种替代选择。凭借外部 IDP 登录方式，您可以绕过基本用户的设置要求，并且仍然能够获授权访问 XProtect 中的组件和设备。

  有关详细信息，请参阅外部 IDP(以作说明) 。

更新硬件数据

- 您现在能够看到 Management Client 中系统侦测到的硬件设备的当前固件版本。

  有关详细信息，请参阅 第 301 页上的更新您的硬件数据。

XProtect Management Server Failover

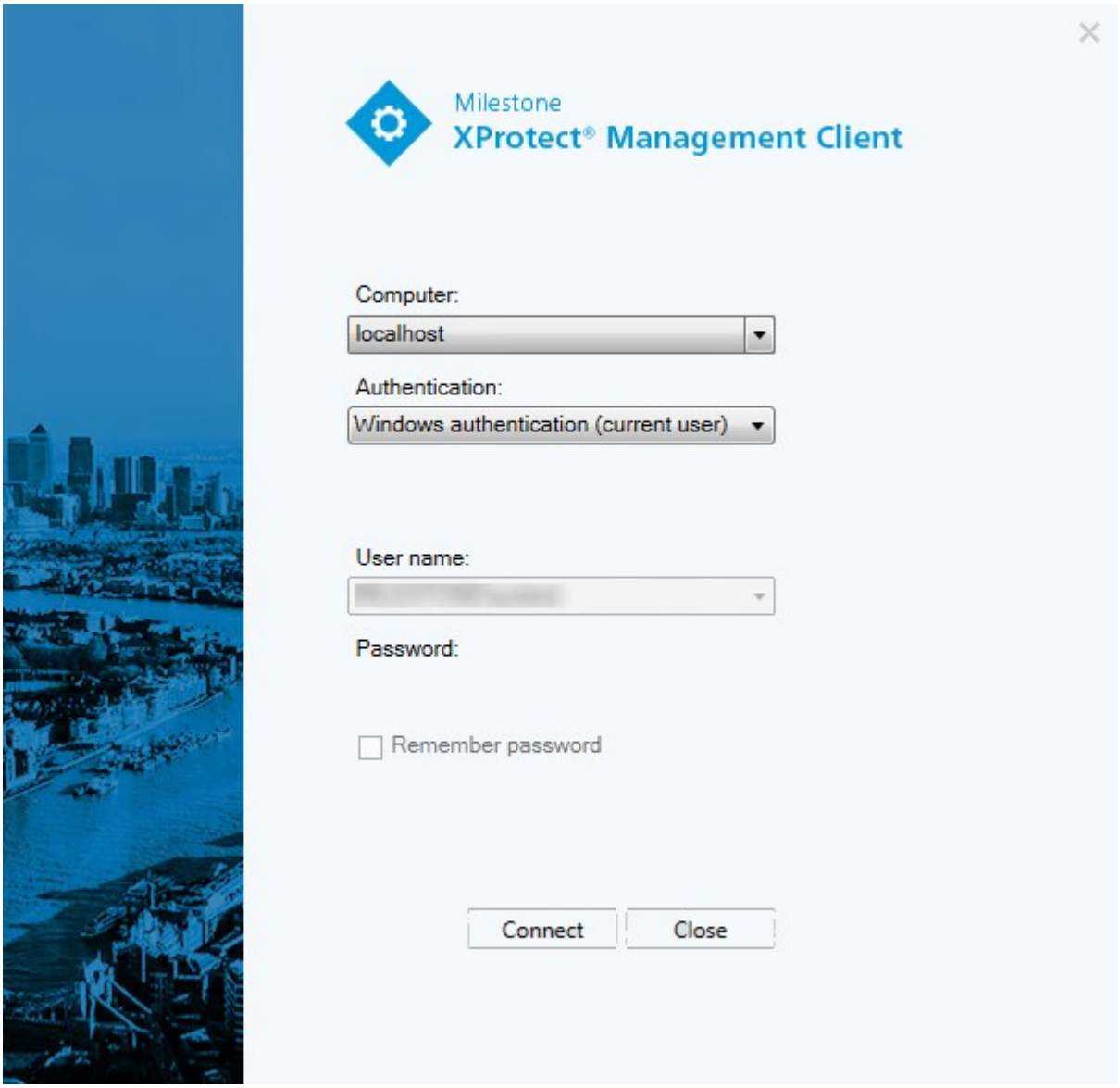
- 您现在可以通过配置两个冗余计算机之间的故障转移管理服务器来实现高系统可用性。如果运行管理服务器的计算机出现故障，则第二个计算机会接管。实时数据复制确保管理服务器、日志服务器和事件服务器的数据库在两个计算机上都是相同的。

  有关详细信息，请参阅 第 35 页上的XProtect Management Server Failover 。

登录(已作说明)

启动 Management Client 时，必须先输入登录信息才能连接到系统。

安装 XProtect Corporate 2016 或 XProtect Expert 2016 或更新版本后，您可以在安装补丁后登录到运行旧版本产品的系统。支持的版本包括 XProtect Corporate 2013 和 XProtect Expert 2013 或更新版本。



登录授权(已解释)

系统允许管理员设置用户，以使这些用户只能在得到具有足够权限的其他用户的登录授权时登录系统。在此情况下，XProtect Smart Client 或 Management Client 在登录期间要求第二次授权。

与内置的**管理员**角色关联的用户始终有权进行授权，而不会被要求进行二次登录，除非该用户与需要执行二次登录的另一个角色相关联。

通过外部 IDP 登录的用户无法设置由第二位用户授权的要求。

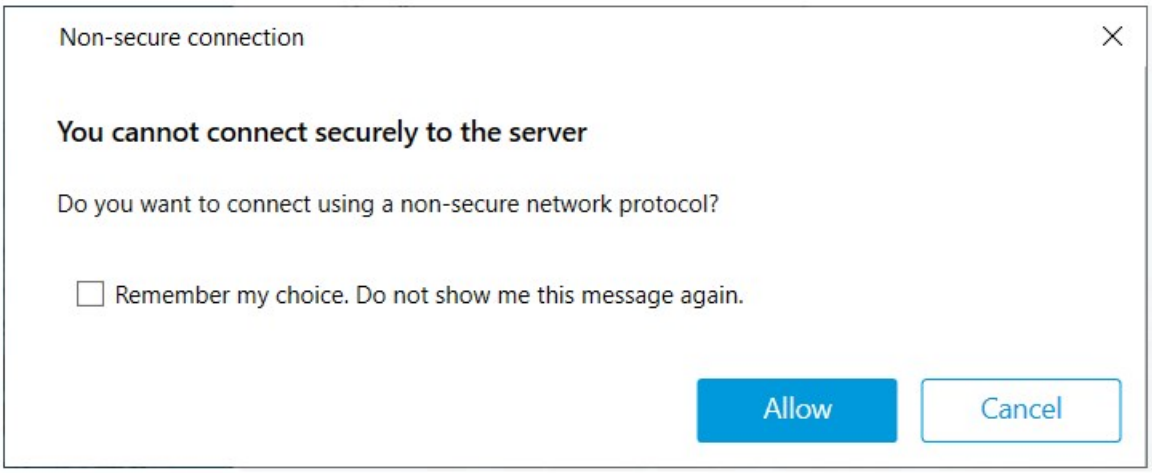
要将登录授权与角色关联：

- 在**信息**选项卡(请参阅角色设置)的**角色**下为所选角色设置**需要登录授权**，从而要求用户在登录时进行额外的授权
- 在**整体安全**选项卡(请参阅角色设置)的**角色**下为所选角色设置**为用户授权**，使用户能够为其他用户的登录提供授权

可为同一个用户选择这两个选项。这意味着将要求用户在登录过程中进行额外的授权，但也可为除该用户外的其他用户的登录提供授权。

使用非安全连接登录

登录 Management Client 时，系统可能会询问您是否要使用非安全网络协议进行登录。



- 单击**允许**以登录并忽略通知。为避免将来收到此通知，可以选择**记住我的选择。不再显示此消息**或单击**工具 > 选项**，然后选择**允许与服务器的非安全连接(需要重新启动 Management Client)**。

有关安全通信的信息，请参阅 第 124 页上的安全通信(已解释)。

更改您的基本用户密码

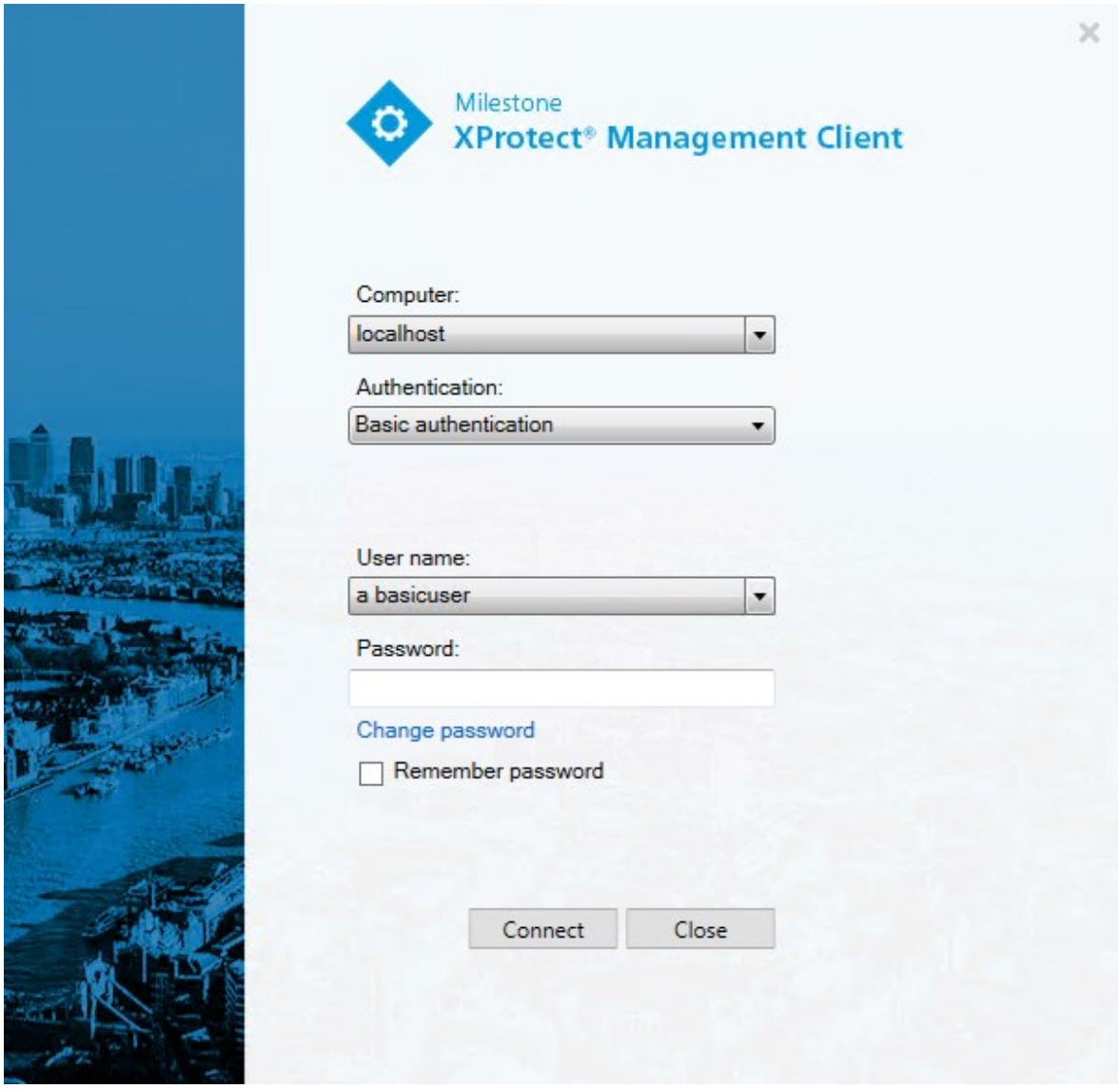
如果您以**基本用户**身份登录，则可以更改密码。如果选择其他身份验证方法，则只有系统管理员才能更改您的密码。更改密码通常会提高 XProtect 视频管理软件系统的安全性。

要求

XProtect 视频管理软件系统的版本必须为 2021 R1 或更新版本。

步骤：

1. 开始 Management Client。登录窗口将打开。
2. 指定您的登录信息。在**身份验证**列表中，选择**基本身份验证**。此时会出现一个带有文本**更改密码**的链接。



3. 单击该链接。此时将打开一个浏览器窗口。
4. 按照说明进行操作并保存更改。
5. 现在您可以使用您的新密码登录 Management Client。

产品概述

XProtect VMS 产品是设计用于各种形状和大小的安装的视频管理软件。无论您是想保护店面免遭破坏，还是想要管理多站点高安全性安装，XProtect 都能让您梦想成真。该解决方案提供对所有设备、服务器和用户的集中管理，并提供由时间表和事件驱动的、极其灵活的规则系统。

本系统包含下列主要组件：

- **管理服务器**，它是安装的中心，由多个服务器构成
- 一个或多个**记录服务器**
- 一个或多个 **XProtect Management Client** 安装
- **XProtect Download Manager**
- 一个或多个 **XProtect® Smart Client** 安装
- 一个或多个 **XProtect Web Client** 使用和/或 **XProtect Mobile** 客户端安装（如有需要）

本系统还包括完全集成的 Matrix 功能，可用于分布式查看从监控系统上的任何摄像机到安装了 XProtect Smart Client 的任何计算机上的视频。

您可以在分布式设置中将系统安装在虚拟服务器或多个物理服务器上。另请参阅第77页上的分布式系统设置。

系统也可在从 XProtect® Smart Client - Player 导出视频证据时，包含独立 XProtect Smart Client。XProtect Smart Client - Player 可让视频证据接收方（如警官或内外部调查人员等）直接浏览和播放导出的记录，而不必在他们的计算机上安装任何软件。

通过安装功能最丰富的产品（请参阅 第 96 页上的产品对比），您的系统可以处理数量不受限制的摄像机、服务器和用户（需要时可跨站点进行）。本系统能够处理 IPv4 以及 IPv6。

系统组件

管理服务器（已作说明）

管理服务器是视频管理软件系统的核心组件。它在 SQL Server 数据库中存储监控系统的配置，该数据库位于管理服务器计算机自身的 SQL Server 上或网络中单独的 SQL Server 上。还可处理用户身份验证、用户权限、规则系统等。为改善系统性能，可以将多个管理服务器作为 Milestone Federated Architecture™ 运行。管理服务器作为服务运行，并且通常安装在专用服务器上。

用户连接到管理服务器进行初始身份验证，然后透明地连接到记录服务器以便访问视频记录等。

SQL Server 安装和数据库（已说明）

管理服务器、事件服务器和日志服务器在一个或多个 SQL Server 安装的 SQL Server 数据库中存储诸如系统配置、警报、事件和日志消息等。管理服务器和事件服务器共享相同的 SQL Server 数据库，而日志服务器 、

XProtect Incident Manager, 和 Identity Provider 每个都具有自己的 SQL Server 数据库。有关 Identity Provider 的详细信息，请参阅 第 58 页上的Identity Provider(已作说明)。有关 XProtect Incident Manager 数据库和日志记录的详细信息，请参阅单独的 XProtect Incident Manager 管理员手册。

系统安装程序包括 SQL Server 的免费版 Microsoft SQL Server Express。

对于与 SQL Server 数据库之间有许多交易的庞大系统或系统，Milestone 建议您在网络上的专用计算机上以及在不用于其他用途的专用硬盘驱动器上使用 SQL Server 的 Microsoft® SQL Server® Standard 或 Microsoft® SQL Server® Enterprise 版。在自己的驱动器上安装 SQL Server 可提高整个系统的性能。

记录服务器(已作说明)

记录服务器负责与网络摄像机和视频编码器通信、记录检索的音频和视频，以及提供对实时与记录音频和视频的客户端访问。此外，记录服务器还负责与通过Milestone 技术连接的其他 Milestone Interconnect 产品进行通信。

设备驱动程序

- 网络摄像机和视频编码器之间的通信，通过专门针对各个设备或相同制造商的一系列相似设备开发的设备驱动程序完成
- 从 2018 R1 版本开始，设备驱动程序分为两个设备软件包：包含较新驱动程序的常规设备软件包和包含较旧驱动程序的旧设备软件包
- 安装记录服务器时，将自动安装常规设备软件包。稍后，您可以下载并安装更新版本的设备软件包，以更新驱动程序
- 只有在系统安装了常规设备软件包的情况下，才能安装旧版设备软件包。如果系统上已经安装了以前的版本，将自动安装旧版设备软件包中的驱动程序。可以在软件下载页面 (https://www.milestonesys.com/downloads/) 手动下载和安装。

媒体数据库

- 记录服务器将检索的音频和视频数据存储在针对记录和存储音频和视频数据优化的定制高性能媒体数据库中
- 媒体数据库支持多个独特的功能，如多级存档、视频整理、加密以及将数字签名添加至记录。

该系统使用记录服务器记录视频馈送，并与摄像机和其他设备通信。监控系统通常由多个记录服务器组成。

记录服务器是已安装 Recording Server 软件并将其配置为与管理服务器通信的计算机。当您展开**服务器**文件夹然后选择**记录服务器**时，可以在**总览**窗格中看到您的记录服务器。

对于早于此管理服务器版本的版本，与录制服务器的向后兼容性将受到限制。您仍可访问旧版本记录服务器上的记录；但如果要更改其配置，请确保它们与该管理服务器版本匹配。Milestone 建议将系统中的所有记录服务器升级至与您的管理服务器相同的版本。

记录服务器支持对客户端和服务的数据流加密：

- 第 264 页上的对客户端和服务器启用加密
- 第 251 页上的查看客户端的加密状态

记录服务器还支持将与管理服务器的连接加密。

- 第 260 页上的从管理服务器启用加密或将加密应用到管理服务器

您具有与管理 recording server 相关的多个选项：

- 第 185 页上的添加硬件
- 第 295 页上的移动硬件
- 第 311 页上的删除记录服务器上的所有硬件
- 第 311 页上的删除记录服务器

如果 Recording Server 服务正在运行，请务必确保 Windows Explorer 或其他程序没有访问与您的系统设置相关的媒体数据库文件或文件夹。否则，记录服务器可能无法重命名或移动相关媒体文件。这可能会使记录服务器停止。要重新启动已停止的记录服务器，请停止 Recording Server 服务，关闭正在访问相关媒体文件或文件夹的程序，并重启 Recording Server 服务。

移动设备服务器(已作说明)

移动设备服务器负责为 XProtect Mobile 客户端和 XProtect Web Client 用户提供系统访问权限。

除了用作两个客户端的系统网关外，移动设备服务器还可以对视频进行转码，因为许多情况下，原始的摄像机视频流太大，不适合客户端用户的带宽。

如果您正在执行**分布式**或**自定义**安装，Milestone 建议在专用服务器上安装移动设备服务器。

事件服务器(已作说明)

事件服务器会处理与事件、警报、地图可能还有通过 MIP SDK 进行的第三方集成相关的各种任务。

事件

- 所有系统事件均合并到事件服务器中，因此合作伙伴在单个地方和接口进行利用系统事件的集成
- 此外，事件服务器允许第三方通过常规事件或分析事件界面将事件发送至系统

警报

- 事件服务器托管警报功能、警报逻辑、警报状态并处理警报数据库。警报数据库存储在管理服务器使用的相同 SQL Server 数据库中

消息

- 消息通信由事件服务器处理，允许插件在 XProtect Smart Client、Management Client、事件服务器和独立服务等环境之间实时发送消息。

地图

- 事件服务器还托管 XProtect Smart Client 中配置和使用的地图

MIP SDK

- 最后，第三方开发的插件可以安装在事件服务器上，并利用对系统事件的访问

日志服务器(已作说明)

日志服务器将整个系统的所有日志消息存储在一个 SQL Server 数据库中。此日志消息 SQL Server 数据库可以与管理服务器的系统配置 数据库存在于同一 SQL Server 上，也可以存在于单独的 上。日志服务器通常安装在与管理服务器相同的服务器上，但为了提升管理服务器和日志服务器的性能，也可以安装在单独的服务器上。

API Gateway(已作说明)

MIP VMS API 基于 OpenAPI 等行业标准协议提供了统一的 RESTful API，用于访问 XProtect VMS 功能，简化集成项目，并作为云连接通信的基础。

XProtect VMS API Gateway 通过 Milestone Integration Platform VMS API (MIP VMS API) 支持这些集成选项。

API Gateway 安装在本地，旨在作为所有当前视频管理软件服务器组件(管理服务器、事件服务器、录制服务器、日志服务器等)上 RESTful API 和 WebSocket 消息 API 服务的前端和公共入口点。API Gateway 服务可以安装在与管理服务器相同的主机上，也可以单独安装，并且可以安装多个(每个安装在各自的主机上)。

RESTful API 部分由每个特定的视频管理软件服务器组件实现，API Gateway 可以简单地传递这些请求和响应，而对于其他请求，API Gateway 将根据需要转换请求和响应。

目前，由管理服务器托管的配置 API 是一个 RESTful API。此外，还提供了由事件服务器托管的 RESTful 事件 API、Websockets 消息 API 和 RESTful 警报 API。

有关详细信息，请参阅 API Gateway 管 理员手册和 Milestone Integration Platform VMS API 参考文档。

故障转移

XProtect Management Server Failover

如果运行 Management Server 服务的独立计算机或 SQL Server 出现硬件故障，则不会影响录制或录制服务器。但是，这些硬件故障可能会导致未登录客户端的操作员和管理员停机。

XProtect Management Server Failover 为管理服务器提供高可用性和灾难恢复。如果一台电脑上的管理服务器不可用，另一台电脑将接管运行系统组件的任务。

您可以使用 SQL Server 数据库的安全实时复制功能，确保在硬件发生故障时不会丢失数据。

XProtectManagementServerFailover可以帮助您减少系统停机时间。在以下情况下，您可以受益于故障转移群集：

- 服务器故障时—您可在解决问题的同时，从另一台计算机运行Management Server服务和SQL Server。
- 需要应用系统更新和安全补丁时—在独立的管理服务器上应用安全补丁可能非常耗时，导致停机时间延长。当您拥有故障转移群集时，您可以在最短的停机时间内应用系统更新和安全补丁。
- 您需要无缝连接时—用户始终可以访问实时和播放视频以及系统的配置。

可在两台计算机之间配置XProtect Management Server Failover。若要使故障转移发挥作用，您需要在每台计算机上安装：

- XProtect Management Server
- XProtect Event Server 服务
- XProtect Log Server 服务
- Microsoft SQL Server(建议)

故障转移管理服务器(已作说明)

通过在 Microsoft Windows 群集中安装管理服务器来实现管理服务器上的故障转移支持。群集随后可以确保在第一台服务器出现故障时，另一台服务器接管管理服务器功能。

故障转移记录服务器(已作说明)

> 可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

故障转移记录服务器是在常规记录服务器变得不可用时进行接管的额外记录服务器。您可以采用两种方式来配置故障转移记录服务器，将其作为**冷后备服务器**或作为**热后备服务器**。

故障转移记录服务器的安装类似于标准记录服务器(请参阅 第 143 页上的安装故障转移记录服务器，通过 Download Manager)。安装了故障转移记录服务器之后，便可在 Management Client 中看到它们。Milestone 建议您将所有故障转移记录服务器安装在单独的计算机上。确保使用管理服务器的正确 IP 地址/主机名配置故障转移记录服务器。在安装过程中，将提供运行故障转移服务器服务所使用的用户帐户的用户权限。它们是：

- 用于启动或停止故障转移记录服务器的启动/停止权限
- 用于读取或写入 RecorderConfig.xml 文件的读取和写入访问权限

如果选择了证书进行加密，则管理员必须在所选证书私钥上向故障转移用户授予读取访问权限。

如果故障转移记录服务器从使用加密的记录服务器接管，Milestone 还建议您准备使用加密的故障转移记录服务器。有关详细信息，请参阅 第 124 页上的安全通信(已解释) 和 第 143 页上的安装故障转移记录服务器，通过 Download Manager。

可在设备级别指定您想要的故障转移支持类型。对于记录服务器上的每台设备，选择全力、仅实时或无故障转移支持。这有助于对故障转移资源进行优先级排序，例如，为视频而不为音频设置故障转移，或仅在重要的摄像机而不在较不重要的摄像机上设置故障转移。

在系统处于故障转移模式时，您无法更换或移动硬件、更新记录服务器或更改设备配置(如存储设置或视频流设置)。

冷后备故障转移记录服务器

在热后备故障转移记录服务器设置中，您可以将多播故障转移记录服务器分到故障转移组中。整个故障转移组专门用于在多台预选的记录服务器中的任意一台变得不可用时进行接管。您可以根据需求创建任意数量的组(请参阅 第 183 页上的为冷后备故障转移记录服务器分组)。

分组具有明显的好处:在之后指定哪些故障转移记录服务器应接管记录服务器时，您可以选择一组故障转移记录服务器。如果所选组包含一台以上的故障转移记录服务器，这样便可使一台以上故障转移记录服务器做好在记录服务器不可用时进行接管的准备，从而确保安全。您可以指定第二组故障转移服务器，当第一组中的所有记录服务器都繁忙时，第二组就接管第一组。故障转移记录服务器一次只能为一个组的成员。

故障转移组中的故障转移记录服务器按顺序排列。该顺序决定了故障转移记录服务器接管记录服务器的顺序。默认情况下，该顺序反映您将故障转移记录服务器加入故障转移组时的顺序:最先放入的就排在最前面。可根据需要进行更改。

热后备故障转移记录服务器

在热后备记录服务器设置中，您可以专门指定一台故障转移记录服务器只接管**一台**记录服务器。因此，系统可使该故障转移记录服务器保持“后备”模式，这意味着它与相应记录服务器的正确/当前配置同步，可以比常规故障转移记录服务器更快地进行接管。如上文所述，热后备服务器仅分配给一台记录服务器，无法进行分组。您无法将已经属于某个故障转移组的故障转移服务器选为热后备记录服务器。

故障转移记录服务器验证

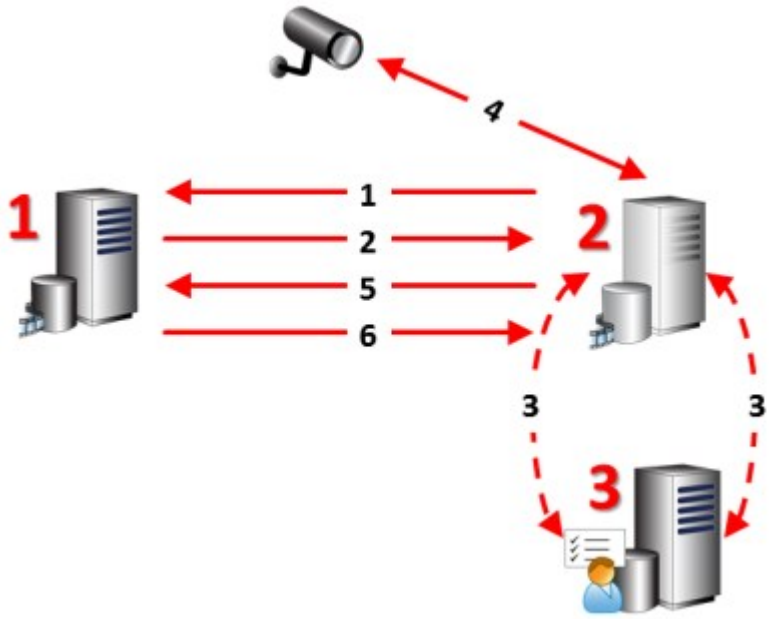
要验证从故障转移服务器到记录服务器的视频数据合并，您必须通过停止记录服务器服务或关闭记录服务器计算机来使记录服务器不可用。

通过拔出网线或使用测试工具阻塞网络而导致的任何手动网络中断都不是有效的方法。

故障转移记录服务器功能(已解释)

- 故障转移记录服务器每 0.5 秒检查一次相关记录服务器的状态。如果录制服务器在 2 秒内无回复，录制服务器将被视为不可用，并且故障转移记录服务器会进行接管
- 在接管不可用的记录服务器时，冷后备故障转移记录服务器需要耗费五秒，再加上故障转移记录服务器的 Recording Server 服务的启动时间以及连接到摄像机所花的时间。相比而言，热后备服务器具有更快的接管速度，因为 Recording Server 服务已经使用正确的配置运行，并且只需启动其摄像机以提供馈送。在启动期间，您将无法存储录像，也无法查看受影响摄像机的实时视频
- 记录服务器重新变为可用时，会自动从故障转移记录服务器进行接管。故障转移记录服务器存储的记录会自动合并到标准记录服务器的数据库中。合并流的时间取决于记录量和网络容量等。合并期间，您将无法浏览故障转移记录服务器接管时间段中的录像
- 如果在冷后备故障转移记录服务器中的合并过程期间，故障转移记录服务器必须从另一个记录服务器接管，它会推迟与记录服务器 A 的合并过程，并从记录服务器 B 接管。
- 当记录服务器 B 重新变为可用时，故障转移记录服务器会开始合并过程并允许记录服务器 A 和记录服务器 B 同时合并回记录。在热后备设置中，热后备服务器无法接管其他记录服务器，因为它只能作为单一记录服务器的热后备。但是如果该记录服务器再次发生故障，热后备服务器将再次接管，并且还会保留前一时间段的记录。
- 记录服务器会持续录制，直到它们合并回主录像服务器或直到故障转移记录服务器用完磁盘空间故障转移解决方案不提供完整冗余，仅可作为将停机时间缩短至最低程度的可靠方法。记录服务器重新变为可用时，Failover Server 服务将确保记录服务器已做好重新存储录像的准备。之后才将存储记录的职责交回标准记录服务器。因此，在流程的这一阶段不太可能丢失录像
- 客户端用户不容易注意到故障转移记录服务器正在接管。故障转移记录服务器接管时会出现短暂中断(通常仅为数秒钟)。在此中断期间，用户无法访问受影响记录服务器的视频。故障转移记录服务器进行接管之后，客户端用户便可恢复查看实时视频。由于最近的记录存储在故障转移记录服务器上，因此可播放故障转移记录服务器接管后的记录。在记录服务器重新工作并从故障转移记录服务器接管之前，客户端无法播放仅存储在受影响的记录服务器上的更早记录。不能访问存档记录。在记录服务器重新工作后，会有一个合并流程，在该流程中故障转移记录将合并回记录服务器的数据库。在此流程中，无法播放故障转移记录服务器接管时间段中的录像
- 在常规故障转移设置中，无需为另一台故障转移记录服务器设置一台故障转移记录服务器作为备份。因为您分配故障转移组，不用分配用于从特定记录服务器进行接管的具体故障转移记录服务器。故障转移组必须包含至少一台故障转移记录服务器，但可根据需要添加任意数量的故障转移记录服务器。如果故障转移组包含一台以上故障转移记录服务器，就有一台以上的故障转移记录服务器能够接管。
- 在热后备设置中，无法为热后备服务器设置故障转移记录服务器或热后备故障转移服务器

故障转移步骤(已解释)



说明
涉及的服务器(红色数字): 1. Recording Server 2. Failover Recording Server 3. Management Server
冷后备设置的故障转移步骤: 1. 为了检查故障转移记录服务器是否运行,它与记录服务器之间必须具有不中断的 TCP 连接。 2. 此连接被中断。 3. 故障转移记录服务器从管理服务器请求记录服务器的当前配置。管理服务器发送请求的配置,故障转移记录服务器接收配置,启动,然后代表记录服务器开始记录。 4. 故障转移记录服务器和相关摄像机交换视频数据。 5. 故障转移记录服务器连续尝试重新建立与记录服务器的连接。 6. 重新建立与记录服务器的连接后,故障转移记录服务器关闭,记录服务器获取在其停机时间记录的视频数据(如果有),然后将视频数据合并回记录服务器数据库中。

说明

热后备设置的故障转移步骤：

1. 为了检查热后备服务器是否运行，它与所分配的记录服务器之间必须具有不中断的 TCP 连接。
2. 此连接被中断。
3. 热后备服务器从管理服务器了解分配的记录服务器的当前配置，并代表其开始记录。
4. 热后备服务器和相关摄像机交换视频数据。
5. 热后备服务器连续尝试重新建立与记录服务器的连接。
6. 重新建立与记录服务器的连接后，热后备服务器回到热后备模式，记录服务器获取在其停机时间记录的视频数据(如果有)，然后将视频数据合并回记录服务器数据库中。

故障转移记录服务器的服务(已解释)

故障转移记录服务器安装有两个服务：

- FailoverServer服务用于处理从记录服务器接管的过程。该服务始终运行，并持续检查相关记录服务器的状态
- Failover Recording Server 服务用于使故障转移记录服务器用作记录服务器。

  在冷后备设置中，该服务仅在必要时启动，即当冷后备故障转移记录服务器应从记录服务器接管时。启动该服务通常需要数秒时间，但根据本地安全设置及其他设置，可能需要更长时间。
  在热后备设置中，该服务始终运行，使热后备服务器比冷后备故障转移记录服务器更快接管。

客户端

Management Client(已作说明)

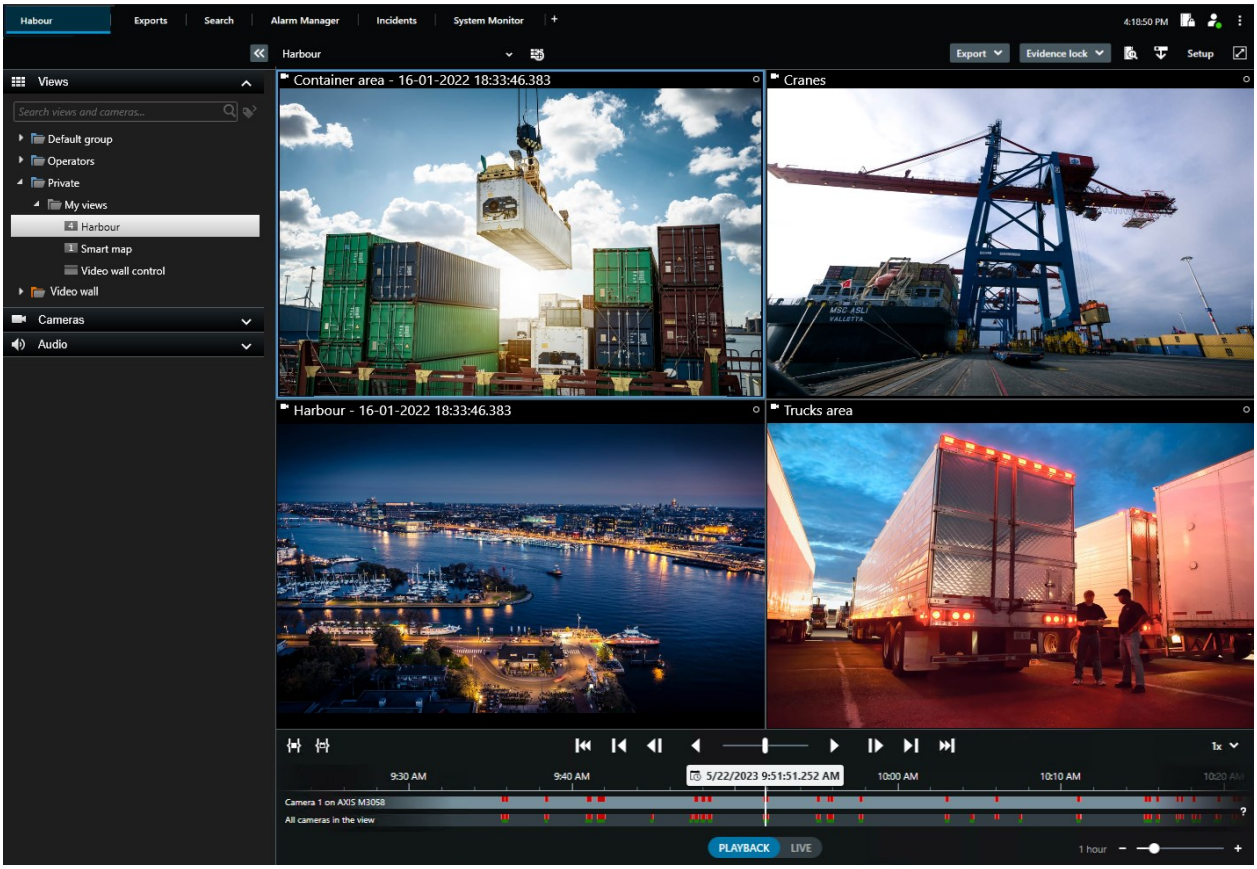
Management Client 是功能丰富的管理客户端，用于系统的配置和日常管理。有数种语言版本。

通常安装在监控系统管理员的工作站或类似设备上。

XProtect Smart Client(已作说明)

XProtectSmartClient是旨在帮助您管理 监控摄像机的桌面应用程序。它使用户可以访问实时和记录的视频，对摄像机和连接的安全设备进行即时控制，并可以对记录和元数据进行高级搜索，从而提供对安全设施的直观控制。

XProtect Smart Client 提供多个本土语言版本，具有自适应的用户界面，可优化以适应不同操作员的任务，并根据具体技能和权限级别进行调整。



界面允许您通过选择浅色或深色主题来定制您在特定工作环境中的视觉体验。它还具有工作经过优化的选项卡和主时间轴，让您轻松进行监控操作。

用户使用 MIP SDK 可以集成多种类型的安全和业务系统以及视频分析应用程序，它们均可通过 XProtect Smart Client 进行管理。

XProtect Smart Client 必须安装在操作员的计算机上。监控系统管理员通过 Management Client 管理对监控系统的访问。客户端所查看的记录由 XProtect 系统的 Image Server 服务提供。该服务在监控系统服务器的后台运行。不需要单独的硬件。

XProtect Mobile 客户端(已解释)

XProtect Mobile 客户端是与 XProtect 系统的其他部分紧密整合的移动监控解决方案。它可以在 Android 平板电脑或智能手机或 Apple® 平板电脑、智能手机或便携式音乐播放器上运行，并允许您访问管理客户端中设置的摄像机、视图和其他功能。

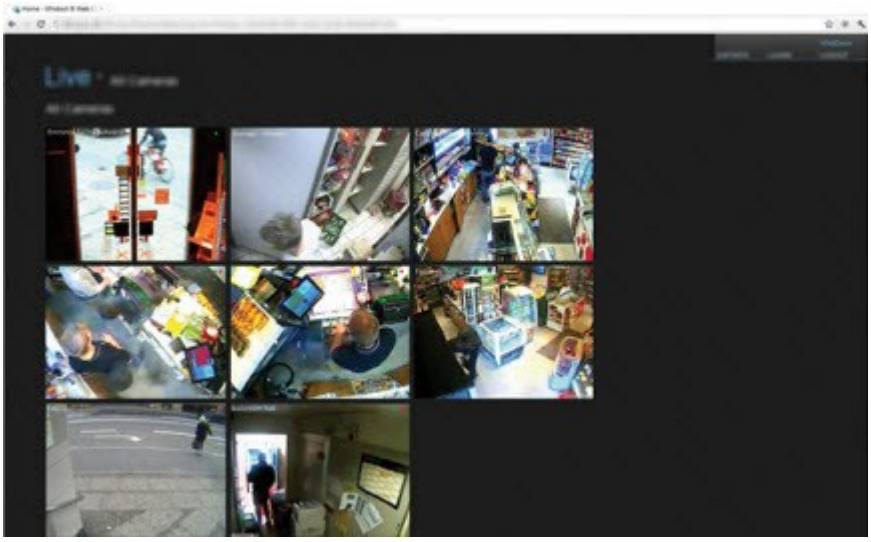
使用 XProtect Mobile 客户端可查看和播放一个或多个摄像机的实时视频和记录视频，控制全景/倾斜/变焦(PTZ)摄像机，触发输出和事件，并使用视频推送功能将设备的视频发送至 XProtect 系统。

如果要将 XProtect Mobile 客户端结合本系统使用，您必须添加 XProtect Mobile 服务器以在 XProtect Mobile 客户端和本系统之间建立连接。设置 XProtect Mobile 服务器后，从 Google Play 或 App Store 免费下载 XProtect Mobile 客户端以开始使用 XProtect Mobile。

您需要为每个设备提供一个设备许可证，以便能够将视频推送到您的 XProtect 系统。

XProtect Web Client(已作说明)

XProtect Web Client 是一款基于 web 的客户端应用程序，用于查看、播放和共享视频。利用它可以即时访问大多数常用监控功能，如查看实时视频，播放记录视频，以及打印和导出证据。这些功能的访问权限取决于 Management Client 中设置的各用户权限。



要启用对 XProtect Web Client 的访问权限，必须安装 XProtect Mobile 服务器以在 XProtect Web Client 和您的系统之间建立连接。XProtect Web Client 本身不要求任何安装，可搭配大多数互联网浏览器使用。一旦设置好 XProtect Mobile 服务器，即可在任何地方从具有互联网接入的任何计算机或平板电脑监控XProtect系统(前提条件是知道正确的外部/互联网地址、用户名与密码)。

XProtect 扩展

XProtect Access(已作说明)

Milestone 开发了各种扩展。扩展是通过附加的专门功能来扩展 XProtect 视频管理软件产品功能的产品。您的 XProtect 许可证文件用于控制对扩展的访问。

要使用 XProtect Access，您必须购买允许您在 XProtect 系统中访问该功能的基本许可证。您还需要用于要控制的每道门的访问控制门许可证。

您可以将 XProtect Access 与具有 XProtect Access 供应商特定插件的供应商的访问控制系统配合使用。

访问控制集成这一新功能使得客户的访问控制系统与 XProtect 的集成变得简单。您将可以：

- 使用 XProtect Smart Client 中的多个访问控制系统通用的操作员用户界面
- 与访问控制系统更快更强地集成
- 适用于操作员的更多功能(请参阅下文)

在 XProtect Smart Client 中，操作员可以：

- 实时监视访问点的事件
- 使用访问请求的操作员辅助通道
- 使用地图集成
- 执行访问控制事件的警报定义
- 调查访问点的事件
- 对门状态进行集中概览和控制
- 获取持卡人信息并进行管理

审核日志从 XProtect Smart Client 记录每个用户在访问控制系统中执行的命令。

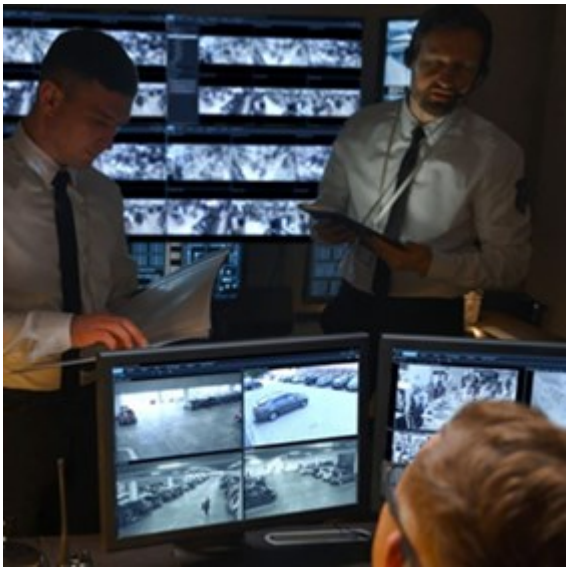
除 XProtect Access 基本许可证之外，您还需要在事件服务器上安装供应商特定的集成插件才能启动集成。

XProtect Incident Manager

Milestone 开发了各种扩展。扩展是通过附加的专门功能来扩展 XProtect 视频管理软件产品功能的产品。您的 XProtect 许可证文件用于控制对扩展的访问。

> 可用的功能取决于正在使用的系统。请参阅Milestone网站 (https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

XProtect Incident Manager 是一个扩展，允许组织记录事件，并将它们与来自 XProtect 视频管理软件的片段证据（视频，也可能是音频）相结合。



XProtectIncidentManager用户可以在事件项目中保存所有事件信息。从事件项目中，他们可以跟踪每个事件的状态和活动。通过这种方式，用户可以有效地管理事件，并轻松地与内部同事和外部机构共享有力的事件证据。

XProtect Incident Manager 帮助组织大致了解他们调查区域内正在发生的事件。这些知识使组织能够采取措施，最大限度地减少将来发生类似事件的可能性。

在XProtectManagementClient中，组织的XProtect视频管理软件管理员可以根据组织的需求，定义XProtect IncidentManager中的可用事件属性。XProtectSmartClient操作员启动、保存和管理事件项目，并向事件项目添加各种信息。这包括自由文本、管理员定义的事件属性以及XProtect视频管理软件中的片段。为实现完全可追溯性，XProtect视频管理软件会记录管理员定义和编辑事件属性的时间，以及操作员创建和更新事件项目的时间。

XProtect LPR(已作说明)

Milestone 开发了各种扩展。扩展是通过附加的专门功能来扩展 XProtect 视频管理软件产品功能的产品。您的 XProtect 许可证文件用于控制对扩展的访问。

可用的功能取决于正在使用的系统。请参阅 Milestone 网站 (https://www.milestonesys.com/products/software/product-index/) 上产品总览页中的完整功能列表。

XProtect LPR 提供基于视频的内容分析 (VCA) 以及与监控系统和 XProtect Smart Client 交互的汽车牌照识别。

借助专业摄像机设置，XProtect LPR 在图像上进行光学字符识别，以读取牌照上的字符。

您可以结合使用 LPR(牌照识别) 和其他监控功能，例如基于录像和事件的激活输出。

XProtect LPR 中的事件示例：

- 触发以特定质量进行的监控系统录制
- 激活警报
- 针对通行/禁行匹配列表进行匹配
- 开启闸门
- 打开灯光
- 将事件的视频推送至安保团队特定人员的计算机屏幕
- 发送手机短信

通过事件，您可以激活 XProtect Smart Client 中的警报。

XProtect Smart Wall(已作说明)

另请参阅XProtect Smart Wall手册。

Milestone 开发了各种扩展。扩展是通过附加的专门功能来扩展 XProtect 视频管理软件产品功能的产品。您的 XProtect 许可证文件用于控制对扩展的访问。

XProtect Smart Wall 是一种高级扩展，使组织可以创建满足其特定安全需求的电视墙。XProtect Smart Wall 提供 XProtect 视频管理软件[1]系统中所有视频数据的概览，并支持任意数量或组合的监视器。

[1]“视频管理软件”的缩写。

XProtect Smart Wall 允许操作员使用一组固定的摄像机和监视器布局查看系统管理员定义的静态电视墙。然而，从操作员可以控制显示内容的层面上说，电视墙也是操作员驱动的。这包括：

- 将摄像机和其他类型的内容推送到电视墙，例如图像、文本、警报和智能地图
- 将整个视图发送到监视器
- 在某些事件的过程中，应用备用预设[1]

最后，显示更改可以通过基于特定事件或时间表自动更改预设的规则进行控制。

XProtect Transact(已作说明)

Milestone 开发了各种扩展。扩展是通过附加的专门功能来扩展 XProtect 视频管理软件产品功能的产品。您的 XProtect 许可证文件用于控制对扩展的访问。

[1]XProtect Smart Client 中一个或多个 Smart Wall 监视器的预定义布局。预设决定了显示哪些摄像机，以及电视墙上每个监视器的内容结构。

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

XProtect Transact 是 Milestone IP 视频监控解决方案的扩展。

XProtect Transact 是用于观察当前交易以及调查过去交易的工具。交易连接到用于监控交易的数字监控视频，以(例如)帮助您证明欺诈或提供针对罪犯的证据。交易行和视频图像之间存在 1 对 1 关系。

交易数据可源自不同类型的交易来源，通常为销售点 (PoS) 系统或自动取款机 (ATM)。

Milestone Open Network Bridge(已作说明)

Milestone 开发了各种扩展。扩展是通过附加的专门功能来扩展 XProtect 视频管理软件产品功能的产品。您的 XProtect 许可证文件用于控制对扩展的访问。

Milestone Open Network Bridge是个开放式 ONVIF 合规界面，用于从 XProtect VMS 系统到其他基于 IP 的安全系统的标准化视频分享。这使得执法部门、监控中心，或类似组织(称为 ONVIF 客户端)能访问从 XProtect VMS 系统到中央监控解决方案的实时和记录视频流。视频流是作为 RTSP 流在互联网上发送的。

关键优势为：

- 实现大型、多厂商安全部署和无缝私有到公共视频集成的真正互操作性和自由选择
- 提供对 XProtect VMS 提供中 H.264 和 H.265 视频流的外部访问，包括实时视频和播放
- 提供标准化界面，能提供一种简单且无问题的方式，将 XProtect VMS 解决方案与警报中心和监控站相集成

本文档提供以下内容：

- 有关 ONVIF 标准的信息以及参考资料链接
- 有关在 XProtect VMS 产品中安装和配置 Milestone Open Network Bridge 的说明
- 关于如何启用各类 ONVIF 客户端以从 XProtect VMS 产品流式传输实时和记录视频的示例

XProtect DLNA Server(已作说明)

Milestone 不再支持此产品。

Milestone 开发了各种扩展。扩展是通过附加的专门功能来扩展 XProtect 视频管理软件产品功能的产品。您的 XProtect 许可证文件用于控制对扩展的访问。

DLNA(数字生活网络联盟)是连接多媒体设备的标准。电子产品制造商让自己的产品获得 DLNA 认证，以实现不同代理商和设备之间的互操作性，从而广范围地散播视频内容。

公共显示屏和电视通常都获得 DLNA 认证，并连接到网络。它们可以扫描网络来寻找媒体内容、连接到设备、请求媒体流进入内置媒体播放器。XProtect DLNA Server 可以被某些 DLNA 认证设备找到，并将直播视频流从选定摄像机传输到附带媒体播放器的 DLNA 认证设备。

DLNA 设备的实时视频延迟为 1-10 秒。这是由设备中缓冲区大小不一引起的。

XProtect DLNA Server 必须连接到与 XProtect 系统相同的网络，并且 DLNA 设备必须连接到与 XProtect DLNA Server 相同的网络。

设备

硬件(已解释)

硬件包括以下两种：

- 直接通过 IP 连接到监控系统记录服务器的物理单元，例如摄像机、视频编码器和 I/O 模块
- Milestone Interconnect 设置中位于远程站点上的记录服务器

有多个选项可用于为系统中的每台记录服务器添加硬件。

如果硬件位于已启用 NAT 的路由器或防火墙之后，您可能需要指定不同的端口号并配置路由器/防火墙，使其映射硬件使用的端口和 IP 地址。

添加硬件向导可帮助您检测网络上的硬件(例如摄像机和视频编码器)，并将它们添加至本系统上的记录服务器。该向导还可帮助您为 Milestone Interconnect 设置添加远程记录服务器。**一次仅为**一台记录服务器添加硬件。

硬件预配置(已解释)

某些制造商要求在首次将硬件添加到视频管理软件系统之前，必须在现成的硬件上设置凭据。这称为硬件预配置，是通过**预配置硬件设备**向导完成的，该向导在 第 185 页上的添加硬件 向导检测到此类硬件时出现。

以下是有关**预配置硬件设备**向导的一些重要信息：

- 在添加到视频管理软件系统之前需要初始凭据的硬件无法使用典型的默认凭据添加，而必须通过向导或直接连接到硬件进行配置
- 您只能将凭据(用户名或密码)应用到标记为**未设置**的字段
- 将硬件**状态**设置为**已配置**后，您将无法更改凭据(用户名或密码)
- 预配置适用于现成的硬件，只需执行一次。预配置后，在以下系统中就可以像管理任何其他硬件一样管理该硬件：Management Client
- 关闭**预配置硬件设备**向导后，预配置的硬件将显示在 第 185 页上的添加硬件 向导中，现在可以将其添加到系统中。

强烈建议您在关闭**预配置硬件设备**向导后，通过完成 第 185 页上的添加硬件 向导，将预配置的硬件添加到系统中。如果不将硬件添加到系统中，Management Client 将不会保留预配置的凭据。

设备(已解释)

硬件具有您可以单独管理的多个设备，例如：

- 物理摄像机具有代表摄像机部件(镜头)以及麦克风、扬声器、元数据、输入和输出(连接或内置)的设备
- 视频编码器具有连接的多个模拟摄像机，它们显示在一个设备列表中，这些设备代表摄像机部件(镜头)以及麦克风、扬声器、元数据、输入和输出(连接或内置)
- I/O 模块具有代表(例如)灯光的输入和输出通道的设备
- 专用音频模块具有代表麦克风和扬声器输入和输出的设备
- 在Milestone Interconnect设置中，远程系统以硬件显示，来自远程系统的所有设备均在一个列表中列出

在您添加硬件时，系统会自动添加硬件的设备。

有关受支持硬件的信息，请参阅 Milestone 网站(https://www.milestonesys.com/support/tools-and-references/supported-devices/)上关于受支持硬件的页面。

以下部分介绍了可以添加的每种设备类型。

摄像机

摄像机设备会将视频流提供给系统，客户端用户可以使用该视频流查看实时视频，或者系统可以记录该视频流以供客户端用户在以后播放。角色决定用户查看视频的权限。

麦克风

在许多设备上，可以连接外部麦克风。部分设备拥有内置麦克风。

麦克风设备会将音频流提供给系统，客户端用户可以使用该音频流实时监听，或者系统可以记录该音频流以供客户端用户在以后播放。可以将系统设置为接收触发相关动作的麦克风特定事件。

角色决定用户监听麦克风的权限。无法从 Management Client 监听麦克风。

扬声器

在许多设备上，可以连接外部扬声器。部分设备拥有内置扬声器。

用户在 XProtect Smart Client 中按讲话按钮时，系统会将音频流发送至扬声器。您也可以从 和 XProtect Web Client XProtect® Mobile中使用该功能。仅在用户讲话时才会记录扬声器音频。角色决定用户通过扬声器讲话的权限。无法从通过 Management Client 扬声器讲话。

如果两个用户同时想讲话，则角色确定用户通过扬声器讲话的权限。作为角色定义的一部分，您可以指定扬声器的优先级，范围为从非常高到非常低。如果两个用户同时想讲话，则角色优先级最高的用户将获得讲话的权限。如果具有相同角色的两个用户同时希望讲话，则适用先到先得的原则。

元数据

元数据设备会将数据流提供给系统，客户端用户可以使用该数据流查看关于数据的信息，如描述视频图像的数据、图像中的内容或对象，或记录图像的位置。元数据可以连接到摄像机、麦克风或扬声器。

元数据可以由以下对象生成：

- 提供数据的设备自身，如提供视频的摄像机
- 第三方系统或通过常规元数据驱动程序进行的集成

设备生成的元数据会自动链接至相同硬件上的一个或多个设备。

角色决定用户查看元数据的权限。

输入

在许多设备上，可将外部设备连接到设备的输入端口。输入设备通常为外部传感器。例如，可以将此类外部传感器用于侦测门、窗户或门禁等是否打开。此类外部输入设备的输入会被本系统视为事件。

可在规则中使用此类事件。例如，可以创建规则，使其指定当激活输入时摄像机开始记录，并在取消激活输入 30 秒后停止记录。

输出

在许多设备上，可将外部设备连接到设备的输出端口。这允许通过本系统激活/取消激活灯光、警笛等。

在创建规则时可以使用输出。您可以创建自动激活或取消激活输出的规则，并创建在输出状态更改时触发动作的规则。

设备组(已解释)

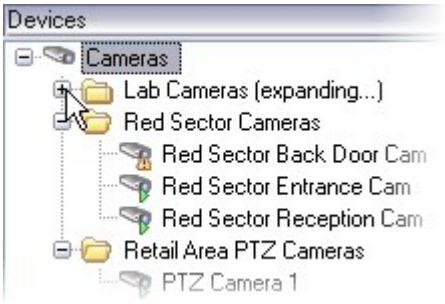
添加硬件向导将指导如何将设备分组到设备组，但始终可根据需要修改组及添加更多组。

将系统上不同类型的设备(摄像机、麦克风、扬声器、元数据、输入和输出)分组的优点包括：

- 设备组有助于维护对系统上设备的直观总览
- 设备可存在于数个组中
- 您可创建子组以及子组中的子组
- 您可为设备组内的所有设备一次性指定共同属性

- 通过设备组设置的设备属性并不针对设备组保存，而是保存在各台设备上
- 处理角色时，您可为设备组内的所有设备一次性指定共同安全设置
- 处理规则时，您可为设备组内的所有设备一次性应用规则

可根据需要添加任意数量的设备组，但不得在同一设备组内混合不同类型的设备(如摄像机和扬声器)。



创建数量**少于** 400 台设备的设备组，以便查看和编辑所有属性。

如果删除设备组，则仅删除设备组本身。如果要从系统中删除某台设备(如摄像机)，请在记录服务器级别上执行该操作。

以下示例基于将摄像机分组到设备组中的情况，但该原则同样适用于所有设备

添加设备组

指定设备组中要包含的设备

为设备组中的所有设备指定共同属性

媒体存储

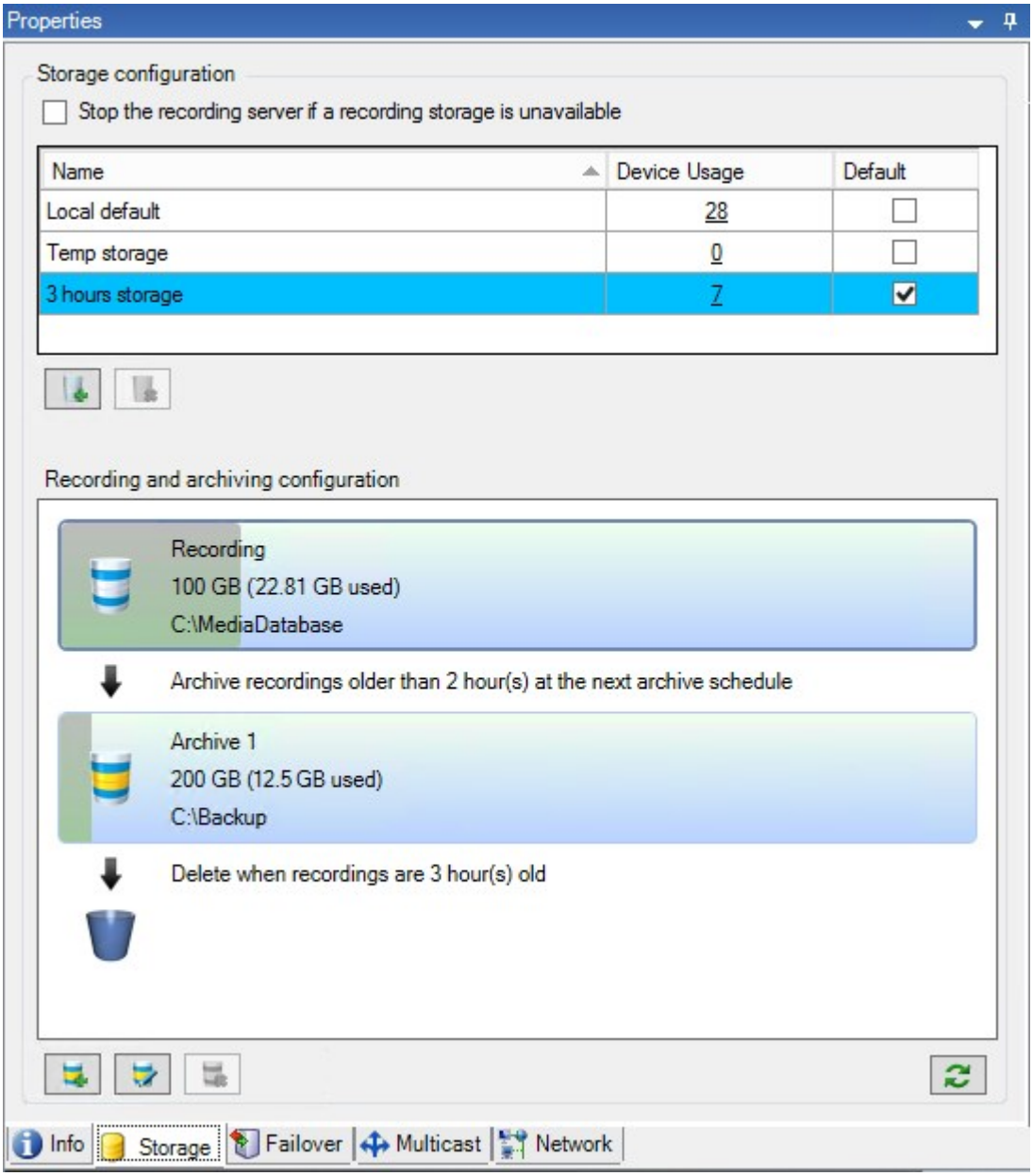
存储和存档(已解释)

可用的功能取决于正在使用的系统。请参阅 Milestone 网站 (https://www.milestonesys.com/products/software/product-index/) 上产品总览页中的完整功能列表。

在**存储**选项卡上，您可以设置、管理和查看所选记录服务器的存储。

对于记录存储和存档，横条显示当前的可用空间量。如果记录存储不可用，您可以指定记录服务器的行为。如果您的系统包含故障转移服务器，这最为常用。

如果您正在使用**证据锁定**，则会显示一条垂直的红线，指明证据锁定脚本使用的空间。



当摄像机记录视频或音频时，所有指定记录均默认存储在为设备定义的存储中。每个存储都包含一个记录存储，用于将记录内容保存到记录数据库**记录**中。存储没有默认的存档，但是您可以自行创建。存储没有默认的存档，但是您可以自行创建。

为避免录像数据库满负荷运行，您可创建更多存储(请参阅 第 171 页上的添加新存储)。您还可在每个存储中创建存档(请参阅 第 172 页上的在存储中创建存档)，并启动存档流程以存储数据。

> 归档过程将记录自动从照摄像机的记录数据库等位置传输到另一个位置。这样，可存储的记录量将不受记录数据库容量的限制。通过使用存档，还可将记录备份至其他介质。

您可以在每个记录服务器上配置存储和存档。

将已存档的记录存储在本地或可访问的网络驱动器上后，即可使用 XProtect Smart Client 查看它们。

如果硬盘驱动器发生故障，记录存储不可用，则横条会变成红色。仍然可以在 XProtect Smart Client 中查看实况视频，但是在硬盘驱动器恢复之前，记录和存档都会停止。如果系统配置了故障转移记录服务器，您可以指定记录服务器停止运行，以便使故障转移服务器接管(请参阅 第 170 页上的指定录制存储不可用时的行为)。

以下内容主要提及摄像机和视频，但对于扬声器、麦克风以及音频和声音同样适用。

Milestone 建议，记录存储和存档使用专用硬盘驱动器，以防止硬盘性能降低。当格式化硬盘时，将其**分配单位大小**设置从 4 更改为 64 千字节很主要。这将显著提高硬盘的记录性能。您可以在 Microsoft 网站 (https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95) 上阅读有关如何分配单元大小的详细信息和帮助信息。

如果空闲空间小于 5GB，总是会将数据库中最旧的数据自动存档(或在未定义下一个存档时删除)。如果空闲的空间不到 1GB，则会将数据删除。数据库始终需要 250MB 的空闲空间。如果由于未能足够快地删除数据而达到此限制，则尝试写入数据库可能会失败，在这种情况下，在释放足够的空间之前，不会将更多数据写入数据库。数据库的实际最大大小为您指定的吉字节数减去 5GB。

对于符合 FIPS 140-2 的系统，如果使用不符合 FIPS 的密码对 2017 R1 之前版本的 XProtect VMS 导出和存档媒体数据库进行了加密，则需要将数据存档在启用 FIPS 之后仍可访问的位置。有关如何配置 XProtect VMS 以在符合 FIPS 140-2 的模式下运行的详细信息，请参阅强化指南中的FIPS 140-2 合规部分。

将设备连接到存储

为记录服务器配置存储和存档设置后，您可以为单个摄像机或一组摄像机启用存储和存档。您要从单个设备或从设备组完成该操作。请参阅 第 172 页上的将设备或一组设备连接到存储。

有效存档

当为一台摄像机或一组摄像机启用存档时，记录存储的内容会以您定义的间隔自动移动到第一个存档。

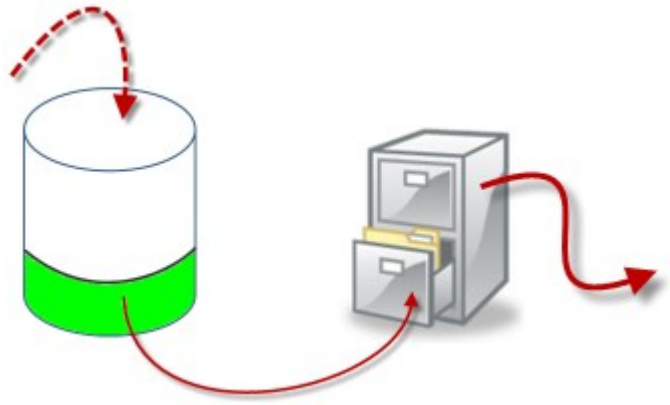
根据您的要求，您可以为您的各存储配置一个或更多存档。存档位于记录服务器计算机自身或本系统可访问的其他位置，如网络驱动器。

通过有效设置存档，可以优化存储需求。通常，特别是长期而言，希望存档记录占用的空间越小越好，即使可能稍微降低图像的质量。您通过调整数个彼此依赖的设置，从记录服务器的**存储**选项卡执行有效的存档操作：

- 记录存储保留
- 记录存储大小
- 存档保留

- 存档大小
- 存档时间表
- 加密
- 每秒帧数 (FPS)。

大小字段分别定义了记录存储的大小(如圆柱状所示)及其存档的大小:



通过记录存储的保留时间和大小设置(如圆柱体白色区域所示),您可以定义记录必须经过多长时间才进行存档。在我们的示例中,您将在记录已经过足够时间时存档记录。

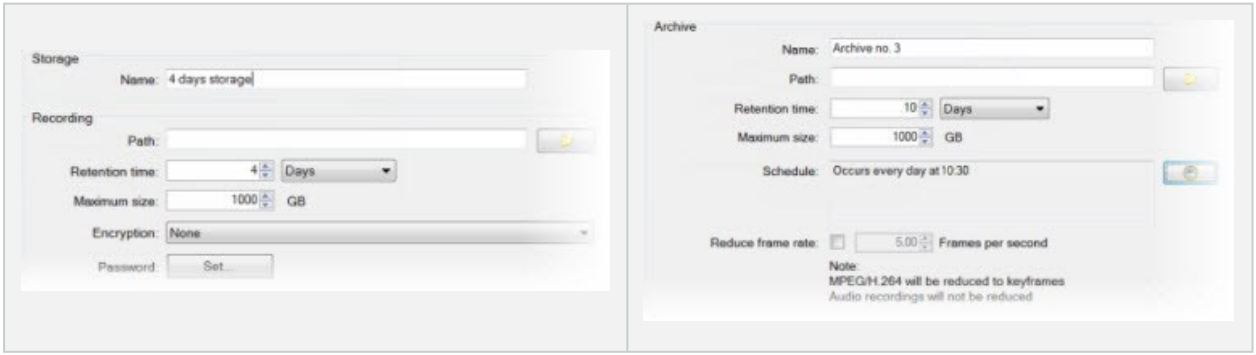
存档的保留时间和大小设置定义记录在存档中保留多长时间。记录在存档中保留指定的时间,或直到存档达到指定的大小限制。当达到这些设置时,系统开始改写存档中的旧记录。

存档时间表定义存档的频率和进行的时间。

FPS 确定数据库中数据的大小。

要存档记录,所有这些参数的设置必须相互一致。这意味着下一存档的保留期限必须始终长于当前存档或记录数据库的保留期限。这是因为声明的存档保留天数包含之前在该过程中声明的所有保留。存档的频率必须始终高于保留期限,否则可能丢失数据。如果保留时间为 24 小时,任何超过 24 小时的数据将被删除。因此,为了让您的数据安全地移动到下一存档,存档周期必须小于 24 小时。

示例:这些存储(左侧图像)的保留时间为 4 天,而后续存档(右侧图像)的保留时间为 10 天。存档设置为每天 10:30 进行,可以确保存档频率远高于保留时间。



您也可以通过使用规则和事件控制存档。

存档结构(已解释)

当存档录制时,它们存储在存档内的特定子目录结构中。

> 在您系统的所有常规使用中,当系统用户使用 XProtect Smart Client 浏览所有录像时,无论这些录像是否存档,子目录结构将对系统用户完全透明。如果您希望备份您存档的录制,则了解子目录结构将非常有帮助。

在记录服务器的各存档目录中,系统会自动创建单独子目录。这些子目录按设备和存档数据库的名称命名。

由于在相同存档中可存储来自不同摄像机的录制,并且由于可能定期执行各摄像机的存档,所以还会进一步地自动添加子目录。

这些子目录各自大约代表 1 小时的录制。如果按一小时进行拆分,使可以在达到允许的最大存档大小时,仅删除相对较小部分的存档数据。

子目录的名称是在设备后加上表明录制来源(边缘摄像机或通过 SMTP)的信息,**再加上**包含在子目录中的最近数据库录制的日期和时间。

命名结构

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most
recent recording]\
```

如果来自边缘存储:

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of
most recent recording]\
```

如果来自 SMTP:

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of
most recent recording]\
```

实际示例

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

子目录

会进一步自动添加子目录。这些子目录的数量和性质取决于实际录制的性质。例如,如果录制从技术层面上划分为片段,则将添加多个不同的子目录。已将移动侦测用于触发录制时的情况常常如此。

- **Media**：该文件夹包含实际媒体，该媒体是视频或音频（其中一种）
- **MotionLevel**：该文件夹包含使用我们的移动侦测算法从视频数据生成的移动级别栅格。该数据允许 XProtect Smart Client 中的智能搜索功能执行非常快速的搜索
- **Motion**：系统将移动片段存储在该文件夹中。移动片段是一个时间段，在该段时间内在视频数据中检测到了移动。例如，XProtect Smart Client 中的时间轴使用了该信息
- **录制**：系统将录制片段存储在该文件夹中。录制片段是一个时间段，在该段时间内在视频数据中存在连贯录制。例如，该信息用于绘制 XProtect Smart Client 中的时间轴
- **Signature**：该文件夹用于保留为媒体数据（在 Media 文件夹中）生成的签名。利用该信息，您可以确认媒体数据自录制以来未遭篡改

如果希望备份存档，了解子目录结构的基本知识可以使您有目标地进行备份。

备份示例

要备份整个存档的内容，则备份所需的存档目录及其所有内容。例如，备份以下路径下的所有内容：

```
...F:\OurArchive\
```

要备份特定摄像机从特定时段开始的录制，则仅备份相关子目录的内容。例如，备份以下路径下的所有内容：

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

记录的预缓冲和存储（已作说明）

预缓冲用于在实际触发事件发生前记录音频和视频。如果您想要针对会触发记录的事件（如开门）进行音频或视频记录，预缓冲非常有用。

这种预缓冲之所以可行，是因为系统会不间断接收来自已连接设备的视频和音频数据流，并在定义预缓冲期间暂时存储它们。

- 如果记录规则被触发，临时记录将在规则配置好的预记录时间里被永久化
- 如果未触发记录规则，预缓冲的临时记录将在定义预缓冲时间之后被自动删除

临时预缓冲记录的存储

您可以选择临时预缓冲记录的存储位置：

- 在内存中；将预缓冲期间限制为 15 秒。
- 在磁盘上（在介质数据库中）；您可以选择所有值。

存储到内存（而非磁盘）可提高系统性能，但仅适用于较短的预缓冲期间。

当将记录存储在内存中并永久存储一部分临时记录时，会删除剩余的临时记录，且无法恢复。如果您需要能够保留剩余的记录，请将记录存储在磁盘上。

身份验证

Active Directory(已作说明)

Active Directory 是 Microsoft 为 Windows 域网络发布的目录服务。它包含在大多数 Windows Server 操作系统中。它能够识别网络中的资源以便用户或应用程序访问它们。

在安装 Active Directory 后，您可以从 Active Directory 中添加 Windows 用户，但也可以选择在不使用 Active Directory 的情况下添加基本用户。存在与基本用户相关的特定系统限制。

用户(已解释)

术语**用户**主要是指通过客户端连接至监控系统的用户。可通过两种方式配置这些用户：

- 配置为**基本用户**，通过用户名/密码组合来进行身份验证。
- **配置为** Windows 用户，根据 Windows 登录进行身份验证

Windows 用户

通过使用 Active Directory 添加 Windows 用户。Active Directory (AD) 是 Microsoft 为 Windows 域网络实施的目录服务。它包含在大多数 Windows Server 操作系统中。它能够识别网络中的资源以便用户或应用程序访问它们。Active Directory 使用用户和用户组概念。

用户为代表具有用户帐户的个体的 Active Directory 对象。示例：

组是包含若干用户的 Active Directory 对象。在此例中，“管理组”包含三个用户：

组可包含任意数量的用户。通过将组添加到系统，一次即可添加其所有成员。一旦将组添加到系统，随后在 Active Directory 中对组进行的任何更改(例如添加新成员或删除旧成员) 会立即反映在系统中。一个用户可同时为一个以上组的成员。

可以使用 Active Directory 将现有用户和组信息添加到系统，从而获得一些好处：

- 用户和组在 Active Directory 中集中指定，因此您不需要从头开始创建用户帐户
- 您也不需要在系统上配置用户的任何身份验证，因为 Active Directory 会处理身份验证

必须首先为网络上的服务器安装 Active Directory，然后才能通过 Active Directory 服务添加用户和组。

基本用户

如果您的系统无权访问 Active Directory，请创建一个基本用户。有关如何设置基本用户的信息，请参阅 第 250 页上的创建基本用户。

Identity Provider(已作说明)

Identity Provider app pool (IDP) 是为基本用户创建、维护和管理身份信息的系统实体。

Identity Provider 还为依赖的应用程序或服务提供身份验证和注册服务，在这种情况下：记录服务器、管理服务器、Data Collector 和报告服务器。

当您以基本用户身份登录 XProtect 客户端和服务时，您的请求将转到 Identity Provider。通过身份验证后，用户可以调用管理服务器。

Identity Provider 作为管理服务器的一部分在 IIS 中运行，使用相同的 SQL Server 和单独的数据库，并负责创建和处理服务在通信时使用的 OAuth 通信令牌 (Surveillance_IDP)。

Identity Provider 日志可在以下位置找到：`\\ProgramData\Milestone\IDP\Logs`.

外部 IDP(已解释)

IDP是 Identity Provider 的首字母缩略词。外部 IDP 是一种外部应用程序和服务，您可以在其中存储和管理用户身份信息，并向其他系统提供用户身份验证服务。您可以将外部 IDP 与 XProtect 视频管理软件相关联。

XProtect VMS 支持与 OpenID Connect (OIDC) 兼容的外部 IDP。

索赔(已作说明)

声明形成了外部 IDP 和 XProtect 视频管理软件之间的链接。

索赔是用户或应用程序等实体做出的关于自身的声明。在 XProtect VMS 中，索赔可以与决定用户的 XProtect 权限的角色相关联。

索赔是包含索赔名称和索赔值的关键值。例如，索赔名称可以是描述索赔值内容的标准名称，而索赔值可以是组的名称。请参阅外部 IDP 声明的更多示例：来自外部 IDP 的索赔示例。

允许用户从外部 IDP 登录到 XProtect 视频管理软件

- 从外部 IDP 创建用户。您还必须识别 XProtect 视频管理软件以及 XProtect 与外部 IDP 之间的交互。最后，创建声明以将用户标识为 XProtect 视频管理软件中的外部 IDP 用户。
- 在 XProtect 视频管理软件中，创建一个配置，使 Identity Provider 能够连接外部 IDP。有关如何为外部 IDP

创建配置的更多信息，请参阅添加和配置外部 IDP 。

- 从 XProtect VMS 中，通过映射来自外部 IDP 的用户索赔至XProtect角色，以建立用户身份验证。有关如何映射索赔到角色的详细信息，请参阅映射来自外部 IDP 的索赔到 XProtect 中的角色。

重定向 URI

重定向 URI 会指定用户在身份验证成功后进入的页面。在外部 IDP 中，您必须添加管理服务器的地址，后接您在 XProtect Management Client 中定义的**回调路径**。例如 https://management-server-computer.company.com/idp/signin-oidc

外部 IDP 用户的唯一用户名

对于通过外部 IDP 登录 Milestone XProtect 的用户，会自动创建用户名。

外部 IDP 提供了一组声明来为 XProtect 中的用户自动创建名称，在 XProtect 中使用了一种算法，可以从外部 IDP 中选择一个在视频管理软件数据库中唯一的名称。

来自外部 IDP 的声明示例

索赔包含索赔名称和索赔值。例如：

声明名称	声明值
名称	Raz Van
电子邮件	123@domain.com
amr	pwd
idp	00o2ghkgazGgi9BIE5d7
preferred_username	321@domain.com
vmsRole	操作员
locale	en-US
given_name	Raz
family_name	Lindberg
zoneinfo	America/Los_Angeles
email_verified	真

使用索赔的序号来在 中创建用户名XProtect

在 XProtect 中，在 XProtect VMS 中创建用户时的搜索优先级是由下表中的索赔序号控制的。第一个可用索赔名称将在 XProtect VMS 中使用：

声明名称	序号	说明
UserNameClaimType	1	已配置与一个索赔的映射，以定义用户名。声明在**外部 IDP** 选项卡的**工具 > 选项**下的**用于创建用户名的声明**字段中定义。
preferred_username	2	可能来自外部 IDP 的声明。通常用于 Oidc(OpenID 连接) 中此种情况的标准声明。
名称	3	
given_name family_ name	4	名和姓氏组合，比如 Bob Johnson。
电子邮件	5	
第一个可用索赔 + # (第一个可用编号)	6	例如，Bob#1

定义特定索赔以创建用户名于XProtect

XProtect管理员可以定义来自外部IDP的特定声明，该声明用于在XProtect视频管理软件中创建用户名。当管理员定义用于在XProtect视频管理软件中创建用户名的声明时，声明名称必须与来自外部IDP的声明名称完全相同。

- 用于用户名的声明可在**外部 IDP** 选项卡的**工具 > 选项**下的**用于创建用户名的声明**字段中定义。

删除外部 IDP 用户

XProtect 中通过外部 IDP 登录创建的用户的删除方式与基本用户相同，用户创建后可随时删除。

XProtect 中的用户被删除后，如果用户从外部 IDP 再次登录，则会在 XProtect 中创建一个新用户。然而，与 XProtect 中用户相关的数据，如私有视图和角色会丢失，必须在 XProtect 中为用户再次创建这些信息。

如果在 Management Client 中删除了外部 IDP，则通过外部 IDP 连接到视频管理软件的所有用户也会被删除。

安全

角色和角色权限(已作说明)

Milestone XProtect VMS 中的所有用户都属于某个角色。

角色会定义用户的权限(包括用户可以访问的设备)。角色还会定义视频管理系统中的安全与访问权限。

系统随附默认的**管理员**角色,它具有所有系统功能的完全访问权限,但在大多数情况下,您需要在系统中使用多个角色,以区分用户以及用户应该拥有的访问权限。您可以根据需要添加许多角色。请参阅 第 249 页上的将用户和组分配至角色/从角色删除。

例如,您可能需要根据希望 XProtect Smart Client 用户能访问的设备而为这些用户设置不同类型的角色,或者需要设置要求对用户进行区分的类似类型的限制。

若要对用户进行区分,您必须:

- 创建并设置您需要的角色,以满足您组织的业务需求
- 添加用户和用户组,并为其分配应该属于的角色
- 创建 Smart Client 配置文件和 Management Client 配置文件,以定义用户在 XProtect Smart Client 和 Management Client 用户界面中可以查看的内容。

  角色控制的只是访问权限,而不是用户在 XProtect Smart Client 或 Management Client 的用户界面中可以查看的内容。您不需要为永远不会使用 Management Client 的用户创建特定的 Management Client 配置文件。

为了使 Management Client 功能的访问权限受限的 XProtect Smart Client 用户或 Management Client 用户获得可能最好的用户体验,您应该确保角色提供的权限与 Smart Client 或 Management Client 配置文件提供的用户界面元素之间具有一致性。

> ⚠ 若要拥有对 Management Server 的访问权限,重要的一点在于所有角色都启用**连接**安全权限。该权限位于**角色设置** > **Management Server** > 第 433 页上的"整体安全"选项卡(角色)。

要在系统中设置角色,请展开安全角色。

角色权限

可用的功能取决于正在使用的系统。请参阅 Milestone 网站 (https://www.milestonesys.com/products/software/product-index/) 上产品总览页中的完整功能列表。

在系统中创建角色时,可针对相关角色能访问和使用的系统组件或功能为角色分配一些权限。

例如,您可能需要创建的角色仅具有对 XProtect Smart Client 或其他 Milestone 查看客户端中的功能进行访问的权限,仅对特定摄像机具有查看权限。如果创建此类角色,这些角色不应具有访问和使用 Management Client 的权限,而是仅具有 XProtect Smart Client 或其他客户端中的部分或所有功能的访问权限。

若要满足这项区分需求,您可以设置具有一些或大多数典型管理员权限(例如,添加和移除摄像机、服务器及类似功能的权限)的角色。可以创建具有一些或大部分系统管理员权限的角色。例如,如果贵组织需要在能够管理系统子集的人员以及可以管理整个系统的人员之间进行分离,则会涉及这一点。

通过角色，您可以提供对各种系统功能进行访问、编辑或更改的不同的管理员权限。例如，对系统中服务器或摄像机的设置进行编辑的权限。可在**整体安全**选项卡上指定这些权限(请参阅 第 433 页上的"整体安全"选项卡(角色))。若要使不同的系统管理员能启动 Management Client，您必须为该角色授予管理服务器上的读取权限。

> 若要拥有对 Management Server 的访问权限，重要的一点在于所有角色都启用**连接**安全权限。该权限位于**角色设置** > **Management Server** > 第 433 页上的"整体安全"选项卡(角色)。

还可以将角色与从用户界面删除了相应系统功能的 ManagementClient 配置文件关联，从而为每个角色在 ManagementClient 用户界面中应用相同限制。请参阅第 64 页上的 ManagementClient 配置文件(已作说明)了解信息。

要为角色赋予此类区别性管理员权限，具有默认完整管理员角色的人员必须在**安全** > **角色** > **信息选项卡** > **新增**下建立角色。建立新角色时，随后可使用与在系统中建立其他任何角色的相似方式将角色与自己的配置文件关联，或使用系统的默认配置文件。有关详细信息，请参阅 第 248 页上的添加和管理角色。

在指定要与角色关联的配置文件后，请转至**整体安全**选项卡指定角色的权限。

> 对于不同产品，可以为角色设置的权限存在差异。只能在 XProtect Corporate 中为角色赋予所有可用权限。

隐私屏蔽(已作说明)

隐私屏蔽(已作说明)

通过隐私屏蔽，您可以定义摄像机视频在客户端中显示时，使用隐私屏蔽遮盖哪些区域。例如，如果监控摄像机拍摄街道，您可以使用隐私屏蔽来屏蔽建筑物的特定区域(如门和窗)以保护居民的隐私。在某些国家，这是法律要求。

您可以将隐私屏蔽指定为实体或模糊。这些屏蔽可以遮盖实时、记录和导出的视频。

隐私屏蔽应用并锁定到摄像机图像的一个区域，因此被遮盖的区域不会跟随全景/倾斜/变焦移动，而是始终遮盖摄像机图像的同一区域。在某些 PTZ 摄像机上，您可以在摄像机上启用基于位置的隐私屏蔽功能。

有两种类型的隐私屏蔽：

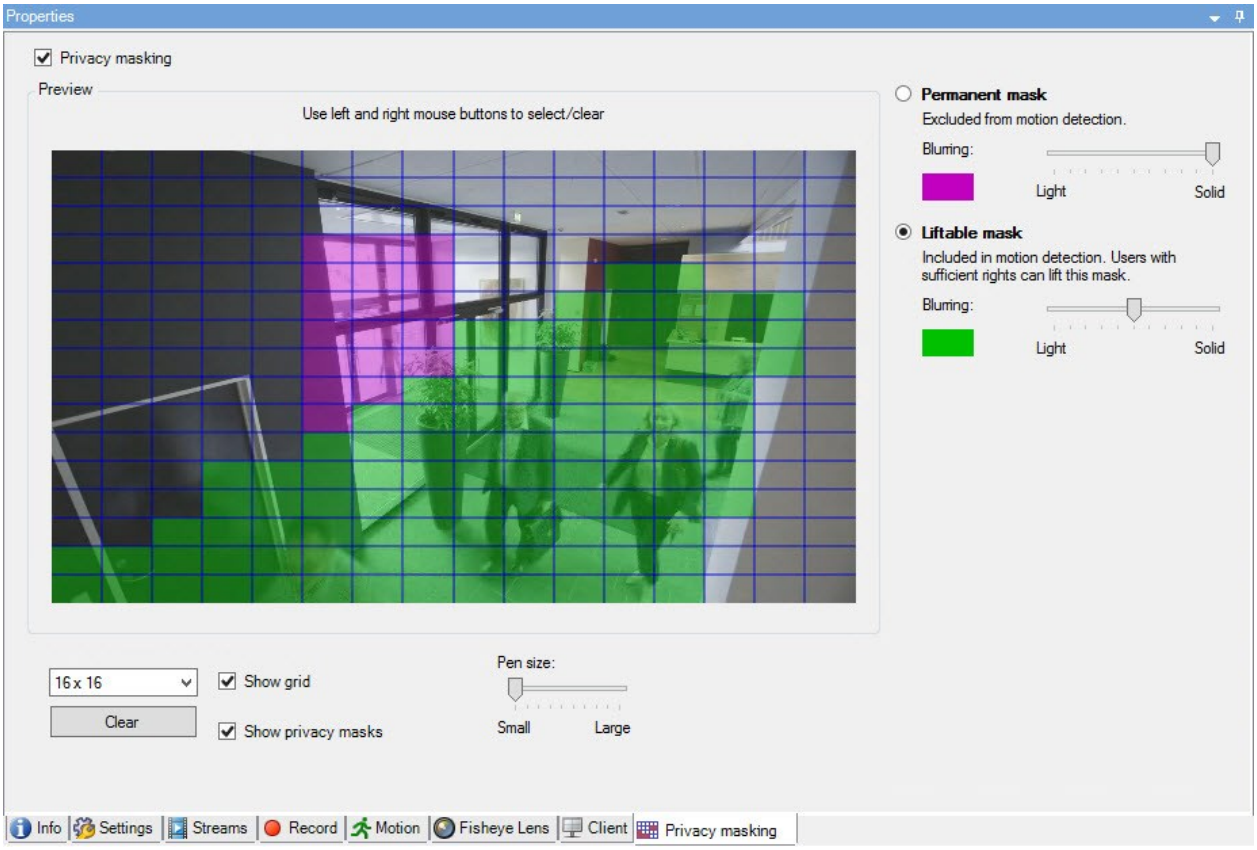
- **永久隐私屏蔽**：有这种屏蔽的区域在客户端中始终被遮盖。可用于遮盖从不需要监视的视频区域，如公共区域或不允许监视的区域。永久隐私屏蔽是排除在移动侦测之外的区域
- **可解除隐私屏蔽**：有这种屏蔽的区域可以在 XProtect Smart Client 中临时由具有解除隐私屏蔽权限的用户解除遮盖。如果已登录的 XProtect Smart Client 用户没有解除隐私屏蔽的权限，系统会要求有权授权的用户同意该解除。
  隐私屏蔽将被解除，直到超时或用户重新应用这些屏蔽。请注意，用户有权访问的所有摄像机的视频都将解除隐私屏蔽

> 如果升级 2017 R3 系统或应用了隐私屏蔽的较旧版本，则屏蔽将转换为可解除屏蔽。

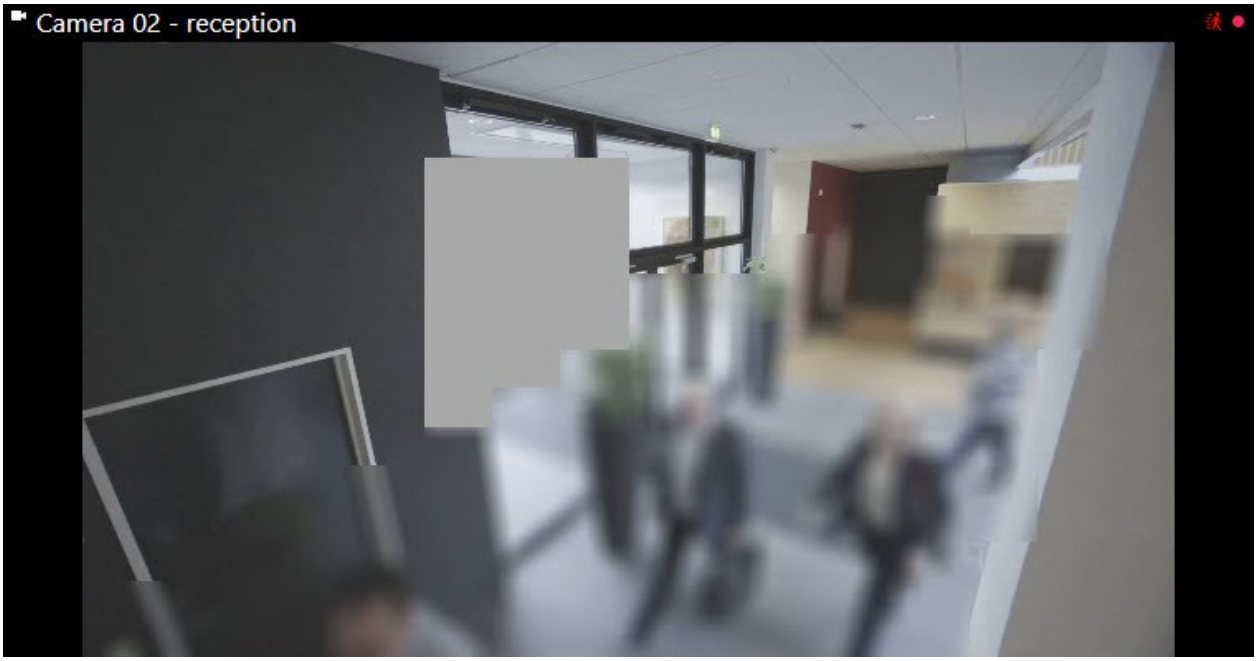
当用户从客户端导出或播放记录的视频时，即使您后来更改或删除了隐私屏蔽，视频也会包含记录时配置的隐私屏蔽。如果在导出时解除隐私保护，则导出的视频**不**包含可解除隐私屏蔽。

> 如果您经常更改隐私屏蔽设置，例如每周一次，系统可能会过载。

已配置隐私屏蔽的**隐私屏蔽**选项卡示例：



这就是它们在客户端中的样子：



您可以通知客户端用户关于永久和可解除隐私屏蔽的设置。

Management Client 配置文件(已作说明)

Management Client 配置文件允许系统管理员修改其他用户的 Management Client 用户界面。将 Management Client 配置文件与角色关联，可将用户界面限制为代表对于每个管理员角色可用的功能。

Management Client 配置文件仅处理系统功能的视觉展示，而不实际访问它。通过与单个用户相关联的角色来授予对系统功能的总体访问权限。有关如何管理某个角色对系统功能的整体访问的信息，请参阅管理 Management Client 配置文件功能的可视性。

可以更改所有 Management Client 元素的可见性设置。默认情况下，Management Client 配置文件可查看 Management Client 中的所有功能。

Smart Client 配置文件(已作说明)

可用的功能取决于正在使用的系统。请参阅Milestone网站 (https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

Milestone XProtect VMS 中的所有用户都属于 Smart Client 配置文件与该用户关联的角色。

角色会定义用户的权限，Smart Client 配置文件会定义用户在 XProtect Smart Client 用户界面中可以查看的内容。

所有 Milestone XProtect VMS 安装都包括默认 Smart Client 配置文件，已将该配置文件设置为使用默认配置，以显示您组织的系统中可用的大部分配置。默认情况下，会始终禁用某些设置。

若组织中存在多个不同角色，您可能需要在 XProtect Smart Client 中禁用特定角色不会/不应访问的功能。

例如，您的某个角色的日常工作可能不需要播放任何视频。为此，您可为该角色创建新的 Smart Client 配置文件，并在其中禁用**播放**模式。在 Smart Client 配置文件中禁用此设置后，若 XProtect Smart Client 用户的角色会使用该 Smart Client 配置文件，则无法在 XProtect Smart Client 用户界面中再查看**播放**模式。

请务必注意，Smart Client 配置文件主要控制的是用户在 XProtect Smart Client 用户界面中可以查看的内容，而不是角色的实际访问权限。这些访问权限(例如，进行读取、修改或删除的访问权限)由角色设置来控制。因此，对于因 Smart Client 配置文件中禁用而无法在用户界面中查看的功能，XProtect Smart Client 用户可以通过其角色而拥有这些功能的权限。

为了使 XProtect Smart Client 用户获得可能最好的用户体验，您应该确保角色提供的权限与 Smart Client 配置文件提供的用户界面元素之间具有一致性。

若要创建或编辑 Smart Client 配置文件，请展开**客户端**，然后选择 **Smart Client 配置文件**。

您也可以了解有关 Smart Client 配置文件、角色和时间配置文件之间的关系以及如何一起使用它们(请参阅 第 227 页上的创建并设置 Smart Client 配置文件、角色和时间配置文件)。

证据锁定(已解释)

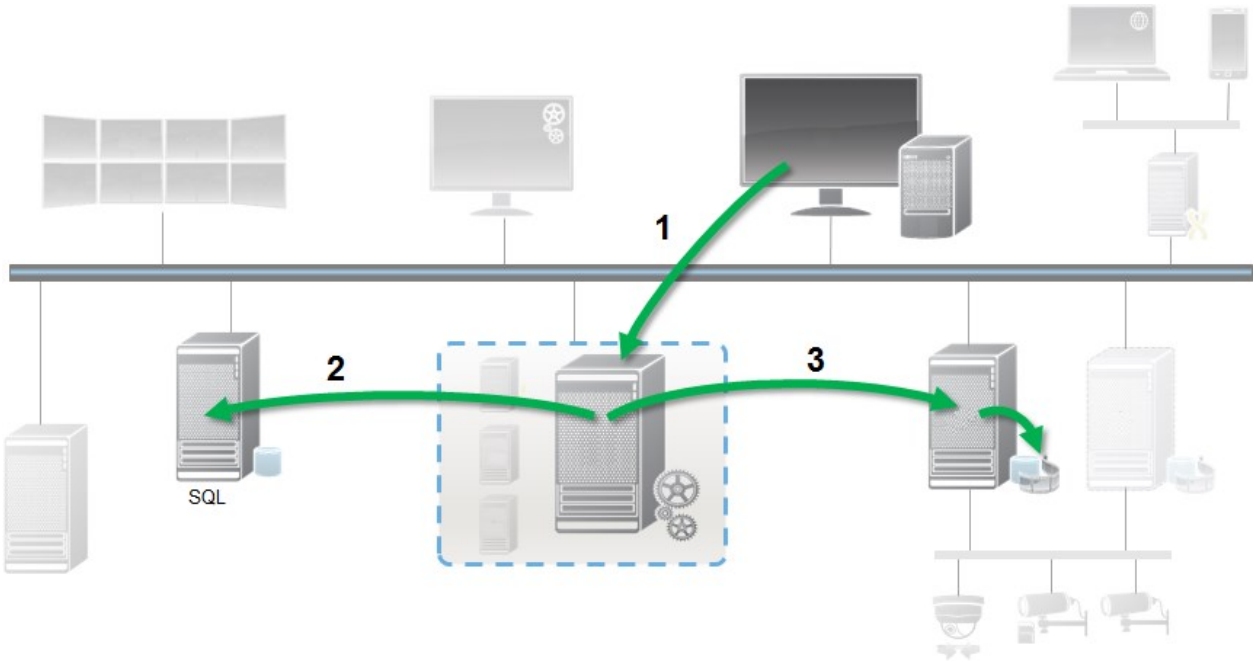
可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

从 XProtect VMS 版本 2020 R2 开始，当您从较早版本升级管理服务器时，将无法在版本 2020 R1 或更早的录制服务器上创建或修改证据锁定，必须先升级录制服务器。
这也意味着，如果硬件已从一个记录服务器(从 2020 R1 或更早版本)移到另一个记录服务器，并且上面仍然有记录，则不能创建或修改证据锁定。

使用证据锁定功能，客户端操作员可以在需要时(例如，进行调查或试用)保护视频片断(包括音频和其他数据)免遭删除。有关详细信息，请参阅 XProtect Smart Client 的用户手册。

数据受到保护后，系统默认保留时间后或其他情况下系统均不会自动删除数据，客户端用户也无法手动删除数据。只有在拥有足够用户权限的用户为证据解锁之后，系统或用户才能删除数据。

证据锁定流程图：



1. XProtect Smart Client 用户创建证据锁定。将信息发送到管理服务器。
2. Management Server 在 SQL Server 数据库中存储有关证据锁定的信息。
3. 管理服务器通知记录服务器在数据库中存储并保护受保护的记录。

当操作员创建证据锁定时，受保护的数据保存在其记录到的记录存储中，并与非受保护数据一起移动到存档磁盘，但是受保护数据将：

- 遵循为证据锁定配置的保留时间。可能保留无限长的时间
- 保持录像的原始质量，即使已为非受保护数据安排了整理也是如此

当操作员创建锁定时，最小尺寸的片段是数据库将记录文件划分到的时间段，默认情况下是一小时的片段。您可以更改此设置，但将要求您在记录服务器上自定义 RecorderConfig.xml 文件。如果小片段跨越两个一小时的时间段，则系统会同时锁定这两个时间段中的记录。

在 Management Client 中的审核日志中，您可以查看用户在何时创建、编辑或删除证据锁定。

当磁盘空间不足时，它不会影响受保护的数据。而最旧的非受保护数据将被删除。如果没有更多要删除的非受保护数据，系统将停止记录。您可以创建由磁盘已满事件触发的规则和报警，以便您自动收到通知。

除了在较长时间内存储更多数据并可能影响磁盘存储外，这样的证据锁定功能不会影响系统性能。

如果您将硬件移动(请参阅 第 295 页上的移动硬件)到另一个记录服务器：

- 由证据锁定保护的记录将以创建证据锁定时定义的保留时间保留在旧的记录服务器上
- 在将摄像机生成的录像移动到另一个记录服务器之前，XProtect Smart Client 用户仍可以使用录像上的证据锁定来保护数据。即使您多次移动摄像机，并且录像存储在多个记录服务器上，也是如此

默认情况下，所有操作员均具有分配给他们的默认证据锁定配置文件，但没有该功能的用户访问权限。要指定角色的证据锁定访问权限，请参阅角色设置的"设备"选项卡(角色)。要指定角色的证据锁定配置文件，请参阅角色设置的"信息"选项卡(角色)。

在 Management Client 中，可以编辑默认证据锁定配置文件的属性，以及创建额外证据锁定配置文件并将其分配至角色。

规则和事件

规则(已作说明)

规则用于指定在特定条件下应执行的动作。示例：当侦测到移动时(条件)，摄像机应开始记录(动作)。

以下是有关使用规则可以执行的操作的示例：

- 开始与停止记录
- 设置非默认的实时帧速率
- 设置非默认的记录帧速率
- 开始与停止 PTZ 巡视
- 暂停与恢复 PTZ 巡视
- 将 PTZ 摄像机移动到特定位置
- 将输出设置为激活/取消激活状态
- 通过电子邮件发送通知
- 生成日志条目
- 生成事件
- 应用新设备设置，如摄像机上的不同分辨率
- 使视频显示在 Matrix 接收方
- 开始与停止插件
- 开始与停止来自设备的馈送

停止设备意味着视频不再会从设备传输到系统，在这种情况下，既不能查看实时视频也不能记录视频。相反，已停止馈送的设备仍然可以与记录服务器通信，并且可通过规则自动启动设备的馈送(与在 Management Client 中手动禁用设备后的情况相反)。

> 某些规则内容可能需要为相关设备启用特定功能。例如，如果相关摄像机未启用记录，则指定摄像机应记录的规则不会工作。创建规则之前，Milestone 建议您检验相关设备是否能够正常工作。

规则复杂度

具体的选项数量取决于您要创建的规则类型，以及系统上可用的设备数量。规则可以提供高度的灵活性：您可以组合事件和时间条件，可以在一个规则中指定多个动作，并且通常可以创建涵盖系统上多个设备或所有设备的规则。

还可以根据需要创建简单或复杂的规则。例如，可以创建非常简单的基于时间的规则：

示例	说明
非常简单的基于时间的规则	在星期一的 08.30 至 11.30 之间(时间条件)，摄像机 1 和摄像机 2 应在时间段开始时启动记录(动作)并在时间段结束时停止记录(停止动作)。
非常简单的基于事件的规则	当在摄像机 1 上侦测到移动时(事件条件)，摄像机 1 应立即开始记录(动作)，然后在 10 秒后停止记录(停止动作)。 即使基于事件的规则被一台设备上的事件激活，仍然可以指定应在一台或多台其他设备上执行动作。
涉及多台设备的规则	当在摄像机 1 上侦测到移动时(事件条件)，摄像机 2 应立即开始记录(动作)，并且连接到输出 3 的警笛应立即响起(动作)。然后在 60 秒后，摄像机 2 应停止记录(停止动作)，并且连接到输出 3 的警笛应停止响声(停止动作)。
组合了时间、事件和设备的规则	当摄像机 1 上侦测到移动(事件条件)，并且当天是星期六或星期日(时间条件)时，摄像机 1 和摄像机 2 应立即启动记录(动作)，并应向安全管理器发送通知(动作)。然后，当摄像机 1 和摄像机 2 上不再侦测到移动时再隔 5 秒后，两台摄像机均应停止记录(停止动作)。

根据贵组织的需求，通常最好创建很多简单规则，而不是少量复杂规则。即使这意味着系统中要有更多的规则，但这是一种简单的规则概览方法。让规则保持简单同时也意味着，在取消激活/激活单独的规则元素时拥有更高的灵活性。使用简单规则，可以在需要时取消激活/激活整个规则。

规则和事件(已作说明)

规则是本系统中的核心元素。规则用于确定极为重要的设置，如摄像机在何时进行记录，PTZ 摄像机应在何时进行巡视，何时发送通知等。

例如，指定在侦测到移动时，特定摄像机应开始记录的规则：

事件是您使用**管理规则**向导时的核心元素。在该向导中，事件主要用于触发动作。例如，您可以创建一个规则，使其指定**一旦**侦测到移动，监控系统应采取**动作**，开始从特定摄像机记录视频。

以下类型的条件可以触发规则：

名称	说明
事件	当监控系统上发生事件时(例如，当侦测到移动时，当系统接收到来自外部传感器的输入时)。
时间间隔	当您进入特定的时间段时(例如， `Thursday 16th August 2007 from 07.00 to 07.59` 或`every Saturday and Sunday`。
故障转移时间间隔	故障转移处于活动状态或非活动状态的时间段。
重复时间	当您设置要在详细的经常性计划上执行的操作时。 例如： • 每周二的 15:00 至 15:30 之间每 1 小时 • 每 3 个月的第 15 天 11:45 • 每天的 15:00 至 19:00 之间每 1 小时 时间基于安装有 Management Client 的服务器的本地时间设置。

您可以使用规则和事件的下列功能：

- **规则**：规则是本系统中的核心元素。监控系统的行为在很大程度上由规则确定。创建规则时，可以使用所有类型的事件
- **时间配置文件**：时间配置文件是 Management Client 中定义的时间段。当在 Management Client 中创建规则时，使用它们来(例如)创建规则，以指定在特定时间配置文件内应采取的特定动作
- **通知配置文件**：您可以利用通知配置文件设置现成的电子邮件通知，这些通知可由规则自动触发，例如当特定事件发生时触发
- **用户定义事件**：用户定义的事件是自定义事件，让用户可以在系统中手动触发事件，或处理来自系统的输入
- **分析事件**：分析事件是从外部第三方视频内容分析(VCA)提供商收到的数据。您可以将分析事件用作警

报的基础

- **常规事件**:使用常规事件,可通过IP网络向系统发送简单字符串,从而在XProtect事件服务器中触发动作

时间配置文件(已作说明)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

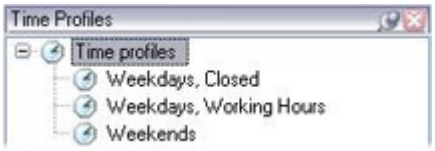
时间配置文件是管理员定义的时间段。创建规则时,可以使用时间配置文件,例如,指定在特定时间段内应采取特定动作的规则。

时间配置文件还会与 Smart Client 配置文件一起分配至角色。默认情况下,所有规则都会被分配默认时间配置文件**始终**。这意味着,对于使用此默认时间配置文件的角色的成员,其用户权限在系统中没有任何基于时间的限制。您还可为角色分配备用时间配置文件。

时间配置文件可以基于一个或多个单一时间段、基于一个或多个重复时间段或基于单一和重复时间的组合。许多用户可能熟悉日历应用程序中单个和重复时间段的概念,例如 Microsoft® Outlook 中的时间段。

时间配置文件始终以本地时间应用。这意味着,如果系统拥有位于不同时区的记录服务器,那么与时间配置文件相关的任何动作(例如在摄像机上记录)应以各个记录服务器的本地时间执行。示例:如果有时间配置文件覆盖时间段 08:30 至 09:30,则位于纽约的记录服务器上的相关动作将在纽约当地时间的 08:30 至 09:30 执行,而位于洛杉矶的记录服务器将在数小时后,洛杉矶当地时间的 08:30 至 09:30 执行相同的动作。

通过展开**规则和事件 > 时间配置**文件创建和管理时间配置文件。**时间配置文件**列表会打开:仅作示例:



有关时间配置文件的替代文件的信息,请参阅日长时间配置文件(已作说明)。

日长时间配置文件(已解释)

当摄像机放置在外面时,通常需要在变黑时降低摄像机分辨率,启用黑/白或更改其他设置,并在变亮时执行相反操作。摄像机放置在离赤道越北或越南的地方,一年中日出和日落时间的变化越大。因此不可能使用正常的固定时间配置文件来根据光的条件调整摄像机设置。

在这种情况下,您可以创建用来定义指定地理区域日出和日落的日长时间配置文件。通过地理坐标,系统会计算每天的日出和日落时间,甚至包含夏令时。因此,时间配置文件会自动跟随所选区域每年日出/日落的变化,确保配置文件只在需要的时间处于活动状态。所有时间和日期都基于管理服务器的时间和日期设置。您还可以为开始(日出)和结束时间(日落)设置正或负偏移(按分钟)。开始和结束时间的偏移可以相同或不同。

创建规则和角色时,均可使用日长配置文件。

通知配置文件(已解释)

使用通知配置文件,可以设置现成电子邮件通知。通知可由规则自动触发,例如当特定事件发生时触发。

创建通知配置文件时,指定消息文本并决定是否要在电子邮件通知中包含静态图像和 AVI 视频剪辑。

> ⚠ 您可能需要禁用阻止应用程序发送电子邮件通知的任何电子邮件扫描器。

创建通知配置文件的要求

必须首先为电子邮件通知指定邮件服务器设置,然后才可以创建通知配置文件。

如果在邮件服务器上安装必要的安全证书,则可以保护与邮件服务器的通信。

如果您希望电子邮件通知能够包含 AVI 影片剪辑,必须首先指定压缩设置:

1. 前往 **工具 > 选项**。这将打开**选项**窗口。
2. 在 **邮件服务器**选项卡 (第 334 页上的"邮件服务器"选项卡(选项)) 上配置邮件服务器,并在**AVI 生成**第 335 页上的"AVI 生成"选项卡(选项)选项卡 () 上配置压缩设置。

用户定义事件(已解释)

如果所需事件不在事件总览列表中,可创建自己的用户定义事件。使用此类用户定义事件,可将其他系统集成到监控系统中。

利用用户定义事件,可使用从第三方访问控制系统接收的数据作为系统中的事件。这些事件随后可以触发动作。这样,就可以(例如)在某人进入建筑物时开始记录相关摄像机的视频。

用户定义事件还可用于在 XProtect Smart Client 中查看实时视频时手动触发事件,如果在规则中使用,还可用于自动触发。例如,当发生用户定义事件 37 时,PTZ 摄像机 224 应停止巡视,并转到预设位置 18。

通过角色,可以定义哪些用户能够触发用户定义事件。用户定义事件可以通过两种方式使用,如果需要可同时使用:

事件	说明
提供在 XProtect Smart Client 中手动触发事件的功能	在这种情况下,用户定义事件使得最终用户能够在 XProtect Smart Client 中查看实时视频时手动触发事件。当因为 XProtect Smart Client 用户手动触发而发生用户定义事件时,规则可以触发应在系统上执行的一个或多个动作。
提供通过 API 触发事件的功能	在这种情况下,用户定义事件可以从监控系统以外触发。以这种方式使用用户定义事件时,需要在触发用户定义事件时使用单独的 API(应用程序接口;用于创建或自定义软件应用程序的一组生成块)。以这种方式使用用户定义事件需要通过 Active Directory 进行身份验证。这样可确保即使可以从监控系统以外触发用户定义事件,仍然只有授权用户能够执行。

事件	说明
	此外，用户定义事件可以通过 API 与元数据关联，从而定义特定设备或设备组。在使用用户定义事件触发规则时，这个功能很好用：避免每个设备都有一个基本上做同样的事情的规则。示例：某公司使用访问控制，拥有 35 个入口，每个入口都有一个访问控制设备。当访问控制设备激活时，在系统中触发用户定义事件。该用户定义事件用于一项规则，使得在与激活的访问控制设备关联的摄像机上启动记录。哪台摄像机与哪项规则关联是在元数据中定义的。如此一来，公司不需要 35 个用户定义事件以及 35 个由用户定义事件触发的规则。只需要 1 个用户定义事件和 1 个规则即可。 以此方式使用用户定义事件时，可能并非始终希望这些事件可以在 XProtect Smart Client 中手动触发。您可以使用角色来定义哪些用户定义事件应在 XProtect Smart Client 中可见。

分析事件(已解释)

分析事件通常是从外部第三方视频内容分析 (VCA) 提供商收到的数据。

使用分析事件作为警报基础基本上是有三个步骤的过程：

- 第一步，启用分析事件功能并设置其安全性。使用被允许地址的列表控制哪些用户可以将事件数据发送到系统以及服务器在哪个端口上进行监听
- 第二步，创建分析事件(可能带有事件说明)，然后进行测试
- 第三步，使用分析事件作为警报定义的来源

在**站点导航**窗格的**规则和事件**列表中设置分析事件。

要使用基于 VCA 的事件，则需要第三方 VCA 工具向系统提供数据。使用哪个 VCA 工具完全取决于您，只要该工具提供的数据遵循格式要求即可。有关分析事件的 MIP SDK 文档中对此格式进行了说明。

有关更多详细详细，请联系系统供应商。第三方 VCA 工具由独立的合作伙伴开发，基于 Milestone 开放式平台提供解决方案。这些解决方案可能会影响系统的性能。

常规事件(已解释)

使用常规事件，可通过 IP 网络向本系统发送简单字符串，从而在 XProtect 事件服务器中触发动作。

可以通过 TCP 或 UDP 发送字符串的任何硬件或软件均可用于触发常规事件。本系统能够分析接收到的 TCP 或 UDP 数据包，并在符合特定条件的情况下自动触发常规事件。这样，便可以将本系统与外部资源集成，例如访问控制系统和警报系统。目的在于允许尽可能多的外部资源与系统交互。

采用数据来源的概念，可以避免必须采用符合本系统标准的第三方工具。数据来源允许您与特定 IP 端口上的特定硬件或软件进行通信，并微调对到达端口的字节的解释方式。每个常规事件类型都与数据来源配对，并决定用来与特定硬件或软件通信的语言。

使用数据来源需要有关 IP 网络的基本知识以及要连接的单独硬件或软件的特定知识。您可以使用很多参数，但没有现成解决方案来实现该操作。基本上，本系统提供工具，但不提供解决方案。与用户定义事件不同，常规事件没有身份验证。这样会更易于触发，但是为了避免危害安全性，只接受来自本地主机的事件。您可以从**选项**菜单的**常规事件**选项卡上允许其他客户端 IP 地址。

Webhook(已说明)

Webhook 是使 Web 应用程序能够相互通信的 HTTP 请求，便于在发生预定义事件时在应用程序之间发送实时数据，例如，在用户登录到系统或摄像机报告错误时，将事件数据发送到预定义的 Webhook 端点。

Webhook 端点 (webhook URL) 是发送事件数据的预定义目标地址，很像一个单向电话号码。

您可以使用 Webhook 来构建对 XProtect 中的所选事件进行订阅的集成。触发事件时，会将 HTTP POST 发送到您为该事件定义的 Webhook 端点。HTTP POST 主体包含采用 JSON 格式的事件数据。

Webhook 不会针对数据或触发的事件而对系统进行轮询，而是由系统在发生事件时将事件数据推送到 Webhook 端点，与轮询解决方案相比，这会降低 Webhook 的资源需求，并加快设置速度。

可以将 Webhook 设置为在使用或不使用代码脚本的情况下进行集成。

> 您应该验证XProtect发送的事件数据是否遵循您所在国家/地区既有的数据和隐私保护法规。

默认情况下，在 XProtect 2023R1 或更高版本上已安装 Webhook 功能并随时可供使用，Management Client 的**规则**选项卡上会显示 **Webhook** 操作。

警报

警报(已作说明)

> 该功能仅在安装 XProtect Event Server 后才能工作。

本文将介绍如何设置由事件触发的警报以显示在系统中。

根据事件服务器中处理的功能，警报功能提供对整个组织中任意数量安装(包括任何其他 XProtect 系统)中的警报的集中总览、控制和扩展。可以将其配置为基于以下任一项生成警报：

- **系统相关的内部事件**

  例如:移动、服务器响应/未响应、存档问题、磁盘空间不足等。

- **集成的外部事件**

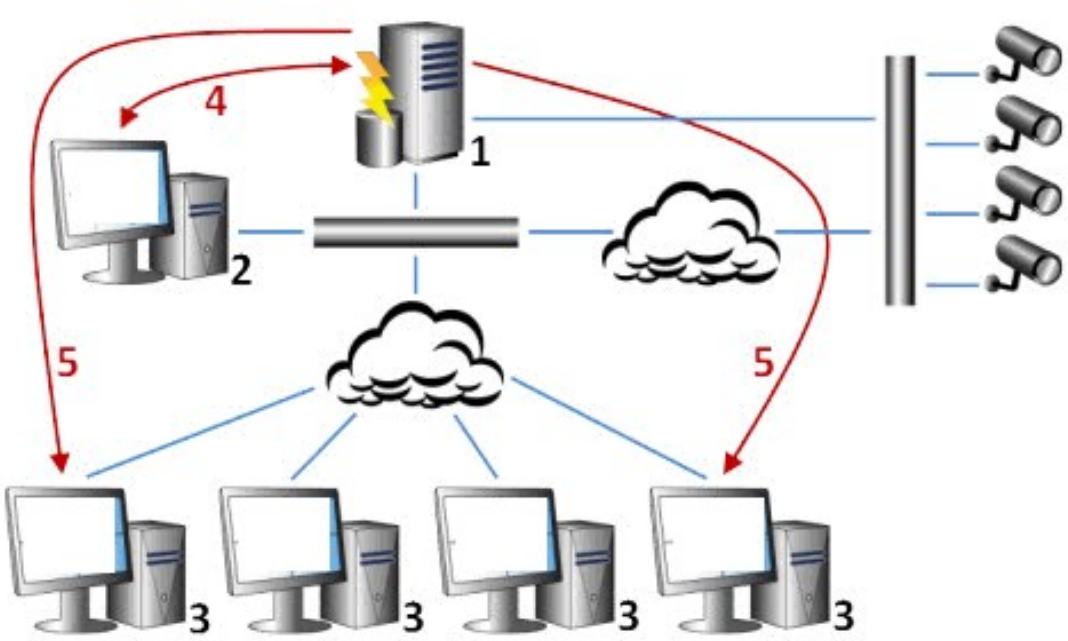
  此组由多个外部事件类型组成:

  - **分析事件**

    通常是从外部第三方视频内容分析 (VCA) 提供商收到的数据。

  - **MIP 插件事件**

    通过 MIP SDK, 第三方供应商可开发本系统的自定义插件(例如, 集成到外部访问控制系统或类似功能)。



图例:

1. 监控系统
2. Management Client
3. XProtect Smart Client
4. 警报配置
5. 警报数据流

您可以处理和分配 XProtect Smart Client 的警报列表中的警报。还可以将警报与 XProtect Smart Client 的智能地图地图和地图功能集成。

警报配置

警报配置包括:

- 基于角色的动态警报处理设置
- 所有组件的集中技术总览:服务器、摄像机和外部装置
- 所有输入警报和系统信息的集中日志设置
- 插件处理,允许自定义地集成其他系统,如外部访问控制或基于 VCA 的系统

一般而言,通过导致警报的对象的可见性来控制警报。这意味着有四个可能方面对有关警报以及哪些用户能够控制/管理警报和进行到何种程度会起到作用:

名称	说明
来源/设备可见性	如果导致警报的设备未设置为对用户角色可见,用户将不能在 XProtect Smart Client 中的警报列表中看到警报。
触发用户定义事件的权限	该权限用于确定用户角色是否可以触发 XProtect Smart Client 中的所选用户定义事件。
外部插件	如果系统中设置了任何外部插件,则这些插件可能会控制用户处理警报的权限。
常规角色权限	确定用户是只被允许查看警报,或者还被允许管理警报。 **警报**用户可以对警报进行哪些操作,取决于用户的角色以及为该特定角色配置的设置。

在**选项**中的**警报和事件**选项卡上,可指定警报、事件和日志的设置。

智能地图

智能地图(已解释)

在 XProtect® Smart Client 和 XProtect Mobile 中,智能地图功能让您能够以在地理上正确的方式查看和访问世界各地多个位置的设备。与地图(其中每个位置具有不同地图)不同,智能地图 可以在单一视图中提供总体情况。

智能地图功能的以下配置在 Management Client 中完成。

- 配置可以为智能地图选择的地理背景。这包括将智能地图与以下服务之一集成：
  - Bing Maps
  - Google Maps
  - Milestone Map Service
  - OpenStreetMap
- 在 XProtect Management Client 或 XProtect Smart Client 中启用 Bing Maps 或 Google Maps
- 在 XProtect Smart Client 中启用智能地图的编辑，包括设备
- 在 XProtect Management Client 中将您的设备按地理位置放置
- 使用 Milestone Federated Architecture 设置智能地图

将智能地图与 Google Maps 集成(已作说明)

要将 Google Maps 嵌入到智能地图中，您需要从 Google 获取地图静态 API 密钥。要获取该 API 密钥，首先必须创建一个 Google Cloud 计费帐户。根据每月的地图加载量向您收费。

获得 API 密钥后，必须在 XProtect Management Client 中输入该密钥。另请参阅 第 278 页上的在以下对象中启用 Bing Maps 或 Google Maps：Management Client。

若您位于限制性防火墙之后，则允许访问所使用的域会很重要。您可能需要在运行 Smart Client 的每台机器上使用 maps.googleapis.com，以允许 Google Maps 的流出流量。

有关详细信息请参阅：

- Google Maps Platform - 入门：https://cloud.google.com/maps-platform/
- Google Maps 平台计费指南：https://developers.google.com/maps/billing/gmp-billing
- 地图静态 API 开发者指南：https://developers.google.com/maps/documentation/maps-static/dev-guide

将数字签名添加到 Maps Static API 密钥

如果您希望 XProtect Smart Client 操作员每天发出超过 25000 个地图请求，则您需要为您的Maps Static API密钥设置数字签名。通过数字签名，Google 服务器可以验证是否有任何使用您的 API 密钥生成请求的站点被授权这样做。但是，无论使用要求如何，Google 都建议使用数字签名作为附加的安全层。要获取数字签名，您必须检索签名秘密。有关详细信息，请参阅 https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual。

将智能地图与 Bing Maps 集成(已作说明)

要将 Bing Maps 嵌入到智能地图中，您需要一个基本密钥或企业密钥。区别在于基本密钥是免费的，但在交易变成计费或拒绝访问地图服务之前允许数量有限的交易。企业密钥不是免费的，但允许不限制数量的交易。

有关 Bing Maps 的详细信息，请参阅 https://www.microsoft.com/en-us/maps/licensing/。

获得 API 密钥后，必须在 XProtect Management Client 中输入该密钥。请参阅 第 278 页上的在以下对象中启用 Bing Maps 或 Google Maps：Management Client。

若您位于限制性防火墙之后，则允许访问所使用的域会很重要。您可能需要在运行 Smart Client 的每台机器上使用 *.virtualearth.net，以允许 Bing Maps 的流出流量。

缓存 智能地图 文件(已解释)

如果您使用 Google Maps 作为地理背景，则不会缓存文件。

您用于地理背景的文件从 拼贴图服务器中进行检索。文件存储在缓存文件中的时间取决于 XProtect Smart Client 中**设置**对话框内**已移除缓存智能地图文件**列表所选择的值。文件的存储时间还可以是：

- 无限期(**从不**)
- 如果文件未被使用，则为 30天(**当连续 30 天未被使用时**)
- 当操作员退出 XProtect Smart Client 时(**退出时**)

当您更改拼贴图服务器的地址时，会自动生成缓存文件夹。先前的地图文件保留在您本地计算机的关联缓存文件中。

结构

分布式系统设置

分布式系统设置示例。可以根据需要指定足够大的摄像机、记录服务器和所连接客户端的数目。

分布式设置中的所有计算机都必须位于域或工作组中。

图例：

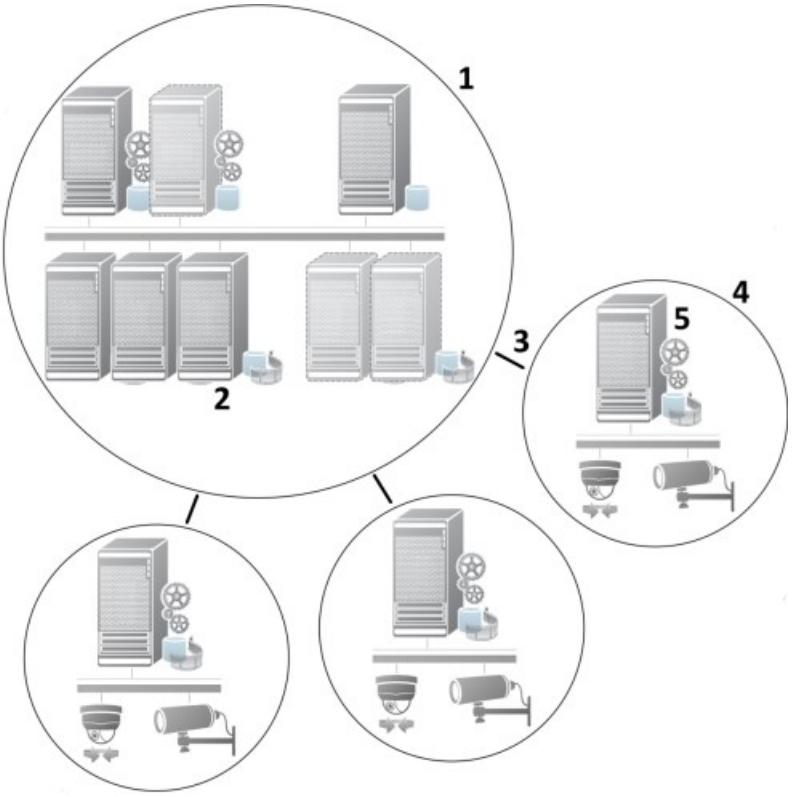
1. Management Client(s)
2. 事件服务器
3. Microsoft 群集
4. 管理服务器
5. 故障转移管理服务器
6. 服务器，它安装有 SQL Server
7. 故障转移记录服务器
8. 记录服务器
9. XProtect Smart Client(s)
10. IP 视频摄像机
11. 视频编码器
12. 模拟摄像机
13. PTZ IP 摄像机
14. 摄像机网络
15. 服务器网络

Milestone Interconnect(已作说明)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

Milestone Interconnect™允许您将一些物理上分散的较小远程 XProtect 安装与一个 XProtect Corporate 中央站点集成。这些小型站点称为远程站点，可安装在船舶、公共汽车或火车等移动设备上。这意味着此类站点无需永久性地连接到网络。

以下图示将显示如何在系统上设置 Milestone Interconnect：



1. Milestone Interconnect 中央 XProtect Corporate 站点
2. Milestone Interconnect **驱动程序**(处理中央站点的记录服务器与远程站点之间的连接,通过添加硬件向导添加远程系统时必须在驱动程序列表中选中)
3. Milestone Interconnect 连接
4. Milestone Interconnect 远程站点(具有系统安装、用户、摄像机等的完整远程站点)
5. Milestone Interconnect 远程系统(远程站点上的实际技术安装)

可使用中央站点中的**添加硬件**向导向中央站点添加远程站点(请参阅向中央 第 272 页上的向中央 Milestone Interconnect 站点添加远程站点 站点添加远程站点)。

每个远程站点均独立运行,并且可以执行任何常规监控任务。根据网络连接和相应的用户权限(请参阅第272页上的分配用户权限),MilestoneInterconnect可直接实时查看远程站点摄像机并在中央站点上播放远程站点记录。

中心网站只能查看和访问可由指定用户帐户(在添加远程站点时)访问的设备。这允许本地系统管理员控制对中央站点及其用户可用的设备。

在中央站点上,您可以查看针对互连摄像机的系统自身状态,但无法直接查看远程站点的状态。要监视远程站点,可使用远程站点事件在中央站点上触发警报或其他通知(请参阅 第 274 页上的配置中央站点以响应来自远程站点的事件)。

它还可以根据事件、规则/时间表或 XProtect Smart Client 用户的手动请求将远程站点录像传输至中央站点。

仅 XProtect Corporate 系统可作为中央站点。所有其他产品(包括 XProtect Corporate)均可作为远程站点。不同设置在版本、摄像机数量以及(如果可能)中央站点处理源自远程站点的设备和事件的方式上都有区别。有关 XProtect 设置中具体 Milestone Interconnect 产品如何相互作用的详细信息,请转到 Milestone Interconnect 网站(https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/)。

选择 Milestone Interconnect 或 Milestone Federated Architecture(已解释)

Milestone Interconnect™ 在物理分布式系统中,如果中央站点上的用户需要访问远程站点上的视频,可以在 或 Milestone Federated Architecture™ 之间进行选择。

在以下情况下,Milestone 建议选择 Milestone Federated Architecture:

- 中央站点和联合站点之间的网络连接稳定
- 网络使用相同域
- 大型站点较少
- 带宽足以满足所需用途

在以下情况下,Milestone 建议选择 Milestone Interconnect:

- 中央站点和远程站点之间的网络连接不稳定
- 您或您的组织需要在远程站点上使用其他 XProtect 产品
- 网络使用不同域或工作组
- 小型站点很多

Milestone Interconnect 和授予许可

要运行 Milestone Interconnect,您需要中央站点上的 Milestone Interconnect 摄像机许可证以查看来自远程站点上的硬件设备的视频。所需的 Milestone Interconnect 摄像机许可证数量取决于要从其接收数据的远程站点上的硬件设备的数量。只有 XProtect Corporate 可作为中央站点。

Milestone Interconnect 摄像机许可证的状态列在中央站点的**许可证信息**页面上。

Milestone Interconnect 设置(已解释)

可使用三种方法来运行 Milestone Interconnect。如何运行设置将取决于网络连接、记录播放方式以及您是否检索远程记录及检索的程度。

以下介绍了三种最有可能出现的设置:

直接从远程站点播放(网络连接良好)

这是一种最直接了当的设置。中央站点与其远程站点持续处于联机状态,中央站点用户直接从远程站点播放远程记录。这需要使用**从远程系统播放记录**选项(请参阅 第 273 页上的直接从远程站点摄像机启用播放)。

根据规则或 XProtect Smart Client 从远程站点检索所选的远程记录片断(定期受限网络连接)

当所选记录片断(源自远程站点)应集中存储以确保独立于远程站点时使用。在网络故障或网络限制的情况下,独立性至关重要。您在**远程检索**选项卡上配置远程记录检索设置(请参阅 第 369 页上的远程检索选项卡)。

可在需要时从 XProtect Smart Client 启动远程记录检索,或者可以设置规则。在一些情况下,远程站点联机,而在其他情况下,远程站点在大部分时间均脱机。这通常取决于具体行业。对于一些行业,中央站点通常与其远程站点永久地联机(例如,一个零售总部(中央站点)和多个商店(远程站点))。对于另一些行业,例如运输业,远程站点处于移动状态(例如公共汽车、火车、船舶等),因此只能随机建立网络连接。如果网络连接在远程记录检索过程中发生故障,作业将在下一次机会到来时继续。

如果系统在**远程检索**选项卡上指定的时间间隔之外检测到自动检索或从 XProtect Smart Client 进行检索的请求,系统将接受检索请求,但会在到达选择的时间间隔之后才开始检索。新的远程记录检索作业将排队,并在到达允许的时间间隔之后启动。可从**系统仪表板 -> 当前任务**中查看搁置中的远程记录检索作业。

连接失败后,默认情况下从远程站点检索缺失的远程记录

像记录服务器使用摄像机上的边缘存储那样使用远程站点。通常,远程站点与其中央站点联机,向中央站点发送实时流供记录。如果网络由于某种原因发生故障,中央站点将会丢失录制片段。但是,一旦网络重新建立,中央站点就会自动检索停机期间的远程记录。这需要在摄像机的**记录**选项卡上使用连接恢复时**自动检索远程记录**选项(请参阅 第 273 页上的从远程站点摄像机检索远程记录)。

可将以上解决方案任意组合以满足您组织的特殊需要。

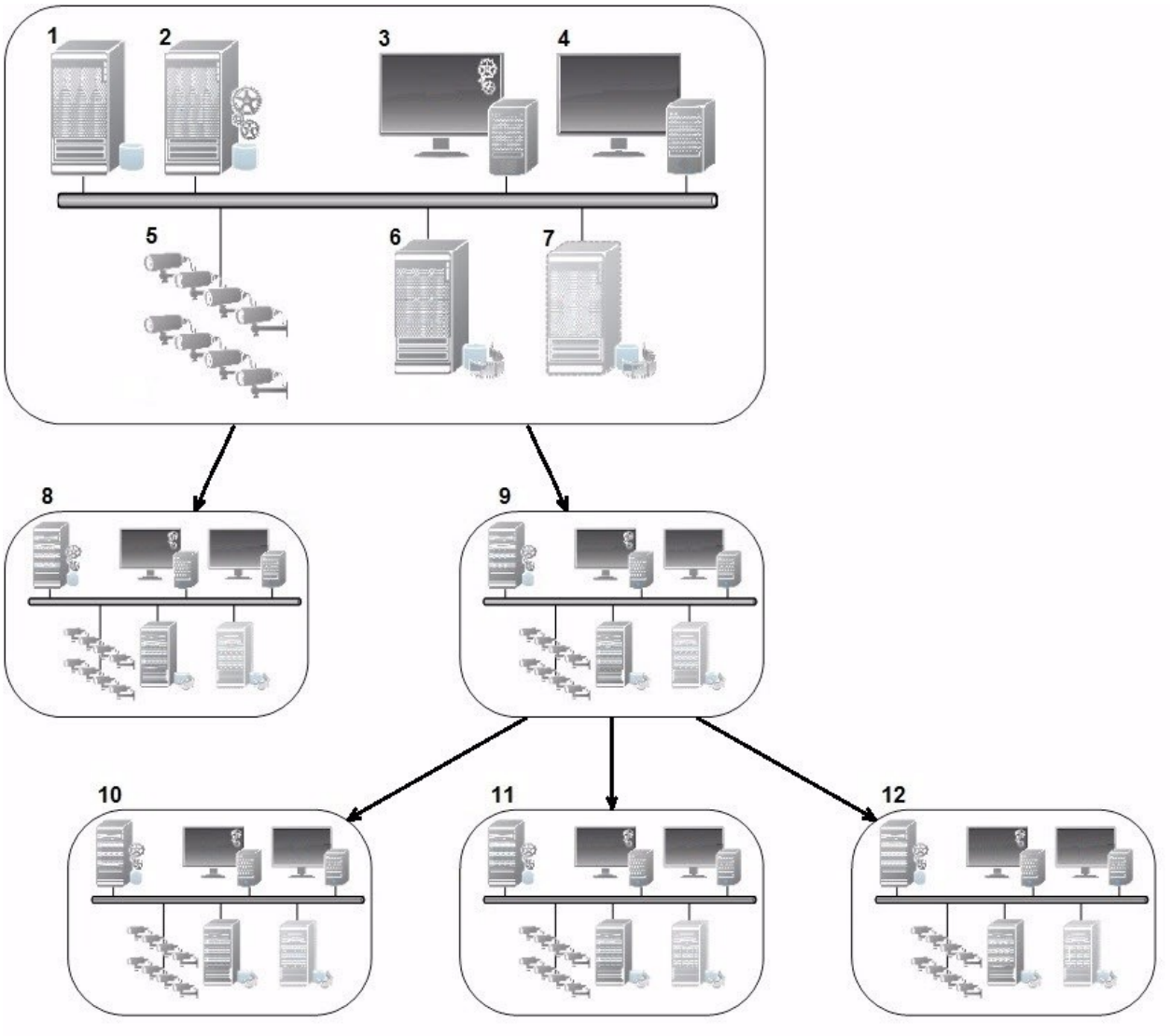
正在配置 Milestone Federated Architecture

XProtect Expert 只能作为子站点进行联合。

Milestone Federated Architecture 将多个独立的标准系统链接到父/子站点的联合层级中。具有足够权限的客户端用户可以无缝访问跨各个站点的视频、音频和其他资源。根据各个站点的管理员权限,管理员可以集中管理联合分层中的 2018 R1 版本和更新版本的所有站点。

基本用户在 Milestone Federated Architecture 系统中不受支持,因此您必须通过 Active Directory 服务将用户添加为 Windows 用户。

Milestone Federated Architecture 设置为具有一个中央站点(顶层站点)和不限数量的联合点(请参阅 第 267 页上的设置系统以运行联合站点)。当登录到站点时,您可以访问关于其所有子站点以及这些子站点的子站点的信息。当您从父站点请求链接时,将在两个站点之间建立链接(请参阅 第 269 页上的将站点添加至层次结构)。子站点只能链接到一个父站点。当将子站点添加到联合站点分层时,如果您不是子站点的管理员,则请求必须得到子站点管理员的接受。



Milestone Federated Architecture 设置的组件：

1. 服务器，它安装有 SQL Server
2. 管理服务器
3. Management Client
4. XProtect Smart Client
5. 摄像机
6. 记录服务器
7. 故障转移记录服务器
8. 到 12。联合点

分层同步

父站点包含其当前连接的所有子站点、子站点的子站点等的更新列表。联合站点分层在站点之间具有计划的同步，以及每次有站点被系统管理员添加或删除时的同步。系统对分层进行同步时按层级进行，每个层级均转发并返回通信信息，直至到达请求信息的服务器。系统每次发送的数据小于 1MB。根据级别的数量，对层级的更改需要一定时间才能在 Management Client 中显示。不能计划自己的同步。

数据通信

在用户或管理员查看实时或录制视频或者配置站点时，系统会发送通信或配置数据。数据量取决于所查看或配置的内容及其数量。

Milestone Federated Architecture 与其他产品和系统要求

- 三个主要版本均支持在 Management Client 中打开 Milestone Federated Architecture，其中包括当前正在发行的版本。在超出该范围的 Milestone Federated Architecture 设置中，您需要一个与服务器版本匹配的单独 Management Client。
- 如果中央站点使用 XProtect Smart Wall，则您也可以使用联合站点分层中的 XProtect Smart Wall 功能。
- 如果中央站点使用 XProtect Access，并且 XProtect Smart Client 用户登录到联合站点分层中的站点，则来自联合站点的访问请求通知也将出现在 XProtect Smart Client
- 可以将 XProtect Expert 2013 系统或更新版本系统作为子站点而非父站点添加到联合站点分层
- Milestone Federated Architecture 不需要额外许可证
- 有关用户案例和优点的详细信息，请参阅关于 Milestone Federated Architecture 的白皮书。

建立联合站点分层

当您在 Management Client 中开始构建层级之前，Milestone 建议您绘制出所需的站点链接方式。

在联合分层中将每个站点均作为具有标准系统组件、设置、规则、计划、管理员、用户和用户权限的一般独立系统进行安装和配置。如果您已经安装并配置站点，并且仅需要将它们在联合站点分层中组合起来，则您的系统便做好了设置的准备。

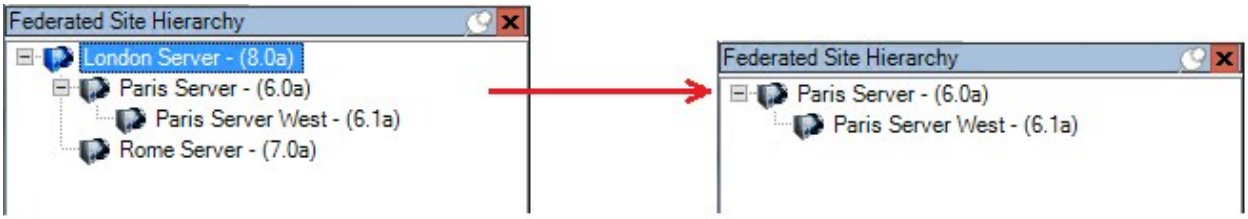
在安装各站点后，您必须将它们设置为以联合站点运行(请参阅 第 267 页上的设置系统以运行联合站点)。

要启动分层，您可以登录到要用作中央站点的站点，并添加(请参阅 第 269 页上的将站点添加至层次结构)第一个联合站点。当建立链接后，这两个站点会在 Management Client 的**联合站点层级**窗格中自动创建联合站点层级，您可以向其中添加更多站点以扩展联合层级。

在创建联合站点分层后，用户和管理员可登录某站点以访问该站点及其可能具有的任何联合点。对联合点的访问权限取决于用户权限。

您可以向联合分层中添加任意数量的站点。此外，您还可以将较旧版本产品上的站点链接到较新的版本，反之亦然。版本号将自动出现，并且不能删除。您登录到的站点始终位于**联合站点分层**窗格顶部，被称为主站点。

以下是 Management Client 中的联合站点示例。在左侧，用户已登录至顶部站点。在右侧，用户已登录至其中一个子站点，即 Paris 服务器，它当时是主站点。



Milestone Federated Architecture 中的状态图标

这些图标代表站点的可能状态：

说明	图标
整个分层中的顶层站点是可操作的。	
整个分层中的顶层站点仍然是可操作的，但需要注意一个或多个问题。显示在顶层站点图标的顶部。	
站点可操作。	
站点正在等待在分层中获得接受。	
站点正在连接，但尚不可操作。	

本系统使用的端口

下面列出了所有 XProtect 组件及其所需的端口。例如，如果要确保防火墙只阻止无需的网络通信，您必须指定系统所用的端口。您只能启用这些端口。列表中还包括用于本地程序的端口。

它们被分为两组：

- **服务器组件**（服务）在特定的端口上提供服务，因此它们需要在这些端口上听取客户端的请求。因此，需要在 Windows Firewall 中打开这些端口以进行入站和出站连接
- **客户端组件**（客户端）发起与服务器组件上特殊端口的连接。所以，这些端口需要打开，以进行入站连接。在 Windows Firewall 中，出站连接通常被默认为开启

毫无疑问，针对服务器组件的端口必须打开以进行入站连接，而针对客户端组件的端口必须打开以进行出站连接。

您应记住服务器组件可以作为其他服务器组件的客户端。这些未在此文档中明确列出。

端口号为默认号，但是可以进行更改。如果您需要更改无法通过 Milestone 配置的端口，请联系 Management Client 支持部门。

服务器组件(入站连接)

以下各部分列出了针对特定服务需要打开的端口。要确定哪个端口应该在特定的计算机上打开,您需要考虑在该计算机上运行的所有服务。

Management Server 服务和相关流程

端口号	协议	程序	连接来自	作用
80	HTTP	IIS	所有服务器和 XProtect Smart Client 及 Management Client	端口 80 和端口 443 的用途是相同的。但是,视频管理软件使用哪个端口取决于您是否使用证书来保护通信。 • 当您没有使用证书保护通信时,视频管理软件使用端口 80。 • 当您使用证书保护通信时,视频管理软件使用端口 443,但从事件服务器到管理服务器的通信除外。从事件服务器到管理服务器的通信使用 Windows 安全框架 (WCF) 和端口 80 上的 Windows 身份验证。
443	HTTPS	IIS		
6473	TCP	Management Server 服务	Management Server Manager 托盘图标,仅本地连接。	显示状态并管理服务。
8080	TCP	管理服务器	仅针对本地连接。	服务器上内部进程之间的通信。
9000	HTTP	管理服务器	Recording Server 服务	用于服务器之间的内部通信的 Web 服务。
12345	TCP	Management Server 服务	XProtect Smart Client	系统和 Matrix 接收方之间的通信。 您可以更改 Management Client 中的端口号。
12974	TCP	Management Server 服务	Windows SNMP 服务	与 SNMP 扩展代理的通信。 不要将此端口用于其他目的,即使您的系统未应用 SNMP 也是如此。 在 XProtect 2014 系统或更低版本的系统中,端口号为 6475。 在 XProtect 2019 R2 系统和更低版本的系统中,端口号为 7475。

SQL Server 服务

端口号	协议	程序	连接来自	作用
1433	TCP	SQL Server	Management Server 服务	通过 Identity Provider 存储和检索配置。
1433	TCP	SQL Server	Event Server 服务	通过 Identity Provider.存储和检索事件。
1433	TCP	SQL Server	Log Server 服务	通过 Identity Provider 存储和检索日志条目。

Data Collector 服务

端口号	协议	程序	连接来自	作用
7609	HTTP	IIS	在管理服务器计算机上:在所有其他服务器上的 Data Collector 服务。 在其他计算机上:在管理服务器上的 Data Collector 服务。	系统监视器。

Event Server 服务

端口号	协议	程序	连接来自	作用
1234	TCP/UDP	Event Server 服务	将常规事件发送到 XProtect system 的任何服务器。	监听外部系统或设备的常规事件。 只有当相关的数据源被启用时。
1235	TCP	Event Server 服务	将常规事件发送到 XProtect system 的任何服务器。	监听外部系统或设备的常规事件。 只有当相关的数据源被启用时。
9090	TCP	Event Server 服务	将分析事件发送到 XProtect 系统的任何系统或设备。	监听外部系统或设备的分析事件。 只有当分析事件功能被启用时才相关。
22331	TCP	Event Server 服务	XProtect Smart Client 和 Management Client	配置、事件、警报和地图数据。

端口号	协议	程序	连接来自	作用
22332	WS/WSS HTTP/HTTPS*	Event Server 服务	API Gateway 和 Management Client	事件/状态订阅、事件 REST API、Websockets 消息 API 和警报 REST API。
22333	TCP	Event Server 服务	MIP 插件和应用程序。	MIP 信息。

*在访问 HTTP 以访问仅 HTTPS 端点时将返回 403 错误。

Recording Server 服务

端口号	协议	程序	连接来自	作用
25	SMTP	Recording Server 服务	摄像机、编码器以及 I/O 设备。	监听设备的事件消息。 默认禁用该端口。 (已弃用) 启用此选项将为非加密连接打开一个端口，不建议这样做。
5210	TCP	Recording Server 服务	故障转移记录服务器。	故障转移记录服务器运行后合并数据库。
5432	TCP	Recording Server 服务	摄像机、编码器以及 I/O 设备。	监听设备的事件消息。 默认禁用该端口。
7563	TCP	Recording Server 服务	XProtect Smart Client, Management Client	检索视频和视音频以及 PTZ 指令。
8966	TCP	Recording Server 服务	Recording Server Manager 托盘图标，仅本地连接。	显示状态并管理服务。
9001	HTTP	Recording Server 服务	管理服务器	用于服务器之间的内部通信的 Web 服务。

端口号	协议	程序	连接来自	作用
				如果正在使用记录服务器的多个实例，则每个实例都需要有自己的端口。其他端口将是 9002、9003 等。
11000	TCP	Recording Server 服务	故障转移记录服务器	轮询记录服务器的状态。
12975	TCP	Recording Server 服务	Windows SNMP 服务	与 SNMP 扩展代理的通信。 不要将此端口用于其他目的，即使您的系统未应用 SNMP 也是如此。 在 XProtect 2014 系统或更低版本的系统中，端口号为 6474。 在 XProtect 2019 R2 系统和更低版本的系统中，端口号为 7474。
65101	UDP	Recording Server 服务	仅针对本地连接	监听驱动程序的事件通知。

除了上述 Recording Server 服务的入站连接，Recording Server 服务还会建立与以下项的出站连接：

- 摄像机
- NVR
- 远程互连站点(Milestone 互连 ICP)

Failover Server 服务和 Failover Recording Server 服务

端口号	协议	程序	连接来自	作用
25	SMTP	Failover Recording Server 服务	摄像机、编码器以及 I/O 设备。	监听设备的事件消息。 默认禁用该端口。 (已弃用)启用此选项将为非加密连接打开一个端口，不建议这样做。

端口号	协议	程序	连接来自	作用
5210	TCP	Failover Recording Server 服务	故障转移记录服务器	故障转移记录服务器运行后合并数据库。
5432	TCP	Failover Recording Server 服务	摄像机、编码器以及 I/O 设备。	监听设备的事件消息。 默认禁用该端口。
7474	TCP	Failover Recording Server 服务	Windows SNMP 服务	与 SNMP 扩展代理的通信。 不要将此端口用于其他目的，即使您的系统未应用 SNMP 也是如此。
7563	TCP	Failover Recording Server 服务	XProtect Smart Client	检索视频和视音频以及 PTZ 指令。
8844	UDP	Failover Recording Server 服务	故障转移记录服务器之间的通信。	服务器之间的通信。
8966	TCP	Failover Recording Server 服务	Failover Recording Server Manager 托盘图标，仅本地连接。	显示状态并管理服务。
8967	TCP	Failover Server 服务	Failover Server Manager 托盘图标，仅本地连接。	显示状态并管理服务。
8990	HTTP	Failover Server 服务	Management Server 服务	监视 Failover Server 服务的状态。
9001	HTTP	Failover Server 服务	管理服务器	用于服务器之间的内部通信的 Web 服务。

除了上述故障转移服务器/FailoverRecordingServer服务的入站连接，故障转移服务器/FailoverRecordingServer服务还会与常规录像机、摄像机和手机视频推送建立出站连接。

Log Server 服务

端口号	协议	程序	连接来自	作用
22337	HTTP	Log Server 服务	所有 XProtect 组件，但 Management Client 和记录服务器除外。	写入、读取和配置日志服务器。

Mobile Server 服务

端口号	协议	程序	连接来自	作用
8000	TCP	Mobile Server 服务	Mobile Server Manager 托盘图标，仅本地连接。	SysTray 应用程序。
8081	HTTP	Mobile Server 服务	Mobile 客户端、Web 客户端以及 Management Client。	发送数据流；视频和音频。
8082	HTTPS	Mobile Server 服务	Mobile 客户端和 Web 客户端。	发送数据流；视频和音频。
40001 - 40099	HTTP	Mobile Server 服务	记录服务器服务	Mobile Server 手机视频推送。 默认禁用该端口范围。

LPR Server 服务

端口号	协议	程序	连接来自	作用
22334	TCP	LPR Server 服务	事件服务器	检索已识别的牌照和服务器状态。 事件服务器必须装有 LPR 插件，以便进行连接。
22334	TCP	LPR Server 服务	LPR Server Manager 托盘图标，仅本地连接。	SysTray 应用程序

Milestone Open Network Bridge 服务

端口号	协议	程序	连接来自	作用
580	TCP	Milestone Open Network Bridge 服务	ONVIF 客户端	身份验证并请求视频流配置。
554	RTSP	RTSP 服务	ONVIF 客户端	将被请求的视频流传输到 ONVIF 客户端。

XProtect DLNA Server 服务

端口号	协议	程序	连接来自	作用
9100	HTTP	DLNA Server 服务	DLNA 设备	发现设备并提供 DLNA 频道配置。请求视频流。
9200	HTTP	DLNA Server 服务	DLNA 设备	将被请求的视频流传输到 DLNA 设备。

XProtect Screen Recorder 服务

端口号	协议	程序	连接来自	作用
52111	TCP	XProtect Screen Recorder	Recording Server 服务	从监控器提供视频。其显示和运行方式与记录服务器上的摄像机相同。 您可以更改 Management Client 中的端口号。

XProtect Incident Manager 服务

端口号	协议	程序	连接来自	作用
80	HTTP	IIS	XProtect Smart Client 和 Management Client	端口 80 和端口 443 的用途是相同的。但是，视频管理软件使用哪个端口取决于您是否使用证书来保护通信。 • 当您没有使用证书保护通信时，视频管理软件使用端口 80。 • 当您使用证书保护通信时，视频管理软件使用端口 443。
443	HTTPS	IIS		

服务器组件(出站连接)

Management Server 服务

端口号	协议	连接到	作用
443	HTTPS	用于托管许可证管理服务的许可证服务器。通过 https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx 进行通信	激活许可证来通信。

Recording Server 服务

端口号	协议	连接到	作用
80	HTTP	摄像机、NVR、编码器 互连的站点	身份验证、配置、数据流、视频和音频。 登录
443	HTTPS	摄像机、NVR、编码器	身份验证、配置、数据流、视频和音频。
554	RTSP	摄像机、NVR、编码器	数据流、视频和音频。
7563	TCP	互连的站点	数据流和事件。
11000	TCP	故障转移记录服务器	轮询记录服务器的状态。
40001 - 40099	HTTP	移动设备服务器服务	移动设备服务器手机视频推送。 默认禁用该端口范围。

Failover Server 服务和 Failover Recording Server 服务

端口号	协议	连接到	作用
11000	TCP	故障转移记录服务器	轮询记录服务器的状态。

Event Server 服务

端口号	协议	连接到	作用
80	HTTP	API Gateway 和 Management Server	从 API Gateway 访问配置 API
443	HTTPS	API Gateway 和 Management Server	从 API Gateway 访问配置 API
443	HTTPS	Milestone Customer Dashboard 通过 https://service.milestonesys.com/	从 XProtect 系统将状态、事件和错误消息发送到 Milestone Customer Dashboard。

Log Server 服务

端口号	协议	连接到	作用
443	HTTP	日志服务器	将消息转发到日志服务器。

API Gateway

端口号	协议	连接到	作用
443	HTTPS	Management Server	RESTful API
22332	WS/WSS HTTP/HTTPS*	Management Client	事件/状态订阅、事件 REST API、Websockets 消息 API 和警报 REST API。

摄像机、编码器和 I/O 设备(入站连接)

端口号	协议	连接来自	作用
80	TCP	记录服务器和故障转移记录服务器	身份验证、配置以及数据流;视频和音频。
443	HTTPS	记录服务器和故障转移记录服务器	身份验证、配置以及数据流;视频和音频。
554	RTSP	记录服务器和故障转移记录服务器	数据流;视频和音频。

摄像机、编码器和 I/O 设备(出站连接)

端口号	协议	连接到	作用
25	SMTP	记录服务器和故障转移记录服务器	发送事件通知(弃用)
5432	TCP	记录服务器和故障转移记录服务器	发送事件通知。 默认禁用该端口。
22337	HTTP	日志服务器	将消息转发到日志服务器。

只有少数摄像机可以建立出站连接。

客户端组件(出站连接)

XProtect Smart Client、XProtect Management Client、XProtect Mobile 服务器

端口号	协议	连接到	作用
80	HTTP	API Gateway 和 Management Server 服务	API Gateway 中的身份验证和其他 API。
443	HTTPS	API Gateway 和 Management Server 服务	当启用加密时,对基本用户进行身份验证,API Gateway 中的其他 API。
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com 位于 52.178.114.226)	Management Client 和 Smart Client 偶尔通过访问帮助 URL 检查联机帮助是否可用。
7563	TCP	Recording Server 服务	检索视频和视音频以及 PTZ 指令。
22331	TCP	Event Server 服务	警报。

XProtect Web Client、XProtect Mobile 客户端

端口号	协议	连接到	作用
8081	HTTP	XProtect Mobile 服务器	检索视频和音频流。
8082	HTTPS	XProtect Mobile 服务器	检索视频和音频流。

API Gateway

端口号	协议	连接到	作用
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API

应用程序池

视频管理软件包含标准应用程序池，例如 .NET v4.5、.NET v4.5 Classic 以及 DefaultAppPool. 您的系统上可用的应用程序池显示在互联网信息服务(IIS) 管理器中。除上述标准应用程序池外，Milestone XProtect VMS 随附了一组VideoOS应用程序池。

Milestone XProtect 中的应用程序池

在下表中，您可以获得随 Milestone XProtect 一起交付的 VideoOS 应用程序池的概览。

名称	身份	作用
.NET v4.5	ApplicationPoolId	标准IIS功能
.NET v4.5 Classic	ApplicationPoolId	标准IIS功能
DefaultAppPool	ApplicationPoolId	标准IIS功能
VideoOS ApiGateway	NetworkService	托管 XProtect API 网关，这是未来的公共 API 和 VMS 网关。
VideoOS Classic	NetworkService	托管传统组件，例如本地帮助，主要是为了确保向后兼容。
VideoOS IDP	NetworkService	托管 Identity Provider API。为基本用户

名称	身份	作用
		Identity Provider创建、维护和管理身份信息，并为依赖应用程序或服务提供身份验证和注册服务。
VideoOS IM	NetworkService	托管 XProtect Incident Manager API。XProtect Incident Manager 记录事件并将其与来自其 XProtect VMS 的片段证据(视频以及可能音频)相结合。
VideoOS Management Server	NetworkService	托管配置 API、服务器组件 API 和其他 Management Server 服务，管理用户授权。
VideoOS ReportServer	NetworkService	托管负责收集和创建警报和事件报告的 Web 应用程序。
VideoOS ShareService	NetworkService	托管促进 XProtect Mobile 客户端的用户之间书签和实时视频共享的服务。

使用应用程序池

从**互联网信息服务(IIS)** 窗口中的**应用程序池**页面，您可以添加应用程序池或设置应用程序池默认值，并且可以查看由每个应用程序池托管的应用程序。

打开应用程序池页面

1. 从 Windows **开始**菜单中，打开**互联网信息服务 (IIS) 管理器**。
2. 在**连接**窗格中，单击您的环境名称，然后单击**应用程序池**。
3. 在**操作**下，单击**添加应用程序池**或**设置应用程序池默认值**，以执行任何此类任务。
4. 在**应用程序池**页面上选择一个应用程序池，以在**操作**下为每个应用程序池显示更多选项。

产品对比

XProtect VMS 包括以下产品：

- XProtect Corporate
- XProtect Expert

- XProtect Professional+
- XProtect Express+
- XProtect Essential+

请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

授予许可

许可证(已解释)

免费 XProtect Essential+

如果您已安装 XProtect Essential+，则可以免费运行系统和八个设备许可证。已启用自动许可证激活，硬件将在添加至系统后激活。

只有当您升级到更高级的 XProtect 产品并需要更改您的 SLC(软件许可证号)(请参阅 第 106 页上的更改软件许可证号)时，本主题的其余部分以及本文档中的其他与许可证相关的主题才可能与您相关。

XProtect 视频管理软件产品的许可证(XProtect Essential+ 除外)

软件许可证文件和 SLC

在购买软件和许可证时，您将获得：

- 每封电子邮件都会收到订单确认和以您的 SLC(软件许可证号)命名的软件许可证文件及其 .lic 扩展名
- Milestone Care 覆盖范围

您的 SLC 也印刷在订单确认书上，由多个数字和字母组成(用连字符分组)，类似于：

- 产品版本 2014 或更低：xxx-xxxx-xxxx
- 产品版本 2016 或更高：xxx-xxx-xxx-xx-xxxxxx

软件许可证文件包含有关您购买的视频管理软件产品、XProtect 扩展和许可证的所有信息。Milestone 建议您将有关 SLC 的信息和软件许可证文件的副本存储在安全的地方，以备日后使用。您还可以在 Management Client 中的**许可证信息**窗口中查看 SLC。您可以在**站点导航**窗格 -> **基本**节点 -> **许可证信息**中打开**许可证信息**窗口。例如，在创建 My Milestone 用户帐户、与经销商联系以寻求支持或需要对系统进行更改时，可能需要软件许可证文件或您的 SLC。

安装和许可的总体流程

要开始操作，可从我们的网站(https://www.milestonesys.com/downloads/)下载软件。在安装软件时(请参阅第 126 页上的安装新的 XProtect 系统)，系统会要求您提供软件许可证文件。没有软件许可证文件的话，您无法完成安装。

安装完成并添加了一些摄像机之后，必须激活许可证(请参阅 第 100 页上的许可证激活(已作说明)。您可以从**的**许可证信息 Management Client 窗口激活您的许可证。在这里，您还可以查看同一 SLC 上的所有安装的许可证总览。您可以在**站点导航**窗格 -> **基本**节点 -> **许可证信息**中打开**许可证信息**窗口。

许可证类型

XProtect 许可系统中有几种许可证类型。

基本许可证

您必须至少具有以下其中一个 XProtect 视频管理软件产品的基本许可证。您也可以拥有一个或多个 XProtect 扩展基本许可证。

设备许可证

您必须至少具有多个设备许可证。通常，您需要为每个硬件设备提供一个设备许可证，其中包含您要添加到系统中的摄像机。但是，这可能因硬件设备而异，并且取决于该硬件设备是否为受 Milestone 支持的硬件设备。有关详细信息，请参阅 第 99 页上的支持的硬件设备 和 第 99 页上的不支持的硬件设备。

如果要使用 XProtect Mobile 中的视频推送功能，则每个移动设备或平板电脑还需要一个设备许可证，才能将视频推送到系统。

连接到您摄像机的扬声器、麦克风或输入和输出设备不需要设备许可证。

支持的硬件设备

通常，您需要为每个硬件设备提供一个设备许可证，其中包含您要添加到系统中的摄像机。但是，一些支持的硬件设备需要多个设备许可证。您可以在 Milestone 网站 (https://www.milestonesys.com/support/tools-and-references/supported-devices/) 上的受支持硬件列表中查看硬件设备所需的设备许可证数量。

对于具有多达 16 个通道的视频编码器，每个视频编码器 IP 地址只需要一个设备许可证。一个视频编码器可具有一个或多个 IP 地址。

但是，如果视频编码器具有 16 个以上的通道，则视频编码器上每个激活的摄像机都需要一个设备许可证，前 16 个激活的摄像机也需要一个设备许可证。

不支持的硬件设备

不支持的硬件设备需要使用视频通道为每个激活的摄像机提供一个设备许可证。

不支持的硬件设备不会显示在 Milestone 网站 (https://www.milestonesys.com/support/tools-and-references/supported-devices/) 上支持的硬件列表中。

Milestone Interconnect™ 的摄像机许可证

要运行 Milestone Interconnect，您需要中央站点上的 Milestone Interconnect 摄像机许可证以查看来自远程站点上的硬件设备的视频。所需的 Milestone Interconnect 摄像机许可证数量取决于要从其接收数据的远程站点上的硬件设备的数量。只有 XProtect Corporate 可作为中央站点。

XProtect 扩展许可证

大多数 XProtect 扩展都需要其他许可证类型。软件许可证文件中还包含有关扩展许可证的信息。某些扩展具有自己的单独软件许可证文件。

许可证激活(已作说明)

您的 SLC 必须在安装之前进行注册(请参阅 第 123 页上的注册软件许可证号)。必须激活与 SLC 连接的不同许可证,才能使已安装的 XProtect 视频管理软件和 XProtect 扩展正常工作,并使各个硬件设备能够将数据发送到系统。有关所有 XProtect 许可证类型的总览,请参阅 第 98 页上的许可证类型。

有几种激活许可证的方法。所有这些都在**许可证信息**窗口中提供。激活的最佳方法取决于组织的策略以及您的管理服务器是否可以访问 Internet。要了解如何激活许可证,请参阅 第 103 页上的激活您的许可证。

XProtect视频管理软件的初始许可证激活后,由于 XProtect 许可系统具有内置的灵活性,因此您不必在每次添加带摄像机的硬件设备时都激活设备许可证。有关这些灵活性的详细信息,请参阅 第 100 页上的许可证激活的宽限期(已作说明) 和 第 101 页上的无需激活的设备变更(已解释)。

自动在线激活序列号(已解释)

为了便于在在组织策略允许的情况下进行维护和保持灵活性,Milestone建议您启用自动许可证激活。自动许可证激活需要管理服务器联机。有关如何启用自动许可证激活的信息,请参阅第104页上的启用自动许可证激活。

启用自动许可证激活的好处

- 在添加、删除或更换硬件设备或进行其他影响许可证使用的更改后,系统会在几分钟后激活您的硬件设备。因此,您很少需要手动启动许可证激活。请参阅第100页上的当仍然需要手动激活许可证时中的一些例外。
- “无需激活的设备变更”的已使用次数始终为零。
- 没有任何硬件设备在宽限期内且有过期的风险。
- 如果您的一个基本许可证在 14 天内到期,您的 XProtect 系统也会 - 作为额外的预防措施 - 每晚自动尝试激活您的许可证。

当仍然需要手动激活许可证时

如果您对系统进行以下更改,则需要手动激活许可证。

- 购买更多许可证(请参阅 第 105 页上的获取更多许可证)
- 升级到更新版本或更高级的视频管理软件系统(请参阅 第 323 页上的升级要求)
- 购买或续订 Milestone Care 订阅
- 获得更多无需激活的设备变更的允许(请参阅 第 101 页上的无需激活的设备变更(已解释))

许可证激活的宽限期(已作说明)

安装视频管理软件并添加设备(硬件设备、Milestone Interconnect 摄像机或门许可证)后,如果您决定不启用自动许可证激活,则这些设备将在 30 天的宽限期内运行。在 30 天宽限期结束之前,如果没有更多“无需激活的设备变更”,则必须激活许可证,否则设备将停止向监控系统发送视频。

无需激活的设备变更(已解释)

“无需激活的设备变更”功能为 XProtect 许可系统提供了内置的灵活性。因此，即使您决定手动激活许可证，也不必每次添加或删除硬件设备时都激活许可证。

“无需激活的设备变更”数量随安装而有所不同，基于多个变量进行计算。有关详细说明，请参阅第 101 页上的计算“无需激活的设备变更”数量(已作说明)。

上次激活许可证一年后，您使用“无需激活的设备变更”次数将自动重置为零。在重设之后，您就可以继续添加和更换硬件设备而无需激活许可证。

如果您的监控系统在较长时间内处于脱机状态(例如，监控系统位于长时间巡航的船上，或监控系统位于不具有互联网访问的偏僻位置)，您可以联系 Milestone 经销商并请求更大数量的无需激活的设备变更。

您必须解释为什么您认为自己有资格获得更多数量的无需激活的设备变更。Milestone 将逐个确定每个请求。如果您被授予了更大数量的无需激活的设备变更，您必须在 XProtect 系统上激活许可证以注册这一更大的数量。

计算“无需激活的设备变更”数量(已作说明)

“无需激活的设备变更”的可用数量根据三个变量进行计算。如果您具有 Milestone 软件的多个安装实例，则这些变量适用于其中的每一个。变量包括：

- **C%**，这是激活的许可证总数的固定百分比
- **Cmin**，这是“无需激活的设备变更”数量的固定最小值
- **Cmax**，这是“无需激活的设备变更”数量的固定最大值

“无需激活的设备变更”数量绝不能小于 **Cmin** 值或大于 **Cmax** 值。基于 **C%** 变量计算的值将随您已在系统中每个安装上激活的设备数量而有所不同。通过“无需激活的设备变更”添加的设备不计为由 **C%** 变量激活。

Milestone 定义了所有这三个变量的值，这些值取决于无需激活的变更。这些变量的值随产品而有所不同。

基于 %= 15%、Cmin = 10、Cmax = 100 的示例

您购买 100 个设备许可证。然后，您将 100 个摄像机添加到系统中。除非您已经启用自动许可证激活，否则“无需激活的设备变更”数量仍然为零。您激活了许可证，现在有 15 个“无需激活的设备变更”。

您购买 100 个设备许可证。然后，您将 100 个摄像机添加到系统并激活许可证。“无需激活的设备变更”现在数量为 15。然后，您决定从系统中删除硬件设备。您现在有 99 个已激活的设备，“无需激活的设备变更”数量已降至 14。

您购买 1000 个设备许可证。然后，您添加 1000 个摄像机并激活许可证。“无需激活的设备变更”数量现在为 100。根据 **C%** 变量，您现在应该有 150 个“无需激活的设备变更”，但是 **Cmax** 变量只允许您有 100 个“无需激活的设备变更”。

您购买 10 个设备许可证。然后，您将 10 个摄像机添加到系统并激活许可证。由于 **Cmin** 变量，您“无需激活的设备变更”数量现在为 10。如果仅根据 **C%** 变量计算数字，则您只有 1 (15% 的 10 = 1.5，舍入为 1)。

您购买 115 个设备许可证。然后，您将 100 个摄像机添加到系统并激活许可证。您现在的“无需激活的设备变更”为 15。您使用 15 个“无需激活的设备变更”中的 15 个，添加了 15 个设备变更而不激活。现在，您从系统中删除了 50 个摄像机，“无需激活的设备变更”数量降至 7。这意味着先前使用 15 个“无需激活的设备变更”添加的摄像机中有 8 个进入了宽限期。现在，您添加了 50 个新摄像机。由于您上次激活许可证时在系统上激活了 100 个摄像机，因此“无需激活的设备变更”数量回到 15，而先前移入宽限期的 8 个摄像机现在又作为无需激活的设备变更移回来。50 个新摄像机进入宽限期。

Milestone Care™(已作说明)

Milestone Care 是产品在其整个生命周期内 XProtect 的完整服务和支持计划的名称。

您可以通过Milestone Care访问我们的支持网站 (https://www.milestonesys.com/support/) 上不同类型的自助材料，例如知识库文章、指南和教程。

如需其他优惠，您可以购买更多提前Milestone Care订阅。

Milestone Care Plus

如果您有Milestone Care Plus订阅，您还可以访问当前 XProtect VMS 产品的免费更新，并且可以以优惠的价格升级到更高级的 XProtect VMS 产品。Milestone Care Plus 还提供其他功能：

- 客户仪表板服务
- 智能连接功能
- 完整的推送通知功能

Milestone Care Premium

如果您具有 Milestone Care Premium 订阅，也可以联系 Milestone 支持以请求帮助。与 Milestone Care 支持人员联系时，请记住提供有关您的 Milestone ID 的信息。

高级Milestone Care订阅的到期、续订和购买

在Milestone Care Plus已安装产品Milestone Care Premium表的**许可证信息**窗口中，可以看到更高级 **和** 订阅类型的到期日期。请参阅 第 107 页上的已安装产品。

如果在安装系统后决定购买或续订 Milestone Care 订阅，则必须手动激活许可证，然后显示正确的 Milestone Care 信息。请参阅 第 104 页上的联机激活许可证 或 第 105 页上的脱机激活许可证。

许可证和硬件更换(已作说明)

如果系统中的摄像机出现故障，或者您由于其他原因而要更换新摄像机，则以下是一些最佳做法。

如果从记录服务器中删除摄像机，则可以释放设备许可证，但是您也将失去对所有数据库(摄像机、麦克风、输入、输出)和旧摄像机设置的完全访问权限。要保留对旧摄像机数据库的访问权，并在将旧摄像机更换为新摄像机时重新使用其设置，请使用以下相关选项。

更换摄像机时使用相同的摄像机

如果用相同(制造商、品牌和型号)的摄像机进行更换,并且为新摄像机提供与旧摄像机相同的 IP 地址,则您将保留对旧摄像机所有数据库的完全访问权限。新摄像机继续使用与旧摄像机相同的数据库和设置。在这种情况下,您可以将网络电缆从旧摄像机移动到新摄像机,而无需更改 Management Client 中的任何设置。

更换摄像机时使用其他摄像机

如果用其他(制造商、品牌和型号)的摄像机进行更换,则必须使用**更换硬件**向导(请参阅 第 298 页上的更换硬件)将旧摄像机的所有相关数据库映射到新摄像机,并重新使用旧摄像机的设置。

更换硬件后激活许可证

如果已启用自动许可证激活(请参阅 第 104 页上的启用自动许可证激活),则新摄像机会自动激活。

如果禁用了自动许可证激活,并且使用了所有无需激活的设备变更(请参阅 第 101 页上的无需激活的设备变更(已解释)),您必须手动激活许可证。有关手动激活许可证的详细信息,请参阅 第 104 页上的联机激活许可证 或 第 105 页上的脱机激活许可证。

获取您的许可证总览

您有很多原因想要获得 SLC 的总览、购买的许可证数量及其状态。以下是其中一部分:

- 您想添加一个或多个新的硬件设备,但您是否有未使用的设备许可证,还是必须购买新的设备许可证?
- 您的部分硬件设备的宽限期是否即将结束?然后,您必须先激活它们,它们才会停止将数据发送到视频管理软件。
- 您可以从以前的联系支持人员那里得知,他们需要有关您的 SLC 和 Milestone Care ID 的信息才能为您提供帮助。但它们是哪些?
- 您安装了许多 XProtect,并且所有安装使用相同的 SLC,但是使用的许可证在哪里,它们的状态如何?

您可以在**许可证信息**窗口中找到以上所有信息以及详细信息。

您可以在**站点导航**窗格 -> **基本**节点 -> **许可证信息**中打开**许可证信息**窗口。

要了解更多有关**许可证信息**窗口中可用的各种信息和功能的详情,请参阅 第 107 页上的"许可证信息"窗口。

激活您的许可证

有几种激活许可证的方法。所有这些都在**许可证信息**窗口中提供。激活的最佳方法取决于组织的策略以及您的管理服务器是否可以访问 Internet。

您可以在**站点导航**窗格 -> **基本**节点 -> **许可证信息**中打开**许可证信息**窗口。

要了解更多有关**许可证信息**窗口中可用的各种信息和功能的详情,请参阅 第 107 页上的"许可证信息"窗口。

启用自动许可证激活

为了便于在在组织策略允许的情况下进行维护和保持灵活性，Milestone 建议您启用自动许可证激活。自动许可证激活需要管理服务器联机。

如果您想了解启用自动许可证激活的所有好处，请参阅 第 100 页上的自动在线激活序列号(已解释)。

1. 从**站点导航**窗格 -> **基本**节点 -> **许可证信息**中，选择**启用自动许可证激活**。
2. 输入要用于自动许可证激活的用户名和密码：
   - 如果您是现有用户，请输入您的用户名和密码登录到软件注册系统
   - 如果您是新用户，请单击**创建新用户**链接建立新用户帐户，然后按照注册步骤进行操作。如果您尚未注册软件许可证号 (SLC)，则必须进行注册

   这些凭据保存在管理服务器上的文件中。
3. 单击**确定**。

如果您之后需要更改用于自动激活的用户名和/或密码，请单击**编辑激活凭据**链接。

禁用自动许可证激活

如果不允许在组织中使用自动许可证激活，或者您改变了主意，则可以禁用自动许可证激活。

禁用方式取决于您以后是否计划再次使用自动许可证激活。

禁用但保留密码以备后用：

1. 从**站点导航**窗格 -> **基本**节点 -> **许可证信息**中，清除**启用自动许可证激活**。用户名和密码仍将保存在管理服务器上。

禁用和删除密码：

1. 从**站点导航**窗格 -> **基本**节点 -> **许可证信息**中，单击**编辑激活凭据**。
2. 单击**删除密码**。
3. 确认您要从管理服务器删除用户名和密码。

联机激活许可证

如果管理服务器可以访问 Internet，但您希望手动启动激活过程，则这是最简单的许可证激活选项。

1. 从**站点导航**窗格 -> **基本**节点 -> **许可证信息**中，选择**手动激活许可证**，然后选择**联机**。
2. 会打开**联机激活**对话框：
   - 如果您是现有用户，请输入您的用户名和密码
   - 如果您是新用户，请单击**创建新用户**链接建立新用户帐户。如果您尚未注册软件许可证号 (SLC)，则必须进行注册
3. 单击**确定**。

如果在联机激活期间收到错误消息，请遵照屏幕说明解决问题或者联系 Milestone 支持。

脱机激活许可证

如果您的组织不允许管理服务器访问 Internet，则必须手动和离线激活许可证。

1. 从**站点导航**窗格 -> **基本**节点 -> **许可证信息**中，选择**手动激活许可证 > 脱机 > 导出要激活的许可证**来导出许可证请求文件 (.lrq)，其中包含您已添加的硬件设备的信息。
2. 系统将自动为许可证请求文件 (.lrq) 提供与 SLC 相同的名称。如果您具有多个站点，请记住重命名文件，以便能够轻松确定哪个文件属于哪个站点。
3. 将许可证请求文件复制到具有互联网访问的计算机，并登录我们的网站 (https://online.milestonesys.com/) 以获取激活的软件许可证文件 (.lic)。
4. 使用 Management Client 将收到的 .lic 文件复制到您的计算机。该文件的名称与您的许可证请求文件的名称相同。
5. 在**站点导航**窗格 -> **基本** 节点 -> **许可证信息**中，选择**脱机激活许可证 > 导入激活的许可证**，然后选择激活的软件许可证文件以将其导入，从而激活您的许可证。
6. **单击**完成以结束激活过程。

在宽限期之后激活许可证

如果您决定使用手动许可证激活，而忘记了在宽限期内激活许可证（硬件设备、Milestone Interconnect 摄像机或门许可证），则设备会变得不可用且无法向监控系统发送数据：

即使许可证的宽限期已过期，激活许可证后，也会保存并使用您进行的设备配置和设置。

要再次启用不可用的设备，请以您的首选方式手动激活许可证。有关详细信息，请参阅 第 105 页上的脱机激活许可证 或 第 104 页上的联机激活许可证。

获取更多许可证

如果要添加，或者已经添加了比当前许可证更多的硬件设备、Milestone Interconnect 系统、门或其他元素，则必须购买其他许可证以使它们能够将数据发送到系统：

- 要得到本系统的更多许可证，请联系您的 XProtect 产品经销商

如果您购买了现有监控系统版本的新许可证：

- 只需手动激活许可证即可访问新许可证。有关详细信息，请参阅 第 104 页上的联机激活许可证 或 第 105 页上的脱机激活许可证。

如果您购买了新许可证和升级的监控系统版本：

- 您会收到更新的软件许可证文件 (.lic)，其中包含新许可证和新版本。必须在安装新版本期间使用新软件许可证文件。有关详细信息，请参阅 第 323 页上的升级要求。

更改软件许可证号

如果您是以临时的软件许可证号 (SLC) 运行安装或如果您已经升级到更高级的 XProtect 产品，您可以将 SLC 更改为永久的或更高级的 SLC。当您收到信的软件许可证文件时，您可以更改您的 SLC，无需任何卸载或重新安装操作。

您可以在管理服务器上本地完成或从 Management Client 远程完成该操作。

从管理服务器托盘图标中

1. 在管理服务器上，转到任务栏的通知区域。

2. 右键单击**管理服务器**图标，选择**更改许可证**。
3. **单击**导入许可证。
4. 接着选择为此目的保存的软件许可证文件。完成后，已选择的软件许可证文件位置将添加在**导入许可证**按钮下方。
5. 单击**确定**即会做好注册 SLC 的准备。请参阅 第 123 页上的注册软件许可证号。

从 Management Client

1. 使用 Management Client 将收到的 .lic 文件复制到您的计算机。
2. 在**站点导航**窗格 -> **基本** 节点 -> **许可证信息**中，选择**脱机激活许可证 > 导入激活的许可证**，然后选择软件许可证文件以将其导入。
3. 打开时，要接受软件许可证文件与目前使用的不同。
4. 您现在已经准备好注册 SLC。请参阅 第 123 页上的注册软件许可证号。

软件许可证文件只会被导入并更改，不会被激活。记得激活您的许可证。有关详细信息，请参阅 第 103 页上的激活您的许可证。

在运行 XProtect Essential+ 时，您只能从管理服务器托盘图标更改许可证。不能从 Management Client 更改许可证。

“许可证信息”窗口

在**许可证信息**窗口中，您可以跟踪在此站点和所有其他站点上共享相同软件许可证文件的所有许可证、您的 Milestone Care 订阅，并确定要如何激活许可证。

您可以在**站点导航**窗格 -> **基本**节点 -> **许可证信息**中打开**许可证信息**窗口。

如果您想全面了解 XProtect 许可系统的工作原理，请参阅 第 98 页上的许可证(已解释)。

已将许可授予

许可证信息窗口的此区域列出了在软件注册期间输入的许可证所有者的详细联系信息。

如果看不到**许可到**区域，请单击窗口右下角的**刷新**按钮。

单击**编辑详细信息**可编辑许可证所有者信息。单击**最终用户许可协议**以查看您在安装之前接受的最终用户许可协议。

Milestone Care

在这里您可以看到有关您当前的 Milestone Care™ 订阅的信息、订阅的到期日期显示在下面的**已安装产品**表中。

有关 Milestone Care 的详细信息，请使用链接或参阅 第 102 页上的 Milestone Care™(已作说明)。

已安装产品

列出有关共享相同软件许可证文件的 XProtect VMS 和 XProtect 扩展的所有已安装基本许证的以下信息：

- 产品和版本
- 产品的软件许可证号 (SLC)
- SLC 的到期日期。通常无限制
- Milestone Care Plus 订阅的到期日期
- Milestone Care Premium 订阅的到期日期

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 20 R	M01-C01-211-01-	Unlimited	16-11-20	16-11-20
Milestone XProtect Smart Wall	M01-P03-100-01-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08-100-01-	Unlimited	Unlimited	

许可证概述 - 所有站点

列出软件许可证文件中已激活的设备许可证和其他许可证的数量，以及系统上可用许可证的总数。在这里，可以很容易地了解到是否可以在不购买额外许可证的情况下扩展系统。

有关在其他站点上激活的许可证的详细状态概述，请单击**授权详细信息 - 所有站点**链接。有关显示的可用信息，请参阅下面的**许可证详细信息 - 当前站点**部分。

License Overview - All sites License Details - All Sites...

License Type	Activated
Device Licenses	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

如果您有 XProtect 扩展的许可证，则可以在**站点导航**窗格中特定于 XProtect 扩展的节点下查看有关这些扩展的更多详细信息。

许可证详细信息 - 当前站点

已激活列列出了此站点上已激活的设备许可证或其他许可证的数量。

您还可以在**无需激活的变更**列中查看已使用的“无需激活的设备变更”的数量(请参阅 第 101 页上的无需激活的设备变更(已解释))，以及每年的可用数量。

如果您具有尚未激活且因此在宽限期内运行的许可证，则这些许可证将于**在宽限期内**列中列出。到期的第一个许可证的到期日期在表下显示为红色。

如果您忘记在宽限期到期前激活许可证，它们将停止向系统发送视频。这些许可证将显示在**宽限期已过期**列中。有关详细信息，请参阅 第 105 页上的在宽限期之后激活许可证。

如果您的已用许可证数量多于可用许可证数量，则这些许可证将列在**无许可证**列中，并且无法用于您的系统中。有关详细信息，请参阅 第 105 页上的获取更多许可证。

如果您在宽限期内有许可证、宽限期已过期或没有许可证，则每次登录ManagementClient时都会有一条消息提醒您。

License Details - Current Site:

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Device Licenses	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

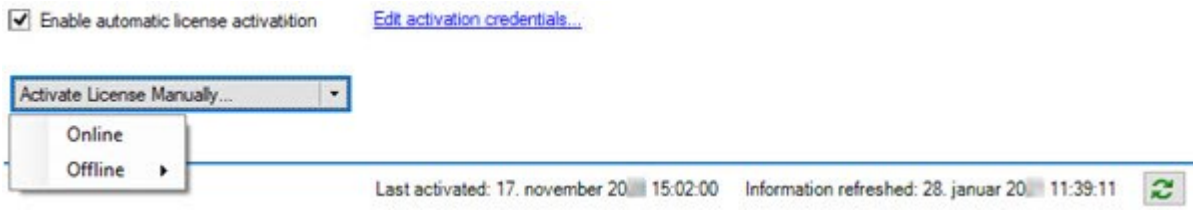
如果您的硬件设备使用多个许可证，则**许可证详细信息 - 当前站点**表下方会出现**单击此处打开完整的设备许可证报告**链接。单击链接时，您可以看到每个硬件设备需要多少个设备许可证。

无许可证的硬件设备在 Management Client 中由感叹号标识。感叹号也用于其他目的。将鼠标移到感叹号上可查看其用途。

用于激活许可证的功能

以下三个表用于：

- 用于启用自动许可证激活的复选框，以及用于编辑在自动激活期间使用的用户凭据的链接。有关详细信息，请参阅 第 100 页上的自动在线激活序列号(已解释) 和 第 104 页上的启用自动许可证激活。
  如果自动激活已失败，将会出现红色的失败消息。有关详细信息，请单击**详细信息**链接。
  有些许可证(如 XProtect Essential+)在启用自动许可证激活时安装，无法禁用该设置。
- 用于手动联机或脱机激活许可证的下拉列表。有关详细信息，请参阅 第 104 页上的联机激活许可证 和 第 105 页上的脱机激活许可证。
- 在窗口右下角，您可以查看许可证的上次激活(自动或手动)时间以及窗口信息的刷新时间。时间戳来自服务器而非本地计算机

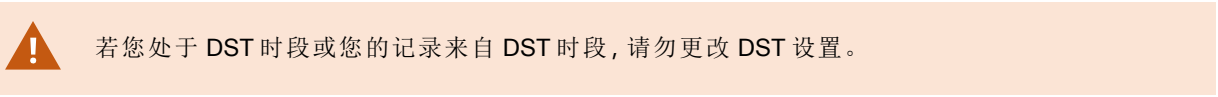


要求和注意事项

夏时制(已解释)

夏时制 (DST) 是一种调快时钟的制度，以延长夜晚利用日光的时间并缩短早晨利用日光的时间。各国家/地区所使用的 DST 不尽相同。

监控系统对于时间极为敏感，在使用时应了解系统处理 DST 的方法，这点极为重要。



若您处于 DST 时段或您的记录来自 DST 时段，请勿更改 DST 设置。

春季：从标准时间切换至 DST

从标准时间切换至 DST 并不复杂，只需将时钟调快一小时即可。

示例：

时钟从标准时间 02:00 调快至 DST 03:00，因此每天就只有 23 个小时。在这种情况下，由于一天中清晨 02:00 至 03:00 这一个小时已不存在，因此该时段不会记录任何数据。

秋季：从 DST 切换至标准时间

在秋季，要从 DST 切换至标准时间，只需将时钟调慢一小时。

示例：

时钟从 DST 02:00 调慢至标准时间 01:00，重复了这一小时，因此一天将会有 25 个小时。时钟在指向 01:59:59 后会立即返回至 01:00:00。如系统不做处理，一般会重复记录这个小时的数据，因此 01:30 的首次记录将被 01:30 的第二次记录覆盖。

为避免发生这样的问题，当系统时间更改超过五分钟时，本系统即会将当前视频存档。您无法在任何客户端直接查看 01:00 小时的第一次记录，但数据已被记录且安全。您可以通过直接打开存档数据库，在 XProtect Smart Client 中浏览该视频。

时间服务器(已解释)

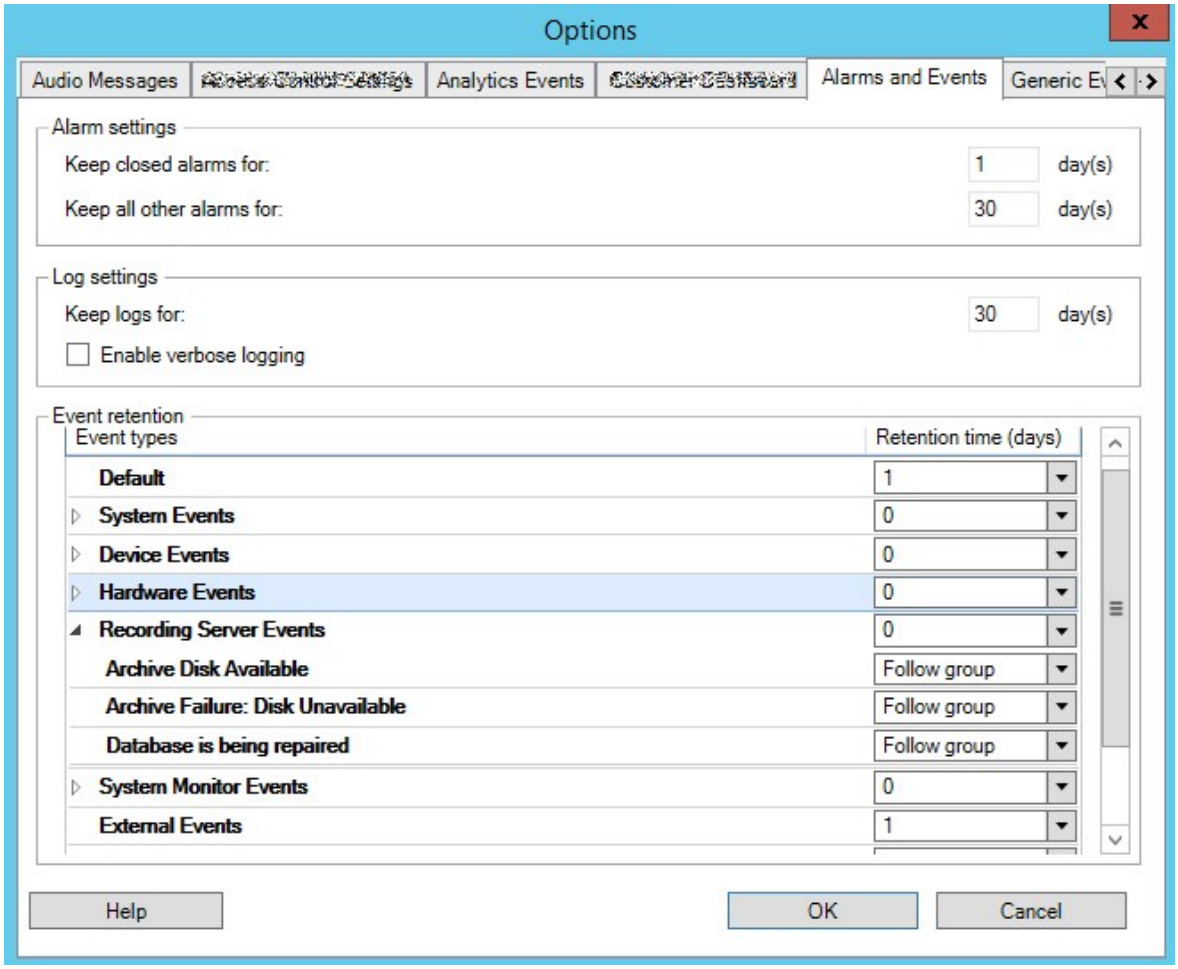
一旦本系统接收到图像，会立即为其添加时间标记。由于摄像机是单独的设备，可能拥有单独的计时设备，因此摄像机时间和本系统时间可能不完全相符。这样可能导致时间混乱。如果摄像机支持时间标记，Milestone 建议通过时间服务器自动同步摄像机和系统时间，以确保稳定同步。

有关如何配置时间服务器的信息，请尝试在 Microsoft 网站 (https://www.microsoft.com/) 上搜索“**时间服务器**”、“**时间服务**”或类似关键词。

限制数据库的大小

为避免 SQL Server 数据库(请参阅 第 32 页上的SQL Server 安装和数据库(已说明) 和数据库)变大到影响系统性能，您可以指定不同类型的事件和警报在数据库中存储的天数。

1. 打开**工具**菜单。
2. 单击**选项>警报和事件**选项卡。



3. 进行必需的设置。有关详细信息，请参阅 第 342 页上的“警报和事件”选项卡(选项)。

IPv6 和 IPv4(已解释)

本系统支持 IPv6 和 IPv4。XProtect Smart Client 也是如此。

IPv6是最新版本的互联网协议(IP)。互联网协议确定IP地址的格式和使用。IPv6与目前仍广泛使用的IP版本IPv4共存。IPv6的开发目的是解决IPv4地址耗尽问题。IPv6地址的长度为128位，而IPv4地址的长度仅为32位。

这意味着互联网通讯簿从 430 亿个唯一地址增长到 340 涧(1 涧 = 10 的 36 次方)个地址。增长系数达 79 千秭(1 千秭 = 10 的 48 次方)。

已有越来越多的组织在网络中实施 IPv6。例如，美国所有联邦机构基础设施均被要求兼容 IPv6。该手册中的示例和图示反映了 IPv4 的使用情况，因为它仍然是使用最广泛的 IP 版本。IPv6 在本系统上也能同样良好地工作。

使用 IPv6 的系统(已解释)

结合 IPv6 使用本系统时，应满足以下条件：

服务器

服务器通常可以使用 IPv4 和 IPv6。但是，如果您的系统中仅有一台服务器(例如管理服务器、记录服务器或故障转移记录服务器)需要特定 IP 版本，那么系统中所有其他服务器都必须使用相同 IP 版本进行通信。

示例：本系统中的所有服务器(其中一个除外)都能使用 IPv4 和 IPv6。例外的服务器只能使用 IPv6。这就意味着所有服务器都必须使用 IPv6 彼此通信。

设备

可以使用 IP 版本不同于网络设备提供用于服务器通信的 IP 版本的设备(摄像机、输入、输出、麦克风、扬声器)，并且记录服务器还支持设备的 IP 版本。另请参阅以下图示。

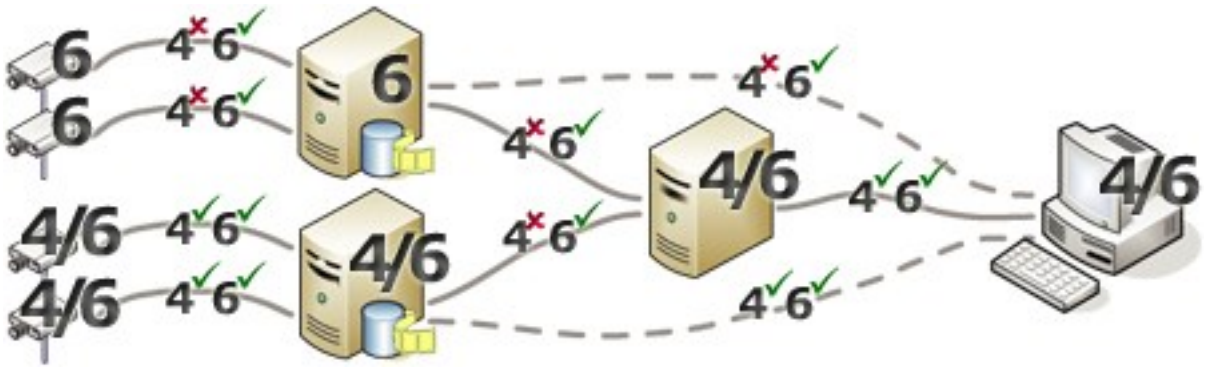
客户端

如果您的系统使用 IPv6，则用户应使用 XProtect Smart Client 进行连接。XProtect Smart Client 支持 IPv6 和 IPv4。

如果您系统中的一个或多个服务器**只能**使用 IPv6，那么 XProtect Smart Client 用户**必须**使用 IPv6 才能与这些服务器通信。在这种情况下，请记住，XProtect Smart Client 安装在技术层面连接到管理服务器进行初始身份验证，然后连接到所需记录服务器以访问录像。

然而，XProtect Smart Client 用户自己不必位于 IPv6 网络上，前提条件是网络设备支持不同 IP 版本之间的通信，并且已在其计算机上安装 IPv6 协议。另请参阅图示。要在客户端计算机上安装 IPv6，请打开命令提示符，输入 ***Ipv6 install***，然后按 **ENTER**。

示例图



示例：由于本系统中的一个服务器仅使用 IPv6，因此与该服务器的所有通信都必须使用 IPv6。然而，该服务器还确定系统中所有其他服务器之间进行通信的 IP 版本。

写入 IPv6 地址(已解释)

IPv6 地址通常写为八个块，每个块包含四个十六进制数字，由冒号分隔。

示例：*2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

可以通过去掉块中的前导零来缩短地址。另请注意，某些四位数字块可能仅包含零。如果连续出现任意数量的此类 0000 块，则可以通过将 0000 块替换为两个冒号来缩短地址(只要地址中只有一个这样的双冒号)。

示例:
2001:0B80:0000:0000:0000:0F80:3FA8:18AB 可以缩短为

2001:B80:0000:0000:0000:F80:3FA8:18AB(删除前导零) 或

2001:0B80::0F80:3FA8:18AB(删除 0000 块) 或者甚至

2001:B80::F80:3FA8:18AB(删除前导零和 0000 块) 。

在 URL 中使用 IPv6 地址

IPv6 地址包含冒号。然而, 冒号也用于其他类型的网络寻址语句。例如, IPv4 使用冒号来分隔 IP 地址和端口号 (在它们均用于 URL 中时) 。IPv6 继承了这一原则。因此, 为避免混淆, 在 IPv6 地址用于 URL 中时, 在其周围添加方括号。

包含 IPv6 地址的 URL 的**示例**:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB], 它当然可以缩短为(例如) *http://[2001:B80::F80:3FA8:18AB]*

包含 IPv6 地址和端口号的 URL 的**示例**:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234, 它当然可以缩短为(例如) *http://[2001:B80::F80:3FA8:18AB]:1234*

有关 IPv6 的详细信息, 请参阅(例如) IANA 网站 (https://www.iana.org/numbers/)。IANA(互联网编号分配机构) 是负责 IP 寻址全球协调的机构。

虚拟服务器

您可以在虚拟化 Windows® 服务器上运行所有系统组件, 如 VMware® 和 Microsoft® Hyper-V®。

为了更好地利用硬件资源, 使用虚拟化是更好的选择。通常情况下, 运行在硬件主机服务器上的虚拟服务器并不利用太多资源来加载虚拟服务器, 并且通常不会同时进行。然而, 记录服务器会记录所有摄像机和视频流。这会造成 CPU、内存、网络和存储系统负载过高。因此, 在虚拟服务器上运行时, 虚拟化的一般优势会在很大程度上消失, 这在很多情况下都是因为它会使用所有可用资源。

如果在虚拟环境中运行, 则务必确保硬件主机的物理内存量与为虚拟服务器分配的物理内存量相同, 并且为运行记录服务器的虚拟服务器分配足够CPU和内存;默认情况下并非如此。通常, 记录服务器需要2-4GB, 具体取决于配置。另一个瓶颈是网络适配器分配和硬盘性能。应考虑在运行记录服务器的虚拟服务器的主机服务器上分配物理网络适配器。这样, 便可以更加轻易地确保对于发送到其他虚拟服务器的通信, 不会造成网络适配器过载。如果网络适配器用于多个虚拟服务器, 则网络通信可能导致记录服务器无法检索和录制所配置数量的图像。

多台管理服务器(群集) (已解释)

管理服务器可安装到服务器群集中的多台服务器上。这样可确保非常短的系统停机时间。如果群集中有服务器出现故障, 群集中的另一个服务器将自动接管故障服务器运行管理服务器的作业。

只能为每个监控安装设置一台活动管理服务器, 但可以安装其他管理服务器以便在发生故障时接管。

默认情况下，Management Server 服务将故障转移的次数限制为六小时内两次。如果超过此值，Management Server 服务便不会由群集服务自动启动。可以更改此限制以更好地满足您的需求。

群集要求

- 搭载Microsoft Windows Server 2016 或更高版本的两台计算机。确保：
  - 要添加为群集节点的所有服务器都在运行相同版本的 Windows Server
  - 要添加为群集节点的所有服务器都加入同一个域
  - 您可以作为本地管理员登录到 Windows 帐户

  关于 Microsoft Windows 服务器中的群集，请参阅故障转移群集 https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster。
- Microsoft SQL Server 安装

  安装于服务器群集外的**外部** SQL Server 和数据库**或**服务器群集中的**内部** SQL Server 服务（群集）（创建内部 SQL Server 服务要求使用能够用作群集 Microsoft® SQL Server® Standard 的 Microsoft® SQL Server® Enterprise 或 SQL Server 版本。

  将管理服务器连接到数据库时，视系统配置密码设置而定，可能会要求您提供当前的系统配置密码。请参阅 第 288 页上的系统配置密码（已解释）。

如果您在故障转移群集环境中工作，建议您在 Server Configurator 中启动任务。这是因为在应用更改时 Server Configurator 可能需要停止服务，并且故障转移群集环境可能会干扰此操作。

保护记录数据库免遭损坏

摄像机数据库可能已损坏。有几个数据库修复选项可解决该问题。Milestone 建议您采取措施，确保摄像机数据库免遭损坏。

硬盘故障：保护驱动器

硬盘驱动器属于机械设备，容易受到外部因素的影响。下面是可能损坏硬盘驱动器并导致摄像机数据库受损的外部因素的示例：

- 振动（确保监控系统服务器及其周围环境都处于稳定状态）
- 高温（确保服务器的通风状况良好）
- 强磁场（避免）

- 停电(确保使用不间断电源 (UPS))
- 静电(确保处理硬盘驱动器时您处于接地保护下)
- 火、水等 (避免)

Windows 任务管理器:在结束进程时请务必小心

当在 Windows 任务管理器下操作时,切勿结束会影响监控系统的任何进程。如果通过单击 Windows 任务管理器中的**结束进程**来结束某个应用程序或系统服务,则进程会被直接终止,不会保存其状态或数据。这可能损坏摄像机数据库。

通常,Windows 任务管理器会在您尝试结束某个进程时显示警告。除非您确定结束该进程不会影响监控系统,否则当系统显示警告消息询问是否确实要终止进程时,请单击**否**。

断电:使用 UPS

数据库受损的一个最常见的原因是记录服务器突然关闭,导致文件没有被保存,操作系统没有正常关闭。造成这种情况可能是由于停电、有人无意中拔掉服务器的电源线或类似事件。

避免记录服务器免遭意外关闭的最好方法是为每台记录服务器配备一台 UPS(不间断电源)。

作为电池驱动的二次电源,UPS 可在电源不稳定的时候为保存打开的文件以及安全关闭系统提供必要的电源。UPS 设计各异,但大多数的 UPS 所包含的软件都可自动保存打开的文件、向系统管理员发出警报等。

针对组织的环境选择适合类型的 UPS 是一个单独的处理过程。但在评估您的需求时,必须切记您需要 UPS 在突然断电时能够供电维持的运行时间。保存打开的文件并正常关闭操作系统可能需要几分钟的时间。

SQL Server 数据库交易日志(已解释)

每次将更改写入 SQL Server 数据库时,SQL Server 数据库都会将此更改记录在其交易日志中。

使用交易日志,您可以通过 Microsoft® SQL Server Management Studio 回滚和撤消对 SQL Server 数据库的更改。默认情况下,SQL Server 数据库会无限期地存储其交易日志,这意味着在经过一段时间后交易日志会累积越来越多的条目。默认情况下,交易日志位于系统驱动器中,并且如果交易日志持续增长,最终可能会使 Windows 无法正常运行。

要避免此类情形,建议定期刷新交易日志。刷新并不会使交易日志文件变小,但可清除其内容,从而避免其增长到超出控制的程度。您的视频管理软件系统不会刷新交易日志。在 SQL Server 中,有多种刷新交易日志的方法。访问 Microsoft 支持页面 https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017,然后搜索*交易日志截断*。

最低系统要求

有关各种视频管理软件应用程序和系统组件的系统要求的信息,请转到 Milestone 网站 (https://www.milestonesys.com/systemrequirements/)。

开始安装前

Milestone 建议您在正式开始安装前先阅读下一章节中所述要求。

准备服务器和网络

操作系统

确保所有服务器都具有全新安装的 Microsoft Windows 操作系统，并且使用最新的 Windows 更新对其执行更新。

有关各种视频管理软件应用程序和系统组件的系统要求的信息，请转到 Milestone 网站 (https://www.milestonesys.com/systemrequirements/)。

Microsoft® .NET Framework

检查所有服务器是否都已安装 Microsoft.NET Framework 4.8 或更高版本。

网络

分配静态 IP 地址或对所有系统组件和摄像机进行 DHCP 保留。为确保网络上有足够的带宽可用，您必须了解系统如何以及何时消耗带宽。网络上的主要负载包括三个元素：

- 摄像机视频流
- 客户端显示视频
- 录制视频的存档

记录服务器从摄像机检索视频流，这会导致网络恒定负载。用于显示视频的客户端会占用网络带宽。如果客户端视图内容没有发生变化，则负载是恒定的。视图内容中的变更、视频搜索或播放会使负载动态化。

录制视频的存档是选配功能，当计算机中的内存系统无足够的空间时，该功能可以让系统将录制视频移到网络存储。这是一个需制定相应计划的作业，您必须对其进行定义。通常情况下，您存档到网络驱动器，这使其成为网络上计划的动态负载。

您的网络必须具备带宽余量，以应对这些峰值流量。这可增强系统响应能力和总体用户体验。

准备 Active Directory

如果希望通过 Active Directory 服务向系统添加用户，则网络上必须存在已安装 Active Directory 并充当域控制器的服务器。

为了便于进行用户和组管理，Milestone 建议在安装 XProtect 系统之前安装并配置 Microsoft Active Directory®。如果在安装系统后将管理服务器添加至 Active Directory，则必须重新安装管理服务器，并使用在 Active Directory 中定义的新 Windows 用户来替换用户。

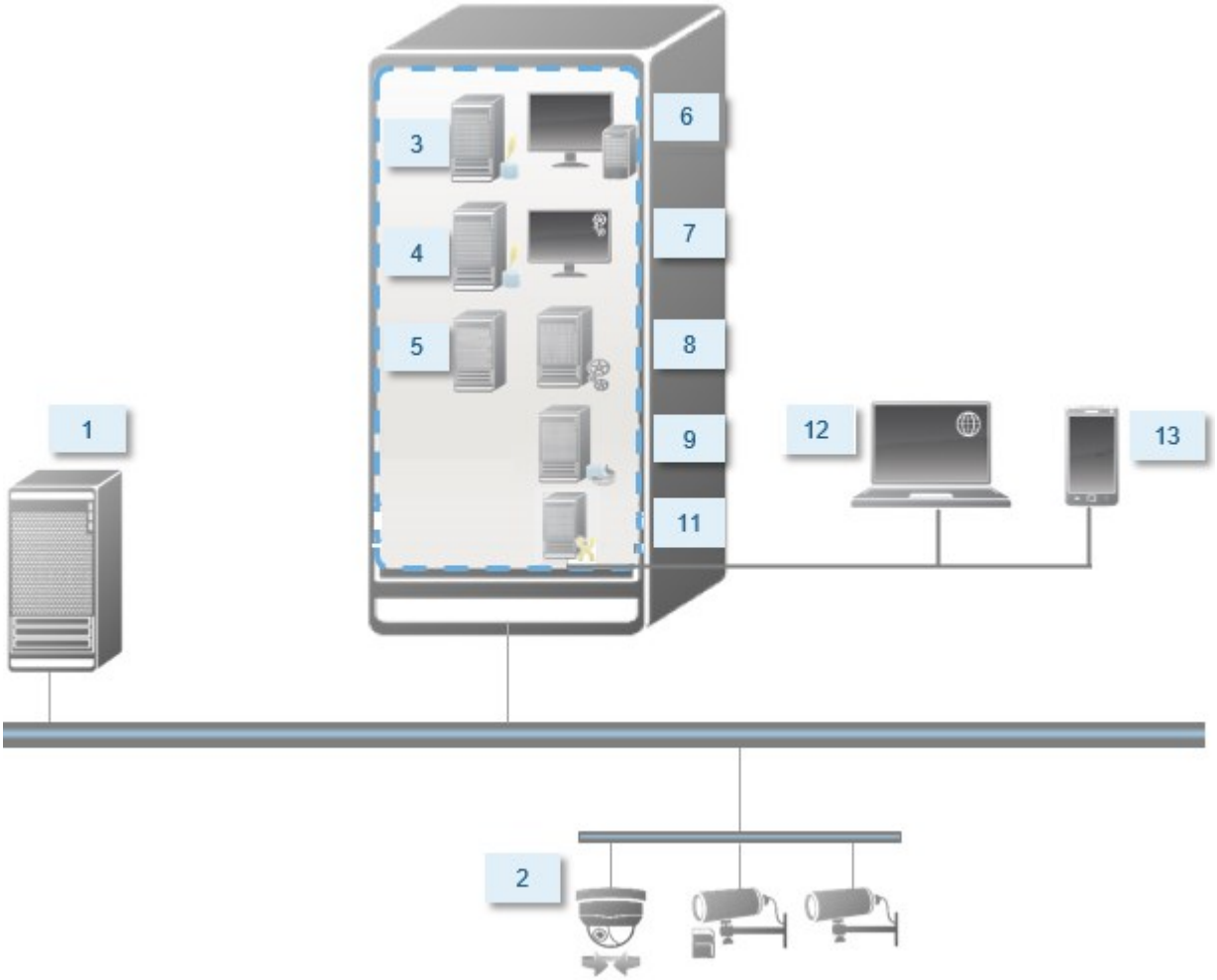
基本用户在 Milestone Federated Architecture 系统中不受支持，因此，如果您计划在系统中使用Milestone Federated Architecture，您必须通过 Active Directory 服务将用户添加为 Windows 用户。如果不安装 Active Directory，则在安装时执行 第 152 页上的工作组安装 中所述的步骤。

安装方法

在安装向导中，您必须决定要使用的安装方式。应根据组织的需要进行选择，但是您很可能已在购买系统时确定了方法。

选项	说明
单台计算机	在当前计算机上安装所有服务器和客户端组件以及 SQL Server。 安装完成后，您可以通过向导配置系统。如果您同意继续，则记录服务器会扫描您的网络以查找硬件，然后您可以选择将哪些硬件设备添加到您的系统中。可以在配置向导中添加的最大硬件设备数取决于您的基本许可证。此外，摄像机在视图中预配置，而且系统会创建默认操作员角色。安装后，XProtect Smart Client 会打开，您可以随时使用系统。
自定义	管理服务器将始终在系统组件列表中被选中并始终进行安装，但您可以在其他服务器和客户端组件中自由选择要在当前计算机上安装的项。 默认情况下不会在组件列表中选中记录服务器，但您可更改此默认设置。您之后可以在其他计算机上安装未选中的组件。

单台计算机安装

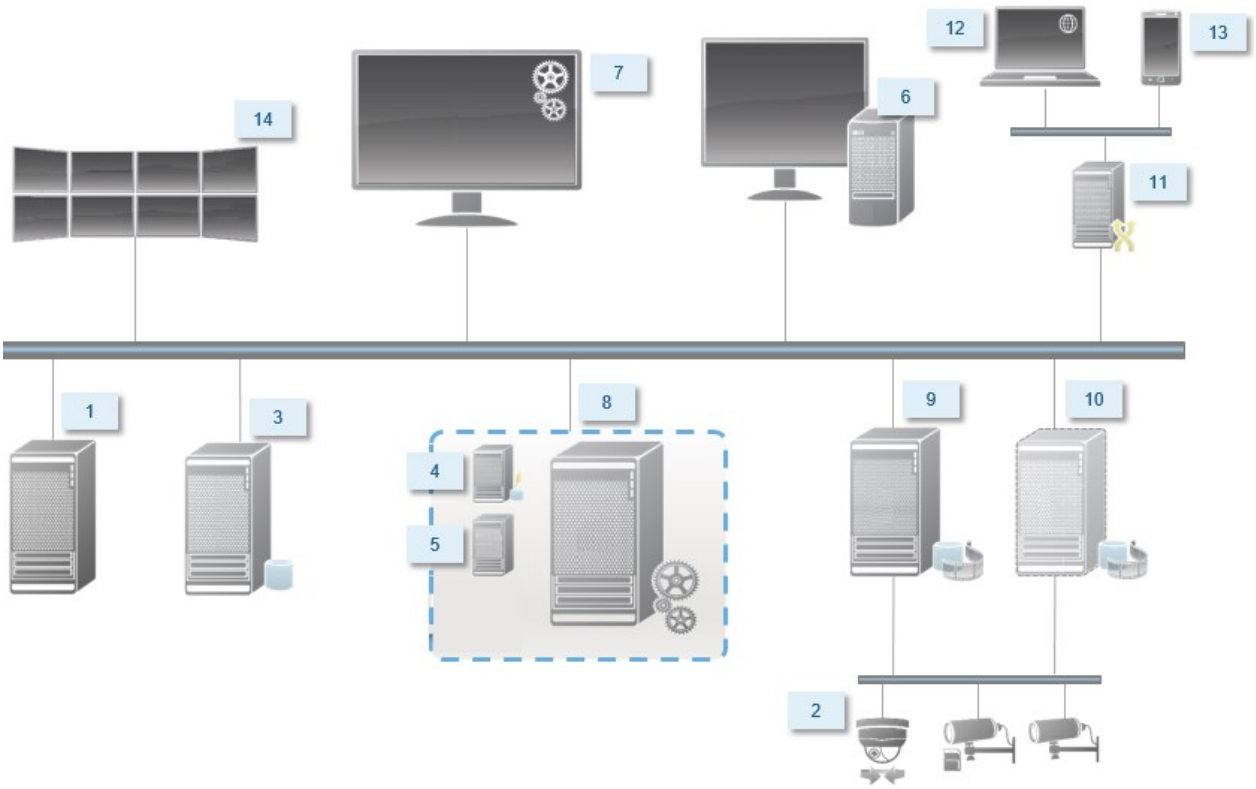


系统中的典型系统组件：

1. **Active Directory**
2. **设备**
3. **服务器，它安装有 SQL Server**
4. **事件服务器**
5. **日志服务器**
6. **XProtect Smart Client**
7. **Management Client**
8. **管理服务器**
9. **记录服务器**

10. **故障转移记录服务器**
11. **XProtect Mobile 服务器**
12. **XProtect Web Client**
13. **XProtect Mobile 客户端**
14. **XProtect Smart Client 和 XProtect Smart Wall**

自定义安装 - 分布式系统组件的示例



取决于 SQL Server 版本

Microsoft® SQL Server® Express 是 SQL Server 的一个免费版本，并且与其他 SQL Server 版本相比，它易于安装和准备使用。在**单台计算机**安装期间，除非已在这台计算机上安装了 Microsoft SQL Server Express，否则将安装 SQL Server。

XProtect VMS 安装包括 Microsoft SQL Server Express 2019 版。并非所有 Windows 操作系统都支持此版本的 SQL Server。在安装 XProtect VMS 之前，请确认您的操作系统是否支持 SQL Server 2019。如果您的操作系统不支持此版本的 SQL Server，请安装支持版本的 SQL Server，然后再开始 XProtect VMS 安装。有关支持的 SQL Server 版本的信息，请参阅 https://www.milestonesys.com/systemrequirements/。

对于与 SQL Server 数据库之间有许多交易的庞大系统或系统，Milestone 建议您在网络上的专用计算机上以及在不用于其他用途的专用硬盘驱动器上使用 SQL Server 的 Microsoft® SQL Server® Standard 或 Microsoft® SQL Server® Enterprise 版。在自己的驱动器上安装 SQL Server 可提高整个系统的性能。

选择服务帐户

在安装中，系统将要求您指定要在此计算机上运行 Milestone 服务的帐户。服务始终在该帐户上运行，无论登录用户是谁。确保帐户拥有所有必要的用户权限，例如用于执行任务的适当权限、正确的网络和文件访问权限以及网络共享文件夹访问权限。

您可以选择预定义的帐户或用户帐户。您的决定应基于要在其中安装系统的环境：

域环境

在域环境中：

- Milestone 建议您使用内置的网络服务帐户

  这将易于使用，即使在您需要将系统扩展到多台计算机的情况下也是如此。

- 您也可以使用域用户帐户，但它们可能更难以配置

工作组环境

在工作组环境中，Milestone 建议您使用拥有所有必要权限的本地用户帐户。这通常是管理员帐户。

> ⚠ 如果您已在多台计算机上安装了系统组件，则所选用户帐户必须配置于您安装中的所有计算机上，并具有相同的用户名、密码和访问权限。

Kerberos 身份验证(已解释)

Kerberos 是一个基于票证的网络身份验证协议。它设计用于为客户端/服务器或服务器/服务器应用提供强大的身份验证功能。

可使用 Kerberos 身份验证替代旧的 Microsoft NT LAN (NTLM) 身份验证协议。

Kerberos 身份验证需要使用相互身份验证，其中客户端和服务相互进行身份验证。这样，您就可以更安全地从 XProtect 客户端向 XProtect 服务器进行身份验证，而不会暴露您的密码。

要在 XProtect VMS 中进行相互身份验证，您必须在 Active Directory 中注册服务主体名称 (SPN)。SPN 是唯一标识实体(如 XProtect server 服务)的别名。采用相互身份验证的每个服务都必须注册 SPN，以便客户端可以在网络上识别服务。如果未正确注册 SPN，则无法进行相互身份验证。

下表列出了您需要注册的不同 Milestone 服务和相应端口号：

服务	端口号
Management Server - IIS	80 - 可配置
Management Server - 内部	8080
Recording Server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334

您需要在 Active Directory 中注册的服务数量取决于您当前的安装。安装 Management Server、Recording Server、Event Server 或 Failover Server 服务时，会自动安装 Data Collector。

您必须为运行该服务的用户注册两个 SPN：一个具有主机名，另一个具有完全合格的域名。

如果您在一个网络用户服务帐户下运行服务，必须为运行此服务的每台计算机注册两个 SPN。

以下是 Milestone SPN 命名方案：

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

下面是运行于具有以下详细信息的计算机上的 Recording Server 服务的 SPN 示例：

```
Hostname: Record-Server1
Domain: Surveillance.com
```

要注册的 SPN：

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

病毒扫描排除(已解释)

与其他任何数据库软件的情形相同，如果在运行 XProtect 软件的计算机上安装了反病毒程序，清除特定文件类型和文件夹以及特定网络通信极为重要。如果不实施这些例外，病毒扫描会占用大量系统资源。除此之外，扫描进程可能临时锁定文件，从而可能导致录制进程中断甚至造成数据库损坏。

需要执行病毒扫描时，请勿扫描包含记录数据库的记录服务器文件夹(默认为 `C:\mediadatabase\`，以及所有子文件夹)。还应避免在存档存储目录上执行病毒扫描。

创建以下额外排除对象：

- 文件类型：.blk、.idx、.pic
- 文件夹和子文件夹：
  - `C:\Program Files\Milestone` 或 `C:\Program Files (x86)\Milestone`
  - `C:\ProgramData\Milestone\IDP\Logs`
  - `C:\ProgramData\Milestone\KeyManagement\Logs`
  - `C:\ProgramData\Milestone\MIPSDK`
  - `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Event Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Log Server`
  - `C:\ProgramData\Milestone\XProtect Management Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb`
- 排除下列 TCP 端口上的网络扫描：

产品	TCP 端口
XProtect VMS	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

或

- 排除以下进程的网络扫描：

产品	进程
XProtect VMS	VideoOS.Recorder.Service.exe、VideoOS.Server.Service.exe、VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

组织可能会有关于病毒扫描的严格准则，但重要的是，上述文件夹和文件应被排除在病毒扫描之外。

如何配置 XProtect VMS 以在 FIPS 140-2 兼容模式下运行？

为了以 FIPS 140-2 操作模式运行 XProtect VMS，您必须：

- 在 FIPS 140-2 批准的操作模式下运行 Windows 操作系统。有关启用 FIPS 的信息，请访问 Microsoft 网站。
- 确保独立的第三方集成可以在启用 FIPS 的 Windows 操作系统上运行
- 以确保 FIPS 140-2 兼容的操作模式连接到设备
- 确保使用兼容 FIPS 140-2 的密码对媒体数据库中的数据进行加密

  这是通过运行媒体数据库升级工具来完成的。有关如何配置 XProtect VMS 以在符合 FIPS 140-2 的模式下运行的详细信息，请参阅强化指南中的FIPS 140-2 合规部分。

在启用 FIPS 的系统上安装 XProtect VMS 之前

虽然可以在启用了 FIPS 的计算机上完成新 XProtect VMS 的安装，但是在 Windows 操作系统上启用了 FIPS 时，您将无法升级 XProtect VMS。

如果要升级，请在安装之前，在属于视频管理软件的所有计算机（包括托管 SQL Server 的计算机）上禁用 Windows FIPS 安全策略。

如果启用了 FIPS，XProtect VMS 安装程序将检查 FIPS 安全策略，并阻止安装开始。

但是，如果要从 XProtect VMS 2020 R3 及更高版本升级，则无需禁用 FIPS。

在所有计算机上安装 XProtect VMS 组件并为 FIPS 准备系统之后，可以在视频管理软件中所有计算机上的 Windows 上启用 FIPS 安全策略。

有关如何配置XProtectVMS以在符合FIPS140-2的模式下运行的详细信息，请参阅强化指南中的FIPS140-2合规部分。

注册软件许可证号

安装之前，您必须知道从 Milestone 收到的软件许可证文件的名称和位置。

您可以安装 XProtect Essential+ 的免费版。该版本可为有限数量的摄像机提供 XProtect VMS 的有限功能。必须具有 Internet 连接才能安装 XProtect Essential+。

您的软件许可证号 (SLC) 印刷在订单确认书上，软件许可证文件以您的 SLC 命名。

Milestone建议您在安装前先到我们的网站 (https://online.milestonesys.com/) 上注册您的 SLC。经销商也有可能已经帮您完成注册。

设备驱动程序(已解释)

系统使用视频设备驱动程序来控制连接到记录服务器的摄像机设备并与之通信。您必须在系统的每台记录服务器上安装视频设备驱动程序。

从 2018 R1 版本开始，设备驱动程序分为两个设备软件包：包含较新驱动程序的常规设备软件包和包含较旧驱动程序的旧设备软件包。

安装记录服务器时，将自动安装常规设备软件包。稍后，您可以下载并安装更新版本的设备软件包，以更新驱动程序。Milestone 会定期发布新版本的设备驱动程序，您可以从我们网站的下载页面 (https://www.milestonesys.com/downloads/) 下载设备软件包。更新视频设备软件包时，可以在已安装的任何版本之上安装最新版本。

只有在系统安装了常规设备软件包的情况下，才能安装旧版设备软件包。如果系统上已经安装了以前的版本，将自动安装旧版设备软件包中的驱动程序。可以在软件下载页面 (https://www.milestonesys.com/downloads/) 手动下载和安装。

请在安装前停止 Recording Server 服务，否则需要重启计算机。

为确保最佳性能，请始终使用最新版本的设备驱动程序。

脱机安装的要求

如果在脱机服务器上安装系统，则需要以下文件：

- `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 文件
- 适用于您 XProtect 系统的软件许可证文件 (SLC)
- 包括所需的 .NET 版本 (https://www.milestonesys.com/systemrequirements/) 的操作系统安装媒体

安全通信(已解释)

安全超文本传输协议 (HTTPS) 是超文本传输协议 (HTTP) 的扩展，用于通过计算机网络进行安全通信。在 HTTPS 中，通信协议使用传输层安全 (TLS) 或其前身安全套接字层 (SSL) 进行加密。

在 XProtect VMS 中，安全通信是通过使用 TLS/SSL 和非对称加密 (RSA) 实现。

TLS/SSL 使用一对密钥(一个私钥和一个公钥)来验证、保护和管理安全连接。

证书颁发机构 (CA) 是任何能够颁发根证书的人。这可以是颁发根证书的互联网服务，或任何手动生成并发放证书的人。CA 可以向 web 服务，即向任何使用 https 通信的软件颁发证书。此证书包含两个密钥，即私钥和公钥。公钥通过安装公共证书安装在 Web 服务的客户端(服务客户端)上。私钥用于签署必须安装在服务器上的

服务器证书。每当服务客户端调用 Web 服务时，Web 服务都会将包含公钥的服务器证书发送到客户端。服务客户端可以使用已安装的公共 CA 证书验证服务器证书。客户端和服务器现在可以使用公共和私人服务器证书来交换密钥，从而建立安全的 TLS/SSL 连接。

对于手动发放的证书，必须在客户端可以进行此类验证前安装证书。

有关 TLS 的更多信息，请参阅传输层安全。

证书具有到期日。XProtect VMS不会在证书即将到期时警告您。如果证书到期：
- 客户端将不再信任具有过期证书的记录服务器，因此无法与其进行通信
- 记录服务器将不再信任具有过期证书的管理服务器，因此无法与其进行通信
- 移动设备将不再信任具有过期证书的移动设备服务器，因此无法与其进行通信

要更新证书，请按照本指南中的步骤进行操作，就像您创建证书时所做的那样。

有关详细信息，请参阅有关如何保护 XProtect VMS 安装的证书指南。

安装

安装新的 XProtect 系统

安装 XProtect Essential+

您可以安装 XProtect Essential+ 的免费版。该版本可为有限数量的摄像机提供 XProtect VMS 的有限功能。必须具有 Internet 连接才能安装 XProtect Essential+。

此版本安装在一台计算机上，请使用**单台计算机**安装选项。**单台计算机**选项在当前计算机上安装所有服务器和客户端组件。

Milestone 建议您在安装之前仔细阅读以下部分：第 116 页上的开始安装前。

对于 FIPS 安装，如果在 Windows 操作系统上启用了 FIPS，则无法升级 XProtect VMS。在安装之前，在属于视频管理软件的所有计算机（包括托管 SQL Server 的计算机）上禁用 Windows FIPS 安全策略。但是，如果要从 XProtect VMS 2020 R3 及更高版本升级，则无需禁用 FIPS。有关如何配置 XProtect VMS 以在符合 FIPS 140-2 的模式下运行的详细信息，请参阅强化指南中的FIPS 140-2 合规部分。

初次安装后，您可以继续使用配置向导。根据您的硬件和配置，记录服务器会扫描网络中是否有硬件。然后，您可以选择将哪些硬件设备添加到您的系统中。摄像机在视图中预先配置，您可以选择启用麦克风和扬声器等其他设备。您还可以选择将操作员角色或管理员角色的用户添加到系统中。安装后，XProtect Smart Client 会打开，您可以随时使用系统。

否则，如果关闭安装向导，则 XProtect Management Client 会打开，您可以在其中进行手动配置，例如将硬件设备和用户添加到系统中。

如果从以前的产品版本升级，则系统不会扫描硬件，也不会创建新视图和用户角色。

1. 从互联网 (https://www.milestonesys.com/downloads/) 下载软件，并运行 `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 文件。
2. 安装文件会解压。根据安全设置，将显示一个或多个 Windows® 安全警告。接受这些警告，解压将继续。
3. 完成后，会出现 **Milestone XProtect VMS** 安装向导。
    1. 选择安装期间使用的**语言**（这不是系统在安装后将使用的语言；系统在安装后将使用的语言会在之后进行选择）。单击**继续**。
    2. 阅读 *Milestone 最终用户许可协议*。选中**我接受许可协议中的条款**复选框，然后单击**继续**。

3. 在**隐私设置**页面上，选择是否要共享使用情况数据，然后单击**继续**。

   如果您希望系统的安装符合 EU GDPR，则不得启用数据收集。有关数据保护和使用数据收集的更多信息，请参阅 GDPR 隐私指南。

   Y您之后可以随时更改您的隐私设置。另请参阅系统设置（“选项”对话框）。

4. 单击 **XProtect Essential+** 链接下载免费许可证文件。

   此时会下载免费许可证文件，而且它会显示在**输入或浏览到许可证文件位置**字段中。单击**继续**。

4. 选择**单台计算机**。

   将出现要安装的组件的列表（您无法编辑此列表）。单击**继续**。

5. 在**分配系统配置密码**页面上，输入保护您的系统配置的密码。在系统恢复或扩展系统（例如添加集群）时，将需要此密码。

   您必须保存此密码并确保其安全，这一点非常重要。如果丢失此密码，则可能会影响恢复系统配置的能力。

   如果您不希望系统配置受到密码保护，请选择**我选择不使用系统配置密码，并且了解系统配置不会被加密**。

   单击**继续**。

6. 在**分配移动设备服务器数据保护密码**页面上，输入密码以加密您的调查。作为系统管理员，在系统恢复或使用其他移动设备服务器扩展系统时，您需要输入此密码才能访问移动设备服务器数据。

   您必须保存此密码并确保其安全。否则可能会损害您恢复移动设备服务器数据的能力。

   如果您不希望调查受到密码保护，请选择**我选择不使用移动设备服务器数据保护密码，并且了解调查不会被加密**。

   单击**继续**。

7. 在**指定记录服务器设置**页面上，指定不同的记录服务器设置：
    1. 在**记录服务器名称**字段中，输入记录服务器的名称。默认为计算机的名称。
    2. **管理服务器地址**字段会显示管理服务器的地址和端口号：localhost:80。
    3. 在**选择媒体数据库位置**字段中，选择视频记录要保存到的位置。Milestone 建议您将视频录制内容保存在与安装软件位置不同且非系统驱动器的位置上。默认位置是可用空间最多的驱动。
    4. 在**视频记录的保留时间**字段，定义希望将记录保留的时长。您可以输入 1 到 365,000 天，默认保留时间是 7 天。
    5. 单击**继续**。
8. 在**选择加密**页面上，您可以保护通信流：
    - 在记录服务器、数据收集器与管理服务器之间

      要为内部通信流启用加密，请在**服务器证书**部分中选择一个证书。

      > 如果加密从记录服务器到管理服务器的连接，则系统会要求您同时还加密从管理服务器到记录服务器的连接。

    - 在记录服务器与客户端之间

      要在记录服务器与从记录服务器检索数据流的客户端组件之间启用加密，请在**流媒体证书**部分中选择一个证书。

    - 在移动设备服务器与客户端之间

      要在从移动设备服务器检索数据流的客户端组件之间启用加密，请在**移动流媒体证书**部分中选择一个证书。

    - 事件服务器和与事件服务器通信的组件之间

      若要启用事件服务器和与事件服务器通信的组件之间的加密，包括**事件服务器和扩展**部分中的 LPR Server，请选择一个证书。

    您可以对所有系统组件使用相同的证书文件，也可以根据系统组件使用不同的证书文件。

    有关准备系统以进行安全通信的详细信息，请参阅：

    - 第 124 页上的安全通信(已解释)
    - Milestone 证书指南

    您还可以通过通知区域中的ManagementServerManager托盘图标在安装后从ServerConfigurator启用加密。

9. 在**选择文件位置和产品语言**页面上，执行以下操作：

   1. 在**文件位置**字段中，选择软件安装位置。

      > 如果计算机上已经安装了任何 Milestone XProtect VMS 产品，则此字段将被禁用。该字段显示将要安装组件的位置。

   2. 在**产品语言**中，选择安装 XProtect 产品时使用的语言。
   3. 单击**安装**。

   软件现在即会安装。如果尚未安装在计算机上，则在安装过程中会自动安装 Microsoft® SQL Server® Express 和 Microsoft IIS。

10. 系统可能会提示您重新启动计算机。重新启动计算机之后，根据安全设置的不同，可能会出现一条或多条 Windows 安全警告。接受这些警告，安装即完成。
11. 安装完成后，会显示计算机上已安装组件的列表。

    单击**继续**将硬件和用户添加到系统中。

    > 如果现在单击**关闭**，您就会绕过配置向导，XProtect Management Client 打开。在 Management Client 中，您可以配置系统，例如将硬件和用户添加到系统中。

12. 在**输入硬件的用户名和密码**页面上，输入硬件的用户名和密码(已从制造商提供的默认值更改)。

    安装程序会扫描网络以获取此硬件以及具有制造商默认凭据的硬件。

    单击**继续**并等待系统扫描硬件。

13. 在**选择要添加到系统中的硬件**页面上，选择要添加到系统中的硬件。单击**继续**并等待系统添加硬件。
14. 在**配置设备**页面上，您可以通过单击硬件名称旁边的编辑图标来添加硬件描述性名称。然后，这个名称将作为硬件设备的前缀。

    扩展硬件节点以启用或禁用硬件设备，如摄像机、扬声器和麦克风。

    > 摄像机默认启用，扬声器和麦克风默认禁用。

    单击**继续**并等待系统配置硬件。

15. 在**添加用户**页面上，您可以将用户作为 Windows 用户或基本用户添加到系统中。这些用户可以是管理员角色或操作员角色。

    定义用户并单击**添加**。

    添加完用户后，请单击**继续**。

16. 完成安装和初始配置后，出现**配置完成**页面，您会看到：
    - 添加到系统中的硬件设备的列表
    - 添加到系统中的用户列表
    - 指向 XProtect Web Client 和 XProtect Mobile 客户端的地址，您可以与用户共享

    单击**关闭**时，XProtect Smart Client 打开，准备就绪。

安装本系统 - 单台计算机选项

单台计算机选项在当前计算机上安装所有服务器和客户端组件。

Milestone 建议您在安装之前仔细阅读以下部分：第 116 页上的开始安装前。

对于 FIPS 安装，如果在 Windows 操作系统上启用了 FIPS，则无法升级 XProtect VMS。在安装之前，在属于视频管理软件的所有计算机（包括托管 SQL Server 的计算机）上禁用 Windows FIPS 安全策略。但是，如果要从 XProtect VMS 2020 R3 及更高版本升级，则无需禁用 FIPS。有关如何配置 XProtect VMS 以在符合 FIPS 140-2 的模式下运行的详细信息，请参阅强化指南中的FIPS 140-2 合规部分。

初次安装后，您可以继续使用配置向导。根据您的硬件和配置，记录服务器会扫描网络中是否有硬件。然后，您可以选择将哪些硬件设备添加到您的系统中。摄像机在视图中预先配置，您可以选择启用麦克风和扬声器等其他设备。您还可以选择将操作员角色或管理员角色的用户添加到系统中。安装后，XProtect Smart Client 会打开，您可以随时使用系统。

否则，如果关闭安装向导，则 XProtect Management Client 会打开，您可以在其中进行手动配置，例如将硬件设备和用户添加到系统中。

如果从以前的产品版本升级，则系统不会扫描硬件，也不会创建新视图和用户角色。

1. 从互联网 (https://www.milestonesys.com/downloads/) 下载软件，并运行 `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 文件。
2. 安装文件会解压。根据安全设置，将显示一个或多个 Windows® 安全警告。接受这些警告，解压将继续。
3. 完成后，会出现 **Milestone XProtect VMS** 安装向导。
    1. 选择安装期间使用的**语言**（这不是系统在安装后将使用的语言；系统在安装后将使用的语言会在之后进行选择）。单击**继续**。
    2. 阅读 *Milestone 最终用户许可协议*。选中**我接受许可协议中的条款**复选框，然后单击**继续**。
    3. 在**隐私设置**页面上，选择是否要共享使用情况数据，然后单击**继续**。

如果您希望系统的安装符合 EU GDPR，则不得启用数据收集。有关数据保护和使用数据收集的更多信息，请参阅 GDPR 隐私指南。

Y您之后可以随时更改您的隐私设置。另请参阅系统设置（“选项”对话框）。

4. 在**输入或浏览许可证文件的位置**中，输入来自 XProtect 提供商的许可证文件。或者，浏览到文件位置 或单击 **XProtect Essential+** 链接下载免费许可证文件。有关免费 XProtect Essential+ 产品的限制，请参阅 第 96 页上的产品对比。系统会先验证许可证文件，然后您才能继续。单击**继续**。

4. 选择**单台计算机**。

   将出现要安装的组件的列表（您无法编辑此列表）。单击**继续**。

5. 在**分配系统配置密码**页面上，输入保护您的系统配置的密码。在系统恢复或扩展系统（例如添加集群）时，将需要此密码。

   您必须保存此密码并确保其安全，这一点非常重要。如果丢失此密码，则可能会影响恢复系统配置的能力。

   如果您不希望系统配置受到密码保护，请选择**我选择不使用系统配置密码，并且了解系统配置不会被加密**。

   单击**继续**。

6. 在**分配移动设备服务器数据保护密码**页面上，输入密码以加密您的调查。作为系统管理员，在系统恢复或使用其他移动设备服务器扩展系统时，您需要输入此密码才能访问移动设备服务器数据。

   您必须保存此密码并确保其安全。否则可能会损害您恢复移动设备服务器数据的能力。

   如果您不希望调查受到密码保护，请选择**我选择不使用移动设备服务器数据保护密码，并且了解调查不会被加密**。

   单击**继续**。

7. 在**指定记录服务器设置**页面上，指定不同的记录服务器设置：
    1. 在**记录服务器名称**字段中，输入记录服务器的名称。默认为计算机的名称。
    2. **管理服务器地址**字段会显示管理服务器的地址和端口号：localhost:80。
    3. 在**选择媒体数据库位置**字段中，选择视频记录要保存到的位置。Milestone 建议您将视频录制内容保存在与安装软件位置不同且非系统驱动器的位置上。默认位置是可用空间最多的驱动。
    4. 在**视频记录的保留时间**字段，定义希望将记录保留的时长。您可以输入 1 到 365,000 天，默认保留时间是 7 天。
    5. 单击**继续**。
8. 在**选择加密**页面上，您可以保护通信流：
    - 在记录服务器、数据收集器与管理服务器之间

      要为内部通信流启用加密，请在**服务器证书**部分中选择一个证书。

      > 如果加密从记录服务器到管理服务器的连接，则系统会要求您同时还加密从管理服务器到记录服务器的连接。

    - 在记录服务器与客户端之间

      要在记录服务器与从记录服务器检索数据流的客户端组件之间启用加密，请在**流媒体证书**部分中选择一个证书。

    - 在移动设备服务器与客户端之间

      要在从移动设备服务器检索数据流的客户端组件之间启用加密，请在**移动流媒体证书**部分中选择一个证书。

    - 事件服务器和与事件服务器通信的组件之间

      若要启用事件服务器和与事件服务器通信的组件之间的加密，包括**事件服务器和扩展**部分中的 LPR Server，请选择一个证书。

    您可以对所有系统组件使用相同的证书文件，也可以根据系统组件使用不同的证书文件。

    有关准备系统以进行安全通信的详细信息，请参阅：

    - 第 124 页上的安全通信(已解释)
    - Milestone 证书指南

    您还可以通过通知区域中的ManagementServerManager托盘图标在安装后从ServerConfigurator启用加密。

9. 在**选择文件位置和产品语言**页面上，执行以下操作：

    1. 在**文件位置**字段中，选择软件安装位置。

    > 如果计算机上已经安装了任何 Milestone XProtect VMS 产品，则此字段将被禁用。该字段显示将要安装组件的位置。

    2. 在**产品语言**中，选择安装 XProtect 产品时使用的语言。
    3. 单击**安装**。

    软件现在即会安装。如果尚未安装在计算机上，则在安装过程中会自动安装 Microsoft® SQL Server® Express 和 Microsoft IIS。

10. 系统可能会提示您重新启动计算机。重新启动计算机之后，根据安全设置的不同，可能会出现一条或多条 Windows 安全警告。接受这些警告，安装即完成。

11. 安装完成后，会显示计算机上已安装组件的列表。

    单击**继续**将硬件和用户添加到系统中。

    > 如果现在单击**关闭**，您就会绕过配置向导，XProtect Management Client 打开。在 Management Client 中，您可以配置系统，例如将硬件和用户添加到系统中。

12. 在**输入硬件的用户名和密码**页面上，输入硬件的用户名和密码(已从制造商提供的默认值更改)。

    安装程序会扫描网络以获取此硬件以及具有制造商默认凭据的硬件。

    单击**继续**并等待系统扫描硬件。

13. 在**选择要添加到系统中的硬件**页面上，选择要添加到系统中的硬件。单击**继续**并等待系统添加硬件。

14. 在**配置设备**页面上，您可以通过单击硬件名称旁边的编辑图标来添加硬件描述性名称。然后，这个名称将作为硬件设备的前缀。

    扩展硬件节点以启用或禁用硬件设备，如摄像机、扬声器和麦克风。

    > 摄像机默认启用，扬声器和麦克风默认禁用。

    单击**继续**并等待系统配置硬件。

15. 在**添加用户**页面上，您可以将用户作为 Windows 用户或基本用户添加到系统中。这些用户可以是管理员角色或操作员角色。

    定义用户并单击**添加**。

    添加完用户后，请单击**继续**。

16. 完成安装和初始配置后，出现**配置完成**页面，您会看到：
    - 添加到系统中的硬件设备的列表
    - 添加到系统中的用户列表
    - 指向 XProtect Web Client 和 XProtect Mobile 客户端的地址，您可以与用户共享

    单击**关闭**时，XProtect Smart Client 打开，准备就绪。

安装本系统 - 自定义选项

自定义选项会安装管理服务器，但您可以选择要在当前计算机上安装的其他服务器和客户端组件。默认情况下，不会在组件列表中选中记录服务器。根据您的选择，您之后可以在其他计算机上安装未选定的系统组件。有关每个系统组件及其角色的详细信息，请参阅第 32 页上的产品概述。其他计算机上的安装是通过名为 Download Manager 的管理服务器的下载网页完成。有关通过 Download Manager 安装的详细信息，请参阅第 157 页上的Download Manager / 下载网页。

Milestone 建议您在安装之前仔细阅读以下部分：第 116 页上的开始安装前。

对于 FIPS 安装，如果在 Windows 操作系统上启用了 FIPS，则无法升级 XProtect VMS。在安装之前，在属于视频管理软件的所有计算机（包括托管 SQL Server 的计算机）上禁用 Windows FIPS 安全策略。但是，如果要从 XProtect VMS 2020 R3 及更高版本升级，则无需禁用 FIPS。有关如何配置 XProtect VMS 以在符合 FIPS 140-2 的模式下运行的详细信息，请参阅强化指南中的FIPS 140-2 合规部分。

1. 从互联网 (https://www.milestonesys.com/downloads/) 下载软件，并运行 `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 文件。
2. 安装文件会解压。根据安全设置，将显示一个或多个 Windows® 安全警告。接受这些警告，解压将继续。
3. 完成后，会出现 **Milestone XProtect VMS** 安装向导。
    1. 选择安装期间使用的**语言**（这不是系统在安装后将使用的语言；系统在安装后将使用的语言会在之后进行选择）。单击**继续**。
    2. 阅读 *Milestone 最终用户许可协议*。选中**我接受许可协议中的条款**复选框，然后单击**继续**。
    3. 在**隐私设置**页面上，选择是否要共享使用情况数据，然后单击**继续**。

        如果您希望系统的安装符合 EU GDPR，则不得启用数据收集。有关数据保护和使用数据收集的更多信息，请参阅 GDPR 隐私指南。

Y您之后可以随时更改您的隐私设置。另请参阅系统设置("选项"对话框)。

4. 在**输入或浏览许可证文件的位置**中,输入来自 XProtect 提供商的许可证文件。或者,浏览到文件位置 或单击 **XProtect Essential+** 链接下载免费许可证文件。有关免费 XProtect Essential+ 产品的限制,请参阅 第 96 页上的产品对比。系统会先验证许可证文件,然后您才能继续。单击**继续**。

4. 选择**自定义**。将显示要安装的组件的列表。除管理服务器之外,列表中的所有组件均为可选项。记录服务器和移动服务器默认不选中。选择您想要安装的系统组件并单击**继续**。

要使系统正常运行,必须至少安装一个 XProtect API Gateway 实例。

在下面的步骤中会安装所有系统组件。对于更加分布式的系统,在该计算机上安装较少的组件,在其他计算机上安装剩余的组件。如果您无法识别安装步骤,可能是因为您尚未选择安装此页面所属的系统组件。在这种情况下,继续执行下一步。另请第 140 页上的安装记录服务器,通过 Download Manager参阅 第 139 页上的通过 Download Manager 安装(已解释)、和 第 145 页上的通过命令行 shell 以静默方式安装(已解释)。

5. 只有当计算机上有多个 IIS 网站时,才会显示**在 IIS 上选择用于 XProtect 系统的网站**页面。您必须选择要用于 XProtect 系统的网站。选择一个有 HTTPS 绑定的网站。单击**继续**。

   如果计算机上未安装 Microsoft® IIS,则会安装它。

6. 在**选择 Microsoft SQL Server**页面上,选择要使用的 SQL Server。另请参阅 第 139 页上的SQL Server 自定义安装期间的选项。单击**继续**。

如果您的本地计算机上没有 SQL Server,则可以安装 Microsoft SQL Server Express,但在较大的分布式系统中,通常会使用网络上的专用 SQL Server。

7. 在**选择数据库**上(仅在选择了现有SQLServer时显示),选择或创建用于存储系统配置的SQLServer数据库。如果选择现有的SQLServer数据库,则决定是要**保留**还是**覆盖**现有数据。如果要升级,请选择保留现有数据,以免丢失您的系统配置。另请参阅第139页上的SQLServer自定义安装期间的选项。单击**继续**。

8. 在**数据库设置**页面上,选择**让安装程序创建或重新创建数据库**或**使用预先创建的数据库**。

9. 若要自动创建或重新创建数据库,请选择**让安装程序创建或重新创建数据库**,然后单击**继续**。

10. 若要使用您为此目的而设置的数据库或已经创建的数据库,请选择**使用预先创建的数据库**。随后您会看到**高级数据库设置**页面。

11. 在**高级数据库设置**页面上,输入 XProtect 组件的服务器和数据库名称。

12. 选择 **Windows 身份验证，不信任服务器证书(建议)**或 **Windows 身份验证，信任服务器证书**，或者选择 **Azure Active Directory Integrated，不信任服务器证书(建议)**

    必须在 Azure AD 或 Windows AD 中创建用于安装的帐户，具体取决于要使用的身份验证类型。帐户不支持多因素身份验证 (MFA)。

    建议 Windows 身份验证选择**(不信任服务器证书)**选项，Azure Active Directory Integrated 必须选择此选项。这是为了确保服务器证书在安装之前经过验证。有关无效服务器证书的详细信息，请参阅安装日志文件。如果选择 **Windows 身份验证、信任服务器证书**选项，可以跳过服务器证书验证。

13. 单击图标验证连接。通过单击图标，您还可以验证服务器证书。
14. 单击**继续**
15. 在**分配系统配置密码**页面上，输入保护您的系统配置的密码。在系统恢复或扩展系统(例如添加集群)时，将需要此密码。

    您必须保存此密码并确保其安全，这一点非常重要。如果丢失此密码，则可能会影响恢复系统配置的能力。

    如果您不希望系统配置受到密码保护，请选择**我选择不使用系统配置密码，并且了解系统配置不会被加密**。

    单击**继续**。

16. 在**分配移动设备服务器数据保护密码**页面上，输入密码以加密您的调查。作为系统管理员，在系统恢复或使用其他移动设备服务器扩展系统时，您需要输入此密码才能访问移动设备服务器数据。

    您必须保存此密码并确保其安全。否则可能会损害您恢复移动设备服务器数据的能力。

    如果您不希望调查受到密码保护，请选择**我选择不使用移动设备服务器数据保护密码，并且了解调查不会被加密**。

    单击**继续**。

17. 在**选择记录服务器的服务帐户**上，选择**该预定义帐户**或**该帐户**来选择记录服务器的服务帐户。

    如果需要，请输入密码。

    > 帐户的用户名必须是一个单词。它不能包含空格。

    单击**继续**。

18. 在**指定记录服务器设置**页面上，指定不同的记录服务器设置：

    1. 在**记录服务器名称**字段中，输入记录服务器的名称。默认为计算机的名称。
    2. **管理服务器地址**字段会显示管理服务器的地址和端口号：localhost:80。
    3. 在**选择媒体数据库位置**字段中，选择视频记录要保存到的位置。Milestone 建议您将视频录制内容保存在与安装软件位置不同且非系统驱动器的位置上。默认位置是可用空间最多的驱动。
    4. 在**视频记录的保留时间**字段，定义希望将记录保留的时长。您可以输入 1 到 365,000 天，默认保留时间是 7 天。
    5. 单击**继续**。

19. 在**选择加密**页面上，您可以保护通信流：

    - 在记录服务器、数据收集器与管理服务器之间

      要为内部通信流启用加密，请在**服务器证书**部分中选择一个证书。

      > 如果加密从记录服务器到管理服务器的连接，则系统会要求您同时还加密从管理服务器到记录服务器的连接。

    - 在记录服务器与客户端之间

      要在记录服务器与从记录服务器检索数据流的客户端组件之间启用加密，请在**流媒体证书**部分中选择一个证书。

    - 在移动设备服务器与客户端之间

      要在从移动设备服务器检索数据流的客户端组件之间启用加密，请在**移动流媒体证书**部分中选择一个证书。

    - 事件服务器和与事件服务器通信的组件之间

      若要启用事件服务器和与事件服务器通信的组件之间的加密，包括**事件服务器和扩展**部分中的 LPR Server，请选择一个证书。

    您可以对所有系统组件使用相同的证书文件，也可以根据系统组件使用不同的证书文件。

    有关准备系统以进行安全通信的详细信息，请参阅：

    - 第 124 页上的安全通信（已解释）
    - Milestone 证书指南

    您还可以通过通知区域中的ManagementServerManager托盘图标在安装后从ServerConfigurator启用加密。

20. 在**选择文件位置和产品语言**页面上，选择程序文件的**文件位置**。

    > 如果计算机上已经安装了任何 Milestone XProtect VMS 产品，则此字段将被禁用。该字段显示将要安装组件的位置。

21. 在**产品语言**中，选择安装 XProtect 产品时使用的语言。单击**安装**。

    软件现在即会安装。安装完成后，您会看到已成功安装的系统组件的列表。单击**关闭**。

22. 系统可能会提示您重新启动计算机。重新启动计算机之后，根据安全设置的不同，可能会出现一条或多条 Windows 安全警告。接受这些警告，安装即完成。

23. 在 Management Client 中配置系统。请参阅 第 165 页上的初始配置任务列表。

24. 根据您的选择，通过 Download Manager 在其他计算机上安装其余系统组件。请参阅 第 139 页上的通过 Download Manager 安装（已解释）。

SQL Server 自定义安装期间的选项

使用以下选项确定要使用的 SQL Server 和数据库。

SQL Server 选项：

- **在此计算机上安装 Microsoft® SQL Server® Express**：仅当您未在计算机上安装 SQL Server 时，才会显示此选项
- **在此计算机上使用 SQL Server**：仅当已在计算机上安装了 SQL Server 时，才会显示此选项
- **通过搜索，在您的网络上选择 SQL Server**：使您能够搜索网络子网上可发现的所有 SQL Server 安装
- **在您的网络上选择 SQL Server**：使您能够输入可能无法通过搜索找到的 SQL Server 地址（主机名或 IP 地址）

SQL Server 数据库选项：

- **新建数据库**：主要用于新安装
- **使用现有数据库**：主要用于现有安装的升级。Milestone 建议您再用现有的 SQL Server 数据库并将现有数据保留在其中，这样就不会丢失系统配置。您还可以选择覆盖 SQL Server 数据库中的数据

安装新的 XProtect 组件

通过 Download Manager 安装（已解释）

如果要在计算机（安装了管理服务器的计算机除外）上安装系统组件，则必须通过 Management Server 的下载网站 Download Manager 安装这些系统组件。

1. 从安装有 Management Server 的计算机上，进入 Management Server 的下载网页。在 Windows 的**开始**菜单中，选择**Milestone > 管理安装页面**，并记下或复制互联网地址，以供以后在其他计算机上安装系统组件时使用。地址通常是 *http://[management 服务器地址]/installation/Admin/default-en-US.htm*。
2. 登录到其他每台计算机以安装一个或多个其他系统组件：
   - Recording Server（有关详细信息，请参阅 第 140 页上的安装记录服务器，通过 Download Manager 或 第 146 页上的以静默方式安装 recording server）
   - Management Client（有关详细信息，请参阅 第 140 页上的通过 Download Manager 安装 Management Client）
   - Smart Client
   - Event Server 记住在安装后重新启动 API 网关。如果以后重命名计算机，还必须重新启动 API 网关。

     > ⚠ 如果要在符合 FIPS 的环境中进行安装，则必须在安装 Event Server 前禁用 Windows FIPS 140-2 模式。

- Log Server(有关详细信息，请参阅 第 148 页上的以静默方式安装日志服务器)
- Mobile Server（有关详细信息，请参阅 XProtect Mobile 服务器手册)

3. 打开互联网浏览器，将 Management Server 的下载网页地址输入到地址栏，然后下载相关的安装程序。
4. 运行安装程序。

如果对不同安装步骤中的选择和设置有疑问，请参阅 第 134 页上的安装本系统 - 自定义选项。

通过 Download Manager 安装 Management Client

如果有 XProtect 系统的几个管理员或您只想要从多个计算机管理 XProtect 系统，您可以按照以下说明安装 Management Client。

Management Client 始终安装在管理服务器上。

1. 从安装有 Management Server 的计算机上，进入 Management Server 的下载网页。在 Windows 的**开始**菜单中，选择**Milestone > 管理安装页面**，并记下或复制互联网地址，以供以后在其他计算机上安装系统组件时使用。地址通常是 *http://[management 服务器地址]/installation/Admin/default-en-US.htm*。
2. 登录到要安装系统组件的计算机。
1. 打开互联网浏览器，将 Management Server 的下载网页地址输入到地址栏，然后按 Enter。
3. 为 **安装程序单击**所有语言Management Client。运行下载的文件。
4. 对所有警告单击**是**。将开始执行解包。
5. 选择安装程序的语言。单击**继续**。
6. 阅读并接受许可协议。单击**继续**。
7. 选择文件位置和产品语言。单击**安装**。
8. 安装已完成。将显示已成功安装的组件的列表。单击**关闭**。
9. 单击桌面上的图标以打开 Management Client。
10. 将出现 Management Client 登录对话框。
11. 在**计算机**字段中指定管理服务器的主机名或 IP 地址。
12. 选择身份验证，输入用户名和密码。单击**连接**。Management Client 即会启动。

    要阅读有关ManagementClient中的功能以及可以通过系统完成的操作的详细信息，单击工具菜单中的**帮助**。

安装记录服务器，通过 Download Manager

如果系统组件分布在单独的计算机上，您可以按照以下说明安装记录服务器。

如果您在**单台计算机**安装，则记录服务器已安装；但如需更多容量，您可以使用相同说明来添加更多记录服务器。

如果需要安装故障转移记录服务器，请参阅 第 143 页上的安装故障转移记录服务器，通过 Download Manager。

1. 从安装有 Management Server 的计算机上，进入 Management Server 的下载网页。在 Windows 的**开始**菜单中，选择**Milestone > 管理安装页面**，并记下或复制互联网地址，以供以后在其他计算机上安装系统组件时使用。地址通常是 *http://[management 服务器地址]/installation/Admin/default-en-US.htm*。
2. 登录到要安装系统组件的计算机。
3. 打开互联网浏览器，将 Management Server 的下载网页地址输入到地址栏，然后按 Enter。
4. 通过选择**记录服务器安装程序**下的**所有语言**，下载记录服务器安装程序。保存安装程序或直接从网页运行安装程序。
5. 选择希望在安装期间使用的**语言**。单击**继续**。
6. 在 **选择安装类型**页面上，选择：

   典型：以默认值安装记录服务器，或

   自定义：以自定义值安装记录服务器。
7. 在**指定记录服务器设置**页面上，指定不同的记录服务器设置：
   1. 在**记录服务器名称**字段中，输入记录服务器的名称。默认为计算机的名称。
   2. **管理服务器地址**字段会显示管理服务器的地址和端口号：localhost:80。
   3. 在**选择媒体数据库位置**字段中，选择视频记录要保存到的位置。Milestone 建议您将视频录制内容保存在与安装软件位置不同且非系统驱动器的位置上。默认位置是可用空间最多的驱动。
   4. 在**视频记录的保留时间**字段，定义希望将记录保留的时长。您可以输入 1 到 365,000 天，默认保留时间是 7 天。
   5. 单击**继续**。
8. 只有在您选择了**自定义**时，才会显示**记录服务器 IP 地址**页面。指定要在此计算机上安装的记录服务器数量。单击**继续**。

9. 在**选择记录服务器的服务帐户**上，选择**该预定义帐户**或**该帐户**来选择记录服务器的服务帐户。

   如果需要，请输入密码。

   > 帐户的用户名必须是一个单词。它不能包含空格。

   单击**继续**。

10. 在**选择加密**页面上，您可以保护通信流：

    - 在记录服务器、数据收集器与管理服务器之间

      要为内部通信流启用加密，请在**服务器证书**部分中选择一个证书。

      > 如果加密从记录服务器到管理服务器的连接，则系统会要求您同时还加密从管理服务器到记录服务器的连接。

    - 在记录服务器与客户端之间

      要在记录服务器与从记录服务器检索数据流的客户端组件之间启用加密，请在**流媒体证书**部分中选择一个证书。

    - 在移动设备服务器与客户端之间

      要在从移动设备服务器检索数据流的客户端组件之间启用加密，请在**移动流媒体证书**部分中选择一个证书。

    - 事件服务器和与事件服务器通信的组件之间

      若要启用事件服务器和与事件服务器通信的组件之间的加密，包括**事件服务器和扩展**部分中的LPR Server，请选择一个证书。

    您可以对所有系统组件使用相同的证书文件，也可以根据系统组件使用不同的证书文件。

    有关准备系统以进行安全通信的详细信息，请参阅：

    - 第 124 页上的安全通信(已解释)
    - Milestone 证书指南

    您还可以通过通知区域中的ManagementServerManager托盘图标在安装后从ServerConfigurator启用加密。

11. 在**选择文件位置和产品语言**页面上，选择程序文件的**文件位置**。

    > 如果计算机上已经安装了任何 Milestone XProtect VMS 产品，则此字段将被禁用。该字段显示将要安装组件的位置。

12. 在**产品语言**中，选择安装 XProtect 产品时使用的语言。单击**安装**。

    软件现在即会安装。安装完成后，您会看到已成功安装的系统组件的列表。单击**关闭**。

13. 安装完记录服务器后，可使用 Recording Server Manager 托盘图标检查其状态，并在 Management Client 中对其进行配置。有关详细信息，请参阅 第 165 页上的初始配置任务列表。

安装故障转移记录服务器，通过 Download Manager

> 如果运行工作组，则必须对故障转移记录服务器使用替代的安装方法（请参阅 第 152 页上的工作组安装）。

1. 从安装有 Management Server 的计算机上，进入 Management Server 的下载网页。在 Windows 的**开始**菜单中，选择**Milestone > 管理安装页面**，并记下或复制互联网地址，以供以后在其他计算机上安装系统组件时使用。地址通常是 *http://[management 服务器地址]/installation/Admin/default-en-US.htm*。

   登录到要安装系统组件的计算机。

2. 打开互联网浏览器，将 Management Server 的下载网页地址输入到地址栏，然后按 Enter。

3. 通过选择**记录服务器安装程序**下的**所有语言**，下载记录服务器安装程序。保存安装程序或直接从网页运行安装程序。

4. 选择希望在安装期间使用的**语言**。单击**继续**。

5. 在**选择安装类型**页面上，选择**故障转移**将记录服务器安装为故障转移记录服务器。

6. 在**指定记录服务器设置**页面上，指定不同的记录服务器设置。故障转移记录服务器的名称，管理服务器的地址以及媒体数据库的路径。单击**继续**。

7. 在**选择记录服务器的服务帐户**页面上以及在安装故障转移记录服务器时，必须使用名为**该帐户**的具体用户帐户。这将创建故障转移用户帐户。如果需要，输入密码并进行确认。单击**继续**。

8. 在**选择加密**页面上，您可以保护通信流：

   - 在记录服务器、数据收集器与管理服务器之间

     要为内部通信流启用加密，请在**服务器证书**部分中选择一个证书。

     > 如果加密从记录服务器到管理服务器的连接，则系统会要求您同时还加密从管理服务器到记录服务器的连接。

   - 在记录服务器与客户端之间

     要在记录服务器与从记录服务器检索数据流的客户端组件之间启用加密，请在**流媒体证书**部分中选择一个证书。

   - 在移动设备服务器与客户端之间

     要在从移动设备服务器检索数据流的客户端组件之间启用加密，请在**移动流媒体证书**部分中选择一个证书。

   - 事件服务器和与事件服务器通信的组件之间

     若要启用事件服务器和与事件服务器通信的组件之间的加密，包括**事件服务器和扩展**部分中的 LPR Server，请选择一个证书。

   您可以对所有系统组件使用相同的证书文件，也可以根据系统组件使用不同的证书文件。

   有关准备系统以进行安全通信的详细信息，请参阅：

   - 第 124 页上的安全通信(已解释)
   - Milestone 证书指南

   您还可以通过通知区域中的ManagementServerManager托盘图标在安装后从ServerConfigurator启用加密。

9. 在**选择文件位置和产品语言**页面上，选择程序文件的**文件位置**。

   > 如果计算机上已经安装了任何 Milestone XProtect VMS 产品，则此字段将被禁用。该字段显示将要安装组件的位置。

10. 在**产品语言**中，选择安装 XProtect 产品时使用的语言。单击**安装**。

    软件现在即会安装。安装完成后，您会看到已成功安装的系统组件的列表。单击**关闭**。

11. 安装完故障转移记录服务器后，可使用 Failover Server 服务托盘图标检查其状态，并在 Management Client 中对其进行配置。有关详细信息，请参阅 第 165 页上的初始配置任务列表。

使用非默认端口安装 XProtect VMS

安装 XProtect VMS 需要特定的端口。尤其是 IIS 中运行的 Management Server 和 API Gateway，并且某些端口必须可用。本主题描述如何在 IIS 上安装 XProtect VMS 和使用非默认端口。这也适用于只安装 API Gateway 的情况。

有关视频管理软件使用的所有端口概述，请参阅 XProtect VMS 管理员手册 (https://doc.milestonesys.com/2023r3/zh-CN/portal/htm/chapter-page-mc-administrator-manual.htm)。

如果尚未在系统上安装 IIS，则 XProtect VMS 安装程序将安装 IIS 并使用具有默认端口的默认网站。

要避免使用 XProtect VMS 默认值，请首先安装 IIS。或者，添加新网站或继续使用默认网站。

如果 HTTPS 还没有绑定，则添加一个绑定，并在计算机上选择一个有效的证书（您需要在 XProtect VMS 安装过程中选择它）。编辑您选择的可用端口的 HTTP 和 HTTPS 绑定的端口号。

运行 XProtect VMS 安装程序并选择**自定义**安装。

在安装过程中，如果有多个网站可用，则会出现**在 IIS 上选择用于XProtect 系统的网站**页面。您必须选择要用于 XProtect 系统的网站。安装程序使用更改后的端口号。

通过命令行 shell 以静默方式安装（已解释）

使用静默安装，系统管理员可以通过大型网络安装和升级 XProtect VMS 和 Smart Client 软件，而无需与用户之间进行任何互动，对最终用户的干扰也很小。

XProtectVMS和SmartClient安装程序（.exe文件）具有不同的命令行变量。它们每个都有自己的命令行参数集，可以在命令行shell中或通过变量文件直接调用它们。在命令行shell中，您还可以在安装程序中使用命令行选项。

您可以将 XProtect 安装程序、它们的命令行参数和命令行选项与用于静默分发和安装软件的工具（例如 Microsoft System Center Configuration Manager（SCCM，也称为 ConfigMgr））结合使用。有关此类工具的详细信息，请访问制造商的网站。您还可以将 Milestone Software Manager 用于远程安装和更新 XProtect VMS、设备软件包和 Smart Client。有关详细信息，请参阅 Milestone Software Manager 的管理员手册。

命令行参数和变量文件

在静默安装期间，您可以指定与不同视频管理软件系统组件紧密相关的设置，以及它们与命令行参数和变量文件之间的内部通信。命令行参数和变量文件应仅用于新安装，因为您不能更改升级过程中命令行参数所代表的设置。

要查看可用的命令行参数并为安装程序生成变量文件，请在命令行 shell 中导航到安装程序所在的目录，然后输入以下命令：

```
[NameOfExeFile].exe --generateargsfile=[path]
```

示例：

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

在已保存的变量文件 (Arguments.xml) 中，每个命令行参数都有一个解释其用途的说明。您可以修改并保存该变量文件，以便命令行参数值适合您的安装需求。

如果要在安装程序中使用变量文件，请通过输入以下命令来使用 `--arguments` 命令行选项：

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

示例：

```
Milestone XProtect VMS Products 2023 R3 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

命令行选项

在命令行 shell 中，您还可以将安装程序与命令行选项结合使用。命令行选项通常会修改命令的行为。

要查看命令行选项的完整列表，请命令行 shell 中导航到安装程序所在的目录，然后输入 `[NameOfExeFile].exe --help`。为了使安装成功，您必须为需要值的命令行选项指定一个值。

您可以在同一命令中同时使用命令行参数和命令行选项。使用 `--parameters` 命令行选项，并用冒号 (:) 分隔每个命令行参数。在下面的示例中，`--quiet`、`--showconsole` 和 `--parameters` 为命令行选项，`ISFAILOVER` 和 `RECORDERNAME` 为命令行参数：

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

以静默方式安装 recording server

当您静默安装时，安装完成时不会通知您。要获得通知，请在命令中包含 `--showconsole` 命令行选项。安装完成后，将出现 Milestone XProtect Recording Server 托盘图标。

在下面的命令示例中，方括号 ([ ]) 内的文本和方括号本身都必须替换为实际值。示例：您可以输入 `d:\program files\`、`d:\record\` 或 `\\network-storage-02\surveillance` 代替 "[path]"。使用 `--help` 命令行选项来了解每个命令行选项值的合法格式。

1. 登录到要安装 Recording Server 组件的计算机。
2. 打开互联网浏览器，将 的以管理员为目标的 Management Server 下载网页地址输入到地址栏，然后按 Enter。

   地址通常是 `http://[management 服务器地址]:[端口]/installation/Admin/default-en-US.htm`。
3. 通过选择 **Recording Server 安装程序**下的**所有语言**，下载记录服务器安装程序。

4. 打开您的首选命令行 shell。要打开 Windows 命令提示符，请打开 Windows“开始”菜单，然后输入 **cmd**。
5. 使用下载的安装程序导航到该目录。
6. 根据以下两种情况之一，继续安装：

情况 1：升级现有安装，或使用具有默认值的 Management Server 组件在服务器上安装

- 输入以下命令，安装开始。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

情况 2：在分布式系统中安装

1. 输入以下命令以生成带有命令行参数的变量文件。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. 从指定路径打开变量文件 (Arguments.xml)，并在需要时修改命令行参数值。

> 确保为命令行参数 SERVERHOSTNAME 和 SERVERPORT 提供有效值。否则，安装无法完成。

4. 保存变量文件。
5. 返回到命令行 shell 并输入下面的命令，以使用在变量文件中指定的命令行参数值进行安装。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=[path]\[filename]
```

以静默方式安装 XProtect Smart Client

当您静默安装时，安装完成时不会通知您。要获得通知，请在命令中包含 `--showconsole` 命令行选项。安装完成后，桌面上将出现 XProtect Smart Client 的快捷方式。

在下面的命令示例中，方括号 ([]) 内的文本和方括号本身都必须替换为实际值。示例：您可以输入 `d:\program files\`、`d:\record\` 或 `\\network-storage-02\surveillance` 代替 "[path]"。使用 `--help` 命令行选项来了解每个命令行选项值的合法格式。

1. 打开互联网浏览器，将 的以最终用户为目标的 Management Server 下载网页地址输入到地址栏，然后按 Enter。

   地址通常是 `http://[management server address]:[port]/installation/default-en-US.htm`。

2. 通过选择**安装程序 XProtect Smart Client** 下的**所有语言**，下载 XProtect Smart Client 安装程序。
3. 打开您的首选命令行 shell。要打开 Windows 命令提示符，请打开 Windows“开始”菜单，然后输入 **cmd**。
4. 使用下载的安装程序导航到该目录。
5. 根据以下两种情况之一，继续安装：

情况 1：升级现有安装，或使用默认命令行参数值进行安装

- 输入以下命令，安装开始。

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet
```

情况 2：使用 xml 变量文件作为输入，用自定义命令行参数值进行安装：

1. 输入以下命令以生成带有命令行参数的变量 xml 文件。

```
"XProtect Smart Client 2023 R3 Installer.exe" --generateargsfile=
[path]
```

2. 从指定路径打开变量文件 (Arguments.xml)，并在需要时修改命令行参数值。
3. 保存变量文件。
4. 返回到命令行 shell 并输入下面的命令，以使用在变量文件中指定的命令行参数值进行安装。

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet --arguments=
[path]\[filename]
```

以静默方式安装日志服务器

当您静默安装时，安装完成时不会通知您。要获得通知，请在命令中包含 `--showconsole` 命令行选项。

在下面的命令示例中，方括号 ([]) 内的文本和方括号本身都必须替换为实际值。示例：您可以输入 `d:\program files\`、`d:\record\` 或 `\\network-storage-02\surveillance` 代替 "[path]"。使用 `--help` 命令行选项来了解每个命令行选项值的合法格式。

1. 登录到要安装 Log Server 组件的计算机。
2. 打开互联网浏览器，将 的以管理员为目标的 Management Server 下载网页地址输入到地址栏，然后按 Enter。

   地址通常是 `http://[management 服务器地址]:[端口]/installation/Admin/default-en-US.htm`。
3. 通过选择**日志服务器安装程序**下的**所有语言**，下载日志服务器安装程序。

4. 打开您的首选命令行 shell。要打开 Windows 命令提示符，请打开 Windows“开始”菜单，然后输入 **cmd**。
5. 使用下载的安装程序导航到该目录。
6. 根据以下两种情况之一，继续安装：

情况 1：升级现有安装，或使用默认命令行参数值进行安装

- 输入以下命令，安装开始。

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --showconsole
```

情况 2：使用 XML 变量文件作为输入，用自定义命令行参数值进行安装：

1. 输入以下命令以生成带有命令行参数的变量 xml 文件。

```
"XProtect Log Server 2023 R3 Installer x64.exe" --generateargsfile=
[path]
```

2. 从指定路径打开变量文件 (Arguments.xml)，并在需要时修改命令行参数值。
3. 保存变量文件。
4. 返回到命令行 shell 并输入下面的命令，以使用在变量文件中指定的命令行参数值进行安装。

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --arguments=
[path]\[filename] --showconsole
```

使用专用服务帐户静默安装

如果要无人值守安装 XProtect VMS，必须使用下表中的参数启动安装程序。安装之前，必须创建参数并将其保存在您生成的参数 XML 文件中。

参数	说明
`--quiet`	强制静默安装。
`--arguments`	包含完整配置的参数 XML 文件的路径。路径可能是：`C:\Arguments.xml`.
`--license`	许可证文件的路径。

使用专用服务帐户

此说明基于使用专用服务帐户来实现集成安全。无论哪个用户登录，服务始终在专用帐户上运行，您必须确保该帐户拥有执行任务以及访问网络、文件和共享文件夹等所需的所有权限。

必须在参数 XML 文件中为以下键指定服务帐户：

SERVICEACCOUNT
SERVICEACCOUNT_NONLOC

必须在以下键的值中以纯文本形式指定服务帐户的密码：

ENCRYPTEDPASSWORD

示例：在静默模式下启动安装的命令行：

```
"Milestone XProtect VMS Products 2023 R2 System Installer.exe" --quiet --
arguments=C:\Arguments.xml --license=C:\M01-C01-231-01-ABCDEF.lic
```

示例：基于使用专用服务帐户的参数文件

```
<?xml version="1.0" encoding="utf-8"?>
<CommandLineArguments xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:milestone-systems">
  <InstallEnvironment>
    <Parameters>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>USERACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT_NONLOC</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>sampleaccountpasswordplaintext</Value>
        <Key>ENCRYPTEDPASSWORD</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>%PROGRAMFILES%\Milestone</Value>
        <Key>TARGETDIR</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsXPCO</Key>
```

```
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsDPInstaller</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>false</Value>
        <Key>LEGACY</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>yes</Value>
        <Key>SQL-KEEP-DATA</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>no</Value>
        <Key>SQL-CREATE-DATABASE</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>True</Value>
        <Key>IS_EXTERNALLY_MANAGED</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_MS</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IDP;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IDP</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IM;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IM</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_ES</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_
LogServerV2;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated;Application
Name=Surveillance_LogServerV2</Value>
        <Key>SQL_CONNECTION_STRING_LOG</Key>
      </KeyValueParametersOfStringString>
    </Parameters>
  </InstallEnvironment>
</CommandLineArguments>
```

执行安装前必须满足的先决条件：

- 必须创建服务帐户以及用于执行安装的帐户。
- 必须允许服务帐户在执行安装的计算机上作为服务登录。请参见作为服务登录。
- 必须创建 XProtect 要使用的数据库，且必须在参数 XML 文件中命名数据库，例如：

数据库名称
Surveillance
Surveillance_IDP.
Surveillance_IM.
Surveillance_LogServerV2

- 必须根据以下列表配置数据库：

数据库配置
必须将默认排序规则设置为“SQL_Latin1_General_CP1_CI_AS”
ALLOW_SNAPSHOT_ISOLATION 必须设置为开
READ_COMMITTED_SNAPSHOT 必须设置为开

- 必须为服务帐户和用于在每个数据库中执行安装的帐户创建 SQL server 登录。必须在每个数据库中创建一个数据库用户，该用户必须是每个数据库中 db_owner 角色的成员。

工作组安装

如果您没有使用具有 Active Directory 服务器的域设置而是使用工作组设置，则在安装时执行以下操作。

> 分布式设置中的所有计算机都必须位于域或工作组中。

1. 使用共同管理员帐户登录 Windows。

   > 确保在系统中的所有计算机上使用相同的帐户。

2. 根据需要启动管理服务器或录制服务器安装并单击**自定义**。
3. 根据您在步骤 2 中的选择内容，选择使用共同管理员帐户来安装 Management Server 或 Recording

Server 服务。

4. 完成安装。
5. 重复步骤 1-4 安装要连接的任何其他系统。必须使用共同管理员帐户安装它们。

在群集中安装

在群集中安装之前，请参阅 第 113 页上的多台管理服务器(群集)(已解释) 和 第 114 页上的群集要求。

> 说明和插图可能与您在屏幕上看到的有所不同。

安装管理服务器：

1. 在群集中的第一台服务器上安装管理服务器及其所有子组件。

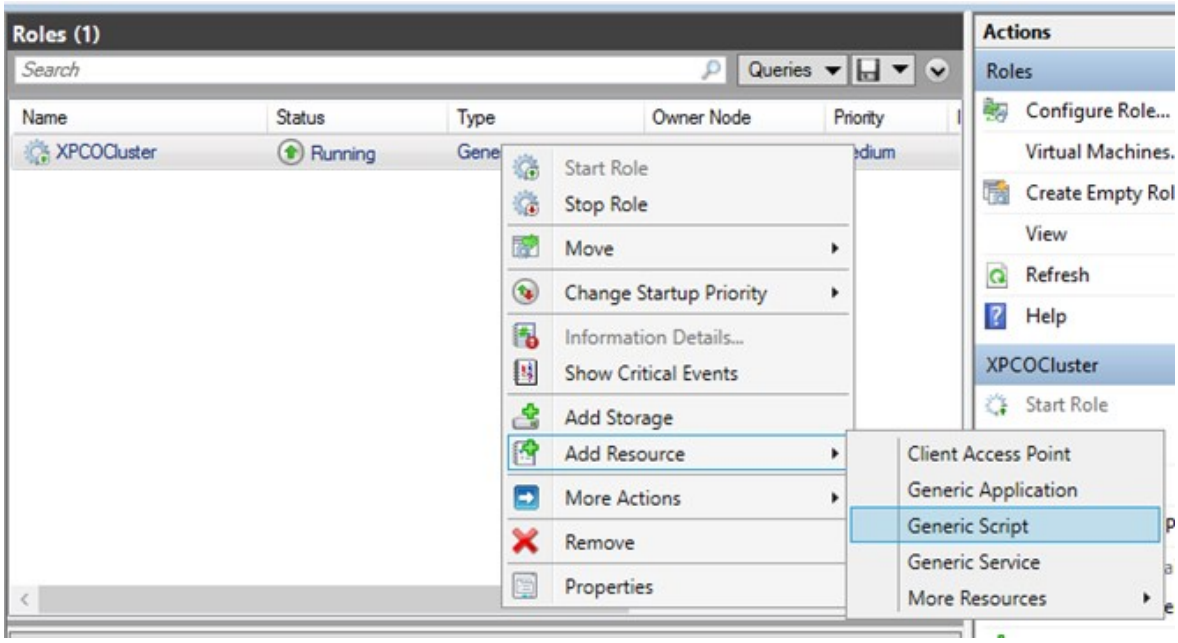
> 管理服务器必须与特定用户一起安装，而不是作为网络服务安装。这要求您使用**自定义**安装选项。此外，特定用户必须能够访问共享的网络驱动器，并且最好有非过期密码。

将 Management Server 服务配置为故障转移群集中的通用服务：

1. 在安装了管理服务器的最后一台服务器上，转到**开始 > 管理工具**，打开 Windows 的**故障转移群集管理**。在**故障转移群集管理**窗口中展开群集，右键单击**角色**，然后选择**配置角色**。

2. 在**高可用向导>在您开始之前**页面中，单击**下一步**。
3. 在**选择角色**页面上，选择**通用服务**，然后单击**下一步**。
4. 在**选择角色**页面上，选择**Milestone XProtect Management Server**服务，**然后单击下一步**。
5. 在**客户端访问点**页面上，指定客户在访问服务时使用的名称(群集的主机名)。主机名称必须与群集名称不同。单击**下一步**。
6. 在**选择存储**页面上，单击**下一步**，因为服务不需要存储。

7. 在**复制注册表设置**页面上，单击**下一步**，因为注册表设置不需要复制。
8. 在**确认页面上**，确认群集服务已根据您的要求配置后，单击**下一步**。
9. 在**配置高可用性**页面上，单击**下一步**。
10. 在**摘要页面**上，单击**完成**以完成管理服务器作为故障转移群集通用服务的配置。
11. 右键单击您刚刚创建的角色，然后单击**添加资源>通用脚本**。选择Milestone XProtect Event Server，将**Milestone XProtect Event Server**服务作为资源添加到**Milestone XProtect Management Server Cluster**服务。



12. 重复步骤 11，并在群集中添加所有必需的服务，例如 Log Server。Milestone XProtect Event Server和Data Collector server都应作为服务添加，以实现最佳部署。此外，应将Milestone XProtect Event Server设置为管理服务器的从属服务，以便事件服务器在管理服务器停止运行后也停止运行。
13. 所有添加的服务都会显示在窗口的底部窗格中。

更新群集 URL:

> 在进行配置更改时，在 Microsoft 故障转移群集管理器上，暂停对服务的控制和监视，以便 Server Configurator 可以进行更改并启动和/或停止 Management Server 服务。如果将故障转移群集服务启动类型更改为手动，则不应导致与 Server Configurator 的任何冲突。

在 Management Server 计算机上：

1. 在安装了管理服务器的每个计算机上启动 Server Configurator。
2. 转到**注册**页面。
3. 单击铅笔 ( ) 符号以使管理服务器地址可编辑。
4. 将管理服务器地址更改为群集的 URL，例如 `http://MyCluster`。
5. 单击**注册**。

在具有使用ManagementServer(例如RecordingServer、MobileServer、EventServer、APIGateway) 的组件的计算机上：

1. 在每个计算机上启动 Server Configurator。
2. 转到**注册**页面。
3. 将管理服务器地址更改为群集的 URL，例如 `http://MyCluster`。
4. 单击**注册**。

为集群环境中的外部 IDP使用证书

在单服务器环境中安装XProtect后，会用数据保护 API (DPAPI) 保护外部 IDP配置数据。如果您在集群中设置管理服务器，必须用证书保护外部 IDP配置数据，以确保流畅的节点故障转移。

有关如何生成证书的详细信息，请参阅 Milestone 证书指南。

必须将证书导入个人证书存储区，并使计算机信任证书。

若要设置数据保护，您必须添加证书的指纹到 Identity Provider 配置。

1. 将证书导入个人证书存储区并确保
   - 证书是有效的
   - Identity Provider app pool (IDP) 帐户拥有证书私钥的权限。

   有关如何验证帐户是否拥有证书私钥的权限的详细信息，请参阅 Milestone 证书指南。
2. 在 Identity Provider(`[Install path]\Milestone\XProtectManagement Server\IIS\Identity Provider`)安装路径中找到 `appsettings.json` 文件。
3. 在该部分中设置证书指纹：

```
"DataProtectionSettings": {
 "ProtectKeysWithCertificate": {
  "Thumbprint": ""
 }

},
```

4. 在所有管理服务器节点上重复步骤 3。
5. 强制执行节点故障转移，以确保证书设置正确。
6. 使用管理客户端再次登录，并应用外部提供商配置。如果已应用配置，则必须在管理客户端中重新输入来自外部 IDP 的客户端密码。

使用证书保护外部 IDP 配置时的错误故障排除

证书无效/证书已过期

如果已配置的指纹证书为不受信任或已过期的证书，则 Identity Provider 无法开始。Identity Provider 日志 (C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log) 将清楚表明证书是否无效。

解决方案：

确保证书是有效的，且在计算机上信任。

缺失证书私钥的权限

Identity Provider 无法在没有私钥权限的情况下保护数据。如果 Identity Provider 没有权限，则以下错误消息会写入 Identity Provider (C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log) 的日志文件：

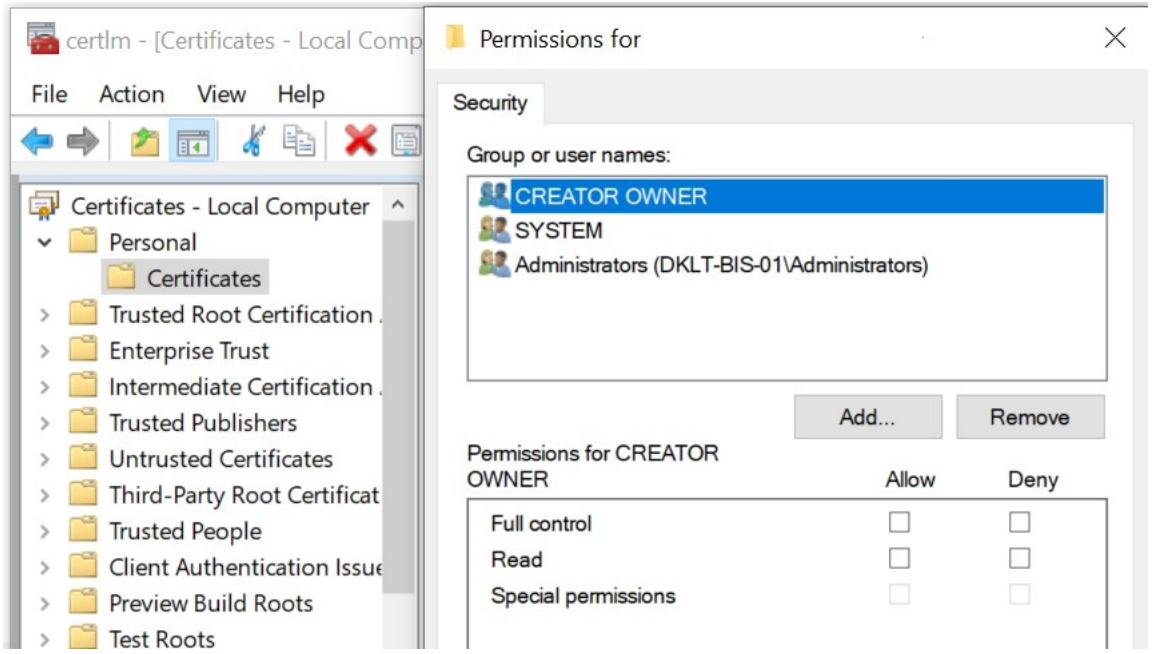
```
ERROR- An exception occurred while processing the key element '<key id="
[installation specific]" version="1" />'.
Internal.Cryptography.CryptoThrowHelper+WindowsCryptographicException:
Keyset does not exist
```

解决方案：

确保 Identity Provider app pool (IDP) 帐户拥有证书私钥的权限。

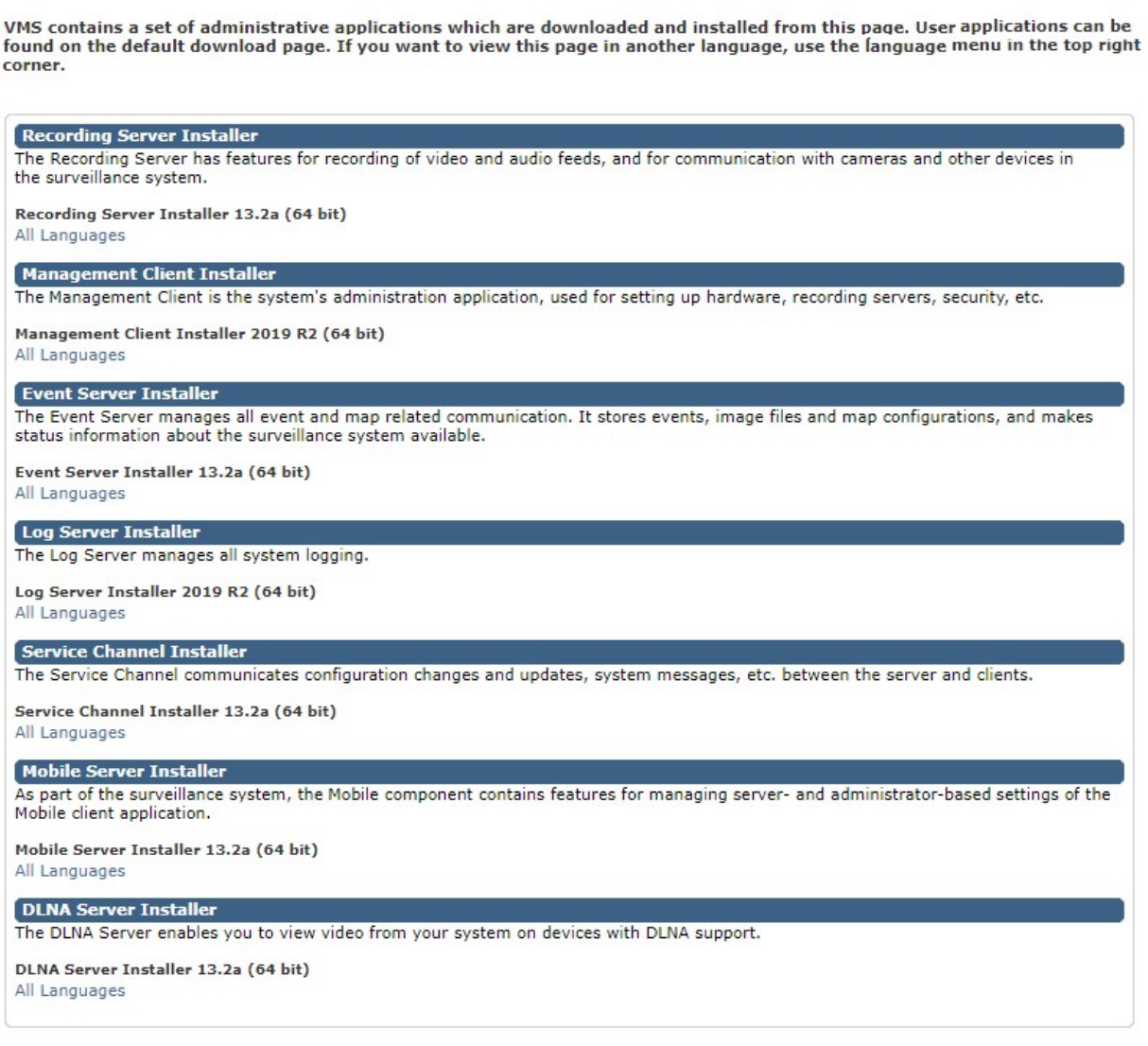
检查证书私钥的权限：

1. 选择 Windows 任务栏上的**开始**并打开管理计算机证书工具 (certlm.msc)。
2. 导航至个人证书存储区并找到用于加密的证书。
3. 右键单击证书，并选择**所有任务 > 管理私钥**。
4. 在**权限**下，确保 Identity Provider app pool (IDP) 帐户拥有读取权限。



Download Manager/下载网页

管理服务器具有内置网页。此网页可让管理员和最终用户从任意位置本地或远程下载和安装所需的 XProtect 系统组件。



该网页能够默认以匹配系统安装语言的语言版本显示两组内容：

- **一个网页以**管理员为目标，让他们可下载和安装关键系统组件。在大多数情况下，此网页在管理服务器安装结束时自动加载并显示默认内容。在管理服务器上，您可以访问该网页，步骤是先选择 Windows 的**开始**菜单，再选择**程序 > Milestone > 管理安装页面**。或者也可输入 URL：

  http://[management server address]:[port]/installation/admin/

  [管理服务器地址]是管理服务器的IP地址或主机名，[端口]是已为IIS配置的、在管理服务器中使用的端口号。

- **一个网页以最终**用户为目标，为他们提供采用默认配置的客户端应用程序的访问权限。在管理服务器上，可从 Windows 的**开始**菜单访问该网页，然后选择**程序 > Milestone > 公共安装页面**。或者也可输入 URL：

  http://[management server address]:[port]/installation/

  [管理服务器地址]是管理服务器的IP地址或主机名，[端口]是已为IIS配置的、在管理服务器中使用的端口号。

两个网页具有一些默认内容，因此可在安装结束后直接使用。但是，作为管理员，您可通过使用 Download Manager 来自定义网页上显示的内容。您也可在两个网页版本之间移动组件。要移动组件，请右键单击它，然后选择要将组件移动至其上的网页版本。

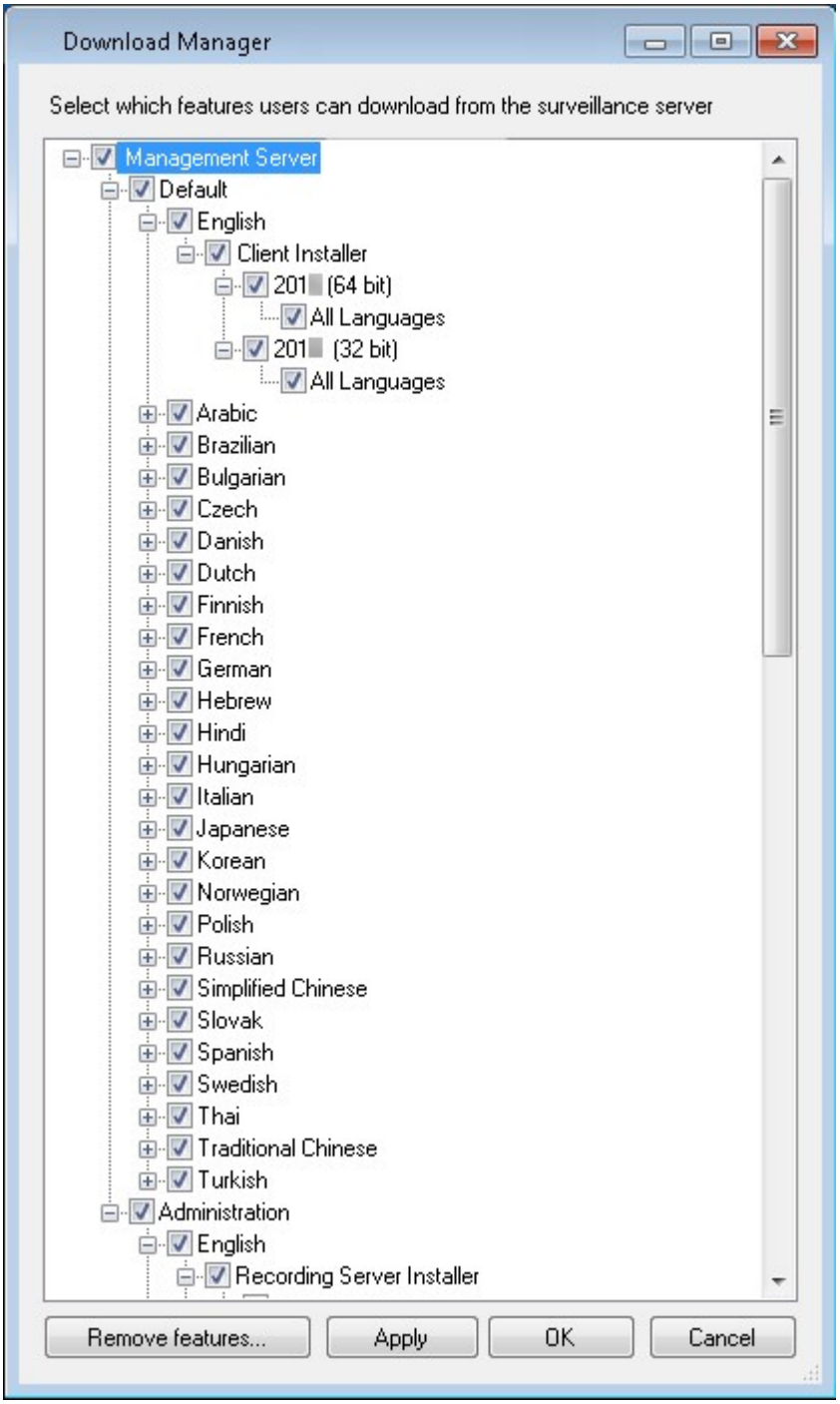
尽管可在 Download Manager 中控制用户可下载和安装哪些组件，但无法将它用作用户权限管理工具。此类权限由 Management Client 中定义的角色决定。

在管理服务器上，您可以访问 XProtect Download Manager，步骤是先选择 Windows 的**开始**菜单，再选择**程序 > Milestone > XProtect Download Manager**。

Download Manager 的默认配置

Download Manager 具有默认配置。这可确保组织中的用户能够从一开始就访问标准组件。

默认配置提供了默认设置，可下载额外或可选的组件。通常从管理服务器计算机访问该网页，但也可从其他计算机访问该网页。



- 第一层:是指您的 XProtect 产品
- 第二层:是指网页的两个目标版本。**默认**是指最终用户查看的网页版本。**管理**是指系统管理员查看的网页版本
- 第三层:是指网页的可用语言

- 第四层:是指用户可用(或通过操作使用户可用)的组件
- 第五层:是指用户可用(或通过操作使用户可用)的每个组件的具体版本
- 第六层:是指用户可用(或通过操作使用户可用)的组件的语言版本

最初仅提供标准组件(并且仅提供与系统本身相同的语言版本)这一点有助于减少安装时间和节省服务器的空间。如果无人使用,就无需在服务器上提供组件或语言版本。

您可以根据需要启用更多组件或语言,也可以隐藏或移除不需要的组件或语言。

Download Manager 的标准安装程序(用户)

默认情况下,以下组件可用于从管理服务器的以用户为目标的下载网页(由DownloadManager控制)进行单独安装:

- 记录服务器,包括故障转移记录服务器在您指定需要故障转移记录服务器 的安装过程中,故障转移记录服务器 最初作为记录服务器下载和安装。
- Management Client
- XProtect Smart Client
- 事件服务器,与地图功能结合使用
- 日志服务器,用于提供必要的系统信息记录功能
- XProtect Mobile 服务器
- 贵组织中可以提供更多选项。

有关设备包的安装,请参阅 第 163 页上的设备软件包安装程序 - 必须下载.

添加/发布 Download Manager 安装程序组件

必须完成两个步骤才能使非标准组件和新版本可用于管理服务器的下载网页。

首先将新组件和/或非标准组件添加到DownloadManager。然后,使用它微调应以网页的不同语言版本提供的组件。

如果 Download Manager 打开,需在安装新组件之前将其关闭。

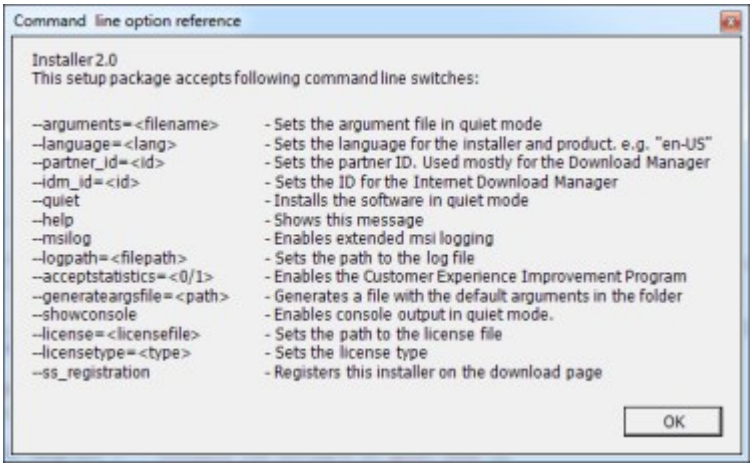
Download Manager将新/非标准文件添加到:

1. 在下载了组件的计算机上,转到 Windows 的**开始**,输入*命令提示符*
2. 在命令提示符*中,使用 :[space]--ss_registration*

   示例:示例:*MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   该文件现在即添加到 Download Manager,但未安装在当前计算机上。

要概览安装程序命令,在*命令提示符*中输入 [space]--*help*,将出现以下窗口:



安装了新组件之后，在 Download Manager 中会默认选中它们，并可通过网页立即向用户提供这些组件。可以通过选择或清除 Download Manager 树形结构中的复选框始终显示或隐藏网页上的功能。

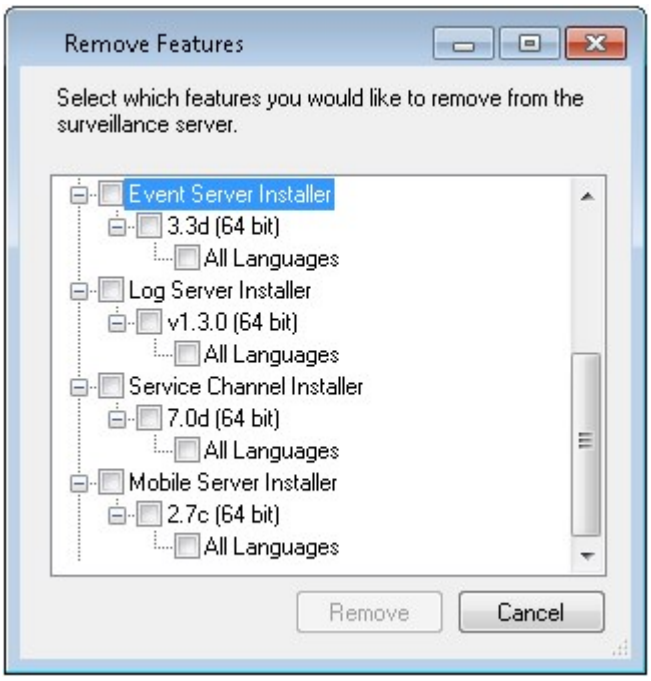
可以更改网页上组件的显示顺序。在 Download Manager 的树形结构中拖动组件项目，将其拉至所需的位置。

隐藏/删除 Download Manager 安装程序组件

有三个选项：

- **可以通过清除** Download Manager 树形结构中的复选框在网页上隐藏组件。组件仍然安装在管理服务器上，您可通过选中 Download Manager 树形结构中的复选框来快速地重新启用组件
- **删除管理服务器上安装的组件**。组件会从 Download Manager 上消失，但其安装文件会保留在 `C:\Program Files (x86)\Milestone\XProtect Download Manager` 中，如果需要，您以后可重新安装组件

  1. 在 Download Manager 中，单击**卸载功能**。
  2. 在**删除功能**窗口中，选择您要删除的功能。



  3. 单击**确定**，然后单击**是**。

- **从管理服务器**删除不需要的功能的安装文件。如果您了解到您的组织不会使用某些功能，上述操作将有助于节省服务器的磁盘空间

设备软件包安装程序 - 必须下载

Download Manager 上没有包括原始安装中包括的设备软件包(包含设备驱动程序)。如果您需要重新安装设备软件包或提供设备软件包安装程序，则必须先将最新的设备软件包安装程序添加或发布到Download Manager：

1. 从 Milestone 网站 (https://www.milestonesys.com/downloads/) 的下载页面获得最新的常规设备软件包。
2. 在同一页面中，您可以下载附带旧驱动程序的旧设备软件包。要检查您的摄像机是否使用旧版设备软件包中的驱动程序，请访问该网站 (https://www.milestonesys.com/community/business-partner-tools/device-packs/)。
3. Download Manager使用 *--ss_registration* 命令进行调用，将其添加/发布到 。

如果没有网络连接，您可以从 Download Manager 重新安装完整的 recording server。recording server 的安装文件位于本地计算机上，这样您便可以自动进行设备软件包的重新安装。

安装日志文件和故障排除

在安装、升级或卸载期间，日志条目将写入各种安装日志文件：主安装日志文件 `installer.log` 以及属于您要安装的不同系统组件的日志文件。所有日志条目都有一个时间戳，最近的日志条目位于日志文件的末尾。

您可以在 `C:\ProgramData\Milestone\Installer\` 文件夹中找到所有安装日志文件。名为 *I.log 或 *I[整数].log 的日志文件是有关新安装或升级的日志文件，而名为 *U.log 或 *U[整数].log 的日志文件是有关卸载的日志文件。如果您已通过 XProtect 合作伙伴购买已经安装了 Milestone 系统的服务器，则可能没有任何安装日志文件。

日志文件包含命令行参数和命令行选项及其在安装、升级或卸载期间所使用的值的有关信息。要在日志文件中查找使用的命令行参数，请根据日志文件搜索**Command Line:**或**Parameter '**。

在故障排除时，首先要看的地方是主安装日志文件 installer.log。如果在安装期间出现过任何异常、错误或警告，则这些已被记录下来。尝试搜索**exception**、**error**或**warning**。“退出代码：0”表示安装成功，“退出代码：1”则相反。您在日志文件中的调查结果可能会使您在Milestone知识库上找到解决方案。如果不能，请与您的 Milestone 合作伙伴联系并共享相关的安装日志文件。

配置

初始配置任务列表

以下检查表列出了配置系统的初始任务。其中一些任务，您可能已在安装过程中完成。

完整的检查表自身并不保证系统完全满足您组织的确切需求。为使系统满足组织的需求，Milestone 建议持续监控和调整系统。

例如，在系统运行时，对不同物理条件下(包括白天/夜晚和有风/无风天气)单个摄像机的移动侦测灵敏度设置进行测试和调整是不错的作法。

规则设置用于确定系统执行的大多数动作(包括何时记录视频)，这是您可以根据组织需求进行更改的配置的另一个示例。

步骤	说明
☑	您已完成系统的初始安装。 请参阅 第 126 页上的安装新的 XProtect 系统。
☑	视需要将试用 SLC 更改为永久性 SLC。 请参阅 第 106 页上的更改软件许可证号。
☑	登录到 Management Client。 请参阅 第 29 页上的登录(已作说明)。
☐	验证每个记录服务器的存储设置是否满足您的需求。 请参阅 第 51 页上的存储和存档(已解释)。
☐	验证每个记录服务器的存档设置是否满足您的需求。 请参阅 第 357 页上的存储和记录设置属性。
☐	侦测将添加到每个记录服务器的硬件(摄像机或视频编码器)。 请参阅 第 185 页上的添加硬件。
☐	配置每个记录服务器的各个摄像机。 请参阅 第 371 页上的摄像机(“设备”节点)。
☐	为单个摄像机或一组摄像机启用存储和存档。从单个摄像机或从设备组完成该操作。 请参阅 第 172 页上的将设备或一组设备连接到存储。

步骤	说明
☐	启用并配置设备。 请参阅 第 369 页上的设备(“设备”节点)。
☐	规则将在很大程度上确定系统的行为。您创建一些用于定义的规则，例如定义摄像机应在何时录制、全景-倾斜-变焦 (PTZ) 摄像机应在何时巡视，以及应在何时发送通知。 创建规则。 请参阅 第 68 页上的规则和事件(已作说明)。
☐	将角色添加到系统。 请参阅 第 60 页上的角色和角色权限(已作说明)。
☐	将用户或用户组添加到每个角色。 请参阅 第 249 页上的将用户和组分配至角色/从角色删除。
☐	激活许可证。 请参阅 第 104 页上的联机激活许可证 或 第 105 页上的脱机激活许可证。

有关如何在**站点导航**窗格中配置系统的详细信息，请参阅 第 330 页上的站点导航窗格。

记录服务器

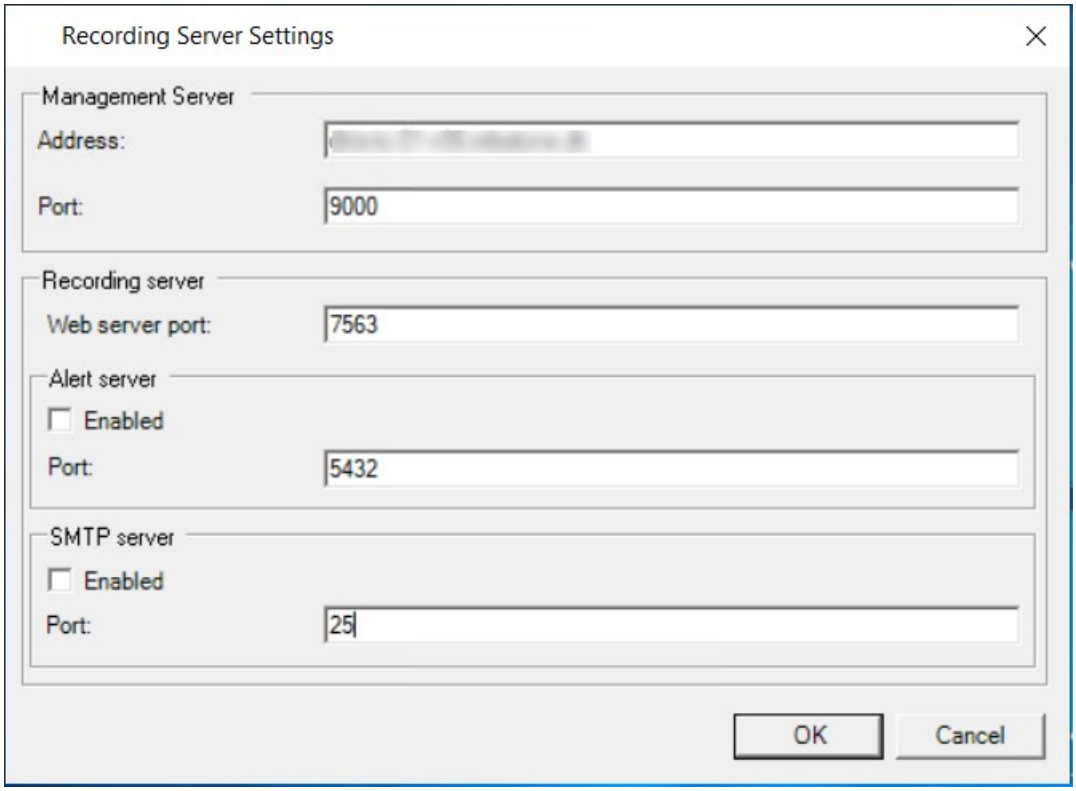
更改或验证记录服务器的基本配置

Management Client 如果未列出已安装的所有记录服务器，最可能的原因是您在安装过程中错误配置了设置参数(例如，管理服务器的 IP 地址或主机名)。

无需重新安装 recording server 以指定管理服务器的参数，但可以更改/验证其基本配置：

1. **在运行 Recording Server 的计算机上**，右键单击通知区域中的 Recording Server 图标。
2. 选择**停止 Recording Server 服务**。
3. **再次右键单击** Recording Server 图标，选择更**改设**置。

   随即显示**记录服务器设置**窗口。



4. 验证或更改，例如，以下设置：
   - **管理服务器**：**地址**：指定记录服务器应连接的管理服务器的 IP 地址或主机名。
   - **管理服务器**：**端口**：指定要在与管理服务器通信时使用的端口号。您可以根据需要进行更改，但该端口号必须始终匹配管理服务器上设置的端口号。请参阅 第 84 页上的本系统使用的端口。
   - **记录服务器**：**Web 服务器端口**：指定与记录服务器的 Web 服务器通信时要使用的端口号。请参阅 第 84 页上的本系统使用的端口。
   - **记录服务器**：**提醒服务器端口**：启用并指定与记录服务器的提醒服务器（监听来自设备的事件消息）进行通信时要使用的端口号。请参阅 第 84 页上的本系统使用的端口.
   - **SMTP 服务器**：**端口**：启用并指定与记录服务器的简单邮件传输协议 (SMTP) 服务进行通信时要使用的端口号。请参阅 第 84 页上的本系统使用的端口.
5. 单击**确定**。
6. 要再次启动 Recording Server 服务，请右键单击**记录服务器**图标，并选择**启动 Recording Server 服务**。

停止 Recording Server 服务意味着当您验证/更改记录服务器的基本配置时，不能录制和查看实时视频。

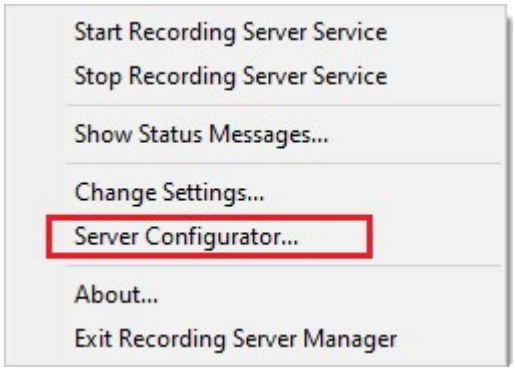
注册记录服务器

安装记录服务器时，大多数情况下会自动注册。但出现以下情况时需要手动注册：

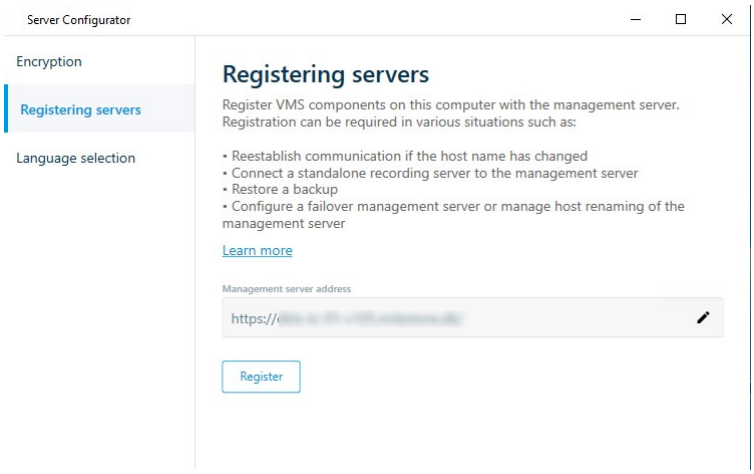
- 您已更换记录服务器
- 记录服务器脱机安装，然后添加到了管理服务器
- 您的管理服务器不使用默认端口。端口号取决于加密配置。有关详细信息，请参阅 第 84 页上的本系统使用的端口。
- 自动注册失败，例如，在更改管理服务器地址、更改带有记录服务器的计算机的名称之后，或者在启用或禁用服务器通信加密设置之后。有关更改管理服务器地址的详细信息，请参阅更改管理服务器计算机的主机名。

在注册记录服务器时，将其配置为连接至管理服务器。处理注册的管理服务器的组成部分是 Authorization Server 服务。

1. 从 Windows“开始”菜单或者从记录服务器托盘图标打开 Server Configurator。



2. 在 Server Configurator中，选择**注册服务器**。



3. 验证管理服务器的地址以及您希望计算机上的服务器连接到的方案(http 或 https)，然后单击**注册**。

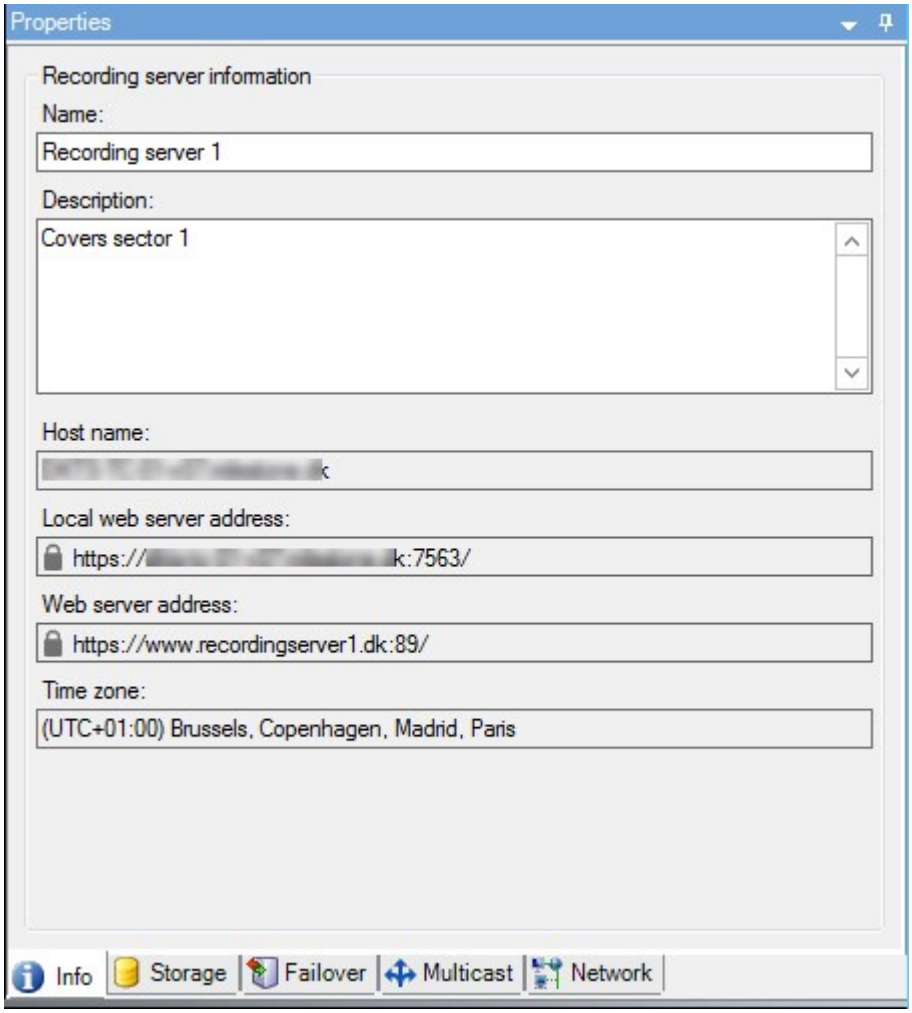
显示确认，表明在管理服务器上的注册已成功。

另请参阅 第 294 页上的更换记录服务器。

查看客户端的加密状态

要验证您的记录服务器是否加密连接：

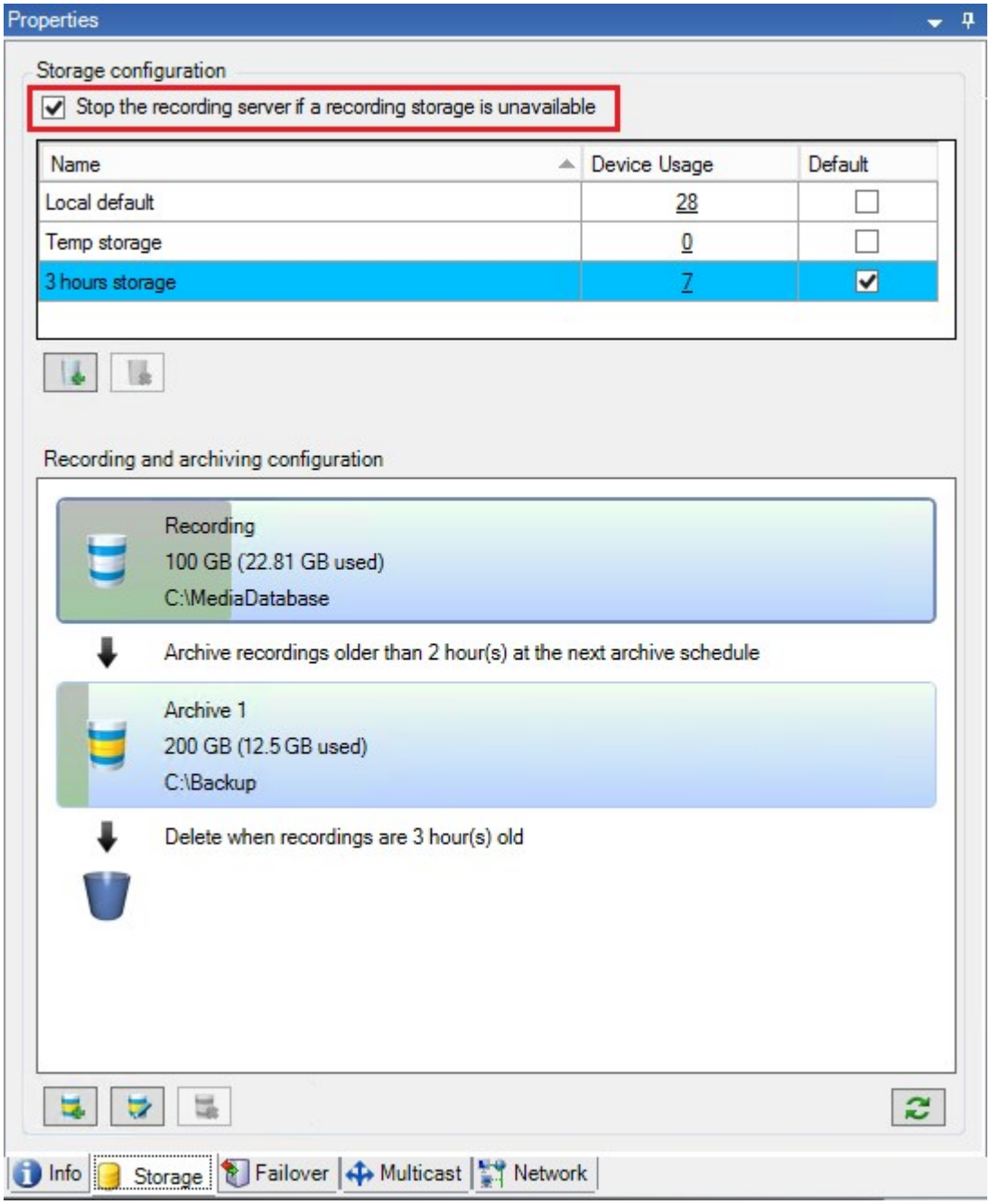
1. 打开 Management Client。
2. 在**站点导航**窗格中，选择**服务器 > 记录服务器**。这会打开记录服务器列表。
3. 在**总览**窗格中，选择相关的记录服务器，然后转到**信息**选项卡。
   如果已对从记录服务器检索数据流的客户端和服务器启用加密，则会在本地 Web 服务器地址和可选 Web 服务器地址前面显示挂锁图标。



指定录制存储不可用时的行为

默认情况下，在记录存储不可用时记录服务器将继续运行。如果系统配置了故障转移记录服务器，您可以指定记录服务器停止运行，以便使故障转移服务器接管：

1. 在相关的记录服务器上，进入**存储**选项卡。
2. 选择**在记录存储不可用时停止运行记录服务器**选项。



添加新存储

添加新存储时，您将始终使用名为 **Recording** 的预定义录像数据库来创建录像存储。您无法重命名数据库。除了录像存储之外，存储还可包含大量存档。

1.  要将额外存储添加到所选记录服务器，单击存**储**配置列表下方的按钮。**将打开**存储和记录设置对话框。
2. 指定相关设置(请参阅 第 357 页上的存储和记录设置属性)。
3. 单击**确定**。

如果需要，现在可以在新存储中创建存档。

在存储中创建存档

存储没有默认的存档，但是您可以自行创建存档。

1. 请在**录制和存档配置**列表中选择相关存储。
2. 单击**录制和存档配置**列表下的  按钮。
3. 在**存档设置**对话框中，指定所需设置(请参阅 第 359 页上的存档设置属性)。
4. 单击**确定**。

将设备或一组设备连接到存储

一旦为记录服务器配置了存储，即可为单个设备(例如摄像机、麦克风或扬声器)或一组设备启用该配置。您也可以选择要为单个设备或设备组使用记录服务器的哪些存储区域。

1. 展开**设备**，根据需要选择**摄像机**、**麦克风**或**扬声器**。
2. 选择设备或设备组。
3. **选择**记录选项卡。
4. **在**存储区域，选取**选**择。
5. **在出现的对话框中**，选择应存储设备记录的数据库，然后单击确定。
6. 在工具栏中，单击**保存**。

在记录服务器的“存储”选项卡上单击存储区域的设备使用数时，可在显示的消息报告中看到设备。

禁用的设备

默认情况下，禁用的设备不会显示在**概览**窗格中。

要显示所有禁用的设备，请在**概览**窗格的顶部单击**筛选器**以打开**筛选器**选项卡并选择**显示禁用的设备**。

要再次隐藏禁用的设备，请取消选中**显示禁用的设备**。

编辑所选存储或存档的设置

1. **要编辑存储**，请在记录和存档配置列表中选择其记录数据库。要编辑存档，请选择存档数据库。
2. 单击**记录和存档配置**列表下的  编辑记录存储**按钮**。
3. 编辑记录数据库或编辑存档。

如果更改数据库的最大大小，系统会自动存档超出新限制的记录。它会将记录自动存档至下一个存档或删除它们，具体取决于存档设置。

启用数字签名以便导出

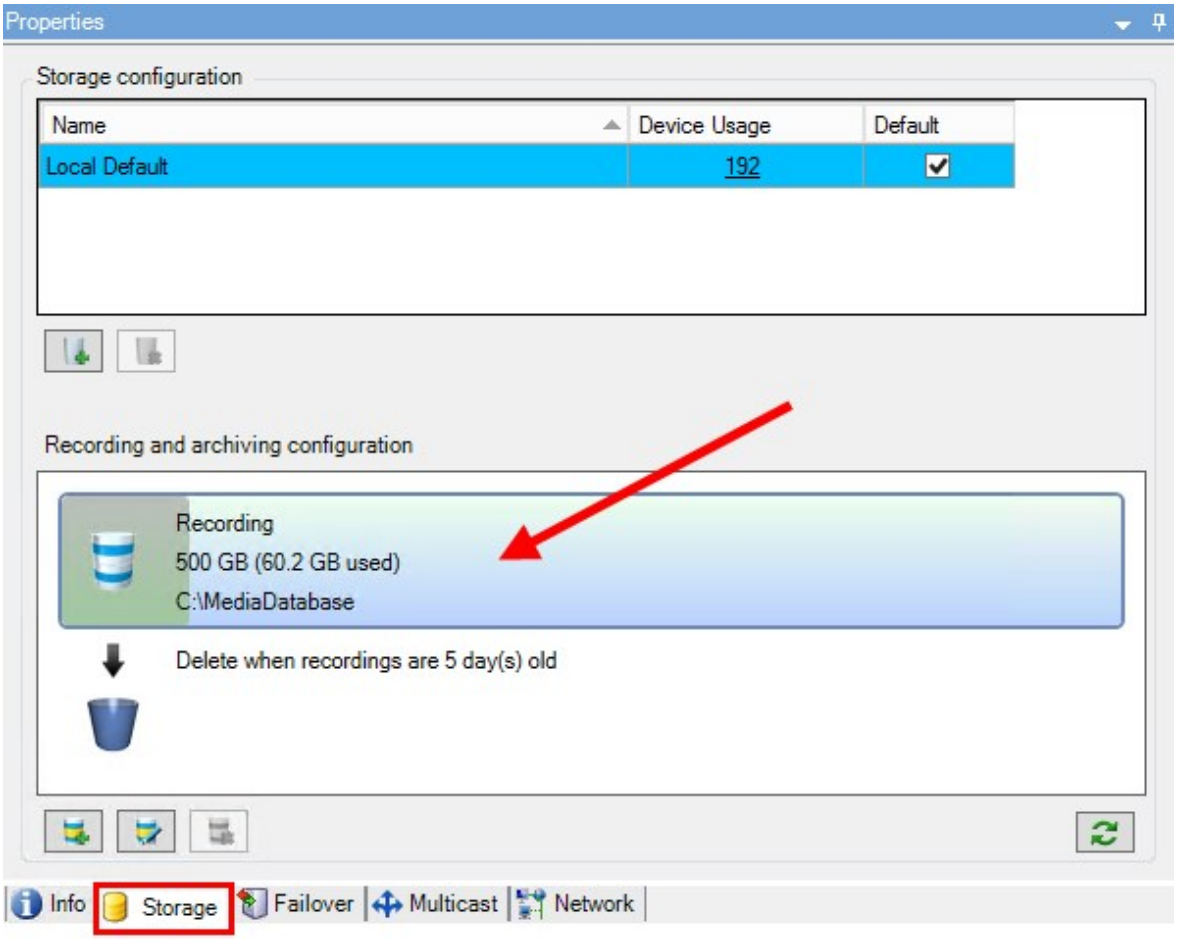
可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

您可以为录制的视频启用数字签名，以便客户端用户确认视频自录制后未被篡改。导出视频后，用户需要在XProtect Smart Client - Player 中对视频进行身份验证。

签名也必须在 XProtect Smart Client > **导出**选项卡 > **导出设置** > **XProtect格式** > **包含数字签名**中激活。否则，XProtect Smart Client - Player 中的**验证签名**按钮不会显示。

1. 在**站点导航**面板中展开**服务器**节点。
2. 单击**记录服务器**。
3. 在“总览”窗格中，单击要为其启用签名的记录服务器。

4. 在**属性**窗格的底部单击**存储**选项卡。



5. 在**录制和存储配置**部分，双击代表录制数据库的水平栏。此时会显示**存储和录制设置**窗口。
6. 选择**签名**复选框。
7. 单击**确定**。

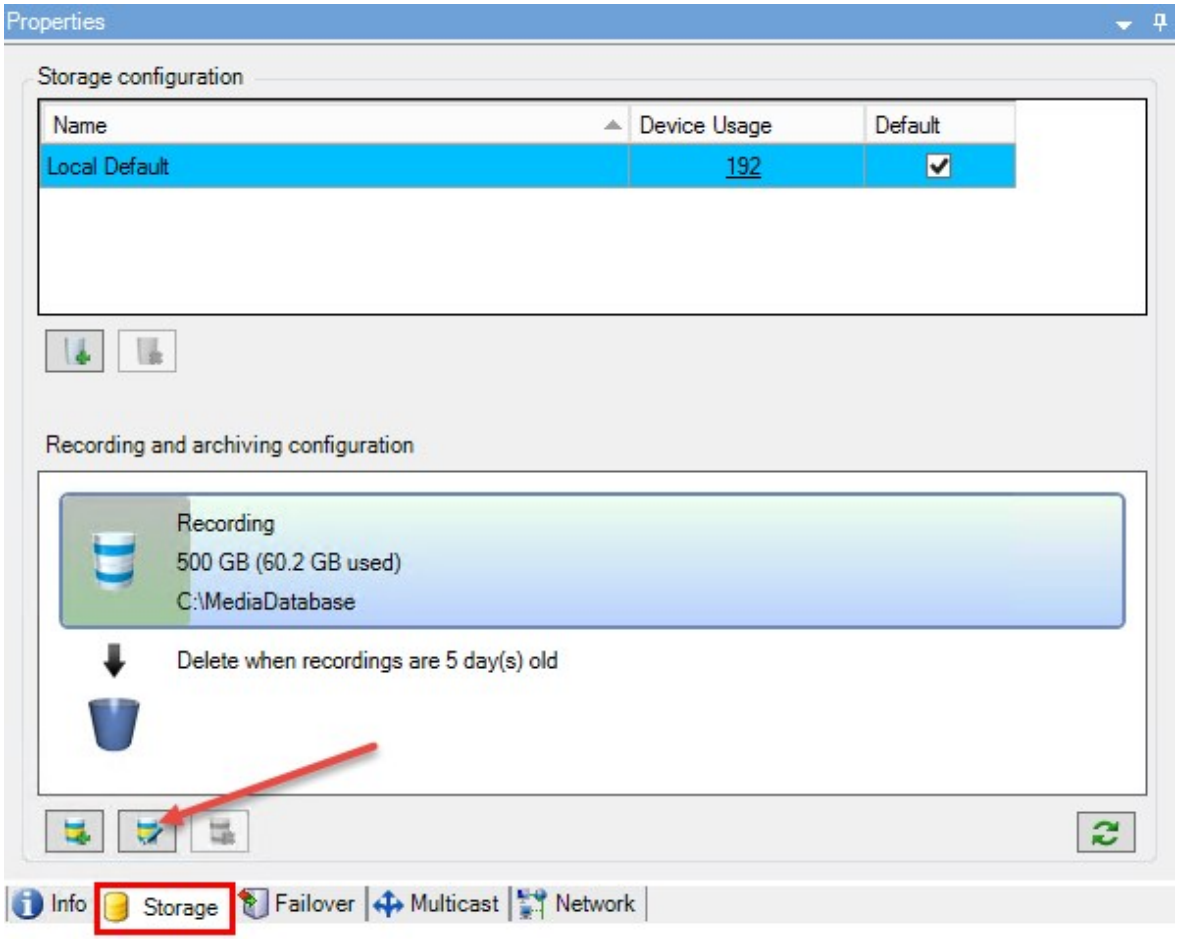
为记录加密

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

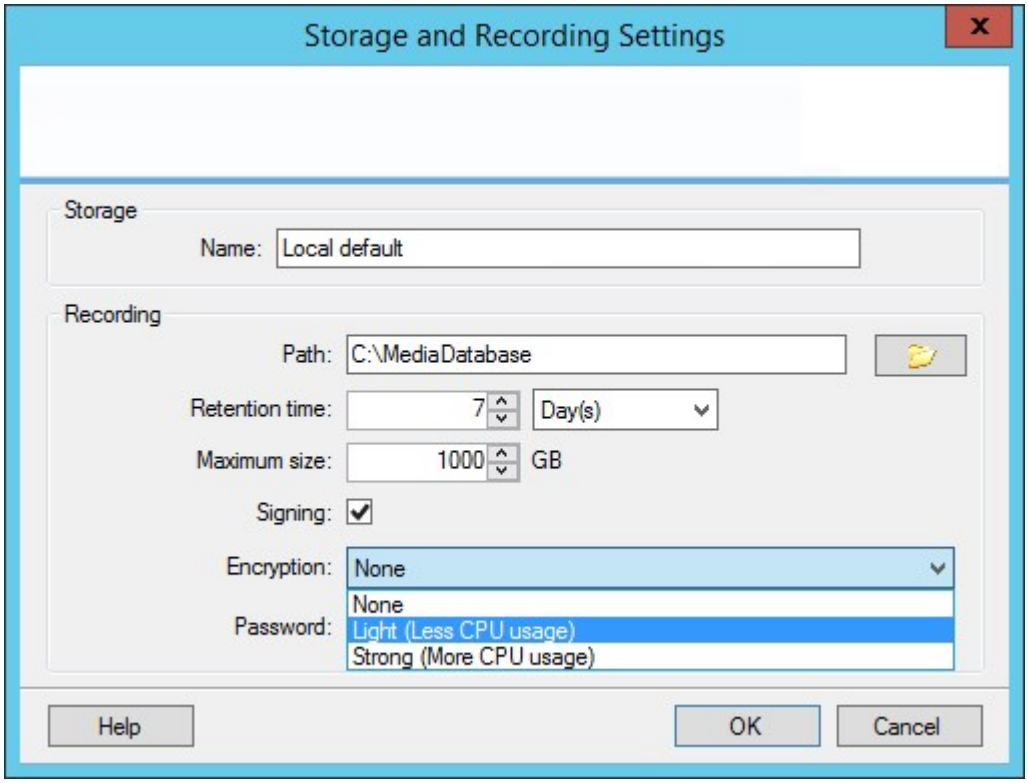
您可以在记录服务器的存储和存档上启用加密，以保护记录。您可以选择轻加密和强加密。启用加密时，还必须指定相关密码。

启用或更改加密设置或密码可能会耗费时间，具体取决于数据库的大小和驱动的性能。
您可以按照**当前任务**中的过程进行操作。
任务正在进行时，**请勿停止**记录服务器。

1. 单击**记录和存档配置**列表下的**编辑记录存储**按钮。



2. 在出现的对话框中，指定加密级别。



3. 系统会自动将您导向到**设置密码**对话框。输入密码并单击**确定**。

备份存档的记录

许多组织希望使用磁带驱动器或类似设备备份记录。具体做法高度个人化，并取决于组织中使用的备份介质。但是，需要记住以下方面：

备份存档，而不是摄像机数据库

始终基于存档的内容而不是基于各摄像机数据库来创建备份。如果根据各摄像机数据库的内容创建备份，可能导致共享冲突或其他故障。

在计划备份时，请确保备份作业不会与指定的存档时间重叠。要在记录服务器的各存储区域中查看各记录服务器的存档计划，请查看**存储**选项卡。

为了确保备份过程中不会发生存档，可以卸载存档，执行备份，然后再次安装存档。安装和卸载存档是通过 Milestone Integration Platform VMS API 进行的。

了解您的存储结构，以便有目标地进行备份

当存档记录时，它们存储在存档内的特定子目录结构中。

在您系统的所有常规使用中，当系统用户使用 XProtect Smart Client 浏览所有录像时，子目录结构将对系统用户完全透明。这对于已存档和未存档记录同样适用。了解子目录的结构非常重要(请参阅 第 55 页上的存档结构(已解释))。如果要备份已存档的记录(请参阅 第 286 页上的备份和还原系统配置)。

从存储中删除存档

1. 从**记录和存档配置**列表中选择存档。

> 只可能删除列表中的最后一个存档。存档不必为空。

2. 单击位于**录制和存档配置**列表下的  按钮。
3. 单击**是**。

> 对于不可用的存档，例如脱机存档，无法验证存档是否包含具有证据锁定的媒体，但可以在用户确认后删除存档。

> 无法删除包含具有证据锁定的媒体的可用存档(联机存档)。

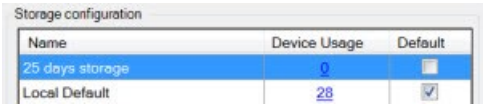
删除存储

您无法删除被设备用作实时录制录像存储的默认存储或存储。
这意味着，您可能需要在删除存储之前，将设备及其尚未存档的任何记录移至其他存储(请参阅 第 295 页上的移动硬件)。

1. 要查看在使用该存储的设备的列表，请单击设备使用数。

> 如果存储中包含已移动到另一个记录服务器的设备的数据，则会显示警告。单击此链接可查看设备的列表。

2. 执行 第 178 页上的将未存档记录从一个存储移动到另一个存储 中的步骤。
3. 继续操作，直至所有设备移动完毕。
4. 选择要删除的存储。



5. 单击  存档配置**列表下的** 按钮。
6. 单击**是**。

将未存档记录从一个存储移动到另一个存储

可从设备的**记录**选项卡中将一个实时记录数据库中的记录移动到另一个实时记录数据库。

1. 选择设备类型。在**总览**窗格中，选择设备。
2. 单击**记录**选项卡。在**存储**区域的上部，单击**选择**。
3. 在**选择存储位置**对话框中，选择数据库。
4. 单击**确定**。
5. 在**记录动作**对话框中，选择是否要移除已存在(但**未存档**到新存储)的记录，或者选择是否要删除它们。
6. 单击**确定**。

分配故障转移记录服务器

在记录服务器的**故障转移**选项卡上，可选择三种不同类型的故障转移设置：

- 无故障转移设置
- 主要/次要故障转移设置(冷待机)
- 热后备设置

如果选择 **b** 和 **c**，则必须选择特定服务器/组。如果选择 **b**，还可选择次要故障转移组。如果记录服务器变得不可用，来自主要故障转移组的故障转移记录服务器将进行接管。如果还选择了次要故障转移组，当主要故障转移组中的所有故障转移记录服务器正忙时，来自次要组的故障转移记录服务器将进行接管。这样，您面临的风险只是在主要和次要故障转移组中的所有故障转移记录服务器都正忙时不能提供故障转移解决方案，而这种情况相当少见。

1. 在**站点导航**窗格中，选择**服务器 > 记录服务器**。这会打开记录服务器列表。
2. 在**总览**窗格中，选择所需的记录服务器，然后转到**故障转移**选项卡。
3. 若要选择故障转移设置类型，请在两者之间进行选择：
   - **无**
   - **主要故障转移服务器组/次要故障转移服务器组**
   - **热后备服务器**

   不可选择相同的故障转移组作为主要和次要故障转移组，也不可选择已经属于故障转移组的常规故障转移服务器作为热后备服务器。
4. 然后，单击**高级故障转移设置**。这会打开**高级故障转移设置**窗口，其中列出了连接到所选记录服务器的所有设备。如果选择了**无**，即可使用高级故障转移设置。系统会保留所做的选择，用于以后的故障转移设置。
5. 要指定故障转移支持的级别，请在列表中为各设备选择**全力支持**、**仅实时**或**禁用**。单击**确定**。
6. 在**故障转移服务通信端口 (TCP)** 字段中，根据需要编辑端口号。

如果您启用了故障转移支持，并且记录服务器被配置为在没有录制存储的情况下继续运行，那么故障转移记录服务器将不会接管。为了执行故障转移支持工作，您必须选择**存储**选项卡上的**如果录制存储不可用，则停止记录服务器**选项。

为记录服务器启用多播

在常规网络通信中，会将一个发件人的各个数据包发送至一个接收方，这就是单播过程。不过，在使用多播时，可以将一个数据包(从服务器)发送至某组内的多个接收方(客户端)。多播可帮助节省带宽。

- 当使用**单播**时，源必须为各接收方传输一个数据流
- 当使用**多播**时，各网段上只要求一个数据流

此处所述的多播**不是**视频从摄像机流向服务器，而是从服务器流向客户端。

使用多播，您使用的是已定义的接收方组，它们基于各种选项，如 IP 地址范围、为单个摄像机启用/禁用多播的能力、定义最大可接受数据包大小 (MTU) 的能力、数据包必须在其间转发的路由器的最大数量 (TTL) 等。

即使记录服务器使用加密，也不会加密多播流。

多播不应与**广播**混淆，后者会将数据发送给连接到网络的任何人，即使数据可能并非与每个人都相关：

名称	说明
单播	将数据从单个来源发送至单个接收方。
多播	将数据从单个来源发送至明确定义的组内的多个接收方。
广播	将数据从单个来源发送至网络上的每个人。因此广播会大幅降低网络通信速度。

要使用多播，您的网络基础结构必须支持 IP 多播标准 IGMP(Internet 组管理协议)。

- 在**多播**选项卡上，选中**多播**复选框

如果多播的整个 IP 地址范围已经在一个或多个记录服务器上使用，则您必须首先释放一些多播 IP 地址，然后才能在其他记录服务器上启用多播。

即使记录服务器使用加密，也不会加密多播流。

为单个摄像机启用多播

只有在为相关摄像机启用多播后，才能使用多播：

1. 在**总览**窗格中，选择记录服务器，并选择所需的摄像机。
2. 在**客户端**选项卡上，选中**实时多播**复选框。对所有相关摄像机重复该操作。

即使记录服务器使用加密，也不会加密多播流。

定义公共地址和端口

如果您需要在公共或不可信网络中以 XProtect Smart Client 访问 VMS，Milestone 建议您通过 VPN 使用安全连接。这能帮助确保 XProtect Smart Client 和 VMS 服务器之间的通信得到保护。

在网络选项卡上定义记录服务器的公共 IP 地址。

为什么使用公共地址?

客户端可能从本地网络以及从互联网连接，在这两种情况下，监控系统都必须提供适当的地址以使得客户端可从记录服务器访问实时和记录的视频：

- 当客户端从本地连接时，监控系统应使用本地地址和端口号回复
- 当客户端从互联网连接时，监控系统应回复记录服务器的公共地址。这是防火墙或 NAT(网络地址转换)路由器的地址，通常也有不同的端口号。地址和端口随后可转发到服务器的本地地址和端口。

1. **要启用公共访问**，请选中启用公共访问复选框。
2. 定义记录服务器的公共地址。输入防火墙或 NAT 路由器的地址，以便从互联网访问监控系统的客户端能够连接到记录服务器。
3. 指定公共端口号。防火墙或 NAT 路由器上使用的端口号最好不同于本地使用的端口号。

在使用公共访问时，请配置防火墙或 NAT 路由器，以便将发送到公共地址和端口的请求转发到相关记录服务器的本地地址和端口。

指定本地 IP 范围

您可以定义监控系统应识别为来自本地网络的本地 IP 范围的列表：

- 在**网络**选项卡上，单击**配置**

筛选设备树

如果您有许多已注册的设备，**总览**窗格中的设备树可能会变得非常大。您可以筛选设备树，以便更容易地找到要使用的设备。

通过使用一些特定设备独有的筛选条件，可以只显示这些特定设备，非常高效。

筛选设备树

- 在**总览**窗格的顶部，单击**筛选器**以打开**筛选器**选项卡。
- 在**在此处输入条件以筛选设备**字段中，输入一个或多个筛选条件，然后单击**应用筛选器**以筛选设备列表。

筛选条件特征

筛选条件适用于设备名称、设备短名称、硬件地址 (IP)、设备 ID 和硬件 ID 字段值。

筛选硬件 ID 和设备 ID 字段值时，部分筛选器匹配项不会显示。因此，在按硬件 ID 或设备 ID 进行筛选时，必须定义完整且准确的标识码。

对于设备名称、设备短名称和硬件地址字段值，会显示部分筛选器匹配项，因此使用筛选器术语“camer”时，将显示设备名称中包含“camera”的所有设备。

筛选条件不区分大小写，使用 "camera" 或 "Camera" 作为筛选条件将获得相同的结果。

指定多个筛选条件

您可以指定多个筛选条件，进一步缩小设备树的筛选范围。应用筛选器时，所有定义的筛选条件都被视为用 AND 连接，这意味着这些条件是叠加的。

例如，如果您输入了两个筛选条件：“摄像机”和“仓库”，则列表会显示设备名称中同时包含“摄像机”和“仓库”的所有设备，但不会显示设备名称中同时包含“摄像机”和“停车场”的设备，也不会显示设备名称中只包含“摄像机”的设备。

如果您指定的筛选器限制范围太窄，请从筛选器字段中移除单个筛选条件，以扩大筛选器限制范围。移除筛选条件时，筛选器会自动应用于设备树。

重置筛选器

如果您从筛选器字段中移除所有筛选器条件，**总览**窗格将重置并重新显示所有设备。

您也可以按 **F5** 重置筛选器并清除**显示禁用的设备**复选框。

禁用的设备

默认情况下，禁用的设备不会显示在**概览**窗格中。

要显示所有禁用的设备，请在**概览**窗格的顶部单击**筛选器**以打开**筛选器**选项卡并选择**显示禁用的设备**。

要再次隐藏禁用的设备，请取消选中**显示禁用的设备**。

故障转移服务器

设置和启用故障转移记录服务器

> 如果禁用了故障转移记录服务器，则必须首先将其启用，然后才能使其从标准记录服务器接管。

执行以下操作来启用故障转移记录服务器和编辑其基本属性：

1. 在**站点导航**窗格中，选择**服务器>故障转移服务器**。这会打开已安装故障转移记录服务器和故障转移组的列表。
2. 在**总览**窗格中，选择所需的故障转移记录服务器。
3. 右键单击并选择**已启用**。该故障转移记录服务器现在即会启用。
4. 要编辑故障转移记录服务器属性，请转到**信息**选项卡。
5. 完成后，转到**网络**选项卡。可在此处指定故障转移记录服务器的公共 IP 地址等信息。在使用 NAT（网络地址转换）和端口转发时会涉及这些信息。有关详细信息，请参阅标准记录服务器的**网络**选项卡。
6. 在**站点导航**窗格中，选择**服务器 > 记录服务器**。选择您想要获得故障转移支持的记录服务器，并分配故障转移记录服务器（请参阅 第 359 页上的“故障转移”选项卡（记录服务器））。

若要查看故障转移记录服务器的状态，请将鼠标放在通知区域的 Failover Recording Server Manager 托盘图标上。随即出现工具提示，会显示在故障转移记录服务器的“说明”字段中输入的文本。这可以帮助您确定故障转移记录服务器配置为从哪台记录服务器进行接管。

> 故障转移记录服务器会定期 ping 管理服务器，以验证其是否上线以及是否能够在需要时请求和接收标准记录服务器的配置。如果阻止 ping，故障转移记录服务器无法从标准记录服务器接管。

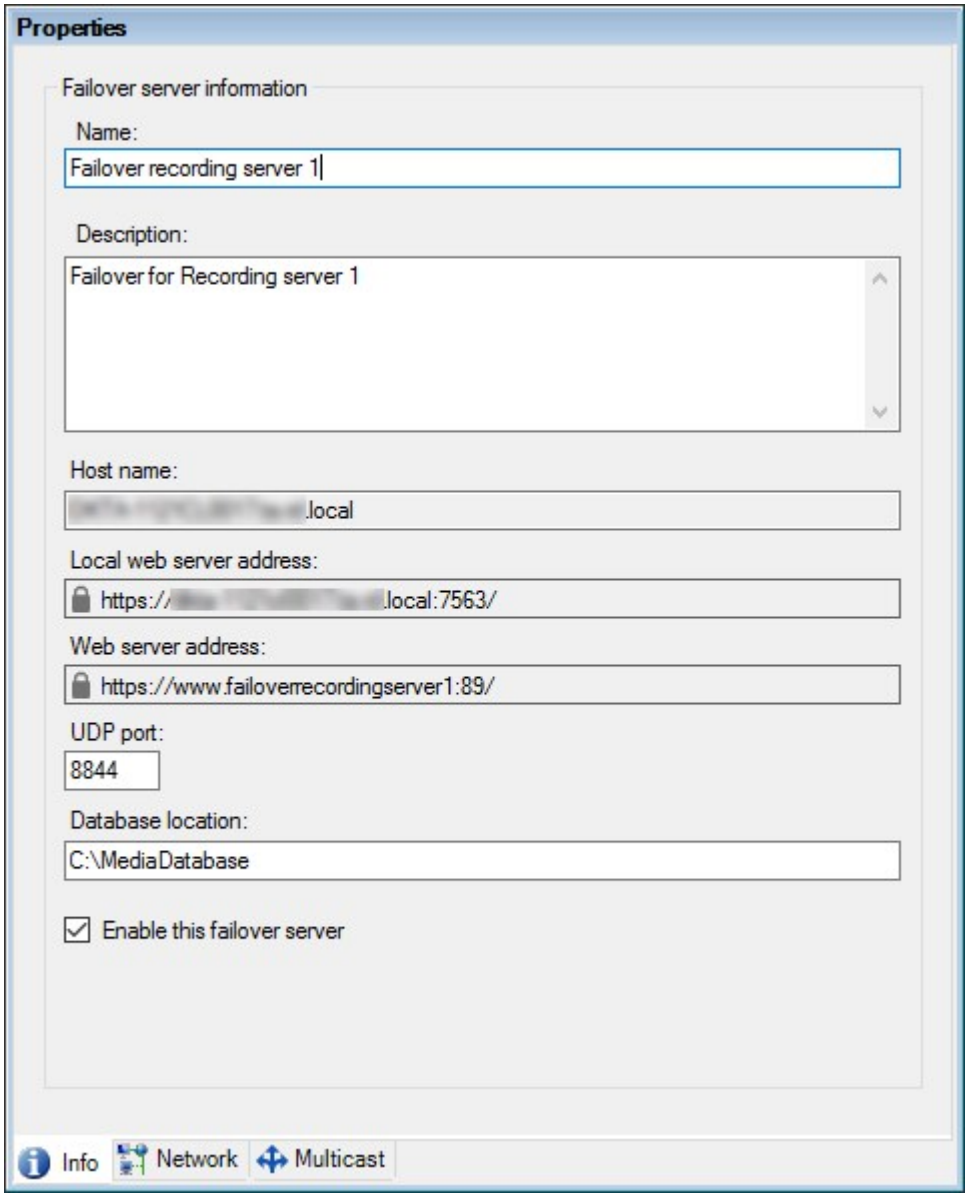
为冷后备故障转移记录服务器分组

1. 选择**服务器 > 故障转移服务器**。这会打开已安装故障转移记录服务器和故障转移组的列表。
2. 在**总览**窗格中，右键单击顶级节点**故障转移组**，然后选择**添加组**。
3. 为新组指定名称（在本例中为*故障转移组 1*）和说明（可选）。单击**确定**。
4. 右键单击您刚才创建的组（*故障转移组 1*）。选择**编辑组成员**。这会打开**选择组成员**窗口。
5. 通过拖放操作或使用按钮将所选故障转移记录服务器从左侧移到右侧。点击**确定**。*所选故障转移记录服务器现在即属于您刚才创建的组*（故障转移组 1）。
6. 转到**片断**选项卡。单击**向上**和**向下**来设置组中常规故障转移记录服务器的内部顺序。

查看故障转移记录服务器上的加密状态

要验证故障转移记录服务器是否使用加密，请执行以下操作：

1. 在**站点导航**窗格中，选择**服务器 > 故障转移服务器**。这会打开故障转移记录服务器列表。
2. 在**总览**窗格中，选择相关的记录服务器，然后转到**信息**选项卡。
   如果已对从记录服务器检索数据流的客户端和服务器启用加密，则会在本地 Web 服务器地址和可选 Web 服务器地址前面显示挂锁图标。



查看状态消息

1. 在故障转移记录服务器，右键单击 **Milestone Failover Recording Server 服务**图标。
2. 选择**显示状态消息**。将出现**故障转移服务器状态消息**窗口，其中列出添加有时间戳的状态消息。

查看版本信息

如果需要联系产品支持部门，那么知道 **Failover Recording Server 服务**的确切版本将非常有用。

1. 在故障转移记录服务器，右键单击 **Milestone Failover Recording Server 服务**图标。
2. 选择**关于**。
3. 出现一个小对话框，其中显示 **Failover Recording Server 服务**的确切版本。

硬件

添加硬件

有多个选项可用于为系统中的每台记录服务器添加硬件。

> 如果硬件位于已启用 NAT 的路由器或防火墙之后，您可能需要指定不同的端口号并配置路由器/防火墙，使其映射硬件使用的端口和 IP 地址。

添加硬件向导可帮助您检测网络上的硬件（例如摄像机和视频编码器），并将它们添加至本系统上的记录服务器。该向导还可帮助您为 Milestone Interconnect 设置添加远程记录服务器。**一次仅为**一台记录服务器添加硬件。

1. 要访问**添加硬件**，请右键单击所需记录服务器并选择**添加硬件**。
2. 选择其中一个向导选项（参见下文）并遵照屏幕说明操作。
3. 安装后，您可以在**总览**窗格中查看硬件及其设备。

> 首次添加硬件时，必须预配置某些硬件。添加此类硬件时，将出现另一个**预配置硬件设备**向导。有关详细信息，请参阅 第 48 页上的硬件预配置（已解释）。

添加硬件（对话框）

硬件包括以下两种：

- 直接通过 IP 连接到监控系统记录服务器的物理单元，例如摄像机、视频编码器和 I/O 模块
- Milestone Interconnect 设置中位于远程站点上的记录服务器

要了解如何向系统添加硬件的详细信息，请参阅 第 185 页上的添加硬件。

名称	说明
高速(推荐)	系统自动扫描记录服务器本地网络上的新硬件。 **选中**显示在其他记录服务器上运行的硬件复选框以查看检测到的硬件是否正在其他记录服务器上运行。 每次向网络添加新硬件并希望在系统中使用该新硬件时可选择此选项。 不能使用此选项在 Milestone Interconnect 设置中添加远程系统。 要同时添加 HTTP 和 HTTPS 硬件，请依次分别选中 **HTTPS(安全)** 单选按钮和 **HTTP(不安全)** 单选按钮来运行**快速**检测。
地址范围扫描	系统将基于以下规格扫描网络寻找相关硬件和 Milestone Interconnect 远程系统： • 硬件用户名和密码。如果硬件使用出厂默认用户名和密码，则不需要 • 驱动程序 • IP 范围(仅 IPv4) • 端口号(默认值为 80) 如果您只想扫描网络的一部分(例如，在扩展系统时)，可选择此选项。
手动	单独指定有关每个硬件和 Milestone Interconnect 远程系统的详细信息。如果您只想添加为数不多的硬件且知道其 IP 地址、相关用户名和密码，或者摄像机不支持自动发现功能，则这是较理想的选择。
远程连接硬件	系统会扫描通过远程连接服务器连接的硬件。 如果您已安装服务器用于(例如) Axis One-click 摄像机连接，则可以使用此选项。 不能使用此选项在 Milestone Interconnect 设置中添加远程系统。

禁用/启用硬件

添加的硬件默认为已启用。

可通过此方法查看硬件是否已被启用/禁用：

已启用
已禁用

禁用添加的硬件(例如出于授予许可或性能目的)

1. 展开记录服务器，右键单击要禁用的硬件。
2. **选择**已启用以将其清除或选中。

编辑硬件

右键单击添加的硬件，然后选择**编辑硬件**以修改 Management Client 中的硬件的网络配置和用户身份验证设置。

编辑硬件(对话框)

对于某些硬件，您还可通过**编辑硬件**对话框将设置直接应用于硬件设备。

如果选中**编辑 Management Client 设置**单选按钮，则**编辑硬件**对话框将显示 Management Client 用于连接到硬件的设置。为确保将硬件设备正确添加到系统，请输入用于连接到制造商的硬件配置界面的相同设置：

名称	说明
名称	显示硬件的名称及其检测到的 地址(在括号中)。
硬件 URL	制造商的硬件配置界面的网址，通常包含硬件的 IP 地址。指定网络中的有效地址。
用户名	用于连接到硬件的用户名。 您在此处输入的用户名不会更改实际硬件设备上的用户名。选择**编辑 Management Client 和硬件设置**单选按钮以修改支持的硬件设备上的设置。
密码	用于连接到硬件的密码。 您在此处输入的密码不会更改实际硬件设备上的密码。选择**编辑 Management Client 和硬件设置**单选按钮以修改支持的硬件设备上的设置。 有关如何更改多个硬件设备上的密码的信息，请参阅 第 191 页上的更改硬件设备上的密码。 作为系统管理员，您需要授予其他用户在 Management Client 中查看密码的权限。有关详细信息，请参阅“硬件”下的角色设置。

如果(为支持的硬件)选中**编辑 Management Client 和硬件设置**单选按钮，则**编辑硬件**对话框将显示有关设置，这些设置也直接应用于硬件设备：

在选中此单选按钮的情况下应用设置将会覆盖硬件设备上的当前设置。在应用设置时，硬件将暂时失去与记录服务器的连接。

名称	说明
名称	显示硬件的名称及其检测到的地址(在括号中)。
网络配置	硬件的网络设置。要调整网络设置，请选择 第 188 页上的配置。
配置	使用 **IP 版本**下拉列表(为支持的硬件设备)指定互联网协议。 • 对于 IPv4，值必须采用以下格式：**(0-999).(0-999).(0-999).(0-999)** • 对于 IPv6，值必须采用八组十六进制数字的格式，每组用冒号分隔。子网掩码必须是介于 **0-128** 之间的数字。 **检查**按钮将测试系统中当前是否存在使用输入的 IP 地址的另一硬件设备。 **检查**无法检测到与已关闭、XProtect VMS 系统外部或暂时没有响应的硬件设备的冲突。
用户名	用于连接到硬件的用户名和级别。从下拉列表中选择另一个用户并使用下面描述的**密码**字段添加新密码。 使用第 189 页上的添加用户部分底部带下划线的操作添加或删除用户(请参阅 第 189 页上的删除用户 或)。 选择不具有制造商指定的最高用户级别的用户可能会导致某些功能不可用。
密码	用于连接到硬件的密码。使用**显示**图标查看当前输入的文本。 更改密码时，请查阅制造商的文档以获取特定硬件设备的密码规则，或使用**生成密码**图标自动生成符合要求的密码。 有关如何更改多个硬件设备上的密码的信息，请参阅 第 191 页上的更改硬件设备上的密码。

名称	说明
	作为系统管理员，您需要授予其他用户在 Management Client 中查看密码的权限。有关详细信息，请参阅“硬件”下的角色设置。
添加 用户	选择带下划线的**添加**链接以打开**添加用户**对话框，并将用户添加到硬件设备。 添加用户会自动将其设置为当前活动用户，并覆盖之前输入的凭据。 创建密码时，请查阅制造商的文档以获取特定硬件设备的密码规则，或使用**生成密码**图标自动生成符合要求的密码。 在硬件设备上检测到的最高用户级别将自动被预先选中。不建议修改**用户级别**的默认值。 选择的**用户级别**如果不是制造商指定的最高用户级别，则可能会导致某些功能不可用。
删除 用户	选择带下划线的**删除**链接以打开**删除用户**对话框，并从硬件设备中删除用户。 您无法删除当前活动用户。要设置新用户，请使用上述**添加用户**对话框，然后使用此界面删除旧用户。

启用/禁用各设备

摄像机默认为**已启用**。

麦克风、扬声器、元数据、输入和**输出**默认为**已禁用**。

这意味着，必须分别启用麦克风、扬声器、元数据、输入和输出，然后才能在系统中使用它们。其原因在于，监控系统依赖于摄像机，而麦克风等的使用则高度取决于每个组织的需要。

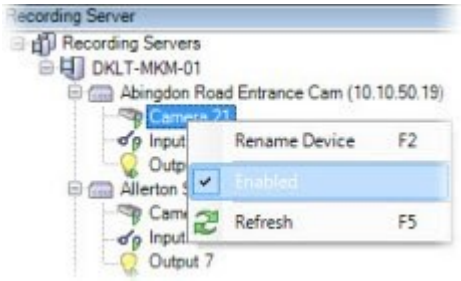
可查看是否已启用/禁用设备(示例显示了输出)：

已禁用

已启用

摄像机、麦克风、扬声器、元数据、输入和输出使用相同的启用/禁用方法。

1. 展开记录服务器和设备。右键单击要启用的设备。
2. **选择**已启用以将其清除或选中。



建立到硬件的安全连接

可使用 SSL(安全套接字层)在硬件和记录服务器之间建立安全 HTTPS 连接。

在继续后续步骤前,请咨询摄像机供应商,以获取硬件证书并将其上传至硬件:

1. **在**总览窗格中,右键单击记录服务器,然后选择硬件。

2. **在**设置选项卡上,启用 HTTPS。默认情况下,未启用。
3. 输入建立 HTTPS 连接所用的记录服务器端口。端口号必须与设备主页上所设置的端口相对应。
4. 根据需要,进行更改并保存。

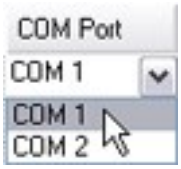
在视频编码器上启用 PTZ

要在视频编码器上启用 PTZ 的使用,请在 PTZ 选项卡上执行以下操作:

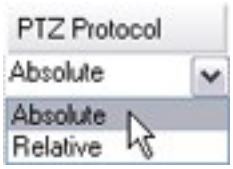
1. **在连接至视频解码器的设备列表中**,为相关摄像机选择启用 PTZ 复选框:

2. **在** PTZ 设备 ID 栏中,检查每个摄像机的 ID。

3. 在 **COM 端口**栏中，选择用于控制 PTZ 功能的视频解码器 COM(串行通信)端口：



4. **在** PTZ 协议栏中，选择想要使用的定位方案：



   - **绝对**：当操作员使用摄像机的 PTZ 控件时，摄像机会相对于固定位置(通常是指摄像机的初始位置)进行调整
   - **相对**：当操作员使用摄像机的 PTZ 控件时，摄像机会相对于其当前位置进行调整

   PTZ协议栏中的内容根据硬件不同会有很大差异。部分会有5到8个不同的协议。另请参阅摄像机文档。

5. 在工具栏中，单击**保存**。

6. 现在即可为每个 PTZ 摄像机配置预设位置和巡视：

   - 添加预设位置(类型 1)
   - 添加巡视配置文件

更改硬件设备上的密码

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

您可以在一次操作中更改多个硬件设备上的密码。

最初，支持的设备是 Canon、Axis、Bosch、Hanwa、Panasonic、Sony、Hikvision 和 ONVIF 兼容硬件设备的型号，但是用户界面会直接向您显示某种型号是否受支持。您也可以访问我们的网站，了解某个型号是否受支持：https://www.milestonesys.com/community/business-partner-tools/supported-devices/

对于不支持设备密码管理的设备，您必须从其网页更改硬件设备的密码，然后在 Management Client 中手动输入新密码。有关详细信息，请参阅 第 187 页上的编辑硬件。

您可以选择：

- 让系统为每个硬件设备生成单独的密码。系统根据硬件设备制造商的要求生成密码。
- 对所有硬件设备使用单个用户定义的密码。应用新密码时，硬件设备会暂时失去与记录服务器的连接。应用了新密码后，屏幕上将显示每个硬件设备的结果。对于不成功的更改，如果硬件设备支持此类信息，则会显示失败的原因。在向导中，您可以创建成功和失败的密码更改报告，但这些结果同时也会记录在**服务器日志**下。

> 对于具有 ONVIF 驱动程序和多个用户帐户的硬件设备，只有具有硬件设备管理权限的 XProtect 管理员能够从 VMS 更改密码。

要求：

- 硬件设备型号通过 Milestone 支持设备密码管理。

步骤：

1. 在**站点导航**窗格中，选择**记录服务器**节点。
2. 右键单击总览窗格中相关的记录服务器或硬件。
3. 选择**更改硬件密码**。将显示向导。
4. 使用大小写字母、数字和以下字符输入密码：**! ( ) * - . _**

   密码最大长度为 64。

> BoschFLEXIDOMEIP室外5000MPNDN-50051摄像头的密码最大长度为19个字符。

5. 按照屏幕上的说明完成更改。

> **密码上次更改**字段根据更改密码的计算机的本地时间设置显示最新密码更改的时间戳。

6. 最后一页显示结果。如果系统无法更新密码，请单击硬件设备旁边的**失败**查看原因。
7. 您还可以单击**打印报告**按钮查看成功和不成功更新的完整列表。
8. 如果要更改失败的硬件设备上的密码，请单击**重试**，这时向导将从失败的硬件设备重新开始。

> 如果选择**重试**，那么从第一次完成向导后，您将无法再访问该报告。

> 由于安全限制，如果您连续多次更改密码失败，那么有些硬件设备可能在一段时间内不可用。不同制造商的安全限制各不相同。

更新硬件设备上的固件

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

Management Client 使您可以更新已添加到视频管理软件系统的硬件的固件。如果多个硬件设备与同一固件文件兼容，则可以同时更新多个硬件设备的固件。

如果某个型号支持固件更新，则会直接向您显示用户界面。您也可以访问 Milestone 网站，了解某个型号是否受支持：https://www.milestonesys.com/community/business-partner-tools/supported-devices/

对于不支持固件更新的设备，必须从其网页更新硬件设备的固件。

更新固件时，硬件设备会暂时断开与记录服务器的连接。

更新固件后，屏幕上将显示每个硬件设备的结果。对于不成功的更改，如果硬件设备支持此类信息，则会显示失败的原因。结果也记录在**服务器日志**下。

对于具有 ONVIF 驱动程序和多个用户帐户的硬件设备，只有具备硬件设备管理权限的 XProtect 管理员才能从视频管理软件更新固件。

要求：

- 硬件设备型号支持通过 Milestone 进行固件更新。

步骤：

1. 在**站点导航**窗格中，选择**记录服务器**节点。
2. 右键单击总览窗格中相关的记录服务器或硬件。
3. 选择**更新硬件固件**。将显示向导。
4. 按照屏幕上的说明完成更改。

   您只能更新与同一固件文件兼容的多个硬件设备。通过 ONVIF 驱动程序添加的硬件位于**其他**下，而不是其制造商名称下。

6. 最后一页显示结果。如果系统无法更新固件，请单击硬件设备旁边的**失败**查看原因。

如果选择的固件文件或硬件设备不兼容，则 Milestone 对硬件设备故障不承担任何责任。

添加并配置外部 IDP

1. 在 Management Client 中，选择**工具 > 选项**并打开**外部 IDP** 选项卡。
2. 在**外部 IDP** 部分中，选择**添加**。
3. 输入外部 IDP 的信息。如需详细了解所需信息，请参阅外部 IDP。

有关如何从您想要在 VMS 中使用的外部 IDP 中登记索赔的详细信息，请参阅从外部 IDP 登记索赔。

设备 - 组

添加设备组

1. 在**总览**窗格中，右键单击要在其下创建设备组的设备类型。
2. 选择**添加设备组**。
3. 在**添加设备组**对话框中，指定新设备组的名称和说明：

当鼠标指针悬停在设备组列表中的设备组上时会显示说明。

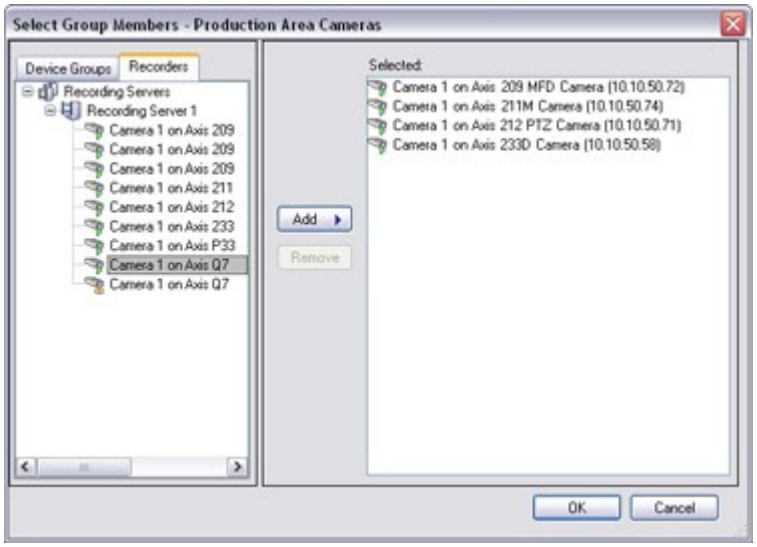
4. 单击**确定**。列表中会显示代表新设备组的文件夹。
5. 继续指定设备组中要包含的设备(请参阅 第 194 页上的指定设备组中要包含的设备)。

指定设备组中要包含的设备

1. 在**总览**窗格中，右键单击相关的设备组文件夹。
2. 选择**编辑设备组成员**。
3. 在**选择组成员**窗口中，选择一个选项卡以找到设备。

设备可能为一个以上设备组的成员。

4. 选择要包含的设备，然后单击**添加**或双击设备：



5. 单击**确定**。
6. 如果一个组中超出了 400 台设备这一限制，可在其他设备组下添加设备组作为子组：

禁用的设备

默认情况下，禁用的设备不会显示在**概览**窗格中。

要显示所有禁用的设备，请在**概览**窗格的顶部单击**筛选器**以打开**筛选器**选项卡并选择**显示禁用的设备**。

要再次隐藏禁用的设备，请取消选中**显示禁用的设备**。

为设备组中的所有设备指定共同属性

使用设备组时，可为给定设备组内的所有设备指定共同属性：

1. 在**总览**中窗格，单击设备组。

   在**属性**窗格中，**适用于设备组所有设备**的所有属性都会在选项卡上分组列出。

2. 指定相关的共同属性。

   在**设置**选项卡上，可在**所有**设备的设置与各台设备的设置之间切换。

3. 在工具栏中，单击**保存**。设置将保存在各台设备上，而不是保存在设备组中。

禁用的设备

默认情况下，禁用的设备不会显示在**概览**窗格中。

要显示所有禁用的设备，请在**概览**窗格的顶部单击**筛选器**以打开**筛选器**选项卡并选择**显示禁用的设备**。

要再次隐藏禁用的设备，请取消选中**显示禁用的设备**。

通过设备组启用/禁用设备

只能通过配置的硬件来启用/禁用设备。除非在添加硬件向导中手动启用/禁用摄像机设备，否则默认会启用摄像机设备，并且默认会禁用所有其他设备。

默认情况下，禁用的设备不会显示在**概览**窗格中。

要显示所有禁用的设备，请在**概览**窗格的顶部单击**筛选器**以打开**筛选器**选项卡并选择**显示禁用的设备**。

要再次隐藏禁用的设备，请取消选中**显示禁用的设备**。

要通过设备组找到需要启用或禁用的设备：

1. **在**站点导航窗格中，选择设备。
2. **在**总览窗格中，展开相关设备组并找到设备。
3. **右键单击设备**，并选择转到硬件。
4. 单击加号节点查看硬件上的所有设备。
5. **右键单击要启用/禁用的设备**，然后选择已启用。

设备 - 摄像机设置

查看或编辑摄像机设置

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的摄像机。
3. 打开**设置**窗口。

您可以查看和编辑选定摄像机或设备组内所有摄像机的设置，例如：

- 默认帧速率
- 分辨率
- 压缩
- 关键帧之间的最大帧数
- 所选定摄像机或设备组中所有摄像机的屏幕日期/时间/文本显示

摄像机的驱动程序决定**设置**选项卡的内容。摄像机类型不同，驱动程序也有所差异。

某些摄像机支持 MJPEG 和 MPEG-4/H.264/H.265 等多种流类型，允许使用多流，请参阅 第 202 页上的管理多流。

预览

如果启用了**预览**窗格，可在更改设置后快速检查更改的效果。

- 要启用**预览**，请单击**视图**菜单，然后单击**预览窗口**。

但是，由于**预览**窗格的缩略图图像使用**选项**对话框中定义的其他帧速率，所以不能使用**预览**窗格来评判更改帧速率的效果。

性能

如果更改**关键帧之间的最大帧数**和**关键帧之间的最大帧数模式**的设置，可能会降低 XProtect Smart Client 中部分功能的性能。例如，XProtect Smart Client 需要调用关键帧来启动视频显示，导致关键帧之间的时间间隔更长，而 XProtect Smart Client 的启动时间也随之增加。

添加硬件

要了解如何向系统添加硬件的详细信息，请参阅 第 185 页上的添加硬件。

启用和禁用鱼眼镜头支持

默认情况下已禁用鱼眼镜头支持。

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**鱼眼镜头**选项卡上，选中或清除**启用鱼眼镜头支持**复选框。

指定鱼眼镜头设置

1. 在**鱼眼镜头**选项卡上，选择镜头类型。
2. 从**摄像机位置/方向**列表中指定摄像机的物理位置/方向。
3. 从 **ImmerVision 启用® panomorph RPL 编号**列表中选择已注册的 Panomorph 镜头 (RPL) 编号。

   这可以确保摄像机所用镜头的标识和正确配置。通常可以在镜头本身上或者镜头的包装盒上找到 RPL 编号。有关 ImmerVision、全景镜头和 RPL 的详细信息，请参阅 ImmerVision 网站 (https://www.immervisionenables.com/)。

   如果选择**通用扭曲恢复**镜头配置文件，请记住配置所需的**视野**。

设备 - 记录

启用/禁用记录

默认情况下，会启用记录。要启用/禁用记录：

1. 在**站点导航**窗格中，选择**记录服务器**。
2. 在**总览**窗格中选择相关设备。
3. 在**记录**选项卡上，选中或清除**记录**复选框。

必须首先为设备启用记录，才能从摄像机记录数据。如果您禁用设备的记录，用于指定记录设备情况的规则将不会起作用。

启用相关设备上的记录

对于摄像机设备，可以启用连接至相同记录服务器的相关设备(如麦克风)的记录。这意味着摄像机进行记录时，相关设备会进行记录。

默认情况下，会为新摄像机设备启用相关设备上的记录，但您可以根据需要启用或禁用它。对于系统中的现有摄像机设备，默认情况下会清除该复选框。

1. 在**站点导航**窗格中，选择**记录服务器**。
2. 在**总览**窗格中选择相关的摄像机设备。
3. 在**记录**选项卡上，选中或清除**相关设备上的记录**复选框。
4. 在**客户端**选项卡上，指定与该摄像机关联的硬件。

如果要启用连接至其他记录服务器的相关设备上的记录，必须创建规则。

管理手动记录

在此之后停止手动记录默认启用，记录时间为五分钟时。这是为了确保系统能够自动停止 XProtect Smart Client 用户发起的所有记录。

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备。
3. 在**记录**选项卡上，选中或清除**在以下项之后停止手动记录**复选框。

启用之后，指定记录时间。指定的分钟数必须足够大，能够满足不同手动记录的需求，而不会造成系统过载。

添加至角色：

必须在**设备**选项卡的**角色**中，向客户端用户授予启动和停止各摄像机手动记录的权限。

在规则中使用：

创建与手动记录相关的规则时，可以使用如下事件：

- 手动记录已开始
- 手动记录已停止

指定记录帧速率

可以为 JPEG 指定记录帧速率。

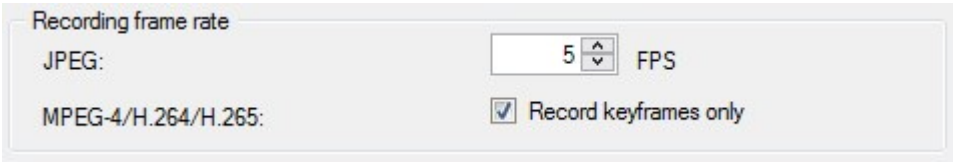
1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备。
3. 在**记录**选项卡上的**"记录帧率"中：(JPEG)** 框，选择或输入记录帧速率（以 FPS（每秒帧数）为单位）。

启用关键帧记录

可以为 MPEG-4/H.264/H.265 视频流启用关键帧记录。这意味着系统会根据规则设置，在只记录关键帧和记录所有帧之间切换。

例如，您可以指定系统在查看不到任何移动时记录关键帧，并切换为仅在侦测到移动时记录所有帧，从而节约存储空间。

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备。
3. 在**记录**选项卡上，选中**仅记录关键帧**复选框。



4. 设置触发功能的规则，请参阅操作和停止操作。

启用相关设备上的记录

对于摄像机设备，可以启用连接至相同记录服务器的相关设备（如麦克风）的记录。这意味着摄像机进行记录时，相关设备会进行记录。

默认情况下，会为新摄像机设备启用相关设备上的记录，但您可以根据需要启用或禁用它。对于系统中的现有摄像机设备，默认情况下会清除该复选框。

1. 在**站点导航**窗格中，选择**记录服务器**。
2. 在**总览**窗格中选择相关的摄像机设备。
3. 在**记录**选项卡上，选中或清除**相关设备上的记录**复选框。

4. 在**客户端**选项卡上，指定与该摄像机关联的硬件。

如果要启用连接至其他记录服务器的相关设备上的记录，必须创建规则。

保存和检索远程记录

为确保在发生网络问题时保存所有远程记录，可以启用在重新建立连接后自动检索记录。

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备。
3. 在**远程记录**下，选择**连接恢复时自动检索远程记录**。如此一来，可在连接重新建立之后立即自动检索记录

只有在所选摄像机支持边缘存储或者是 Milestone Interconnect 设置下的摄像机时，远程记录选项才可用。

所选硬件的类型决定了从何处检索记录：

- 对于使用本地录制存储的摄像机，从摄像机的本地录制存储中检索录像
- 对于 Milestone Interconnect 远程系统，从远程系统的记录服务器中检索录像

除了自动检索外，还可以单独使用以下功能：

- 手动记录
- **从 <设备> 检索并存储远程记录**规则
- **从 <设备> 检索并存储 <开始时间和结束时间> 之间的远程记录**规则

删除记录

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备，然后选择**记录**选项卡。
3. 单击**删除所有记录**按钮以删除设备或设备组的所有记录。

仅当您将组中的所有设备添加到同一服务器时，才可以使用此方法。受保护的数据不会删除。

设备 - 流

自适应流媒体传输(已解释)

自适应流是在同一视图中显示多个实时视频流时使用的流方法。运用自适应流，客户端可以自动选择在分辨率方面与视图项目所请求的流最匹配的实时视频流。自适应流可减少网络负载，提高客户端计算机的解码能力和性能。

在 XProtect Smart Client 中启用自适应流时，您可以设置与视图项目所请求的分辨率最接近匹配的可用视频流。如需更多信息，请参阅启用自适应流。

在 XProtect Smart Client 中，可以将自适应流应用于实时模式和播放模式。在移动设备客户端中，自适应流只能用于实时模式。

应用于播放模式时，流方法称为自适应播放。有关详细信息，请参阅 第 201 页上的自适应播放(已说明)。

自适应播放(已说明)

自适应播放是允许在播放模式下对自适应流加以使用的配置。

自适应播放需要使用两个记录流(主要流和次要流)。若在 Management Client 中已启用这两个流，会对这两个流进行录制。

- 若所播放视频的录制时间在配置次要记录之前，则只会播放主要记录。
- 若所播放视频的录制时间在配置次要记录之后，则视与客户端视图大小最匹配的记录而定，会播放主要或次要记录中的视频。

可用性

> 可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

启用自适应流

您可以在**Smart Client 配置文件**中的**高级**选项卡上，将自适应播放与自适应流一起启用，还必须在**设置 > 高级 > 自适应流**下的 XProtect Smart Client 中启用自适应流。如需有关在 XProtect Smart Client 中启用自适应流的详细信息，请参阅 启用自适应流媒体传输

边缘记录

(可选)您可以将边缘记录用于自适应播放。运用边缘记录，您可以查看分辨率不同于(通常是高于)其余流的流片段。例如，您可以录制低分辨率的主要流，然后合并高分辨率来源的记录。您可以在浏览数据时启用合并的边缘记录。

边缘记录存储在媒体数据库中，会基于各台摄像机而设置这些记录的分辨率。

所播放视频的分辨率

使用自适应播放时，所播放视频的分辨率由主要和次要记录的当前分辨率设置决定。也就是说，在播放时，将根据当前为各记录流而设置的分辨率来选择主要流或次要流。

添加数据流

可以在实时模式和播放模式中查看您为记录而添加的流。

您还可以在启用自适应流的情况下在视图项目中查看录制的视频。播放模式中的自适应流称为自适应播放。

1. 在**数据流**选项卡上，单击**添加**。这会向列表中添加第二个数据流。
2. 在**名称**列中，编辑数据流的名称。名称显示在 XProtect Smart Client 中。
3. 在**实时模式**列中，选择何时需要实时流：
   - **始终**：运行数据流，即使 XProtect Smart Client 用户未请求获取数据流
   - **从不**：数据流关闭。仅在录制数据流的时候使用，例如想进行高质量录制并需要带宽时
   - **需要时执行**：在任何客户端发出请求或将流设置为录制时，流就会开始
4. 在**默认实时流**列中，选择在客户端未请求特定流且自适应流遭禁用时应该使用的默认的流。
5. 在**记录**列中，选择**主要**或**次要**。对于自适应播放，您需要创建每种类型的流。所播放的视频来自主要视频流，在需要时会将次要流包括在内。主要记录必须始终存在。此外，您配置为**主要**的流将用于不同的环境，例如用于移动侦测以及用于从 XProtect Smart Client 中导出。
6. 在**默认播放**下，选择默认的流。若未配置自适应播放，会向客户端提供默认的流。
7. 若希望使用边缘记录，请在**使用边缘记录**列中选择该复选框。如需有关边缘记录的详细信息，请参阅 第 201 页上的边缘记录。
8. 单击**保存**。

> 如果您不需要数据流在无人查看实时视频时运行，则可以修改**默认启动馈送规则**以在请求时使用预定义的**实时客户端馈送请求**事件启动。

管理多流

查看实时视频和播放录制的视频时，并非一定需要相同的视频质量和帧速率。

更改用于记录的流

自适应播放需要将两个流(主要流和次要流)设置为记录。对于实时流，您可以根据摄像机的支持而设置并使用许多实时流。

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关的摄像机。
3. 在**流**选项卡上，选择您希望用于记录的流。
4. 在**实时模式**列表中选择相关选项。**需要时执行**、**始终**和**从不**选项会表明什么时候应该将流应用于客户端。若客户端未发出任何请求，记录将使用已选择**默认实时流**复选框的流。
5. 若要对一个流进行录制，请在**记录**列表中选择**主要**或**次要**。
6. 若要使用自适应播放，请设置两个流，并将其中一个流设置为**主要**，将另一个流设置为**次要**。
7. 若要对流进行录制，请在**记录**列表中选择**主要**或**次要**流。

限制数据传输

您可以设置一组条件，以确保仅在客户端观看时才运行视频流。

为了管理流并限制不必要的数据传输，满足以下条件时流不会开始：

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关的摄像机。
3. 在**流**选项卡上的**实时模式**列表中，选择**需要时**。
4. 在**记录**选项卡上，清除**记录**复选框。
5. 在**移动**选项卡上，清除**移动侦测**复选框。

如果满足这些条件，则只有在客户端观看时才会运行视频流。

示例

示例 1，实时和录制的视频：

- 要查看**实时**视频，您的组织可能倾向于选择帧速率高的 H.264
- 要播放**录制的**视频，您的组织可能倾向于选择帧速率较低的 MJPEG 以保留磁盘空间

示例 2，本地和远程实时视频：

- 要查看**来自本地连接操作点的实时视频**，您的组织可能倾向于选择帧速率高的H.264以获得最高品质的视频
- 要查看**来自远程连接操作点的实时视频**，您的组织可能倾向于选择帧速率和画质较低的 MJPEG，以保留网络带宽

示例 3，自适应流媒体传输：

- 要查看**实时视频并降低 XProtect Smart Client 计算机 CPU 和 GPU 的负载**，您的组织可能倾向于选择多个帧速率高但具有不同分辨率的 H.264/H.265，以匹配使用自适应流媒体传输时 XProtect Smart Client 所要求的分辨率。有关详细信息，请参阅 第 399 页上的Smart Client 配置文件（“客户端”节点）。

> 如果您启用在摄像机**客户端**选项卡上**实时多播**（请参阅“客户端”选项卡（设备）），该功能仅在默认视频流上工作。

即使摄像机支持多数据流，单独的多数据流功能也可能因摄像机的不同而有所差异。有关详细信息，请参阅摄像机文档。

要查看摄像机是否提供不同类型的流，请参阅**“设置”选项卡（设备）**。

设备存储

管理预缓冲

摄像机、麦克风和扬声器支持预缓冲。对于扬声器，只有当 XProtect Smart Client 用户使用**通过扬声器通话**功能时才会发送数据流。也就是说，视触发记录扬声器数据流的方式而定，可能只有少量甚至没有预缓冲可用。

在大多数情况下，当 XProtect Smart Client 用户使用**通过扬声器通话**功能时，您可以设置扬声器记录。在这种情况下，扬声器预缓冲将不可用。

要使用预缓冲功能，设备必须启用并发送数据流至系统。

启用和禁用预缓冲

默认情况下，已启用预缓冲，预缓冲大小为三秒，并存储到内存中。

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备。
3. 在**记录**选项卡上，选中或清除**预缓冲**复选框。
4. 在**客户端**选项卡上，指定与该摄像机关联的硬件。

指定存储位置和预缓冲期间

临时预缓冲记录存储在内存中或磁盘上：

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备，然后选择**记录**选项卡。
3. 在**位置**列表上，选择**内存**或**磁盘**，并指定秒数。
4. 如果需要超过 15 秒的预缓冲期间，则选择**磁盘**。

指定的秒数必须足够大，能够满足您所定义的不同记录规则的需求。

如果将位置更改为**内存**，则系统会自动将期间减少到 15 秒。

在规则中使用预缓冲

当您创建触发记录的规则时，您可以选择在实际事件之前一段时间必须启动记录(预缓冲)。

示例：下方规则指定摄像机的记录必须在侦测到摄像机上的移动前 5 秒内启动。

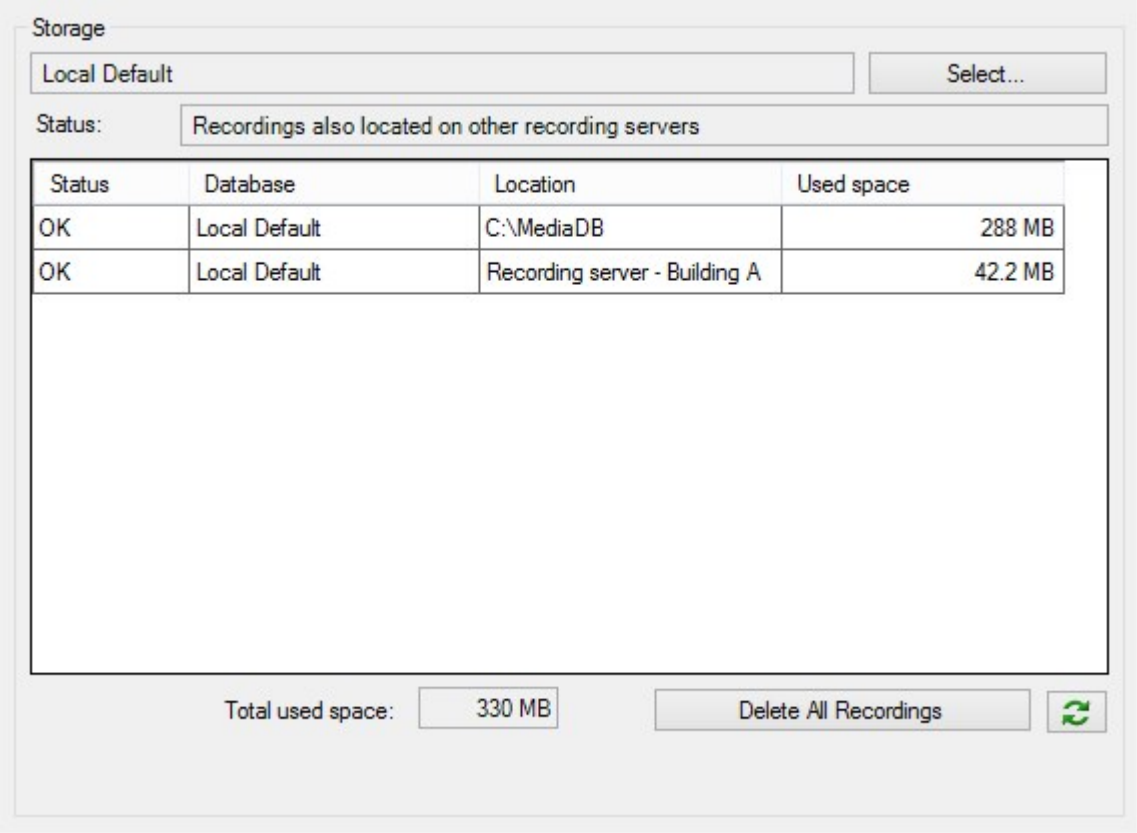
要在规则中使用预缓冲记录功能，您必须在用于记录的设备上启用预缓冲，同时必须将预缓冲长度设置为至少与规则指定的长度相同。

监视设备的数据库状态

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备，然后选择**记录**选项卡。

在**存储**下，您可以监控和管理已添加到同一记录服务器的设备或设备组的数据库。

在表格上方，您可以查看所选数据库及其状态。在此示例中，选定数据库为默认的 **Local Default**，其状态为**记录还位于其他记录服务器上**。其他服务器指的是建筑物 A 中的记录服务器。



选定数据库的可能状态

名称	说明
记录还位于其他记录服务器上	数据库处于活动状态且正在运行，并具有还位于其他记录服务器上的存储中的记录。

名称	说明
存档也位于旧存储中	数据库处于活动状态并且正在运行，同时还在其他存储中具有存档。
活动	数据库处于活动状态并且正在运行。
所选设备的某些数据正在移动到另一位置	数据库处于活动状态并且正在运行，且系统正在将组中一个或多个所选设备的数据从一个位置移动到另一个位置。
设备的数据正在移至另一位置	数据库处于活动状态并且正在运行，且系统正在将所选设备的数据从一个位置移动到另一个位置。
信息在故障转移模式中不可用	当数据库处于故障转移模式时，系统无法收集数据库的状态信息。

在窗口中继续往下，您可以看到每个数据库的状态(**正常**、**脱机**或**旧存储**)、每个数据库的位置以及每个数据库使用的空间量。

如果所有服务器都已联机，则您可以在**已用总空间**字段中查看用于整个存储的总已用空间。

有关存储配置的信息，请参阅"存储"选项卡(记录服务器)。

将设备从一个存储移到另一个存储

当您选择一个新的位置来存储记录时，将不会移动现有的记录。现有记录将保留在当前位置，其条件由它们所属的存储配置来定义。

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关设备，然后选择**记录**选项卡。
3. 单击**存储**下的**选择**，为设备选择录制存储位置。

记录将根据您选择的存储的配置进行存档。

设备移动侦测

移动侦测(已作说明)

移动侦测配置是系统的关键元素：移动侦测配置决定了系统生成移动事件的时间，并且通常还决定了记录视频的时间。

花些时间为每台摄像机寻找最佳可能移动侦测配置，有助于在后来避免一些操作，例如避免不必要的记录。鉴于摄像机物理位置的不同，在不同的物理条件(白天/夜晚、刮风/无风天气等)下测试移动侦测设置是个不错的方法。

您可以指定与摄像机视图中需要多少变化量才能被视为移动相关的设置。例如，您可以指定移动侦测分析之间的间隔，以及应该忽略移动的视图区域。您还可以调节移动侦测的准确性，从而调节系统资源的负载。

图像质量

在配置摄像机的移动侦测之前，Milestone 强烈建议配置摄像机的图像质量设置，如分辨率、视频编码解码器和流设置等。您可以在设备的**属性**窗口中的**设置**选项卡上执行此操作。如果您以后更改图像质量设置，应始终在更改后测试任何移动侦测配置。

隐私屏蔽

> 如果您定义了带有永久性隐私屏蔽的区域，则这些区域内不会进行移动侦测。

启用和禁用移动侦测

指定摄像机运动侦测的默认设置

1. 在**工具**菜单下，单击**选项**。
2. 在**常规**选项卡上的**自动启用添加新摄像机设备时**下，选中**移动侦测**复选框。

启用或禁用特写摄像机的移动侦测

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的摄像机。
3. 在**移动**选项卡上，选中或清除**移动侦测**复选框。

> 禁用摄像机的移动侦测时，摄像机的移动侦测相关规则也将不起作用。

启用或禁用硬件加速

添加摄像机时，用于移动侦测的自动硬件加速视频解码是默认设置。记录服务器使用 GPU 资源(如果可用)。这将降低视频移动分析期间的 CPU 负载，同时提高记录服务器的常规性能。

启用或禁用硬件加速

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关的摄像机。
3. 在**移动**选项卡上的**硬件加速**下，选择**自动**以启用硬件加速，或者选择**关**以禁用此设置。

使用 GPU 资源

移动侦测的硬件加速视频解码使用以下设备上的 GPU 资源：

- 支持 Intel Quick Sync 的 Intel CPU
- NVIDIA® 显示连接到记录服务器的适配器

负载平衡和性能

自动完成不同资源之间的负载平衡。在**系统监视器**节点中，您可以验证 NVIDIA GPU 资源上的当前运动分析负载是否在**系统监视器阈值**节点的指定限制范围内。NVIDIA GPU 负载指示器是：

- NVIDIA 解码
- NVIDIA 内存
- NVIDIA 渲染

如果负载过高，您可以通过安装多个 NVIDIA 显示器适配器将 GPU 资源添加到您的记录服务器。Milestone 不建议使用您 NVIDIA 显示器适配器的可伸缩链接接口 (SLI) 配置。

NVIDIA 产品的计算能力各不相同。

使用NVIDIAGPU的移动侦测的硬件加速视频解码需要计算能力版本6.x(Pascal)或更新版本。

- 要了解 NVIDIA 产品的计算能力，请访问 NVIDIA 网站 (https://developer.nvidia.com/cuda-gpus/)。
- 要了解视频移动侦测是否已针对特定摄像机进行硬件加速，请对记录服务器日志文件启用日志录制。将级别设置为**调试**，会将诊断信息记录到 DeviceHandling.log. 日志遵循以下模式：
  [time] [274] DEBUG - [guid] [name] 已配置的解码：自动：实际解码：Intel/NVIDIA

记录服务器的 OS 版本和 CPU 生成可能会影响硬件加速视频移动侦测的性能。GPU 内存分配往往是较早版本的瓶颈(通常限制在 0.5 GB 到 1.7 GB 之间)。

基于 Windows 10 / 服务器 2016 和第 6 代 CPU (Skylake) 或更新版本的系统可以将 50% 的系统内存分配给 GPU，从而消除或降低这一瓶颈。

第 6 代 Intel CPU 不能提供 H.265 的硬件加速解码功能，因此对于这些 CPU 版本，其性能与 H.264 大致相当。

启用手动灵敏度以定义移动

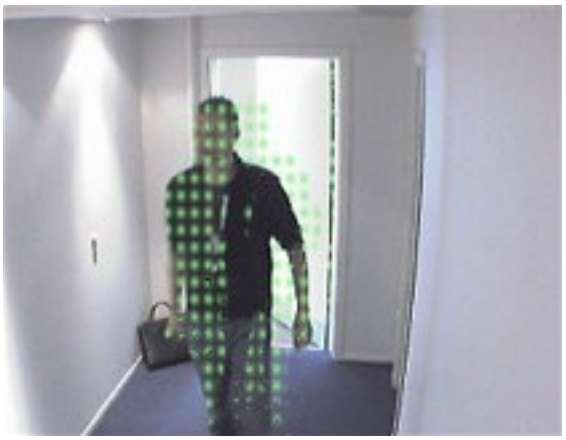
灵敏度设置决定了图像中的每个像素必须变化多少才能被视为移动。

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的摄像机。
3. **选中**移动选项卡上的**手动灵敏**度复选框。
4. 向左拖动滑块可提高灵敏度级别，向右拖动可降低灵敏度级别。

   灵敏度级别越高，在将每个像素视为移动之前，允许的变化越小。

   灵敏度级别越低，在将每个像素视为移动之前，允许的变化越大。

   其中侦测到移动的像素在预览图像中以绿色突出显示。
5. 选择其中仅突出显示您视为移动的侦测对象的滑块位置。



可以通过滑块右侧的数字来比较并设置摄像机之间的确切灵敏度设置。

指定阈值以定义移动

移动侦测阈值决定了图像中的每个像素必须变化多少才能被视为移动。

1. 向左拖动滑块可提高移动级别，向右拖动可降低移动级别。
2. 选择其中仅侦测您视为移动的侦测对象的滑块位置。

移动指示栏中的黑色垂直线用于显示移动侦测阈值：当侦测到的移动在选定侦测阈值级别之上时，此栏的颜色将从绿色变为红色，表示正向侦测。

如果超出阈值，移动指示栏将使颜色从绿色更改为红色，表示侦测到正向移动。

指定移动侦测的排除区域

可以为一组摄像机配置所有设置，但通常单独设置每台摄像机的排除区域。

具有永久隐私屏蔽的区域也是排除在移动侦测之外的区域。选择**显示隐私屏蔽**复选框，以显示它们。

例如，如果摄像机记录的区域背景中有树在风中摇摆或常有车辆路过，则禁用特定区域中的移动侦测功能有助于避免侦测无关移动。

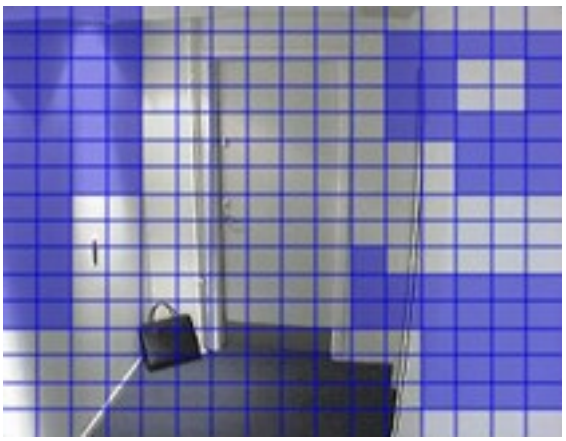
如果将排除区域结合 PTZ 摄像机使用，并且对摄像机进行全景/倾斜/变焦操作，排除区域将被摄像机图像（而非对象）所遮挡，因而**不**会相应移动。

1. 要使用排除区域，请选中**使用排除区域**复选框。

   栅格将预览图像分隔为可选区域。

2. 要定义排除区域，请在按住鼠标左键的同时将鼠标指针拖到预览图像中的所需区域上。使用鼠标右键清除栅格区域。

可以根据需要定义足够多的排除区域。排除区域显示为蓝色：



蓝色排除区域将只出现在**移动**选项卡上的预览图像中，而非 Management Client 或访问客户端中的其他任何预览图像中。

设备 - 预设摄像机位置

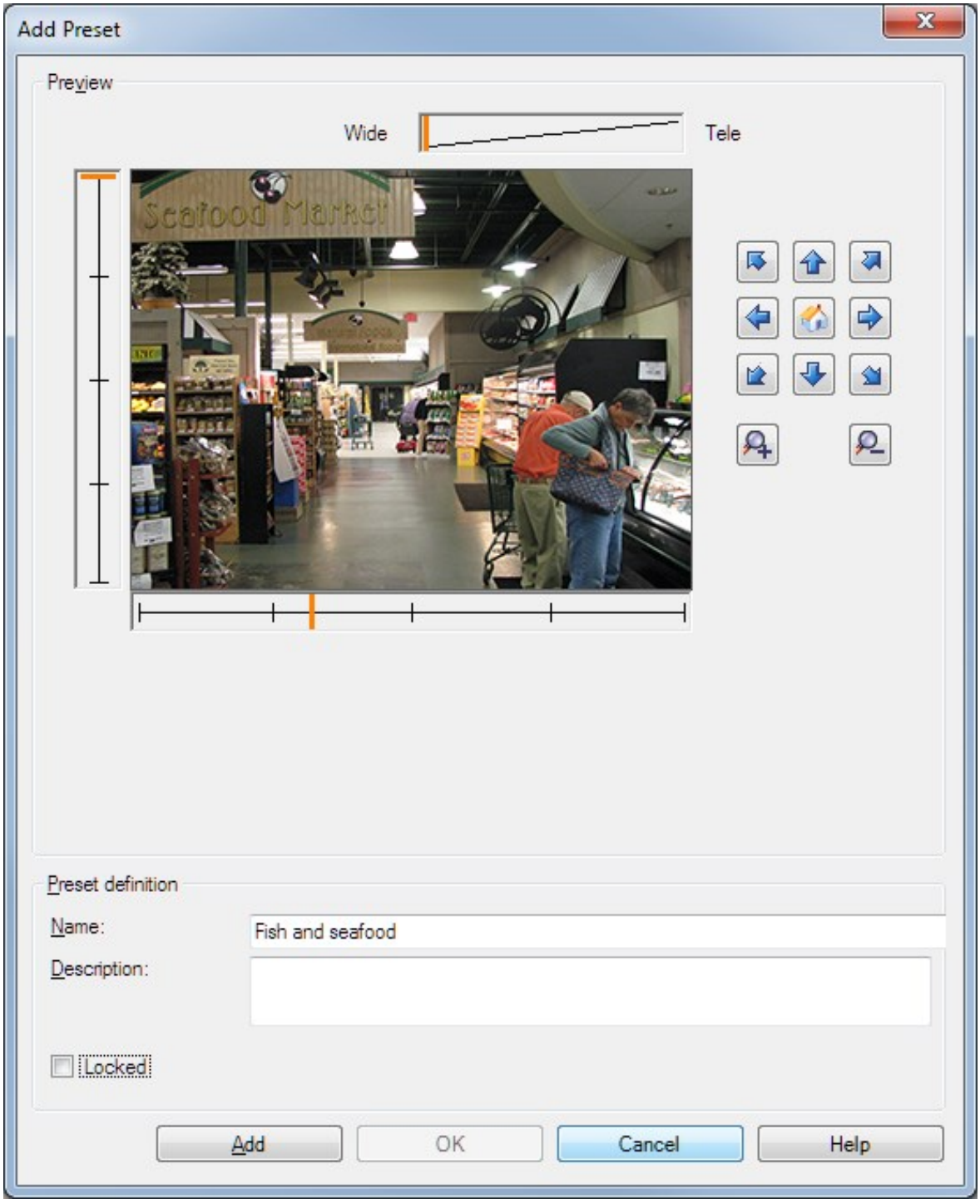
初始预设位置

可以在摄像机主页上定义摄像机的初始预设位置。主页上可用的 PTZ 功能取决于摄像机。

添加预设位置（类型 1）

要为摄像机添加预设位置：

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**预设**选项卡上，单击**新**。将出现**添加预设**窗口：



4. **添加预设**窗口显示摄像机的实时预览图像。使用导航按钮和/或滑块，将摄像机移动至所需位置。
5. 在**名称**字段中，指定预设位置的名称。
6. 在**说明**字段中输入预设位置的说明(可选)。
7. 如果需要锁定预设位置，请选择**已锁定**。只有具有足够权限的用户能解在之后解锁位置。
8. 单击**添加**以指定预设。重复添加，直到生成所需的预设。
9. 单击**确定**。将关闭**添加预设**窗口，并将位置添加到**预设**选项卡的摄像机可用预设位置列表中。

使用摄像机的预设位置(类型 2)

除了可以在系统中指定预设位置外，对于某些 PTZ 摄像机，也可以在摄像机自身上指定预设位置。通常是通过访问产品特定的配置网页进行。

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**预设**选项卡上，选择**使用设备中的预设**以将预设导入系统。

   之前为摄像机定义的所有预设都将被删除，并且所有定义规则和巡视计划表都将受到影响，同时 XProtect Smart Client 用户可用的预设也会被删除。
4. 单击**删除**可删除用户不需要的预设。
5. 如果要更改预设的显示名称(参阅重命名预设位置(仅限类型 2))，请单击**编辑**。
6. 如果以后想要编辑这类设备定义的预设，应在摄像机上编辑，然后重新导入。

指定摄像机的预设位置作为默认值

如果需要，可以指定 PTZ 摄像机的其中一个预设位置作为摄像机的默认预设位置。

设置默认预设位置非常有用，因为这可允许您定义规则，以指定 PTZ 摄像机应在特定情况下(例如手动操作 PTZ 摄像机后)转到默认预设位置。

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**预设**选项卡上的**预设位置**下，从已定义的预设位置列表中选择预设。
4. 选中列表下方的**默认预设**复选框。

只能将一个预设位置定义为默认预设位置。

如果您在**选项 > 常规**中选择了**使用默认预设作为 PTZ 初始位置**，则将使用默认预设位置，而非 PTZ 摄像机定义的初始位置。

指定默认预设作为 PTZ 初始位置

具有必要用户权限的 Management Client 和 XProtect Smart Client 用户可以使用客户端中的**初始位置**按钮，将系统设置为使用默认预设位置，而非 PTZ 摄像机的初始位置。

必须为摄像机定义默认预设位置。如果未定义默认预设位置，则在客户端中激活**初始位置**按钮时不会发生任何改变。

启用设置 PTZ 初始位置

1. 选择 **工具 > 选项**。
2. 在**常规**选项卡的**录制服务器**组中，选择**使用默认预设作为 PTZ 初始位置**。
3. 指定一个预设位置作为摄像机的默认预设位置。

要指定默认预设位置，请参阅 第 212 页上的指定摄像机的预设位置作为默认值

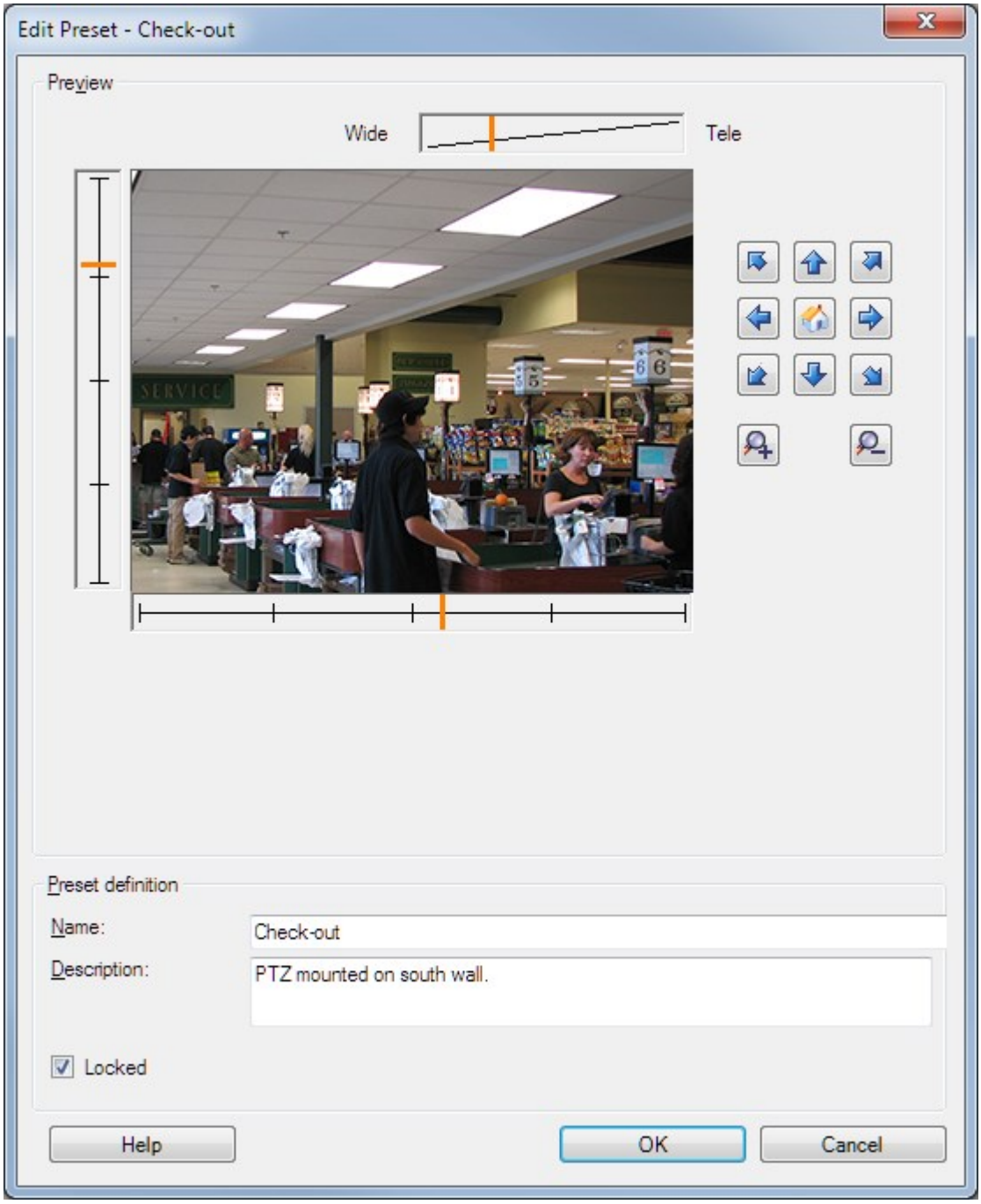
另请参阅 第 331 页上的系统设置(“选项”对话框)

编辑摄像机的预设位置(仅类型 1)

要编辑系统中定义的现有预设位置：

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的摄像机。
3. 在**预设**选项卡上的“预设位置”下，从摄像机的可用预设位置列表中选择预设位置。

4. 单击**编辑**。此操作将打开**编辑预设**窗口：

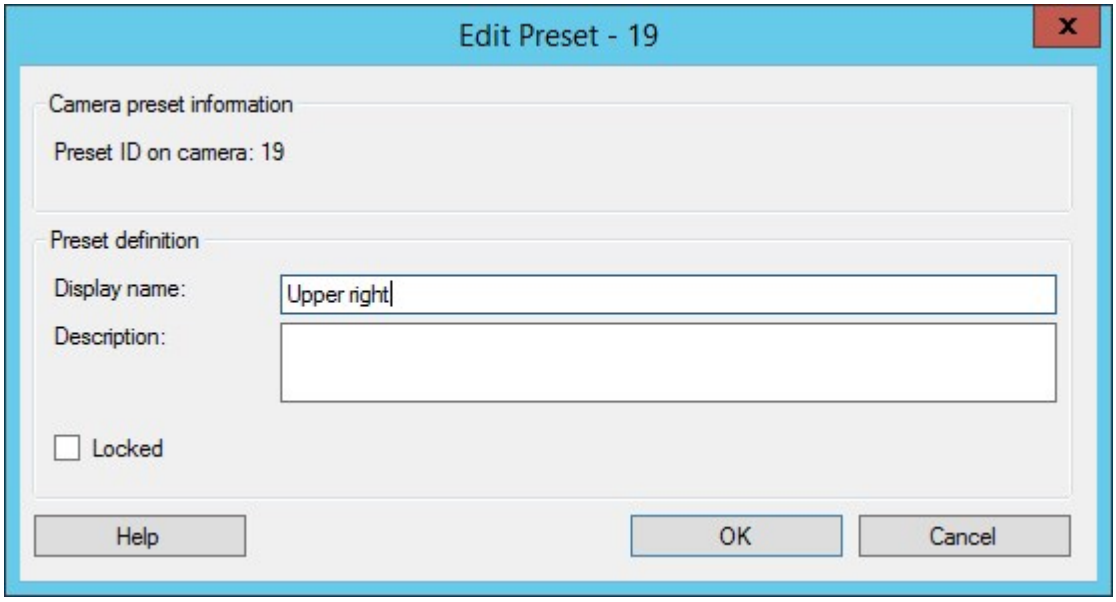


5. **编辑预设**窗口显示预设位置的实时视图。使用导航按钮和/或滑块，按需要更改预设位置。
6. 根据需要更改预设位置的名称/编号和说明。
7. 如果需要锁定预设位置，请选择**已锁定**。只有具有足够权限的用户能解在之后解锁位置。
8. 单击**确定**。

重命名摄像机的预设位置(仅类型 2)

要编辑在摄像机中定义的预设位置的名称:

1. 在**站点导航**窗格中,选择**设备**,然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**预设**选项卡的摄像机可用预设列表中选择预设位置。
4. 单击**编辑**。此操作将打开**编辑预设**窗口:



5. 根据需要更改预设位置的名称,以及添加预设位置的说明。
6. 如果需要锁定预设名称,请选择**已锁定**。如果要阻止 XProtect Smart Client 中的用户或拥有受限安全权限的用户更新预设名称或删除预设,可锁定预设名称。锁定的预设由该图标 表示。只有具有足够权限的用户能解在之后解锁预设名称。
7. 单击**确定**。

测试预设位置(仅类型 1)

1. 在**站点导航**窗格中,选择**设备**,然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**预设**选项卡的摄像机可用预设位置列表中选择预设位置。
4. 单击**激活**。
5. 摄像机移动至所选预设位置。

设备 - 巡视

巡视配置文件和手动巡视(已作说明)

巡视配置文件定义了如何进行巡视。包括摄像机在预设位置间的移动顺序，以及在每个位置应该停留多久等内容。可以创建数量不受限制的巡视配置文件，并且可在规则中使用这些配置文件。例如，可以创建规则，使其指定白天营业时间使用一个巡视配置文件，而在夜晚使用另一个配置文件。

手动巡视

例如，在应用规则中的巡视配置文件之前，您可以使用手动巡视来测试该巡视配置文件。也可以使用手动巡视来从其他用户或从规则激活的巡视接管巡视，前提是您拥有更高的 PTZ 优先级。

如果摄像机已经在执行巡视或由其他用户控制，则只有在您具有更高优先级的情况下才能启动手动巡视。

如果您在摄像机运行由规则激活的系统巡视时启动手动巡视，则当您停止手动巡视时系统将恢复该巡视。如果另一个用户运行手动巡视，但您具有更高的优先级且启动您的手动巡视，则其他用户的手动巡视将无法恢复。

如果您不自行停止手动巡视，该巡视会继续，直到基于规则的巡视或具有更高优先级的用户接管。当基于规则的系统巡视停止时，系统将恢复您的手动巡视。如果另一个用户启动手动巡视，则您的手动巡视将停止，并且将不再恢复。

当您停止手动巡视并且已为巡视配置文件定义结束位置时，摄像机将返回到此位置。

添加巡视配置文件

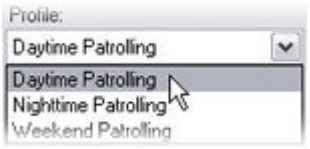
必须先在**预设**选项卡中为摄像机指定至少两个预设位置才能使用巡视功能，请参阅添加预设位置(类型 1)。

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**巡视**选项卡上，单击**添加**。将出现**添加配置文件**对话框。
4. 在**添加配置文件**对话框中，指定巡视配置文件的名称。
5. 单击**确定**。如果名称不唯一，该按钮将被禁用。

新巡视配置文件添加至**配置文件**列表中。现在即可指定巡视配置文件的预设位置和其他设置。

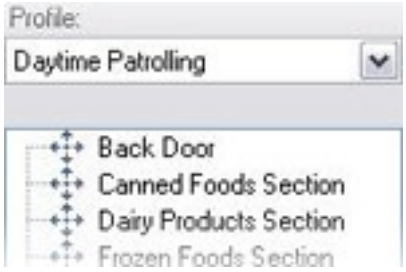
指定巡视配置文件中的预设位置

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在 **巡视**选项卡上，在**配置文件**列表中选择巡视配置文件：



4. 单击 **添加**。
5. 在 **选择 PTZ 预设**对话框中，选择巡视配置文件的预设位置：

6. 单击**确定**。选定预设位置将添加到巡视配置文件的预设位置列表中：



7. 摄像机根据巡视配置文件进行巡视时，将使用列表顶部的预设位置作为第一个停止点。从顶端向下的第二个预设位置是第二个停止点，以此类推。

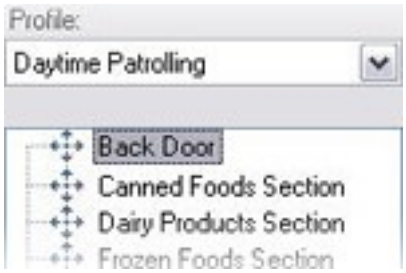
指定各预设位置的时间

巡视时，PTZ 摄像机在巡视配置文件指定的各预设位置默认停留 5 秒钟。

要更改秒数：

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**巡视**选项卡上，在**配置文件**列表中选择巡视配置文件。

4. 选择想要更改时间的预设位置：



5. 在**位置上的时间(秒)**字段中指定时间。
6. 如果需要，可针对其他预设位置重复此步骤。

自定义转换 (PTZ)

默认情况下，摄像机从一个预设位置移动到另一个预设位置(称为**转换**)所需的时间预估为三秒。在此期间，默认将禁用摄像机上的移动侦测，因为当摄像机在预设位置之间移动时，可能会侦测到无关移动。

仅当摄像机支持 PTZ 扫描并且是在系统服务器上配置和存储的预设位置的类型(类型 1 PTZ 摄像机)时，才能自定义转换速度。否则，**速度**滑块将变灰。

可以自定义以下内容：

- 预估转换时间
- 摄像机在转换期间的移动速度

要自定义不同预设位置之间的转换：

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**巡视**选项卡上的**配置文件**列表中选择巡视配置文件。
4. 选中**自定义转换**复选框。

转换指示添加至预设位置列表中。

5. 在列表中，选择转换。

6. 在**预期时间(秒)**字段中，指定预估转换时间(秒数)。

7. 使用**速度**滑块指定转换速度。当滑块位于其最右侧位置时，摄像机将以其默认速度移动。滑块越向左移动，摄像机在选定转换期间的移动速度越慢。
8. 根据需要，对其他转换重复上述操作。

指定巡视时的结束位置

可以指定摄像机在根据所选巡视配置文件巡视结束后移动到特定预设位置。

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**巡视**选项卡的**配置文件**列表中，选择相关的巡视配置文件。
4. 选中**完成时转到特定位置**复选框。将打开**选择预设**对话框。
5. 选择结束位置，然后单击**确定**。

> 可选择摄像机的任意预设位置作为结束位置，并非必须选择巡视配置文件中使用的预设位置。

6. 所选结束位置添加至配置文件列表中。

当根据所选巡视配置文件进行的巡视结束时，摄像机将转到指定的结束位置。

保留和释放 PTZ 会话

根据您的监控系统，您可以保留 PTZ 会话。

有运行保留 PTZ 会话的安全权限的管理员可在此模式下运行 PTZ 摄像机。这可阻止其他用户控制摄像机。在保留 PTZ 会话中，标准 PTZ 优先级系统将被忽略，以避免具有更高 PTZ 优先级的用户中断会话。

您可以从 XProtect Smart Client 和 Management Client 中操作保留 PTZ 会话中的摄像机。

如果需要对 PTZ 摄像机或其预设执行紧急更新或维护而不被其他用户中断，则有必要保留 PTZ 会话。

保留 PTZ 会话

1. 在**站点导航**窗格中，选择**设备**，然后选择**摄像机**。
2. 在**总览**窗格中选择相关的 PTZ 摄像机。
3. 在**预设**选项卡中选择PTZ会话，然后单击**保留**。

如果优先级比您更高的用户在控制摄像机，或者其他用户已保留摄像机，则您不能启动保留的 PTZ 会话。

释放 PTZ 会话

释放按钮可用于释放您当前的 PTZ 会话，以便其他用户可以控制摄像机。当您单击**释放**时，PTZ 会话将立即结束，并将对操作摄像机的第一个用户可用。

拥有安全权限**释放 PTZ 会话**的管理员有权随时释放其他用户的保留 PTZ 会话。例如，如果您需要保持 PTZ 摄像机或其预设，或者如果其他用户在紧急情况下偶然阻止摄像机，这将非常有用。

指定 PTZ 会话超时

Management Client和具有必需用户权限的 XProtect Smart Client 用户可手动中断 PTZ 摄像机的巡视。

您可以指定在为系统上的所有 PTZ 摄像机恢复定期巡视之前应经过的时间量：

1. 选择**工具 > 选项**。
2. 在 **选项**窗口的**常规**选项卡上，从以下项目中选择时间量：
   - **手动 PTZ 会话的超时**列表(默认为 15 秒)。
   - **暂停巡视会话的超时**列表(默认为 10 分钟)。
   - **保留的 PTZ 会话的超时**列表(默认为 1 小时)。

   这些设置将应用于本系统上的所有 PTZ 摄像机。

您可以分别为每个摄像机更改这些超时。

1. 在**站点导航**窗格中，单击**摄像机**。
2. 在“总览”窗格中，选择摄像机。
3. 在 **预设**选项卡上，从以下内容中选择时间量：
   - **手动 PTZ 会话的超时**列表(默认为 15 秒)。
   - **暂停巡视会话的超时**列表(默认为 10 分钟)。
   - **保留的 PTZ 会话的超时**列表(默认为 1 小时)。

   这些设置仅应用于此摄像机。

设备 - 规则事件

添加或删除设备的事件

添加事件

1. 在**总览**窗格中，选择设备。
2. 选择**事件**选项卡，然后单击**添加**。**这将打开**选择驱动程序事件窗口。
3. 选择事件。一次只能选择一个事件。
4. 如果要查看所有事件的完整列表以允许您添加已经添加的事件，请选择**显示已添加的事件**。
5. 单击**确定**。
6. 在工具栏中，单击**保存**。

删除事件

> 删除事件时，它会影响使用该事件的所有规则。

1. 在**总览**窗格中，选择设备。
2. 选择**事件**选项卡，然后单击**删除**。

指定事件属性

可以为添加的每个事件指定属性。属性的数量取决于设备和事件。为了使事件按预期工作，必须在设备以及在**[事件]**选项卡上以同样方式指定部分或全部属性。

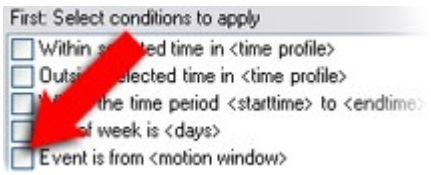
使用事件的多个实例

要能够为事件的不同实例指定不同的属性，您可以多次添加事件。

> 以下示例特定于摄像机。

示例：摄像机已配置了两个移动窗口，名为 A1 和 A2。您已添加了两个动作启动 (HW) 事件实例。在其中一个实例的属性中，您已指定使用移动窗口 A1。在另一个实例的属性中，您已指定使用移动窗口 A2。

在规则中使用事件时，可以指定事件应基于在特定移动窗口中侦测到的移动才能触发规则：



设备 - 隐私屏蔽

启用/禁用隐私屏蔽

默认情况下，禁用隐私屏蔽功能。

要启用/禁用摄像机的隐私屏蔽功能：

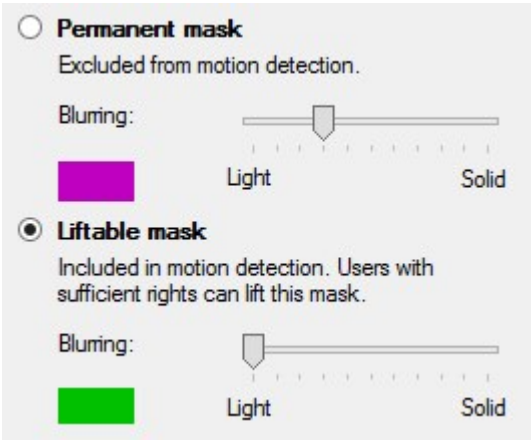
1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关的摄像机设备。
3. 选中或清除**隐私屏蔽**选项卡上的**隐私屏蔽**复选框。

在 Milestone Interconnect 安装中，中央站点将忽略在远程站点上定义的隐私屏蔽。如果要应用相同的隐私遮蔽，您必须在中央站点上重新定义它。

定义隐私屏蔽

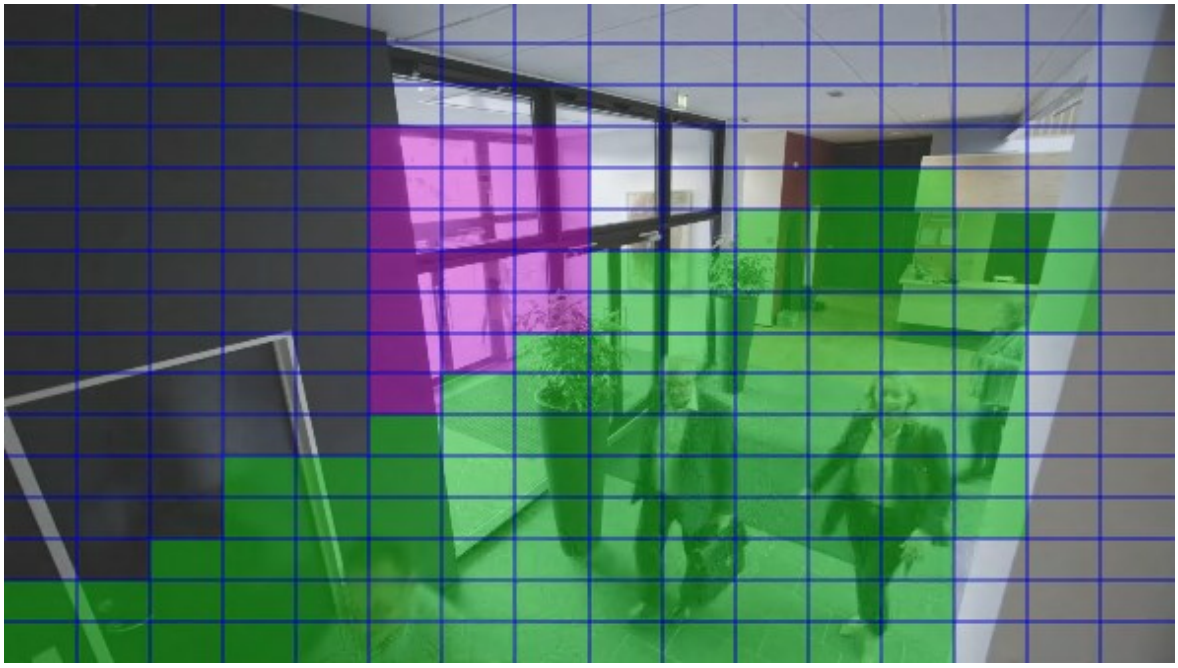
在**隐私屏蔽**选项卡上启用隐私屏蔽功能时，栅格将应用于摄像机预览。

1. 在**站点导航**窗格中，选择**设备**。
2. 在**总览**窗格中选择相关的摄像机。
3. 在**隐私屏蔽**选项卡上，要用隐私屏蔽覆盖区域，请首先选择**永久屏蔽**或**可解除屏蔽**以定义您想要永久的还是可解除的隐私屏蔽。



4. 将鼠标指针拖到预览上。左键单击以选择一个网格。右键单击以清除一个网格。

5. 可以根据需要定义足够多的隐私屏蔽区域。有永久隐私屏蔽的区域以紫色显示，有可解除隐私屏蔽的区域以绿色显示。



6. 定义在客户端显示时，如何显示视频中的遮盖区域。使用滑块从一点点模糊调节到完全不透明屏蔽。

> 永久隐私屏蔽也出现在**移动**选项卡上。

7. 在 XProtect Smart Client 中，检查隐私屏蔽是否按照定义显示。

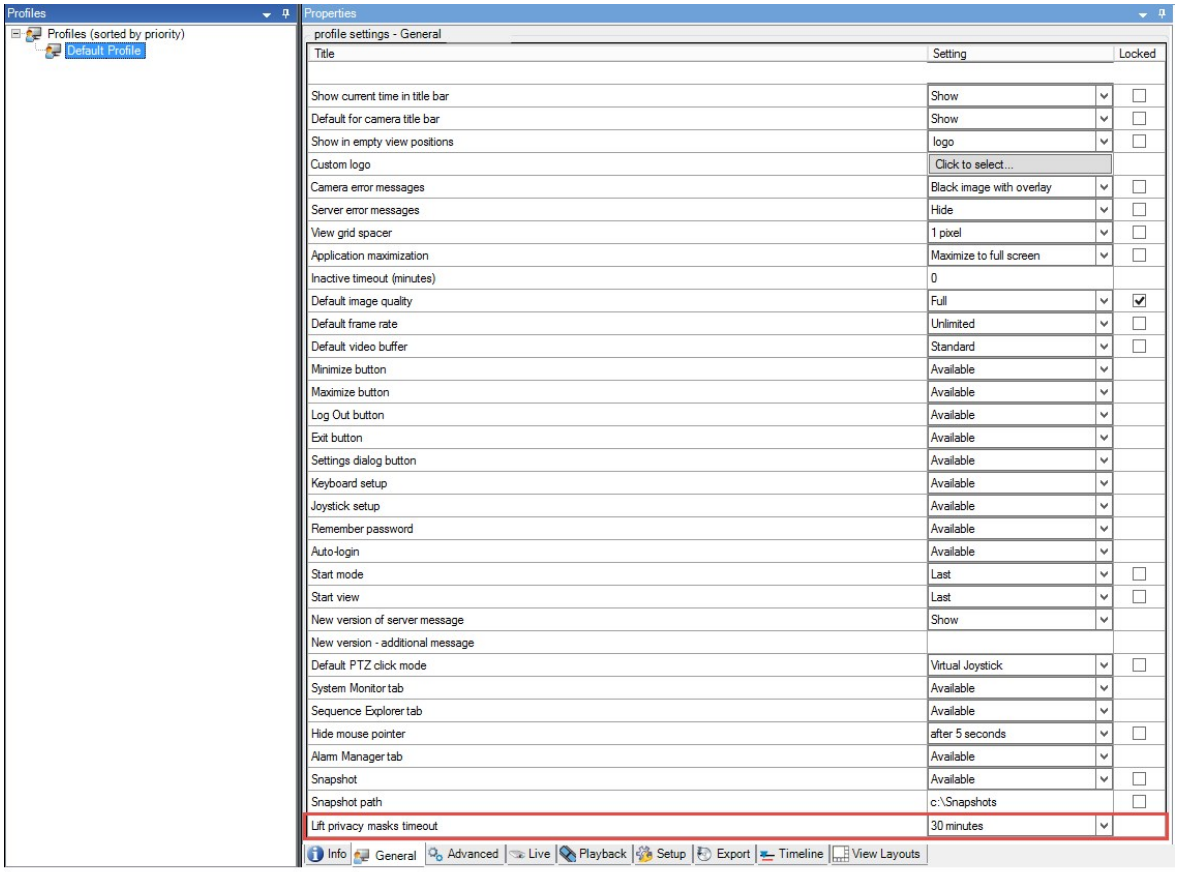
更改可解除隐私屏蔽的超时时间

默认情况下，隐私屏蔽会在 XProtect Smart Client 中解除 30 分钟，然后自动应用，但您可以更改设置。

> 更改超时时间时，请记住对与具有可解除隐私屏蔽权限的角色关联的 Smart Client 配置文件执行此操作。

要更改超时时间：

1. 在 **Smart Client 配置文件**下，选择相关的 Smart Client 配置文件。
2. 在**常规**选项卡上，找到**可解除隐私屏蔽超时**。



3. 选择值：
   - **2 分钟**
   - **10 分钟**
   - **30 分钟**
   - **1 小时**
   - **2 小时**
   - **直到退出**
4. 单击**保存**。

授予用户解除隐私屏蔽的权限

默认情况下，用户没有解除 XProtect Smart Client 中的隐私屏蔽的权限。

要启用/禁用权限：

1. 在**站点导航**窗格中，选择**安全**，然后选择**角色**。
2. 选择您要授予权限的角色，以解除隐私屏蔽。
3. 在**整体安全**选项卡上，选择**摄像机**。
4. 为**解除隐私屏蔽**权限选择**允许**复选框。

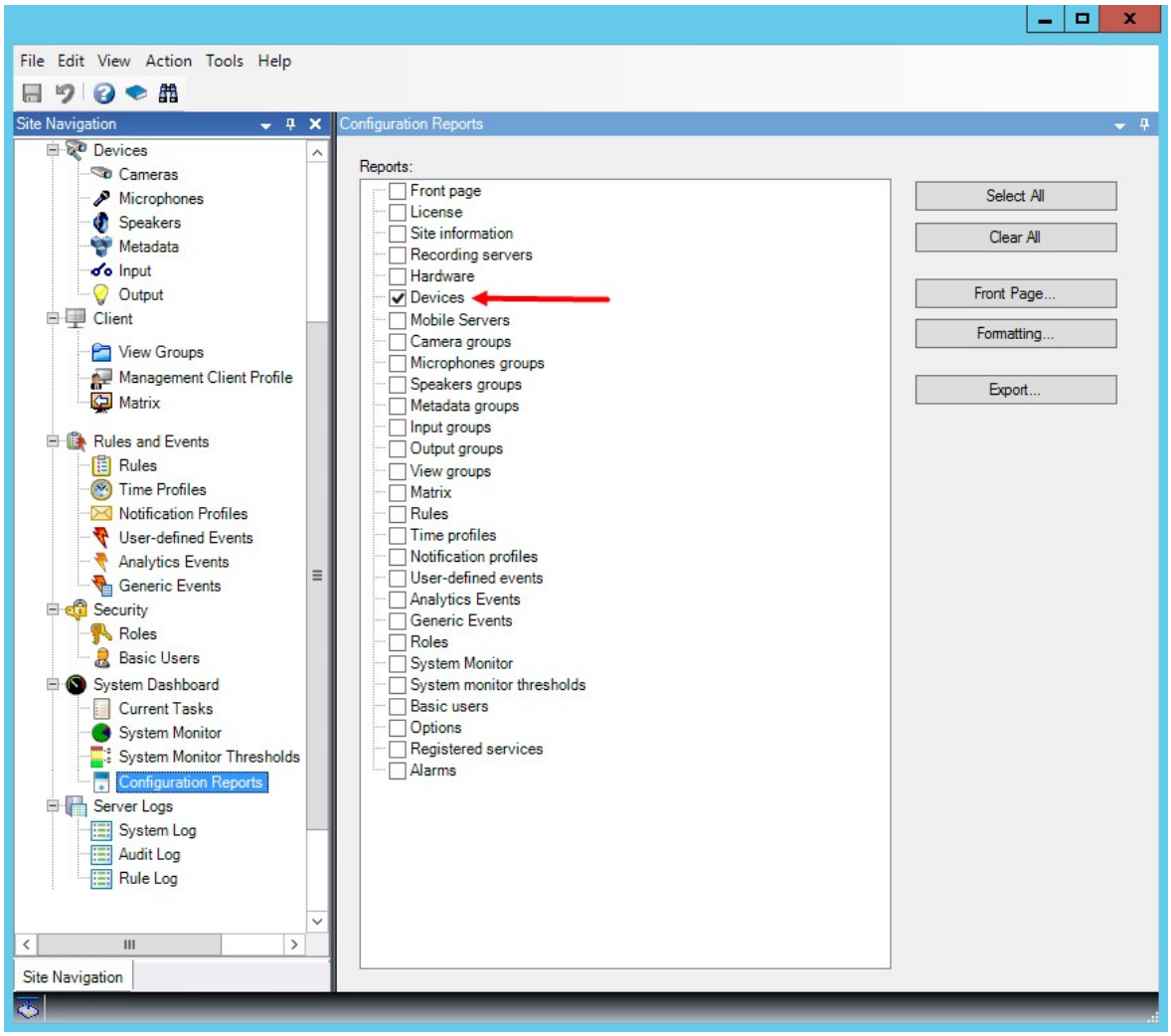
您分配给此角色的用户可以为自己解除配置为可解除屏蔽的隐私屏蔽，也可以为其他 XProtect Smart Client 用户授权解除屏蔽。

创建隐私屏蔽配置报告

设备报告包含有关摄像机当前隐私屏蔽设置的信息。

要配置报告：

1. 在**站点导航**窗格中，选择**系统仪表板**。
2. 在**配置报告**下，选择**设备**报告。



3. 如果想修改报告，您可以更改首页和格式。
4. 单击**导出**，系统将创建 PDF 文件形式的报告。

有关报告的详细信息，请参阅 第 257 页上的使用系统配置打印报告。

客户端

视图组(已解释)

系统在客户端中呈现来自一台或多台摄像机的视频的方式称为视图。视图组是一个或多个此类视图的逻辑组的容器。在客户端，视图组显示为可展开的文件夹，用户可从其中选择组和希望查看的视图：

XProtect Smart Client 的示例：箭头表示视图组，其包含逻辑组(称为 Amenities)，它依次包含 3 个视图。

默认情况下，在 Management Client 中定义的每个角色也会作为视图组创建。在 Management Client 中添加角色时，该角色将默认作为视图组显示在客户端中以供使用。

- 对于分配至相关角色的用户/组，您可以基于角色来为其指定视图组。如果想要更改这些视图组权限，可以稍后在角色中执行相应设置
- 基于角色的视图组使用角色的名称。

  示例：如果将角色的名称创建为**大楼 A 保安人员**，它将在 XProtect Smart Client 中显示为名称为**大楼 A 保安人员**的视图组。

  除了添加角色时得到的视图组之外，还可以根据需要创建任意数量的其他视图组。您还可以删除视图组，包括添加角色时自动创建的视图组。
- 虽然每次添加角色时都会创建视图组，但是视图组不必与角色保持一致。如果需要，您可以对视图组进行添加、重命名或删除操作

> 如果您重命名某个视图组，则已经连接的客户端用户必须注销并再次登录后，名称更改才可见。

添加视图组

1. 右键单击**视图组**，然后选择**添加视图组**。将打开**添加视图组**对话框。
2. 输入新视图组的名称和可选说明，然后单击**确定**。

在您指定此类权限前，任何角色都无权使用新添加的视图组。如果您已经指定哪些角色可以使用新添加的视图组，已连接的具有相关角色的客户端用户必须注销并再次登录后，才能查看视图组。

Smart Client 配置文件

添加和配置 Smart Client 配置文件

您首先必须创建 Smart Client 配置文件，然后才能对其进行配置。

1. **右键单击 Smart Client** 配置文件。
2. 选择**添加 Smart Client 配置文件**。
3. 在**添加 Smart Client 配置文件**对话框中，输入新配置文件的名称和说明，然后单击**确定**。
4. 在**总览**窗格中，单击刚创建的配置文件以对其进行配置。
5. 调整一个、多个或所有可用选项卡上的设置，然后单击**确定**。

复制 Smart Client 配置文件

如果您的 Smart Client 配置文件具有复杂设置或权限并需要类似的配置文件，则与从头创建新配置文件相比，复制已经存在的配置文件并对复制的配置文件进行较小调整可能相对容易一些。

1. 单击 **Smart Client 配置文件**，右键单击**总览**窗格中的配置文件，选择**复制 Smart Client 配置文件**。
2. 在显示的对话框中，为复制的配置文件提供独特的新名称和说明。单击**确定**。
3. 在**总览**窗格中，单击刚创建的配置文件以进行配置。配置内容包括调整可用选项卡中的一个、多个或所有选项卡上的设置：单击**确定**。

创建并设置 Smart Client 配置文件、角色和时间配置文件

使用 Smart Client 配置文件时，了解 Smart Client 配置文件、角色和时间配置文件之间的交互十分重要：

- Smart Client 配置文件用于处理以下方面的用户权限设置XProtect Smart Client
- 角色用于处理客户端、MIP SDK 和其他项的安全设置
- 时间配置文件用于处理这两种配置文件类型的时间方面的设置

结合使用这三个功能可为 XProtect Smart Client 用户权限提供唯一控制和自定义功能。

示例：您需要允许 XProtect Smart Client 设置中的用户仅在常规工作时间（8:00 至 16:00）查看选定摄像机的实时视频（非播放）。一种设置方式可以为：

1. 创建 Smart Client 配置文件，为其命名，例如**仅实时**。
2. 指定**仅实时**的所需实时/播放设置。
3. 创建配置文件，为其命名，例如**仅白天**。
4. 指定**仅白天**的所需时间段。
5. 创建新角色，为其命名，例如**保安(选定摄像机)**。
6. 指定**保安(选定摄像机)**可以使用的摄像机。
7. 指定**仅实时**Smart Client配置文件和**仅白天**时间配置文件给**保安(选定摄像机)**角色，以连接这三个元素。

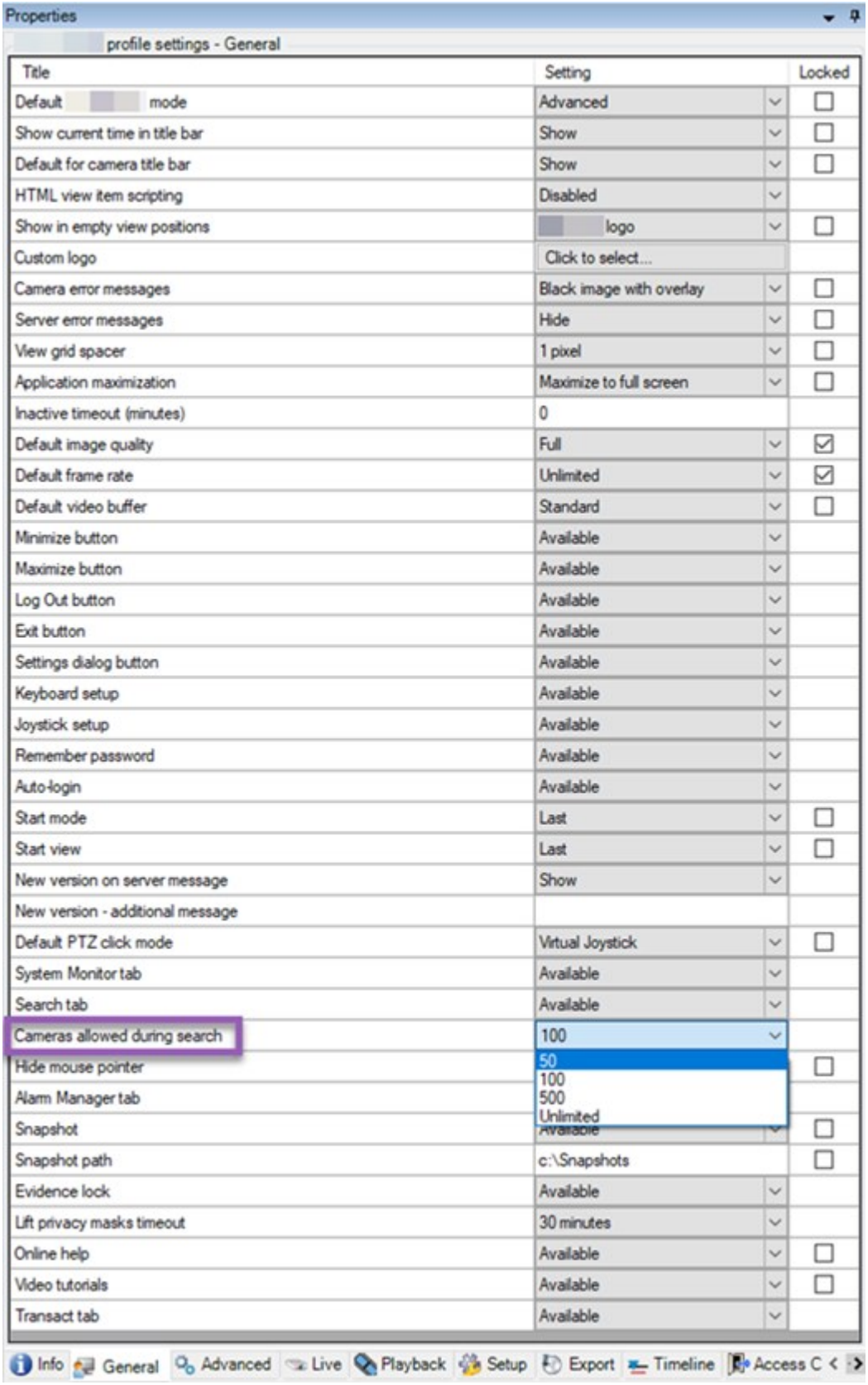
现在就混合了三个功能，创建了想要的结果，并给您留下了轻松微调和调整的空间。您可以按不同顺序进行设置，例如首先创建角色，然后创建 Smart Client 配置文件和时间配置文件，或者按照其他任何偏好的顺序设置。

设置搜索期间允许的摄像机数量

您可以配置操作员可以添加到 XProtect Smart Client 的搜索中的摄像机数量。默认值为 **100**。如果超出摄像机限制，则操作员会收到警告。

1. 在 XProtect Management Client 中，展开**客户端 > Smart Client 配置文件**。
2. 选择相关的配置文件。

3. 单击**常规**选项卡。


Properties
profile settings - General
Title
Setting
Locked
Default mode
Advanced
Show current time in title bar
Show
Default for camera title bar
Show
HTML view item scripting
Disabled
Show in empty view positions
logo
Custom logo
Click to select...
Camera error messages
Black image with overlay
Server error messages
Hide
View grid spacer
1 pixel
Application maximization
Maximize to full screen
Inactive timeout (minutes)
0
Default image quality
Full
Default frame rate
Unlimited
Default video buffer
Standard
Minimize button
Available
Maximize button
Available
Log Out button
Available
Exit button
Available
Settings dialog button
Available
Keyboard setup
Available
Joystick setup
Available
Remember password
Available
Auto-login
Available
Start mode
Last
Start view
Last
New version on server message
Show
New version - additional message
Default PTZ click mode
Virtual Joystick
System Monitor tab
Available
Search tab
Available
Cameras allowed during search
100
50
100
500
Unlimited
Hide mouse pointer
Alarm Manager tab
Snapshot
Snapshot path
c:\Snapshots
Evidence lock
Available
Lift privacy masks timeout
30 minutes
Online help
Available
Video tutorials
Available
Transact tab
Available
Info
General
Advanced
Live
Playback
Setup
Export
Timeline
Access C

4. 在搜索过程中允许的**摄像机**中，选择以下值之一：
    - **50**
    - **100**
    - **500**
    - **不受限制**
5. 保存更改。

更改默认导出设置

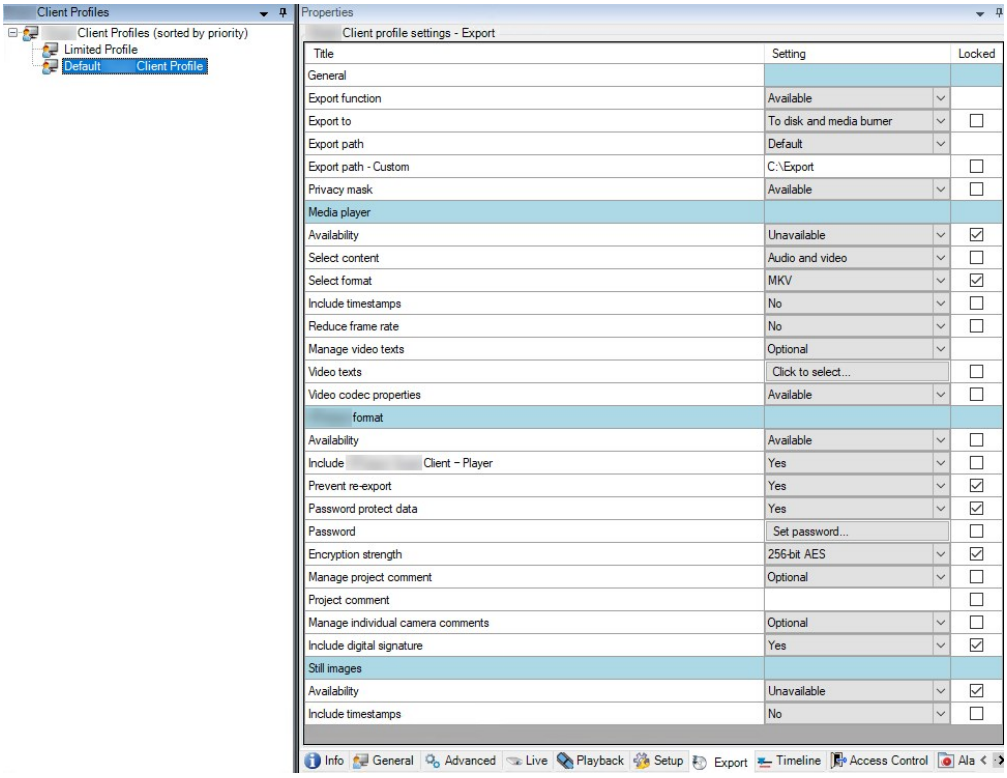
当您安装 XProtect 视频管理软件系统时，XProtect Smart Client 中定义导出选项的默认导出设置会受到限制，以确保最高级别的安全性。您可以更改这些设置，为操作员提供更多选项。

默认设置

- 只有 XProtect 格式可用
    - 已阻止重新导出
    - 导出受密码保护
    - 256 位 AES 加密
    - 数字签名已添加
- 无法导出为 MKV 格式或 AVI 格式
- 无法导出静态图像

步骤：

1. 在 XProtect Management Client 中，展开**客户端 > Smart Client 配置文件**。
2. 选择**默认 Smart Client 配置文件**。
3. 在**属性**窗格中，选择**导出**选项卡。



4. 要在 XProtect Smart Client 中提供受限格式，请找到设置并选择**可用**。
5. 要使操作员能够更改 XProtect Smart Client 中的设置，请清除相关设置旁边的**锁定**复选框。
6. 如果相关，请更改其他设置。
7. (可选) 登录 XProtect Smart Client 以验证您的设置是否已应用。

Management Client 配置文件

添加和配置 Management Client 配置文件

如果不想使用默认配置文件，可以创建 Management Client 配置文件，然后对其进行配置。

1. **右键单击 Management Client** 配置文件。
2. 选择**添加 Management Client 配置文件**。
3. 在**添加 Management Client 配置文件**对话框中，输入新配置文件的名称和说明，然后单击**确定**。
4. 在**总览**窗格中，单击刚创建的配置文件以对其进行配置。
5. 在**配置文件**选项卡上，从 Management Client 配置文件选择或清除功能。

复制 Management Client 配置文件

如果您的 Management Client 配置文件具有需要重复使用的设置，则可复制已经存在的配置文件并对复制的配置文件进行较小调整，而不用从头创建新配置文件。

1. 单击**ManagementClient配置文件**，右键单击**总览**窗格中的配置文件，选择**复制ManagementClient配置文件**。
2. 在显示的对话框中，为复制的配置文件提供独特的新名称和说明。单击**确定**。
3. 在**总览**窗格中，单击配置文件，然后转到**信息**选项卡或**配置文件**选项卡来对配置文件进行配置。

管理 Management Client 配置文件功能的可见性

将 Management Client 配置文件与角色关联，可将用户界面限制为代表对于每个管理员角色可用的功能。

将 Management Client 配置文件与角色相关联

1. 展开**安全**节点并单击**角色**。
2. 在**角色设置**窗口的**信息**选项卡上，将配置文件与角色相关联。有关详细信息，请参阅"信息"选项卡(角色)。

管理角色对系统功能的整体访问

Management Client 配置文件仅处理系统功能的视觉展示，而不实际访问它。

管理角色对系统功能的整体访问：

1. 展开**安全**节点并单击**角色**。
2. 单击**整体安全**选项卡，然后选择相应的复选框。有关详细信息，请参阅 第 433 页上的"整体安全"选项卡(角色)。

在**整体安全**选项卡上，确保启用**连接**安全权限，以便授予所有角色对 Management Server 的访问权限。

除了内置的管理员角色，只有与角色(已在**整体安全**选项卡上向其授予针对管理服务器的**管理安全**权限)关联的用户才能添加、编辑和删除 Management Client 配置文件。

限制配置文件功能的可见性

可以更改所有 Management Client 元素的可见性设置。默认情况下，Management Client 配置文件可查看 Management Client 中的所有功能。

1. 展开“客户端”节点，然后单击 Management Client 配置文件。
2. 选择一个配置文件，然后单击“配置文件”选项卡。
3. 清除相关功能的复选框，从而针对具有与该 Management Client 配置文件相关联角色的任何 Management Client 用户，在视觉上从 Management Client 删除该功能

Matrix

Matrix 和 Matrix 接收方(已作说明)

Matrix 是一项用于远程发布视频的功能。

Matrix 接收方是具有 XProtect Smart Client 的计算机，在 Matrix 中被定义为 Management Client 接收方。

利用 Matrix，可以将系统网络中任意摄像机的视频推送至任何正在运行的 Matrix 接收方。

要查看 Matrix 中添加的 Management Client 接收方的列表，请展开**站点导航**窗格中的**客户端**，然后选择 **Matrix**。将在 Matrix 属性**窗格中显示**配置的列表。

在 Management Client 中，您必须添加每个 Matrix 收件方来接收 Matrix 触发的视频。

定义发送视频至 Matrix 接收方的规则

要发送视频至 Matrix 接收方，必须在触发向相关 Matrix 接收方进行视频传输的规则中包含 Matrix 接收方。要实现该操作：

1. 在**站点导航**窗格中，展开**规则和事件 > 规则**。右键单击**规则**，以打开**管理规则**向导。第一步，选择规则类型，第二步，选择条件。
2. 在 **管理规则**的步骤 3(**步骤 3:动作**)中，选择**设置 Matrix 以查看<设备>**动作
3. 在初始规则说明中单击 Matrix 链接。
4. 在**选择 Matrix 配置**对话框中，选择相关 Matrix 接收方，然后单击**确定**。
5. 在初始规则说明中单击**设备**链接，并选择想要从其发送视频至 Matrix 接收方的摄像机，然后单击**确定**以确认选择。
6. **如果完成了规则请单击**完成，或者根据需要定义其他动作和/或停止动作。

Matrix 如果删除了 Matrix 接收方，包含接收方的所有规则都将停止工作。

添加 Matrix 接收方

要在 Matrix 中添加现有的 Management Client 接收方：

1. **展开 Matrix 客户端**，然后选择 。
2. **右键单击 MatrixMatrix 配置**并选择添加 。
3. **填写 Matrix** 添加对话框中的字段。
    1. **在** Matrix 地址字段中输入所需接收方的 IP 地址或主机名。
    2. 在**端口**字段输入 Matrix 接收方安装所使用的端口号。
4. 单击**确定**。

此时即可在规则中使用 Matrix 接收方。

> 本系统不会检查指定的端口号或密码是否正确，或者指定的端口号、密码或类型是否与实际 Matrix 接收方一致。请确保输入信息正确无误。

将同一视频发送至数个 XProtect Smart Client 视图

您可以将相同的视频发送到多个 Matrix 视图中的 XProtect Smart Client 位置，前提是这些视图的 Matrix 位置共享相同的端口号和密码：

1. 在 XProtect Smart Client 中，创建相关视图和共享相同端口号与密码的 Matrix 位置。
2. 在 Management Client 中，添加相关 XProtect Smart Client 作为 Matrix 接收方。
3. 您可以在规则中包含 Matrix 接收方。

规则和事件

添加规则

添加规则时，**管理规则**向导会引导您操作，其中仅列出相关选项。

它确保规则不会缺失所需的元素。根据规则的内容，会自动建议适合的停止动作（即，当规则不再适用时应执行何种动作），从而确保不会意外创建永不结束的规则。

事件

添加基于事件的规则时，可以选择不同类型的事件。

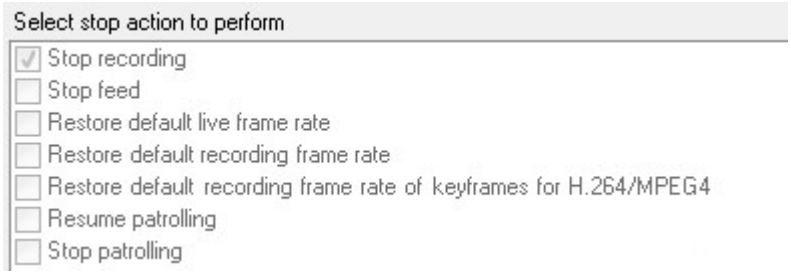
- 请参阅事件总览以获取总览以及对您可以选择的事件类型的描述。

操作和停止操作

添加规则时，可以在不同的操作之间进行选择。

一些操作需要停止操作。例如，如果选择了操作**开始记录**，将开始录记录可能会无限期继续下去。因此，操作**开始录制**有一个强制停止操作，称为**停止录制**。

管理规则向导可确保您在必要时指定停止操作：



选择停止操作。在示例中，请注意强制停止操作(选中，变灰)、非相关停止操作(变灰)和可选停止操作(可选择)。

- 有关可以选择的开始和停止操作的总览，请参阅操作和停止操作。

创建规则

1. 右键单击**规则**项目>**添加规则**。这会开**管理规则**向导。该向导会引导您完成指定规则内容的过程。
2. 分别在**名称**和**说明**字段中指定新规则的名称和说明。
3. 选择规则的相关条件类型：在发生特定事件时执行一个或多个动作的规则，或者在进入特定时间段时执行一个或多个动作的规则。
4. 单击**下一步**转到向导的第二步。在向导的第二步，可以为规则定义更多条件。
5. 选择一个或多个条件，例如**工作日为<day>**：

   根据您的选择，在向导窗口的下半部分编辑规则说明：

   单击**粗斜体**的带下划线项目以指定其具体内容。例如，单击我们示例中的**天**链接，可以选择在一周中的一天或多天应用规则。

6. 如果已指定具体条件，则单击**下一步**移至向导的下一步，然后选择规则应涵盖的动作。根据规则的内容和复杂度，您可能需要定义更多步骤，例如停止事件和停止动作。例如，如果某规则指定设备在某个时间间隔(例如，星期四 08:00 至 10:30)期间执行特定动作，向导会要求您指定当时间间隔结束后应执行何种动作。

7. 如果规则的条件达成，规则在创建好之后就会默认处于活动状态。如果不希望规则直接处于活动状态，则请清除**活动**复选框。
8. 单击**完成**。

验证规则

可以一次验证单个规则或所有规则的内容。**在创建规则时**，管理规则向导可确保规则的所有元素都有效。

当规则存在一段时间后，规则的一个或多个元素会受其他配置的影响，规则也可能无法工作。例如，在规则由特定时间配置文件触发的情况下，如果您已删除该时间配置文件或不再拥有其权限，则该规则不会工作。可能很难掌握这类意外的配置影响。

规则验证可帮助您追踪受影响的规则。验证按规则进行；每个规则都是独立验证的。**您无法相互验证规则**（例如，为了查看某个规则是否与另一个规则冲突），即使使用验证所有规则功能也是如此。

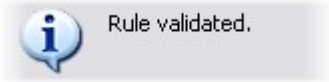
验证规则

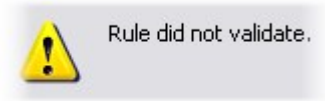
1. 单击**规则**，然后选择要验证的规则。
2. 右键单击规则，然后单击**验证规则**。
3. 单击**确定**。

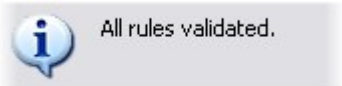
验证所有规则

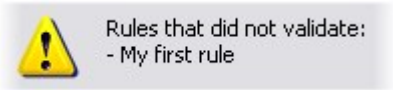
1. 右键单击**规则**项，然后单击**验证所有规则**。.
2. 单击**确定**。

对话框会通知您，规则验证是否成功。如果您选择验证多个规则并且一个或多个规则未成功，则对话框将列出受影响规则的名称。









您无法验证规则本身之外的先决条件配置是否可能会阻碍规则工作。例如，某项规则指定当特定摄像机侦测到移动时应开始记录，如果规则本身中的元素正确，即使相应的摄像机未启用移动侦测(在摄像机级别启用，而非通过规则启用)，该规则仍会验证。

编辑、复制和重命名规则

1. 在**总览**窗格中，右键单击相关规则。
2. 选择：

   编辑规则或**复制规则**或**重命名规则**。**管理规则**向导将打开。
3. 如果选择**复制规则**，向导将打开，并显示所选规则的副本。单击**完成**以创建副本。
4. 如果选择**编辑规则**，则向导将打开，您可以输入更改。单击**完成**以接受更改。
5. 如果选择**重命名规则**，您可以直接重命名规则名称文本。

取消激活和激活规则

只要规则条件达成，系统即会应用规则，也就是说，规则会处于活动状态。如果不希望规则处于活动状态，可以取消激活规则。当取消激活规则后，本系统将不会应用规则，即使符合规则的条件。规则取消激活后，您可以轻松激活。

取消激活规则

1. 在**总览**窗格中，选择规则。
2. 清除**属性**窗格中的**活动**复选框。
3. 单击工具栏中的**保存**。
4. 带红色 x 的图标表示**规则**列表中的规则已取消激活：

激活规则

当您要再次激活规则时，请选择规则，再选中**触发**复选框，然后保存设置即可。

指定时间配置文件

1. 在**时间配置文件**列表中，右键单击**时间配置文件>添加时间配置文件**。此操作将打开**时间配置文件**窗口。
2. 在**时间配置文件**窗口中，在**名称**字段内输入新时间配置文件的名称。在**说明**字段中输入新时间配置文件的说明(可选)。

3. 在**时间配置文件**窗口的日历中，选择**日视图**、**周视图**或**月视图**，然后在日历内右键单击并选择**添加单一时间**或**添加重复时间**。
4. 为时间配置文件指定时间段后，单击**时间配置文件**窗口的**确定**。系统会将新时间配置文件添加至**时间配置文件**列表中。如果在稍后阶段希望编辑或删除时间配置文件，则可以从**时间配置文件**列表进行操作。

添加单一时间

选择**添加单一时间**时，会出现**选择时间**窗口：

您系统上的日期和时间格式可能会不同。

1. 在**选择时间**窗口中，指定**开始时间**和**结束时间**。**如果时间覆盖全天**，则选中全天事件复选框。
2. 单击**确定**。

添加重复时间

选择**添加重复时间**时，会出现**选择重复时间**窗口：

1. 在**选择时间**窗口中，指定时间范围、重复模式和重复范围。
2. 单击**确定**。

> 时间配置文件可包含多个时间段。如果想要时间配置文件包含更多时间段，请添加更多单一时间或重复时间。

重复时间

当您设置要在详细的经常性计划上执行的操作时。

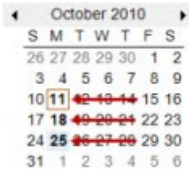
例如：

- 每周二的 15:00 至 15:30 之间每 1 小时
- 每 3 个月的第 15 天 11:45
- 每天的 15:00 至 19:00 之间每 1 小时

> 时间基于安装有 Management Client 的服务器的本地时间设置。

编辑时间配置文件

1. 在**总览**窗格的**时间配置文件**列表中，右键单击相关时间配置文件，然后选择**编辑时间配置文件**。此操作将打开**时间配置文件**窗口。
2. 依照需要编辑时间配置文件。如果已更改时间配置文件，则单击**时间配置文件**窗口中的**确定**。您将会返回**时间配置文件**列表。



> 在**时间配置文件信息**窗口中，可根据需要编辑时间配置文件。请记住，时间配置文件可能包含多个时间段，并且时间段可能是重复的。右上角的月份小图总览可帮助您快速总览该时间配置文件所涵盖的时间段，因为包含指定时间的日期以粗体突出显示。

> 在本例中，加粗日期表示您已在数天中指定了时间段，并且在星期一指定了重复时间。

创建日长时间配置文件

1. **展开**规则和事件文件夹**时**间配置文件。
2. 在**时间配置文件**列表中，右键单击**时间配置文件**，然后选择**添加日长配置文件**。
3. 在**日长时间配置文件**窗口中，参考下面的属性表填写需要的信息。要处理明暗之间的转换时期，可以补偿配置文件的激活和取消激活。时间和月份名称以计算机语言/区域设置使用的语言显示。
4. 要在地图中查看输入的地理坐标位置，请单击**在浏览器中显示位置**。这会打开浏览器，供您查看位置。
5. 单击**确定**。

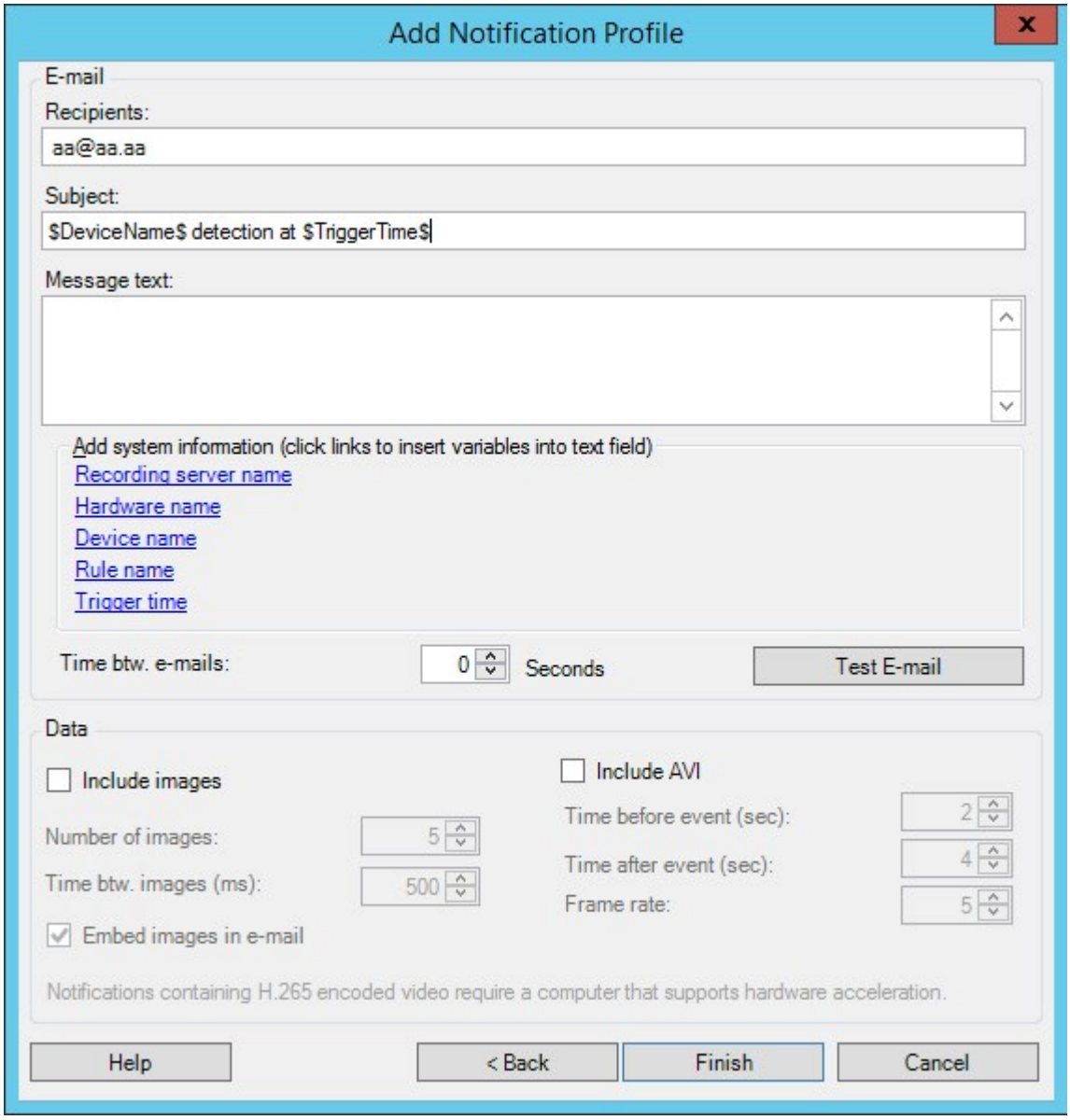
日长时间配置文件属性

名称	说明
名称	配置文件的名称。
说明	配置文件的说明(可选)。
地理坐标	表示分配至配置文件的摄像机的物理位置的地理坐标。
日出偏移	按日出对配置文件激活的补偿分钟数 (+/-)。
日落偏移	按日落对配置文件取消激活的补偿分钟数 (+/-)。
时区	表示摄像机的物理位置的时区。

添加通知配置文件

必须首先为电子邮件通知指定邮件服务器设置，然后才可以创建通知配置文件。有关详细信息，请参阅创建通知配置文件的要求。

1. **展开**规则和事件，右键单击通知配置**文**件 > 添**加通知配置文**件。这将打开**添加通知配置文件**向导。
2. 指定名称和说明。单击**下一步**。
3. 指定收件人、主题、消息文本和电子邮件间隔时间：



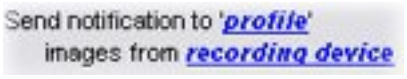
4. 要将测试电子邮件通知发送给指定收件人，请单击**测试电子邮件**。
5. 要包含预警报静态图像，请选择**包含图像**，并指定图像数量、图像之间的时间和图像是否嵌入电子邮件中。
6. 要包含 AVI 视频剪辑，请选择**包含 AVI**，并指定事件前后的时间以及帧速率。

包含编码视频 H.265 的通知需要支持硬件加速的计算机。

7. 单击**完成**。

从规则触发电子邮件通知

1. 右键单击**规则**项，然后单击 **> 添加规则**或**编辑规则**。
2. 在**管理规则**向导中，单击**下一步**转到**选择要执行的操作**列表，然后选择**将通知发送到 <配置文件>**。
3. 选择相关的通知配置文件，以及将包含在通知配置文件的电子邮件通知中的任何记录应来自哪些摄像机。



不能将记录包含在通知配置文件的电子邮件通知中，除非实际正在记录内容。如果您希望电子邮件通知中包含静态图像或 AVI 视频剪辑，则应检验规则是否指定了应执行记录。以下示例来自包含**开始记录**动作和**发送通知到**动作的规则：

添加用户定义事件

无论选择以哪种方式使用用户定义事件，每个用户定义事件都必须通过 Management Client 添加。

1. 展开**规则和事件 > 用户定义的事件**。
2. 在**总览**窗格中，右键单击**事件 > 添加用户定义的事件**。
3. 为新的用户定义事件输入名称，然后单击**确定**。现在，新添加的用户定义事件会显示于**总览**窗格的列表中。

如果用户权限许可，用户现在即可从 XProtect Smart Client 手动触发用户定义事件。

如果删除用户定义事件，则会影响使用该用户定义事件的所有规则。此外，删除的用户定义事件只有在 XProtect Smart Client 用户注销后才会从 XProtect Smart Client 消失。

重命名用户定义事件

如果您重命名用户定义事件，则已经连接的 XProtect Smart Client 用户必须注销并再次登录后，名称更改才可见。

1. 展开**规则和事件 > 用户定义的事件**。
2. 在**总览**窗格中，选择用户定义事件。
3. 在**属性**窗格中，改写现有名称。
4. 在工具栏中，单击**保存**。

添加和编辑分析事件

添加分析事件

1. 展开**规则和事件**，右键单击**分析事件**，并选择**新增**。
2. 在**属性**窗口中，在**名称**字段内输入事件的名称。
3. 如果需要，在**说明**字段中输入说明文本。
4. 在工具栏中，单击**保存**。可通过单击**测试事件**来测试事件的有效性。可以连续更正测试中指出的错误，并且可以在进程中的任何位置运行测试任意所需次数。

编辑分析事件

1. 单击现有分析事件以查看**属性**窗口，可在其中编辑相关字段。
2. 可通过单击**测试事件**来测试事件的有效性。可以连续更正测试中指出的错误，并且可以在进程中的任何位置运行测试任意所需次数。

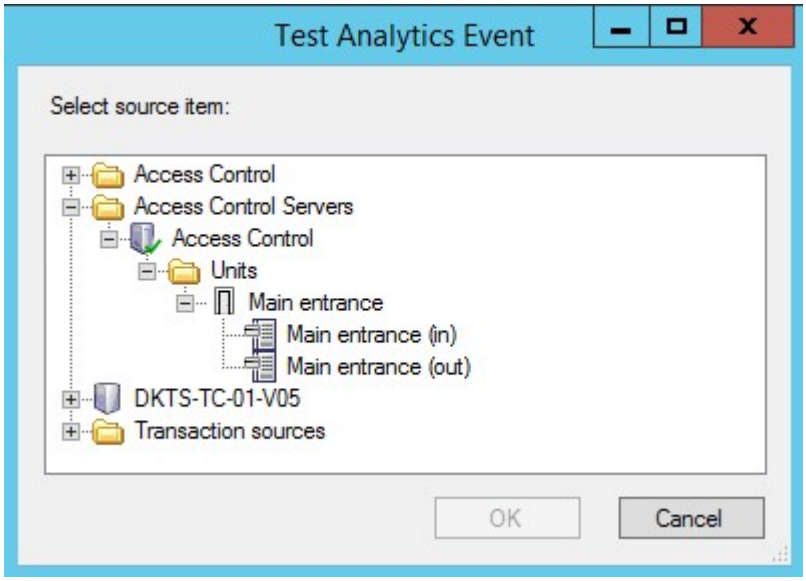
编辑分析事件设置

在工具栏中，转到**工具 > 选项 > 分析事件**选项卡以编辑相关设置。

测试分析事件

创建分析事件后，您可以测试要求（请参阅 第 245 页上的添加和编辑分析事件），如对于已在 Management Client 中启用分析事件功能的要求。

1. 选择现有分析事件。
2. 在属性中，单击**测试事件**按钮。随即出现一个窗口，显示事件的所有可能来源。



3. 选择测试事件的来源，如摄像机。窗口关闭，并出现一个新窗口，该窗口会审查分析事件正常工作必须实现的四个条件。

作为额外测试，在 XProtect Smart Client 中，您可以验证是否已将分析事件发送到事件服务器。为此，打开 XProtect Smart Client 并查看**警报管理器**选项卡中的事件。

添加常规事件

您可以定义常规事件，以帮助 VMS 识别来自外部系统的 TCP 或 UDP 数据包中的特定字符串。根据常规事件，您可以配置 Management Client 以触发动作，如开始记录或发出警报。

要求

您已启用常规事件，并指定允许的源目的地。有关详细信息，请参阅 第 344 页上的“常规事件”选项卡(选项)。

添加常规事件：

1. 展开**规则和事件**。
2. 右键单击**常规事件**并选择**新增**。
3. 填入需要的信息和属性。有关详细信息，请参阅 第 428 页上的常规事件和数据来源(属性)。
4. (可选)要验证搜索表达式是否有效，请在与预期数据包对应的**检查表达式是否符合事件字符串**字段中输入搜索字符串：
   - **匹配** - 可以根据搜索表达式验证字符串
   - **不匹配** - 搜索表达式无效。对其进行更改，然后重试

在 XProtect Smart Client 中，可以验证事件服务器是否已接收到您的常规事件。可以通过选择**事件**在**警报管理器**选项卡的**警报列表**中进行此操作。

身份验证

从外部 IDP 登记索赔

1. 在 Management Client 中，选择**工具 > 选项**并打开**外部 IDP** 选项卡。
2. 在**外部 IDP** 部分中，选择**添加**。
3. 在**已登记索赔**部分中，选择**添加**。
4. 输入关于索赔的信息。有关详细信息，请参阅登记索赔。

将来自外部 IDP 的索赔映射到 XProtect 中的角色

在外部 IDP 站点上，管理员必须创建包含名称和值的声明。随后，索赔会映射到 VMS 中的角色，而用户的特权将由角色决定。

1. 从 Management Client 中的 **站点导航** 窗格中，展开 **安全**节点，然后选择 **角色**。
2. 选择一个角色，选择 **外部 IDP**选项卡，然后选择**添加**。
3. 选择一个外部 IDP 和一个索赔名称，然后输入索赔值。

   索赔名称必须与来自外部 IDP 的索赔名称完全相同。

4. 选择**确定**。

如果删除了外部 IDP，则通过外部 IDP 连接到视频管理软件的所有用户也会被删除。连接到外部 IDP 的所有已注册声明都将被删除，并且与角色的任何映射也将被删除。

通过外部 IDP 登录：

您可以使用外部 IDP登录XProtect Smart Client、XProtect Management Client、XProtect Web Client和 XProtect Mobile 客户端。

1. 在 XProtect Smart Client 或 XProtect Management Client 中的登录对话框的**身份验证**下，选择外部 IDP，然后选择**登录**。在您第一次登录时，您将被重定向到属于外部 IDP 的网页。
2. 提供您的用户名和密码并登录。登录后，您将返回 XProtect 客户端，然后您就完成登录了。

在**工具 > 选项 > 外部 IDP** 下，您可以配置**身份验证**列表上显示的外部 IDP 的名称。

如果外部 IDP 因恢复或更改密码而被禁用，则通过外部 IDP 登录的选项在**身份验证**列表中不可用。此外，如果外部 IDP 被禁用，则从外部 IDP收到的客户端密码将从**工具>选项**下的**外部 IDP**选项卡上的**客户端密码**字段中消失。

安全

添加和管理角色

1. 展开**安全**，然后右键单击**角色**。
2. **选择**添加角色。将打开**添加角色**对话框。
3. 输入新角色的名称和说明，然后单击**确定**。
4. 新角色即会添加至**角色**列表。默认情况下，新角色不拥有与其相关的任何用户/组，但是它拥有相关的大量默认配置文件。
5. 要选择不同的 Smart Client 和 Management Client 配置文件、证据锁定配置文件或时间配置文件，请单击下拉列表。
6. 您现在能将用户/组分配到角色，并可指定它们能访问系统的哪些功能。

有关详细信息，请参阅 第 249 页上的将用户和组分配至角色/从角色删除 和 第 431 页上的角色(“安全性”节点)。

复制、重命名或删除角色

复制角色

如果您的角色具有复杂设置和/或权限并需要类似或基本类似的角色，则与从头创建新角色相比，复制已经存在的角色并对复制的角色进行较小调整可能相对容易一些。

1. 展开**安全**，单击**角色**，右键单击相关角色，然后选择**复制角色**。
2. 在打开的对话框中，为复制的角色提供独特的新名称和说明。
3. 单击**确定**。

重命名角色

如果重命名角色，将不会更改基于该角色的视图组的名称。

1. **展开**安全，然后右键单击**角**色。
2. 右键单击所需的角色，然后选择**重命名角色**。
3. 在打开的对话框中，更改角色的名称。
4. 单击**确定**。

删除角色

1. 展开**安全**，然后单击**角色**。
2. 右键单击不需要的角色，然后选择**删除**。
3. 单击**是**。

> 删除角色将不会删除基于该角色的视图组。

查看有效角色

使用“有效角色”功能，可以查看所选用户或组的所有角色。如果您使用组，该功能很实用；它是查看特定用户属于哪个角色的成员的唯一方式。

1. 通过展开**安全**，然后右键单击**角色**并选择**有效角色**，打开**有效角色**窗口。
2. 如果要了解有关基本用户的信息，请在**用户名**字段中输入名称。单击**刷新**以显示用户的角色。
3. 如果使用 Active Directory 中的 Windows 用户或组，请单击**“...”**浏览按钮。选择对象类型，输入名称，然后单击**确定**。用户的角色会自动显示。

将用户和组分配至角色/从角色删除

要将 Windows 用户或组或基本用户分配至角色/从角色删除：

1. 展开**安全**，然后选择**角色**。然后，在**总览**窗格中选择所需角色：
2. 在**属性**窗格中，选择底部的**用户和组**选项卡。
3. 单击**添加**，然后选择 **Windows 用户**或**基本用户**。

将 Windows 用户和组分配至角色

1. 选择 **Windows 用户**。这将打开**选择用户、计算机和组**对话框：
2. 验证已指定所需的对象类型。例如，如果您需要添加计算机，则单击**对象类型**并标记**计算机**。此外，验证已在**从该位置**字段指定所需域。如果未指定，则单击**位置**浏览所需域。
3. 在**输入对象名称以选择**框中，输入相关用户名、首字母或 Active Directory 可以识别的其他类型标识符。使用**检查名称**功能以验证 Active Directory 是否可识别您已输入的名称或首字母。或者，使用**“高级.....”**功能搜索用户或组。
4. 单击**确定**。选择的用户/组现在便已添加到**用户和组**选项卡中已分配所选角色的用户的列表。可以通过输入以分号 **(;)** 隔开的多个名称添加更多用户和组。

将基本用户分配至角色

1. **选择**基本用户。这将打开**选择要添加到角色的基本用户**对话框：
2. 选择要向其分配该角色的基本用户。
3. 可选：单击**新建**以创建新的基本用户。

4. 单击**确定**。选择的基本用户现在便已添加到**用户和组**选项卡中您已为其分配所选角色的基本用户的列表。

将用户和组从角色删除

1. 在**用户和组**选项卡上，选择您希望删除的用户或组，然后单击选项卡下方的**删除**。如果需要，可以选择一个以上的用户或组，或组和单个用户的组合。
2. 确认您希望删除选择的用户或/和组。单击**是**。

用户还可以通过组成员资格拥有角色。在该情况下，您无法从角色删除单个用户。组成员还可以作为个人保留角色。要查找用户、组或单个组成员拥有哪些角色，请使用**查看有效角色**功能。

创建基本用户

Milestone XProtect VMS 中有两类用户帐户：基本用户和 Windows 用户。

基本用户是您在 Milestone XProtect VMS 中创建的用户帐户。它是专用的系统用户帐户，会进行个人用户的基本用户名和密码身份验证。

Windows 用户是您通过 Microsoft 的 Active Directory 而添加的用户帐户。

基本用户与 Windows 用户之间的一些区别如下：

- 基本用户通过用户名与密码的组合进行身份验证，并且特定于一个系统/站点。请注意，即便在不同的联合站点上创建的两个基本用户具有彼此相同的名称和密码，基本用户也只能访问创建自己的站点。
- Windows 用户根据 Windows 登录进行身份验证，并且特定于计算机。

配置基本用户的登录设置

您可以在 JSON 文件中定义基本用户的登录设置，该文件位于以下位置：`\\Program Files\Milestone\Management Server\IIS\IDP\appsettings.json`。

在该文件中，您可以设置以下参数：

LoginSettings	
"ExpireTimeInMinutes": 5	定义如果用户不执行任何操作，登录会话将过期的时间长度(以分钟为单位)。
LockoutSettings	
"LockoutTimeSpanInMinutes": 5	定义用户将被锁定的时间长度(以分钟为单位)。

"MaxFailedAccessAttempts": 5	定义用户在被锁定之前必须登录的尝试次数。
PasswordSettings	
"RequireDigit": true	定义密码中是否需要基本数字(0 到 9)。
"RequireLowercase": true	定义密码中是否需要小写字符。
"RequireNonAlphanumeric": true	定义密码中是否需要特殊字符 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)。
"RequireUppercase": true	定义密码中是否需要大写字符。
"RequiredLength": 8	定义密码中所需的字符个数。最小密码长度为 {0} 个字符,最大密码长度为 255 个字符。
"RequiredUniqueChars": 1	定义密码中所需的唯一字符个数的最小值。 例如,如果您将所需的唯一字符个数设置为 2,则诸如 aaaaaa、aa、a、b、bb、bbbbbbb 之类的密码将被拒绝。 而 abab、abc、aaab 等将被接受,因为密码中至少有两个唯一字符。 增加密码中唯一字符的个数可以避免容易被猜到的重复序列,从而提高密码强度。

要在系统上创建基本用户:

1. **展开**安全基本**用户**。
2. 在**基本用户**窗格中,右键单击并选择**创建基本用户**。
3. 指定用户名和密码。重复输入密码,以确保您的指定正确无误。

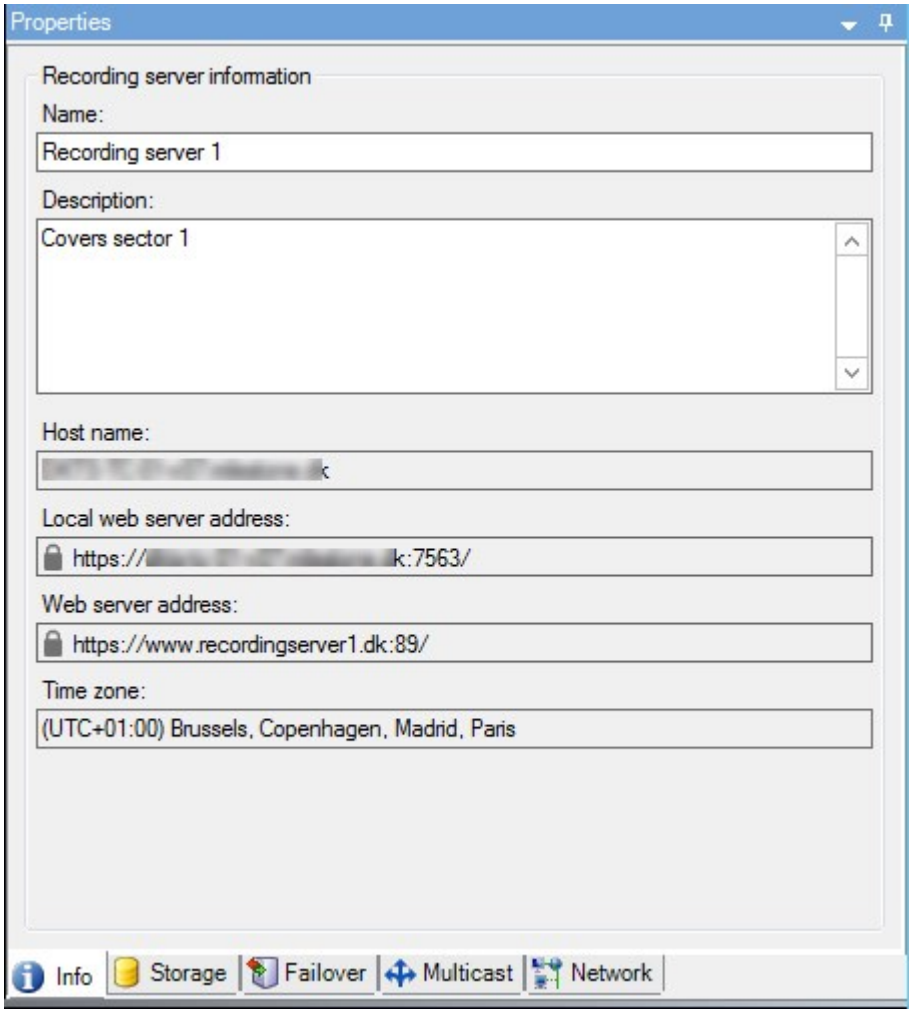
   密码必须满足**appsettings.json**文件中定义的复杂度(请参阅 第 250 页上的配置基本用户的登录设置)。
4. 指定基本用户是否应在下次登录时更改密码。Milestone 建议您选择该复选框,以便基本用户在第一次登录时可以指定自己的密码。

   您只有在创建无法更改密码的基本用户时,才应清除该复选框。此类基本用户包括诸如用于插件和服务器服务身份验证的系统用户。
5. 将基本用户的状态指定为**启用**或**锁定**。
6. **单击**确定创建基本用户。

查看客户端的加密状态

要验证您的记录服务器是否加密连接:

1. 打开 Management Client。
2. 在**站点导航**窗格中，选择**服务器 > 记录服务器**。这会打开记录服务器列表。
3. 在**总览**窗格中，选择相关的记录服务器，然后转到**信息**选项卡。
   如果已对从记录服务器检索数据流的客户端和服务器启用加密，则会在本地 Web 服务器地址和可选 Web 服务器地址前面显示挂锁图标。



系统仪表板

查看记录服务器上当前正在进行的任务

当前任务窗口显示所选记录服务器上正在进行的任务的总览。如果启动的任务需要很长时间并且在后个运行，则可以打开**当前任务**窗口查看任务的进度。冗长的用户启动任务的例子包括固件更新和硬件移动。您可以查看有关任务的开始时间、估计的结束时间和进度的信息。

如果任务没有按预期进行，则原因可能出现在硬件或网络中。示例包括服务器未运行、服务器错误、带宽太小或连接中断。

1. 在**站点导航**窗格中，选择**系统仪表板 > 当前任务**。
2. 选择一个记录服务器以查看其当前任务。

当前任务窗口中显示的信息不会动态更新，而是您打开窗口之时当前任务的快照。如果您已将窗口打开一段时间，请通过选择窗口右下角的**刷新**按钮来刷新信息。

系统监视器(已解释)

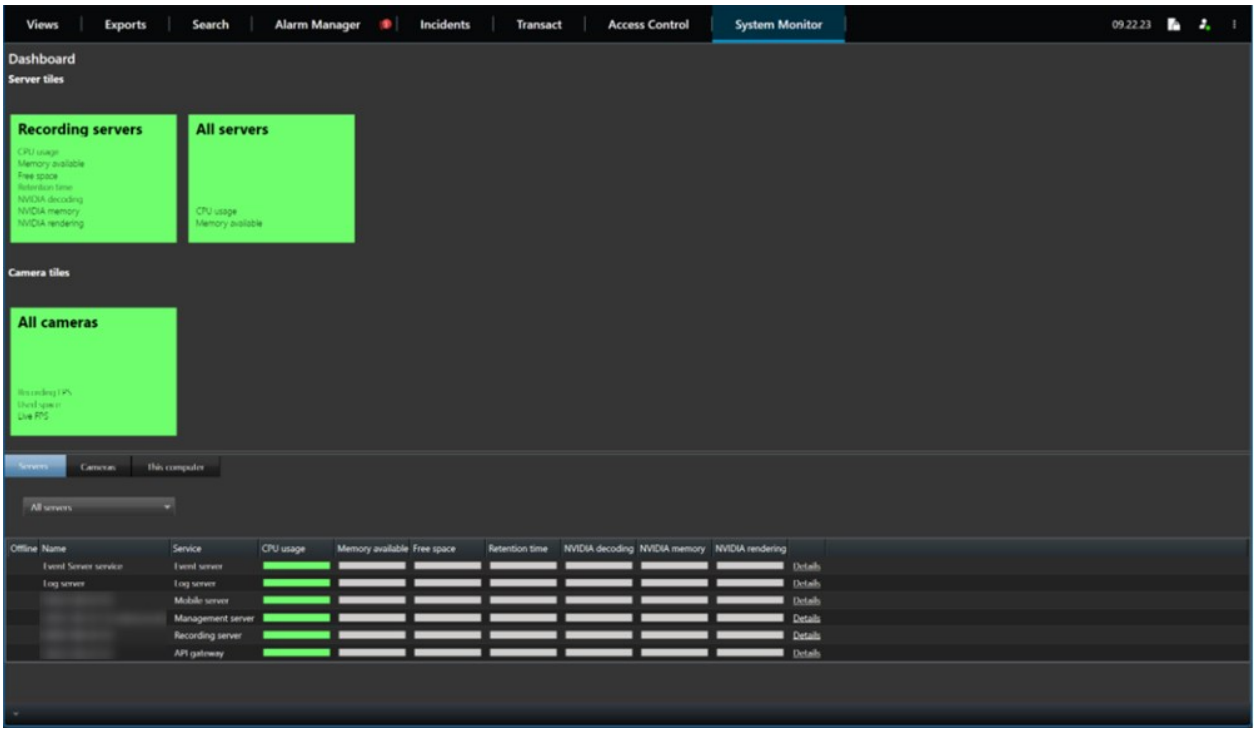
系统监视器功能要求 Data Collector 服务正在运行，并且只能在使用公历(西方)日历的计算机上工作。

系统监视器仪表板(已作说明)

在**系统监视器仪表板**上，您可以轻松了解视频管理软件系统的状况。硬件的状态由拼贴图及其颜色直观地表示：绿色(运行)、黄色(警告)和红色(严重)。当一个或多个硬件处于故障状态时，拼贴图也可能具有错误或警告图标。

默认情况下，系统会显示用于代表所有**记录服务器**、**所有服务器**和**所有摄像机**的拼贴图。您可以自定义这些默认拼贴图的监视参数并创建新的拼贴图。例如，可以设置拼贴图以代表单个服务器、单个摄像机、一组摄像机或一组服务器。

例如，监视参数为对服务器可用的 CPU 使用率或存储。拼贴图仅监视您添加到拼贴图的监视参数。有关第 256 页上的在系统监视器仪表板上编辑摄像机或服务器拼贴图详细信息，请参阅 第 255 页上的在系统监视器仪表板上添加新摄像机或服务器拼贴图、和 第 256 页上的在系统监视器仪表板上删除摄像机或服务器拼贴图。



系统监视器阈值(已解释)

通过系统监视器阈值,您可以定义和调整阈值,**系统监视器仪表板**上的拼贴图应直观地指示您的系统硬件更改状态。例如,当服务器的 CPU 使用率从正常状态(绿色)变为警告状态(黄色)或从警告状态(黄色)变为严重状态(红色)时。

系统具有所有相同类型硬件的默认阈值,因此您可以从安装系统和添加硬件的那一刻起开始监视系统硬件的状态。您可以为单个服务器、摄像机、磁盘和存储设置阈值。要更改阈值,请参阅 第 256 页上的编辑何时应更改硬件状态的阈值。

在系统硬件的使用率或负载仅在一秒钟或类似时间内达到高阈值的情况下,为确保不会看到**临界**或**警告**状态,请使用**计算间隔**。使用正确的计算间隔设置,您将不会收到有关超出阈值的假阳性警报,而只会收到有关持续问题的警报,例如 CPU 使用率或内存消耗。

您还可以设置规则(请参阅规则(已作说明)),以在阈值从一个状态变为另一个状态时执行特定操作或激活警报。

查看硬件的当前状态,并在需要时进行故障排除

在**系统监视器仪表板**上,您可以轻松了解视频管理软件系统的状况。硬件的状态由拼贴图及其颜色直观地表示:绿色(运行)、黄色(警告)和红色(严重)。当一个或多个硬件处于故障状态时,拼贴图也可能具有错误或警告图标。

您可以编辑硬件处于三种状态之一时的阈值。有关详细信息,请参阅第256页上的编辑何时应更改硬件状态的阈值。

系统监视器仪表板回答以下问题:所有服务器服务和摄像机都在运行吗?不同服务器上的 CPU 使用率和可用内存是否足够,以便记录所有内容并可供查看?

1. 在**站点导航**窗格中,选择**系统仪表板 > 系统监视器**。
2. 如果所有拼贴图都是绿色的,并且没有警告或错误图标,则所有监视参数以及由拼贴图代表的所有服务器和摄像机都可以正常运行。
   如果一个或多个拼贴图带有警告或错误图标,或者完全是黄色或红色,请选择这些拼贴图之一进行故障排除。
3. 在带有监视参数(窗口底部)的硬件列表中,找到未运行的硬件。将鼠标悬停在硬件旁边的红色十字标志上,以了解问题所在。
4. (可选)选择硬件右侧的**详细信息**,以查看问题存在多长时间了。启用历史数据收集,以查看一段时间内您的硬件状态。有关详细信息,请参阅 第 255 页上的收集硬件状态的历史数据。
5. 找到解决问题的方法。例如,重新启动计算机、重新启动服务器服务、更换有故障的硬件部件或其他。

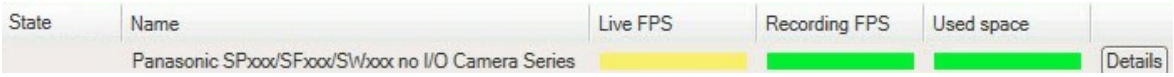
查看硬件的历史状态并打印报告

使用**系统监视器**功能,您可以轻松地了解系统监视器系统的状况总览。而且是在更长的时间段内。

是否有一段时间 CPU 使用率、带宽或其他硬件会面临挑战?使用系统监视器功能找到答案,并确定是否需要升级硬件或购买新硬件以避免将来出现这种情况。

请记住启用历史数据收集。请参阅 第 255 页上的收集硬件状态的历史数据。

1. 在**站点导航**窗格中，选择**系统仪表板 > 系统监视器**。
2. 在**系统监视器**窗口中，选择一个包含您要了解其历史状态的硬件的拼贴图，或者从窗口的下部选择一个服务器或摄像机。
3. 选择相关服务器或摄像机右侧的**详细信息**。



4. 对于服务器，请选择要调查的硬件右侧的**历史记录**。对于摄像机，请选择链接。
5. 如果要打印报告，请选择 PDF 图标。

您只能使用设备当前所在记录服务器的数据来创建历史报告。

如果您从服务器操作系统访问系统监视器的详细信息，可能会出现有关**InternetExplorer 增强安全配置**的消息。按照说明，将**系统监视器**页面添加至**受信任的站点区域**，然后继续操作。

收集硬件状态的历史数据

您可以启用系统硬件上的历史数据收集功能，以查看一段时间内硬件状态的图表并打印报告。有关详细信息，请参阅 第 254 页上的查看硬件的历史状态并打印报告。

1. 在**站点导航**窗格中，选择**系统仪表板 > 系统监视器**。
2. 在**系统监视器**窗口中，选择**自定义**。
3. 在打开的**自定义仪表板**窗口中，选择**收集历史数据**。
4. 选择一个采样时间间隔。间隔越短，SQL Server 数据库、带宽或其他硬件上的负载就越大。历史数据的采样时间间隔还决定了图形的详细程度。

在系统监视器仪表板上添加新摄像机或服务器拼贴图

如果要在物理位置之后以较小的组监视摄像机或服务器，或者要监视具有不同监视参数的某些硬件，则可以在**系统监视器**窗口中添加其他拼贴图。

1. 在**站点导航**窗格中，选择**系统仪表板 > 系统监视器**。
2. 在**系统监视器**窗口中，选择**自定义**。
3. 在打开的**自定义仪表板**窗口中，在**服务器拼贴图**或**摄像机拼贴图**下选择**新建**。

4. 在**新服务器拼贴图/新摄像机拼贴图**窗口中，选择要监视的摄像机或服务器。
5. 在**监视参数**下，选中或清除对应于要在拼贴图中添加或删除的任何参数的复选框。
6. 选择**确定**。新的服务器或摄像机拼贴图现已添加到仪表板上所显示的拼贴图。

在系统监视器仪表板上编辑摄像机或服务器拼贴图

如果要使用其他监视参数监视摄像机或服务器，则可以对其进行调整。

1. 在**站点导航**窗格中，选择**系统仪表板 > 系统监视器**。
2. 在**系统监视器**窗口中，选择**自定义**。
3. 在打开的**自定义仪表板**窗口中，在**"服务器"拼贴图**或**"摄像机"拼贴图**下选择要更改的拼贴图，然后选择**编辑**。
4. 在**编辑仪表板服务器/摄像机"拼贴图**窗口中，选择所有摄像机或服务器、摄像机或服务器组或单个摄像机或服务器以更改其监视参数。
5. 在**监视参数**下，选择要监视的监视参数。
6. 选择**确定**。

在系统监视器仪表板上删除摄像机或服务器拼贴图

如果不再需要监视拼贴图代表的硬件，则可以删除拼贴图。

1. 在**站点导航**窗格中，选择**系统仪表板 > 系统监视器**。
2. 在**系统监视器**窗口中，选择**自定义**。
3. 在打开的**自定义仪表板**窗口中，在**"服务器"拼贴图**或**"摄像机"拼贴图**下选择要更改的拼贴图。
4. 选择**删除**。

编辑何时应更改硬件状态的阈值

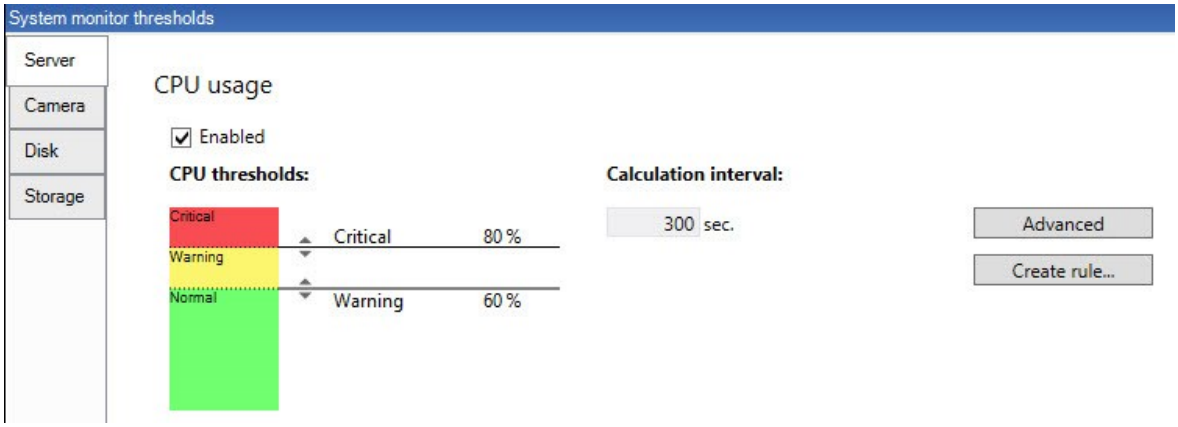
您可以在**系统监视器仪表板**上的硬件在三种状态之间切换时编辑阈值。有关详细信息，请参阅 第 254 页上的系统监视器阈值(已解释)。

您可以修改不同类型硬件的阈值。有关详细信息，请参阅 第 473 页上的系统监视器阈值("系统仪表板"节点)。

默认情况下，系统设置为显示相同硬件类型所有单元的阈值，例如，所有摄像机或服务器。您可以更改这些默认阈值。

您还可以为单个服务器或摄像机或其中的一个子集设置阈值，以允许例如某些摄像机使用比其他摄像机更高的**实时 FPS**或**记录 FPS**。

1. 在**站点导航**窗格中，选择**系统仪表板 > 系统监视器阈值**。
2. 如果尚未启用相关硬件，请选中**已启用**复选框。下图显示了一个示例。



3. 向上或向下拖动阈值控制滑块以增大或减小阈值。有两个滑块(分隔**正常**、**警告**和**关键**状态)可用于阈值控制中显示的每个硬件。
4. 输入计算间隔的值或保留默认值。
5. 如果要在各个硬件上设置值，请选择**高级**。
6. 如果要为特定事件或特定时间间隔指定规则，请选择**创建规则**。
7. 设置阈值级别和计算间隔后，从菜单中选择**文件 > 保存**。

查看系统中的证据锁定

系统仪表板节点下的**证据锁定**会显示当前监控系统上所有受保护数据的总览。

通过筛选查找证据锁定，例如，谁创建了它或何时创建了它。

1. 在**站点导航**窗格中，选择**系统仪表板 > 证据锁定**。
2. 获取总览并找到相关证据。您可以筛选与证据锁定相关的不同元数据并对其进行排序。

证据锁定窗口中显示的所有信息均为快照。按 F5 刷新。

使用系统配置打印报告

在安装和配置视频管理软件系统时，您会做出许多选择，并且可能需要记录这些内容。随着时间的推移，您也很难记住自安装和初始配置以来或刚过去的几个月中更改过的所有设置。这就是为什么可以打印包含您的所有配置选项的报告。

创建配置报告(PDF 格式)时，可以将系统的任何可能的元素添加到报告中。例如，您可以包括许可证、设备配置、警报配置等。您可以选择**排除敏感数据**选项来创建符合 GDPR 的报告(默认情况下启用)。您还可以自定义字体、页面设置和首页。

1. 展开**系统仪表板**并选择**配置报告**。
2. 选择要在报告中包括或排除的元素。
3. **可选**:如果选择了包括首页,请选择**首页**以自定义首页上的信息。在出现的窗口中,填写所需信息。
4. 选择**格式化**以自定义字体、页面大小和页边距。在打开的窗口中选择所需设置。
5. **做好导出的准备后**,选择导出并选择报告的名称和保存位置。

只有在 VMS 系统中具有管理员权限的用户才能创建配置报告。

元数据

显示或隐藏元数据搜索类别和搜索筛选器

具有管理员权限的 XProtect Management Client 用户可以在 Milestone 中显示或隐藏默认的 XProtect Smart Client 元数据搜索类别和搜索筛选器。默认情况下会隐藏这些搜索类别和搜索筛选器。如果您的视频监控系统符合要求,则显示它们会很有用(请参阅 第 479 页上的元数据搜索要求)。

此设置会影响所有 XProtect Smart Client 用户。

此设置不会影响以下对象的可见性:

- 其他,元数据 Milestone 搜索类别和搜索筛选器,例如**移动**、**书签**、**警报**和**事件**
- 第三方搜索类别和搜索筛选器

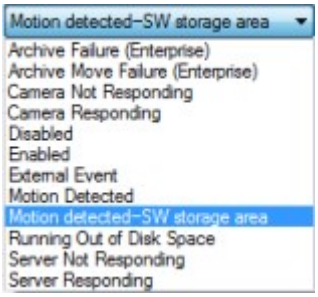
1. 在 XProtect Management Client 的**站点导航**窗格中,选择**元数据使用** > **元数据搜索**。
2. 在**元数据搜索**窗格中,选择要为其更改可见性设置的搜索类别。
3. 要启用搜索类别或搜索筛选器的可见性,请选中相应的复选框。要禁用搜索类别或搜索筛选器的可见性,请取消选中该复选框。

警报

添加警报

要定义警报,您需要创建警报定义,可在其中指定各种信息,例如触发警报的因素、关于操作员所需操作的说明以及警报停止的内容或时间。有关设置的详细信息,请参阅警报定义(警报节点)。

1. 在**站点导航**窗格中，展开**警报**，右键单击**警报定义**。
2. 选择**新增**。
3. 填写以下属性：
   - **名称**：输入警报定义的名称。每当列出警报定义时，将显示警报定义的名称。
   - **说明**：您可为接收警报的操作员编写说明。
   - **触发事件**：使用下拉菜单选择在触发警报时要使用的事件类型及事件消息。

     可供选择的触发事件的列表。将使用分析事件创建和自定义突出显示的触发事件。
   - **来源**：选择应生成事件以触发警报的摄像机或其他设备。选项取决于所选择的事件类型。
   - **时间配置文件**：如果您希望在特定时间间隔内激活警报，请选择该单选按钮，然后在下拉菜单中选择时间配置文件。
   - **事件基于**：如果您希望警报定义由事件激活，则选择该单选按钮，然后指定可激活警报定义的事件。您还必须指定停用警报定义的事件。
4. 在**时间限制**下拉菜单中，指定操作员需要执行操作的时间限制。
5. 在**触发的事件**下拉菜单中，指定要在超出时间限制时触发的事件。
6. 指定其他设置，例如，相关摄像机和初始警报所有者。

修改单个警报定义的权限

如果仅希望特定用户查看和管理警报，可以从XProtectManagementClient修改警报定义的权限。这样，您可以确保：

- 用户只接收与其相关的警报。
- 未经授权的用户无法对警报做出反应。

使用角色对用户进行分组，这些用户对所有警报定义拥有相同的权限。

若要修改警报定义的权限：

1. 在**站点导航**窗格中，展开**安全性**，选择要为其修改权限的角色。
2. 转到**警报**选项卡，展开**警报定义**，查看您定义的警报列表。
3. 选择警报定义以修改权限。

启用加密

从管理服务器启用加密或将加密应用到管理服务器

当您具有以下类型的远程服务器时，可以加密管理服务器和关联的 Data Collector 服务器之间的双向连接：

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

如果您的系统包含多个记录服务器或远程服务器，则必须在所有这些服务器上启用加密。

为服务器组配置加密时，必须使用属于同一 CA 证书的证书启用该加密，或者如果加密被禁用，则必须在该服务器组中的所有计算机上将其禁用。

先决条件：

- 托管管理服务器的计算机上信任服务器身份验证证书

首先，在管理服务器上启用加密。

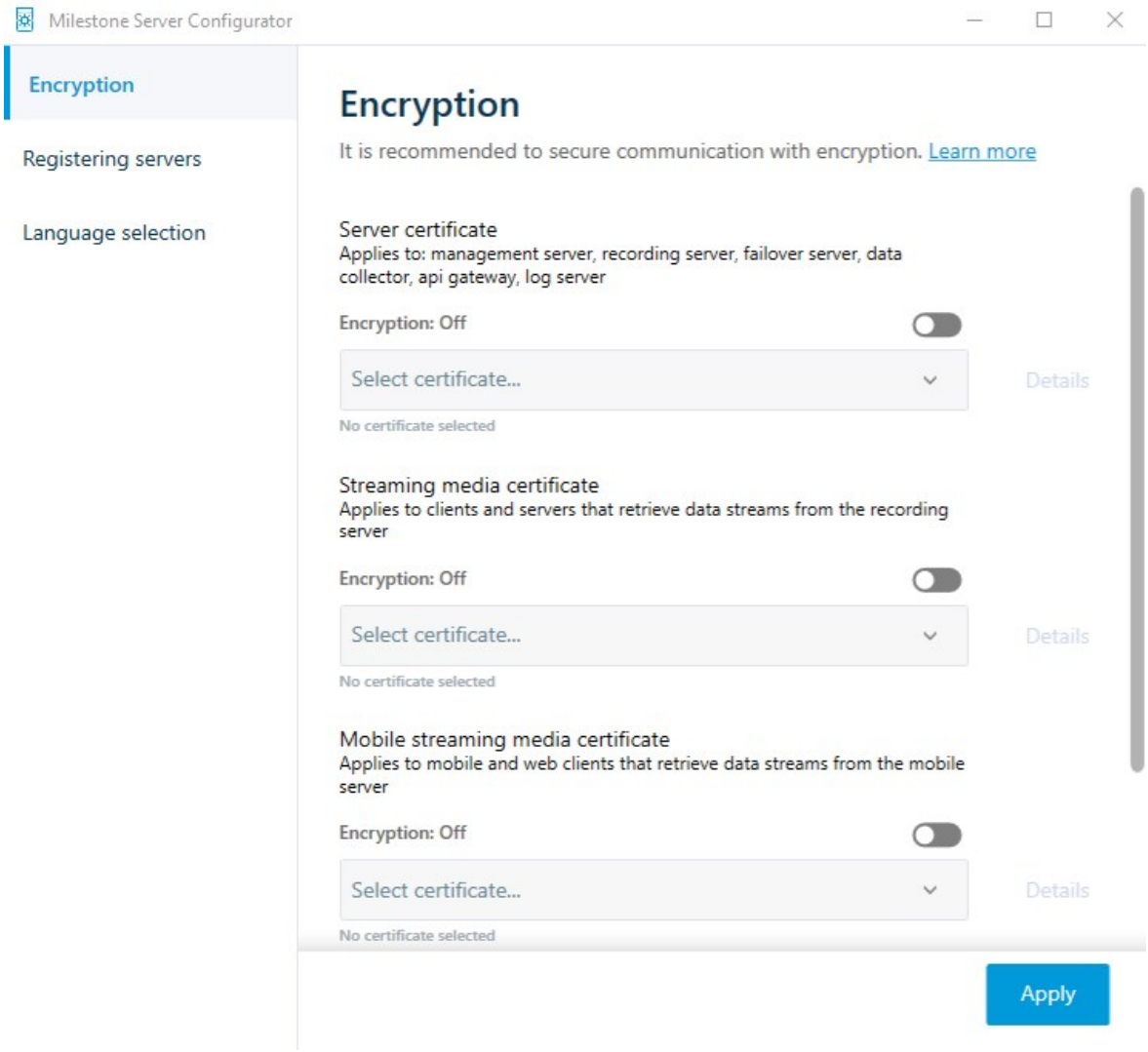
步骤：

1. 在安装了管理服务器的计算机上，从以下位置打开 **Server Configurator**：
   - Windows“开始”菜单

   或

   - Management Server Manager，通过右键单击计算机任务栏上的 Management Server Manager 图标
2. 在 **Server Configurator** 的**服务器证书**下，打开**加密**。
3. 单击**选择证书**以打开一个列表，其中包含具有私钥的 Windows 证书存储中本地计算机上安装的证书的唯一主题名称。
4. 选择一个证书以加密记录服务器、管理服务器、故障转移服务器和Data Collector server之间的通信。

选择**详细信息**以查看有关所选证书的 Windows 证书存储信息。



5. 单击**应用**。

要完成启用加密，下一步是更新每个录制服务器和每个使用 Data Collector(Event Server、Log Server、LPR Server、和 Mobile Server) 的服务器上的加密设置。

有关详细信息，请参阅 第 261 页上的为记录服务器或远程服务器启用服务器加密。

为记录服务器或远程服务器启用服务器加密

您可以加密管理服务器与录制服务器或其他使用 Data Collector 的远程服务器之间的双向连接。

如果您的系统包含多个记录服务器或远程服务器，则必须在所有这些服务器上启用加密。

有关详细信息，请参阅有关如何保护 XProtect VMS 安装的证书指南。

为服务器组配置加密时，必须使用属于同一 CA 证书的证书启用该加密，或者如果加密被禁用，则必须在该服务器组中的所有计算机上将其禁用。

先决条件：

- 您已在管理服务器上启用加密，请参阅第260页上的从管理服务器启用加密或将加密应用到管理服务器。

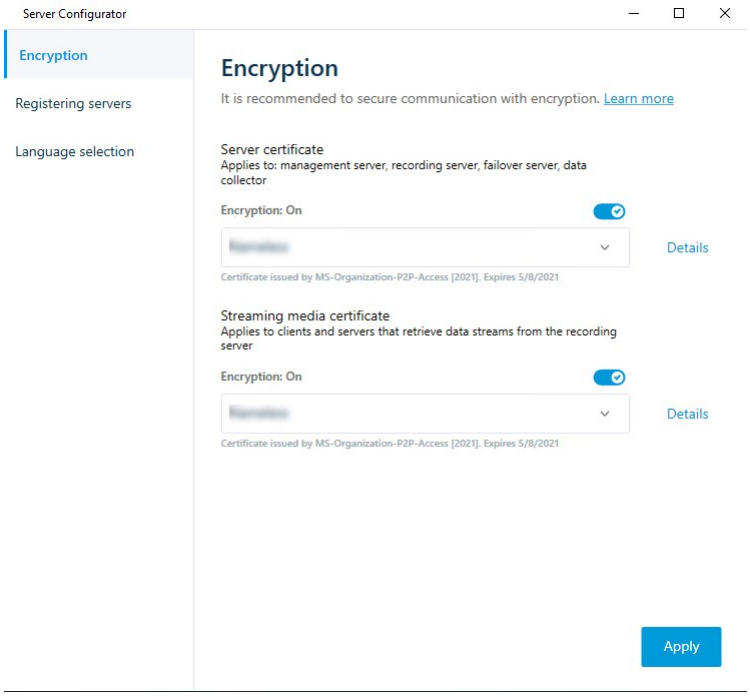
1. 在安装了Management Server 或 Recording Server的计算机上，从以下位置打开 **Server Configurator**：
   - Windows“开始”菜单

   或

   - 服务器管理器，通过右键单击计算机任务栏上的服务器管理器图标
2. 在 **Server Configurator** 的**服务器证书**下，打开**加密**。
3. 单击**选择证书**以打开一个列表，其中包含具有私钥的 Windows 证书存储中本地计算机上安装的证书的唯一主题名称。
4. 选择一个证书以加密记录服务器、管理服务器、故障转移服务器和数据收集器服务器之间的通信。

   选择**详细信息**以查看有关所选证书的 Windows 证书存储信息。

   已经授予 Recording Server 服务用户访问私钥的权限。要求在所有客户端上都信任此证书。



5. 单击**应用**。

应用证书时，记录服务器将停止并重新启动。停止 Recording Server 服务意味着当您验证或更改记录服务器的基本配置时，不能记录和查看实时视频。

启用事件服务器加密

您可以对事件服务器和与事件服务器 通信的组件之间的双向连接进行加密，包括 LPR Server。

为服务器组配置加密时，必须使用属于同一 CA 证书的证书启用该加密，或者如果加密被禁用，则必须在该服务器组中的所有计算机上将其禁用。

先决条件：

- 托管事件服务器的计算机上信任的服务器身份验证证书

首先，在事件服务器上启用加密。

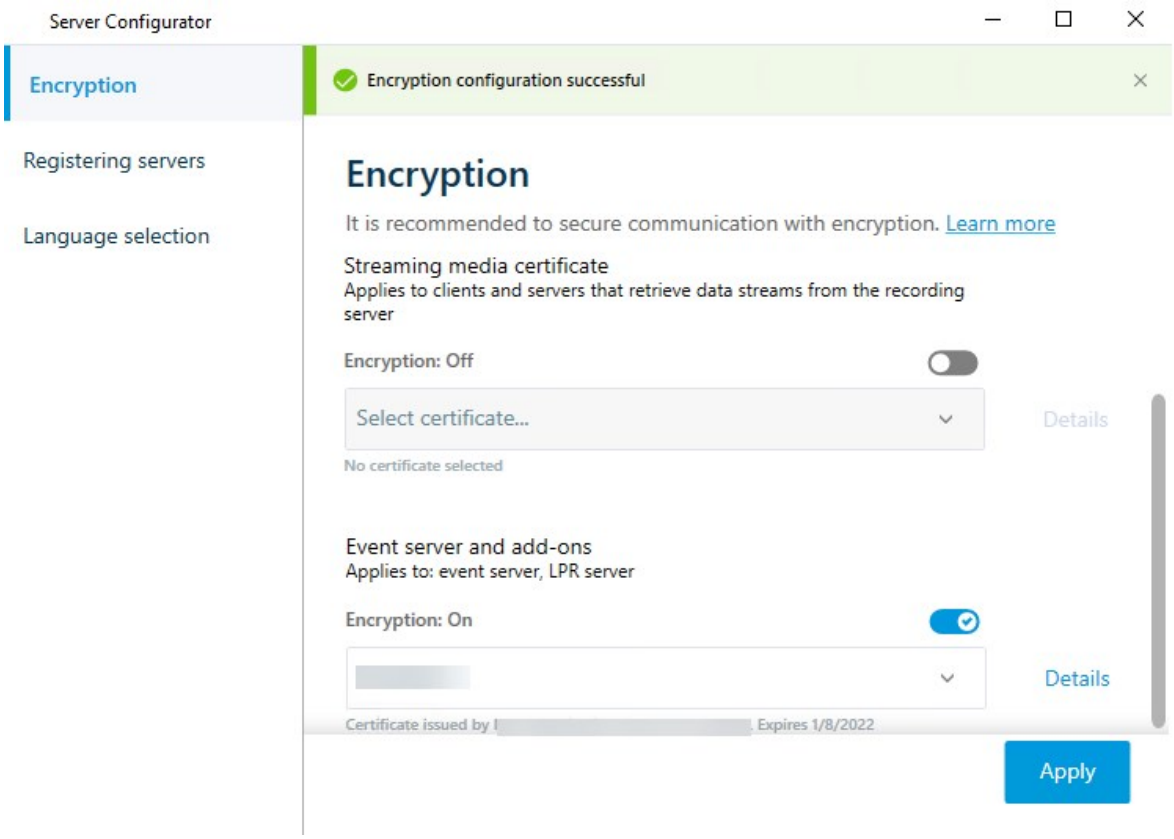
步骤：

1. 在安装了事件服务器的计算机上，从以下位置打开 **Server Configurator**：
   - Windows“开始”菜单

   或

   - Event Server，通过右键单击计算机任务栏上的 Event Server 图标
2. 在 **Server Configurator** 中，**事件服务器和附加产品**下，打开**加密**。
3. 单击**选择证书**以打开一个列表，其中包含具有私钥的 Windows 证书存储中本地计算机上安装的证书的唯一主题名称。
4. 选择证书对事件服务器和相关附加产品之间的通信进行加密。

选择**详细信息**以查看有关所选证书的 Windows 证书存储信息。



5. 单击**应用**。

若要完成启用加密，下一步是更新每个相关扩展上的加密设置。LPR Server

对客户端和服务器启用加密

您可以加密从记录服务器到从记录服务器流式传输数据的客户端和服务器的连接。

> 为服务器组配置加密时，必须使用属于同一 CA 证书的证书启用该加密，或者如果加密被禁用，则必须在该服务器组中的所有计算机上将其禁用。

先决条件：

- 在运行从记录服务器检索数据流的服务的所有计算机上，信任要使用的服务器身份验证证书
- XProtect Smart Client 和所有服务（从记录服务器检索数据流）必须是 2019 R1 或更高版本
- 使用 2019 R1 之前的 MIP SDK 版本创建的某些第三方解决方案可能需要更新

步骤：

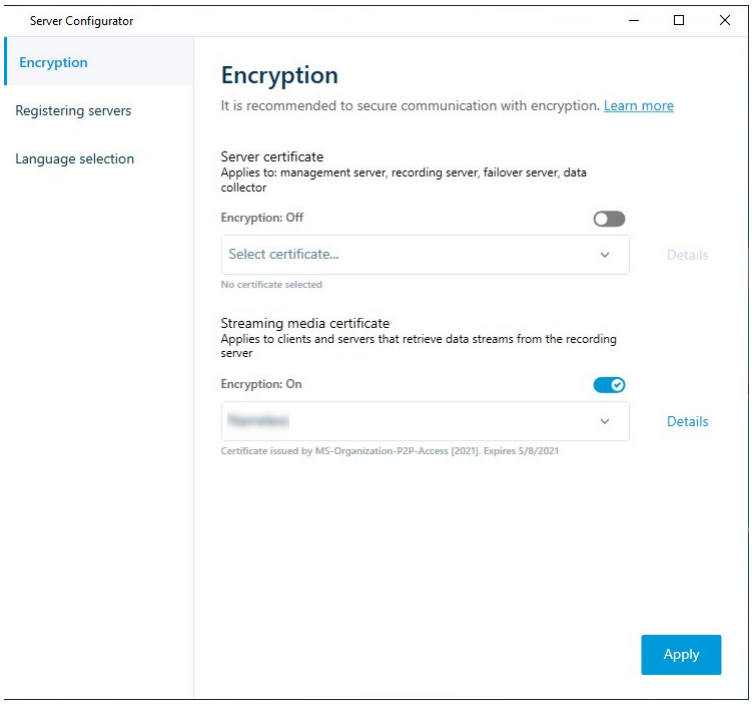
1. 在安装了记录服务器的计算机上，从以下位置打开 **Server Configurator**：
   - Windows“开始”菜单

   或

   - Recording Server Manager，通过右键单击计算机任务栏上的 Recording Server Manager 图标
2. 在 **Server Configurator** 的**流媒体证书**下，打开**加密**。
3. 单击**选择证书**以打开一个列表，其中包含具有私钥的 Windows 证书存储中本地计算机上安装的证书的唯一主题名称。
4. 选择一个证书以加密从记录服务器检索数据流的客户端和服务器之间的通信。

   选择**详细信息**以查看有关所选证书的 Windows 证书存储信息。

   已经授予 Recording Server 服务用户访问私钥的权限。要求在所有客户端上都信任此证书。



5. 单击**应用**。

> 应用证书时，记录服务器将停止并重新启动。停止 Recording Server 服务意味着当您验证或更改记录服务器的基本配置时，不能记录和查看实时视频。

要验证记录服务器是否使用加密，请参阅查看客户端的加密状态。

在移动设备服务器上启用加密

要使用 HTTPS 协议在移动设备服务器与客户端和服务之间建立安全连接，必须在服务器上应用有效证书。该证书会确认证书持有人获得建立连接的授权。

有关详细信息，请参阅有关如何保护 XProtect VMS 安装的证书指南。

为服务器组配置加密时，必须使用属于同一 CA 证书的证书启用该加密，或者如果加密被禁用，则必须在该服务器组中的所有计算机上将其禁用。

由 CA(证书颁发机构)核发的证书包含一系列证书，该系列的根源是 CA 根证书。当设备或浏览器看发现此证书时，会将其根证书与操作系统(Android、iOS、Windows 等)上预先安装的证书进行比较。若该根证书列在预先安装的根证书列表中，操作系统会确保连接至服务器的用户足够安全。这些证书的核发会针对某域名，而且并不免费。

步骤：

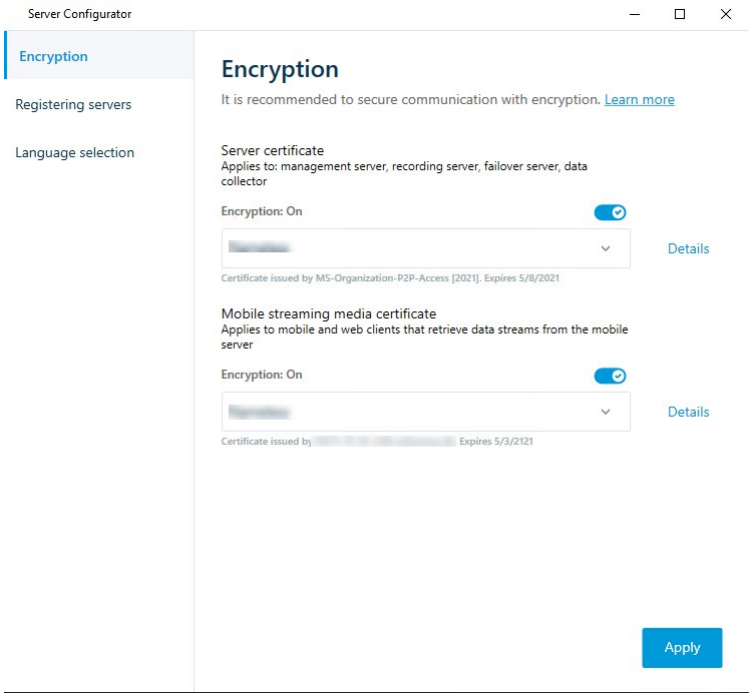
1. 在安装了移动设备服务器的计算机上，从以下位置打开 **Server Configurator**：
   - Windows“开始”菜单

   或

   - Mobile Server Manager，通过右键单击计算机任务栏上的 Mobile Server Manager 图标
2. 在 **Server Configurator** 的**移动流媒体证书**下，打开**加密**。
3. 单击**选择证书**以打开一个列表，其中包含具有私钥的 Windows 证书存储中本地计算机上安装的证书的唯一主题名称。
4. 选择一个证书以加密XProtect Mobile客户端XProtect Web Client与移动设备服务器的通信。

   选择**详细信息**以查看有关所选证书的 Windows 证书存储信息。

已经授予 Mobile Server 服务用户访问私钥的权限。要求在所有客户端上都信任此证书。



5. 单击**应用**。

应用证书时，Mobile Server 服务将重新启动。

Milestone Federated Architecture

设置系统以运行联合站点

要使系统做好针对 Milestone Federated Architecture 的准备，在安装管理服务器时必须进行特定选择。根据 IT 基础结构的设置方式，在三个不同的备选方式中进行选择。

备选方式 1：连接来自同一个域的站点（使用普通域用户）

安装管理服务器之前，必须创建共同域用户，并将此用户配置为联合站点分层中涉及的所有服务器上的管理员。如何连接站点取决于创建的用户帐户。

使用 Windows 用户帐户

1. 在要用作管理服务器的服务器上开始安装产品，并选择**自定义**。
2. 选择使用用户帐户来安装 Management Server 服务。所选用户帐户必须是在所有管理服务器上使用的管

理员帐户。当在联合站点层级中安装其他管理服务器时，您必须使用相同的用户帐户。

3. 完成安装。重复步骤 1-3，以安装要添加到联合站点层级的任何其他系统。
4. 将站点添加至分层（请参阅 第 269 页上的将站点添加至层次结构）。

使用 Windows 内置用户帐户（网络服务）

1. 在要用作管理服务器的第一个服务器上开始安装产品，并选择**单台计算机**或**自定义**。将使用网络服务帐户安装管理服务器。对联合站点层级中的所有站点重复此步骤。
2. 登录到要作为联合站点层级的中心站点的站点。
3. 在 Management Client 中，展开**安全 > 角色 > 管理员**。
4. 在**用户和组**选项卡上，单击**添加**，然后选择 **Windows 用户**。
5. 在对话框中选择**计算机**作为对象类型，输入联合站点的服务器名称，然后单击**确定**将该服务器添加到中央站点的**管理员**角色。重复此步骤，直到以此方式添加所有联合站点，然后退出应用程序。
6. 登录到每个联合站点，按上述的相同方式将以下服务器添加到**管理员**角色：
   - 父站点服务器。
   - 要直接连接到此联合站点的子站点服务器。
7. 将站点添加至分层（请参阅 第 269 页上的将站点添加至层次结构）。

备选方式 2：从不同域连接站点

要跨域连接站点，请确保这些域彼此信任。您在 Microsoft Windows 域配置中设置域以使其相互信任。在联合站点分层中每个站点上的不同域之间建立信任并替换后，请遵循与备选方式 1 的相同说明。有关如何设置受信任域的详细信息，请访问 Microsoft 网站 (https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/)。

Milestone 建议将 Milestone Interconnect 用于在多个域中创建互相连接的多站点系统。

备选方式 3：连接工作组中的站点

连接工作组中的站点时，在联合站点层级中要连接的所有服务器上都必须存在相同的管理员帐户。在安装系统之前，您必须定义管理员帐户。

1. 使用共同管理员帐户登录 **Windows**。
2. 启动产品安装，并单击**自定义**。
3. 选择使用共同管理员帐户来安装 Management Server 服务。
4. 完成安装。重复步骤 1-4 安装要连接的任何其他系统。必须使用共同管理员帐户安装所有这些系统。
5. 将站点添加至分层（请参阅 第 269 页上的将站点添加至层次结构）。

当站点不是域的一部分时，Milestone 建议使用 Milestone Interconnect 来创建互相连接的多站点系统。

不能将域和工作组相混合。这意味着不能将来自域的站点连接至来自工作组的站点，反之亦然。

将站点添加至层次结构

当您展开系统时，只要系统设置正确，便可以向顶层站点及其子站点添加站点。

向 Milestone Federated Architecture 添加非安全站点时，请确保在Management Client中的**工具>选项>常规设置**下启用**允许非安全连接到服务器**。

1. 选择**联合站点层级**窗格。
2. 选择要添加子站点的目标站点，右键单击，然后单击**将站点添加至层次结构**。
3. 在将站点**添加至层次结构**窗口中输入所请求站点的 URL，然后单击**确定**。
4. 父站点将链接请求发送至子站点，之后会将这两个站点之间的链接添加至**联合站点层级**窗格。
5. 如果可以在不请求子站点管理员接受的情况下建立到子站点的链接，则跳到步骤 7。

   如果**不**可以，则子站点将具有等待接受 的图标，直到子站点管理员批准请求。
6. 确保子站点的管理员批准来自子站点的链接请求(请参阅 第 269 页上的接受包含在层次结构中)。
7. 即会建立新的父项/子项链接，并且**联合站点层级**窗格会更新为新子站点的 图标。

接受包含在层次结构中

子站点接收到来自管理员不具有子站点的管理员权限的潜在父站点的链接请求后，它具有正在等待接受图标。

要接受链接请求：

1. 登录站点。
2. 在**联合站点分层**窗格中，右键单击站点，然后单击**接受包含在层级中**。

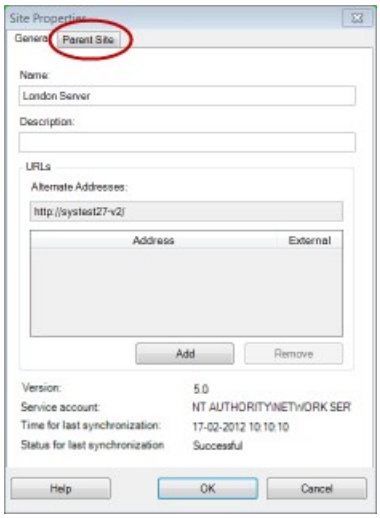
   如果站点运行 XProtect Expert 版本，请您在**站点导航**窗格中右键单击该站点。
3. 单击**是**。
4. 即会建立新的父项/子项链接，并且**联合站点层级**窗格会更新为所选子项的一般站点 图标。

对距父站点较远处的子站点进行的任何更改可能需要一定时间才能反映在**联合站点层级**窗格中。

设置站点属性

您可以查看主站点及其子站点的属性，并有可能可以进行编辑。

1. 在 Management Client 中的**联合站点分层**窗格中，选择相关站点，右键单击，然后选择**属性**。



2. 如果需要，更改以下内容：

   常规选项卡（请参阅 第 492 页上的“常规”选项卡）

   父站点选项卡（请参阅 第 493 页上的“父站点”选项卡）**（仅在子站点上可用）**

   由于同步问题，对远程子项进行的任何更改可能需要一定时间才能反映在**站点导航**窗格中。

刷新站点层次结构

系统通过父项/子项设置的所有级别定期自动同步层级。如果希望看到更改立即反映在层级中，并且不希望等待下一次自动同步，则可以手动刷新层级。

您需要登录站点才能执行手动刷新。刷新只会反映自上次同步以来由该站点保存的更改。这意味着如果更改未到达该站点，手动更新可能不会反映在层级中更下层所做的更改。

1. 登录相关站点。
2. 右键单击**联合站点层级**窗格中的顶层站点，然后单击**刷新站点层次结构**。

   这将需要几秒钟时间。

登录到层级中的其他站点

您可以登录到其他站点并对其进行管理。您登录到的站点是您的主站点。

1. 在**联合站点层级**窗格中，右键单击要登录的站点。
2. 单击**登录到站点**。

   该站点的 Management Client 将打开。
3. 输入登录信息并单击**确定**。
4. 登录完成后，即可对该站点执行管理任务。

更新子站点的站点信息

本节只适用于您使用 XProtect Corporate 或者 XProtect Expert 2014 或更新版本的情况。

在具有许多子站点的大型 Milestone Federated Architecture 设置中，很容易失去总览，并且可能很难找到每个子站点的管理员的联系信息。

因此，您可以将附加信息添加到每个子站点，然后该信息可供中央站点上的管理员使用。

将鼠标悬停在**联合站点分层**窗格中的站点名称上时，您可以阅读有关该站点的信息。更新有关该站点的信息：

1. 登录站点。
2. 单击**站点导航**窗格，然后选择**站点信息**。
3. 单击**编辑**，然后在每个类别中添加相关信息。

将站点从层次结构分离

从站点的父站点分离站点时，站点之间的链接会断开。您可以从中央站点分离站点，以及从站点本身或其父站点分离站点。

1. 在**联合站点层级**窗格中，右键单击站点，然后单击**将站点从层次结构分离**。
2. 单击**是**即会更新**联合站点层级**窗格。

   如果分离的站点具有子站点，它会成为层级中该分支的新顶层站点，并且常规站点图标 会更改为顶层站点 图标。
3. 单击**确定**。

在手动刷新或自动同步后会反映层级的更改。

Milestone Interconnect

向中央 Milestone Interconnect 站点添加远程站点

可使用**添加硬件**向导向中央站点添加远程站点。

要求

- 足够的 Milestone Interconnect 摄像机许可证(请参阅 第 80 页上的Milestone Interconnect 和授予许可)。
- 另一个配置和工作的 XProtect 系统包括用户帐户(基本用户、本地 Windows 用户或 Windows Active Directory 用户),其中包含中央 XProtect Corporate 系统应该能够访问的设备权限
- 中央 XProtect Corporate 站点和远程站点之间的网络连接,及对远程站点上所使用的端口的访问权限或端口转发功能

要添加远程站点:

1. 在中央站点上,展开**服务器**并选择**记录服务器**。
2. 在**总览**窗格中,展开相关的记录服务器,然后右键单击。
3. 选择**添加硬件**启动向导。
4. 在第一页上选择**地址范围扫描**或**手动**,然后单击**下一步**。
5. 指定用户名和密码。必须在远程系统上预定义用户帐户。可根据需要单击**添加**以添加用户名和密码。准备好以后,单击**下一步**。
6. 选择在扫描时使用的驱动程序。在这种情况下,在 Milestone 驱动器之间进行选择。单击**下一步**。
7. 指定要扫描的 IP 地址和端口号。默认端口为 80。点击**下一步**。

   当系统检测远程站点时,请稍候。状态指示器将显示检测过程的进度。如果检测成功,将在**状态**列中显示一条**成功**消息。如果未能添加,您可以单击**失败**错误消息以查看原因。
8. 选择启用或禁用成功检测到的系统。单击**下一步**。
9. 当系统检测硬件并收集特定于设备的信息时,请稍候。单击**下一步**。
10. 选择启用或禁用成功检测到的硬件和设备。单击**下一步**。
11. 选择默认组。单击**完成**。
12. 安装后,您可以在**总览**窗格中查看系统及其设备。

    根据远程站点上所选用户的用户权限,中央站点有权访问所有摄像机和功能或其中的一部分。

分配用户权限

通过创建角色并分配对功能的访问权限,您可以像配置其他摄像机一样为互连摄像机配置用户权限。

1. 在中央站点上的**站点导航**窗格中，展开**安全**，然后选择**角色**。
2. 在"总览"窗格中，右键单击内置管理员角色，然后选择**添加角色**(请参阅添加和管理角色)。
3. 在**设备**选项卡上命名角色并配置设置(参阅"设备"选项卡(角色))和**远程记录**选项卡(请参阅"远程记录"选项卡(角色))。

更新远程站点硬件

如果已在远程站点上更改配置(例如添加或删除摄像机和事件)，则必须更新中央站点上的配置，以反映远程站点上的新配置。

1. 在中央站点上，展开**服务器**并选择**记录服务器**。
2. 在**总览**窗格中，展开所需的记录服务器并选择相关的远程系统。右键单击硬件。
3. 选择**更新硬件**。这会打开**更新硬件**对话框。
4. 此对话框中列出了自 Milestone Interconnect 设置建立或最后一次刷新以来远程系统中的所有更改(移除、更新和添加设备)。单击**确认**可使用这些更改更新中央站点。

直接从远程站点摄像机启用播放

如果中央站点与其远程站点持续连接，则可对系统进行配置，以使用户直接从远程站点播放记录。有关详细信息，请参阅 第 80 页上的Milestone Interconnect 设置(已解释)。

1. 在中央站点上，展开**服务器**并选择**记录服务器**。
2. 在**总览**窗格中，展开所需的记录服务器并选择相关的远程系统。选择相关的互连摄像机。
3. 在"属性"窗格中，选择**记录**选项卡，然后选择**从远程系统播放记录**选项。
4. 在工具栏中，单击**保存**。

在 Milestone Interconnect 安装中，中央站点将忽略在远程站点上定义的隐私屏蔽。如果要应用相同的隐私遮蔽，您必须在中央站点上重新定义它。

从远程站点摄像机检索远程记录

如果中央站点**未**与其远程站点持续连接，则可将系统配置为集中存储远程记录，并且可以配置为在网络连接处于最优状态时检索远程记录。有关详细信息，请参阅 第 80 页上的Milestone Interconnect 设置(已解释)。

为了让用户实际检索记录，您必须为相关角色启用此权限(请参阅角色(安全))。

要配置系统：

1. 在中央站点上，展开**服务器**并选择**记录服务器**。
2. 在**总览**窗格中，展开所需的记录服务器并选择相关的远程系统。选择相关的远程服务器。
3. 在"属性"窗格中，选择**远程检索**选项卡并更新设置(请参阅 第 369 页上的远程检索选项卡)。

如果网络由于某种原因发生故障，中央站点将丢失记录片段。可以将系统配置为在重新建立网络后立即允许中央站点自动检索远程记录以涵盖关闭期间。

1. 在中央站点上，展开**服务器**并选择**记录服务器**。
2. 在**总览**窗格中，展开所需的记录服务器并选择相关的远程系统。选择相关摄像机。
3. 在**属性**窗格中，选择**记录**选项卡，然后选择连接恢复时自动检索远程记录选项(请参阅检索远程记录)。
4. 在工具栏中，单击**保存**。

也可使用规则或在需要时从 XProtect Smart Client 启动远程记录检索。

在 Milestone Interconnect 安装中，中央站点将忽略在远程站点上定义的隐私屏蔽。如果要应用相同的隐私遮蔽，您必须在中央站点上重新定义它。

配置中央站点以响应来自远程站点的事件

您可以使用远程站点上定义的事件来触发中央站点上的规则和警报，从而即时响应来自远程站点的事件。这要求远程站点已连接并已联机。事件的数量和类型取决于在远程系统中配置和预定义的事件。

Milestone 网站 (https://www.milestonesys.com/) 上提供了受支持事件列表。

无法删除预定义的事件。

要求：

- 如果要使用来自远程站点的用户定义/手动事件作为触发事件，必须先在远程站点上创建这些事件
- 请确保您拥有远程站点的事件更新列表(请参阅 第 273 页上的更新远程站点硬件)。

从远程站点添加用户定义/手动事件：

1. 在中央站点上，展开**服务器**并选择**记录服务器**。
2. 在“总览”窗格中，选择相关远程服务器和**事件选项卡**。
3. 此列表包含预定义的事件。单击**添加**以在列表中包括来自远程站点的用户定义或手动事件。

使用远程站点上的事件触发中央站点上的警报：

1. 在中央站点上，展开**警报**并选择**警报定义**。
2. 在“总览”窗格中，右键单击**警报定义**，然后单击**新增**。
3. 根据需要输入值。
4. 在**触发事件**字段中，可在支持的预定义和用户定义事件之间进行选择。
5. 在**来源**字段中，选择用于代表您要从中生成警报的远程站点的远程服务器。
6. 完成后保存配置。

使用远程站点上的事件在中央站点上触发基于规则的动作：

1. 在中央站点上，展开**规则和事件**，并选择**规则**。
2. 在“总览”窗格中，右键单击**规则**，然后单击**添加规则**。
3. 在显示的向导中，选择**对 <事件>执行操作** 。
4. 在**编辑规则说明**区域中，单击**事件**，并在支持的预定义和用户定义事件之间进行选择。单击**确定**。
5. 单击**设备/记录服务器/管理服务器**，并选择用于代表您需要中央站点为其启动动作的远程站点的远程服务器。单击**确定**。
6. 单击**下一步**，进入下一个向导页。
7. 选择您要为该规则应用的条件。如果不选择任何条件，将始终应用规则。单击**下一步**。
8. 选择动作，并在**编辑规则说明**区域中指定详细信息。单击**下一步**。
9. 如果需要，选择停止条件。单击**下一步**。
10. 如果需要，选择停止动作。单击**完成**。

远程连接服务

远程连接服务(已解释)

> 可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

远程连接服务功能包含 Axis Communications 开发的 Axis One-Click 摄像机连接技术。它使系统能够从外部摄像机检索视频(和音频)，其中防火墙和/或路由器网络配置通常会阻止启动与此类摄像机的连接。实际通信通过安全通道服务器(ST 服务器)进行。ST 服务器使用 VPN。只有持有有效密钥的设备才能在 VPN 中工作。这提供了一个安全通道，公共网络可以在这里以安全的方式交换数据。

远程连接服务使您能够

- 在 Axis Dispatch Service 中编辑凭据
- 添加、编辑和删除 ST 服务器
- 注册/注销和编辑 Axis One-Click 摄像机
- 转到与 Axis One-Click 摄像机相关的硬件

为一键式摄像机连接安装安全通道服务器环境

在使用 Axis One-Click 摄像机连接之前，必须先安装合适的 ST 服务器环境。要使用安全通道服务器(ST 服务器)环境和 Axis One-click 摄像机，必须先与系统提供商联系，以获取 Axis Dispatch Services 所需的用户名和密码。

要求

- 请与您的系统提供商联系，以获取 Axis Dispatch Services 所需的用户名和密码
- 确保您的摄像机支持 Axis 视频托管系统。访问 Axis 网站查看支持的设备 (https://www.axis.com/products/axis-guardian)
- 如果需要，请使用最新固件更新 Axis 摄像机。访问 Axis 网站下载固件 (https://www.axis.com/support/firmware)

1. 在每个摄像机的主页上，进入**基本设置**和 **TCP/IP**，然后选择**启用 AVHS** 和**始终**。
2. 从管理服务器，进入 Milestone 下载页面 (https://www.milestonesys.com/downloads/) 并下载 **AXIS One-Click** 软件。运行该程序以设置合适的 Axis 安全通道框架。

添加或编辑安全通道服务器

远程连接服务的通信通过安全通道服务器(ST 服务器)进行。

1. 进行以下操作之一：
   - 要添加ST服务器，请右键单击**Axis安全通道服务器**顶层节点，然后选择**添加Axis安全通道服务器**
   - 要添加 ST 服务器，请右键单击它，然后选择**编辑 Axis 安全通道服务器**
2. 在打开的窗口中，填写相关信息。
3. 如果在安装 **Axis One-Click Connection 组件**时选择使用凭据，请选中**使用凭据**复选框，并填写与 **Axis One-Click Connection 组件**相同的用户名和密码。
4. 单击**确定**。

注册新的 Axis One-Click 摄像机

1. 要在 ST 服务器下注册摄像机，请右键单击它并选择**注册 Axis One-Click 摄像机**。
2. 在打开的窗口中，填写相关信息。
3. 单击**确定**。
4. 摄像机现在出现在相关的 ST 服务器下。

摄像机可以有以下颜色编码：

颜色	说明
红色	初始状态。已注册但未连接至 ST 服务器。
黄色	已注册。已连接至 ST 服务器，但未添加为硬件。
绿色	添加为硬件。可能有也可能没有连接至 ST 服务器。

添加新摄像机时，其状态始终为绿色。连接状态由**总览**窗格中的**录制服务器**上的**设备**反映出来。在**总览**窗格中，可将摄像机分组以便更加轻松地总览摄像机。如果您选择此时**不**在 Axis 分派服务上注册摄像机，则可以稍后从右键单击菜单(选择**编辑 Axis One-Click 摄像机**)执行此操作。

智能地图

地理背景(已解释)

XProtect Smart Client 用户必须先在 XProtect Management Client 中配置地理背景，然后才能选择地理背景。

- **基本世界地图**-使用XProtectSmartClient提供的标准地理背景。它无需任何配置。此地图主要用作一般参考，不包含国家边界、城市或其他详细信息之类的功能。但是，与其他地理背景类似，它也包含地理参考数据
- **Bing Maps** - 连接到 Bing Maps
- **Google Maps** - 连接到 Google Maps
- **Milestone Map Service** - 连接到免费的地图提供商。启用 Milestone Map Service 后，无需进一步设置。

  请参阅启用 Milestone Map Service

- **OpenStreetMap** - 连接到：
  - 您自己选择的商业性拼贴图服务器
  - 您自己的在线或本地拼贴图服务器

  请参阅指定 OpenStreetMap 拼贴图服务器

BingMaps和GoogleMaps选项需要访问互联网，而且您必须从Microsoft或Google购买密钥。

Milestone Map Service 需要访问互联网。

除非使用自己的本地拼贴图服务器，否则 OpenStreetMap 需要访问互联网。

如果您希望系统具有符合 EU GDPR 的安装，则可能不使用以下服务：

- Bing Maps
- Google Maps
- Milestone Map Service

有关数据保护和使用数据收集的更多信息，请参阅 GDPR 隐私指南。

默认情况下，Bing Maps 和 Google Maps 会显示卫星图像(卫星)。您可以更改 XProtect Smart Client 中的图像(例如，更改为航空或地形)以查看不同的细节。

在以下对象中启用 Bing Maps 或 Google Maps：Management Client

可以通过在 Smart Client 输入 Management Client 配置文件的密钥，使其供多个用户使用。分配给配置文件的所有用户都将使用此密钥。

步骤：

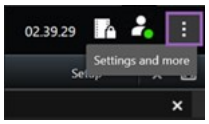
1. 在 Management Client 的**站点导航**窗格中，单击 **Smart Client 配置文件**。
2. 在 **Smart Client** 配置文件窗格中，选择相关的 Smart Client 配置文件。
3. 在**属性**窗格中，单击**智能地图**选项卡：
   - 对于 Bing Maps，在 **Bing Maps 密钥**字段中输入基本密钥或企业密钥
   - 对于 Google Maps，在 **Google Maps 的私钥**字段中输入地图静态 API 密钥
4. 为防止 XProtect Smart Client 操作员使用不同的密钥，请选中**已锁定**复选框。

在以下对象中启用 Bing Maps 或 Google Maps：XProtect Smart Client

要允许 XProtect Smart Client 操作员使用与 Smart Client 配置文件中的密钥不同的密钥，必须在 XProtect Smart Client 的设置中输入密钥：

步骤：

1. 在 XProtect Smart Client 中，打开**设置**窗口。



2. 单击**智能地图**。
3. 根据要使用的地图服务，执行下列操作之一：
   - 对于 Bing Maps，请在 **Bing Maps 密钥**字段中输入密钥。另请参阅 第 77 页上的将智能地图与 Bing Maps 集成(已作说明)。
   - 对于 Google Maps，请在**用于 Google Maps 的私钥**字段中输入密钥。另请参阅 第 76 页上的将智能地图与 Google Maps 集成(已作说明)。

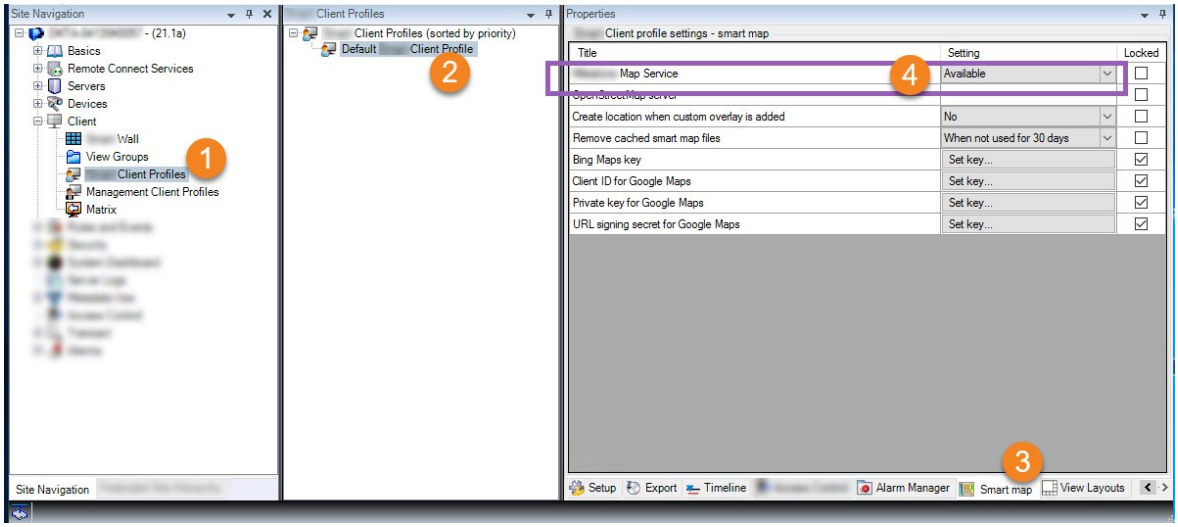
启用 Milestone Map Service

Milestone Map Service 是一项在线服务，可让您连接到 Milestone Systems 的拼贴图服务器。该拼贴图服务器使用免费的商用地图服务。

在智能地图上启用 Milestone Map Service 后，智能地图会将 Milestone Map Service 用作其地理背景。

步骤：

1. 在**站点导航**窗格中，展开**客户端**节点并单击 **Smart Client 配置文件**。
2. 在总览窗格中，选择相关 Smart Client 配置文件。
3. 在**属性**窗格中，单击**智能地图**选项卡。



4. 在 **Milestone Map Service** 字段中，选择**可用**。
5. 要在 XProtect Smart Client 中实施此设置，请选中**锁定**复选框。然后XProtect Smart Client操作员无法启用或禁用 Milestone Map Service。
6. 保存更改。

您也可以在 Milestone Map Service 中的**设置**窗口中启用 XProtect Smart Client。

Milestone Map Service 需要访问互联网。

若您位于限制性防火墙之后，则允许访问所使用的域会很重要。您可能需要在运行 Milestone Map Service 的每台机器上使用 maps.milestonesys.com，以允许 Smart Client 的流出流量。

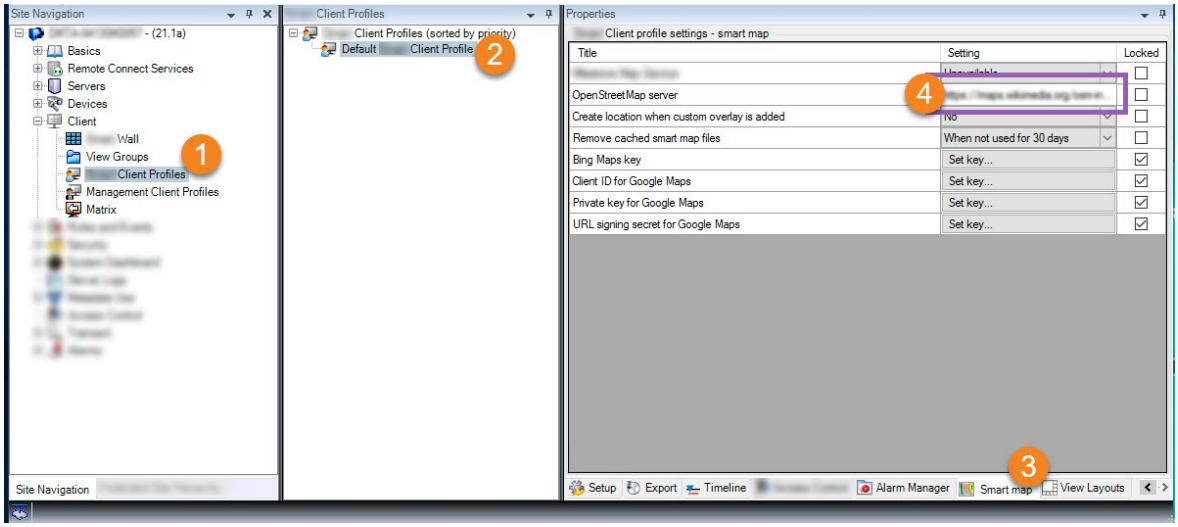
指定 OpenStreetMap 拼贴图服务器

如果您使用 **OpenStreetMap** 选项作为智能地图的地理背景，则必须指定检索拼贴图的位置。您可以通过指定拼贴图服务器地址来执行此操作，可以使用商业性拼贴图服务器或本地拼贴图服务器。例如，如果您的组织有自己的区域(如机场或港口)地图。

也可以在 XProtect Smart Client 的**设置**窗口中设置拼贴图服务器地址。

步骤：

1. 在**站点导航**窗格中，展开**客户端**节点并单击 **Smart Client 配置文件**。
2. 在总览窗格中，选择相关 Smart Client 配置文件。
3. 在**属性**窗格中，单击**智能地图**选项卡。



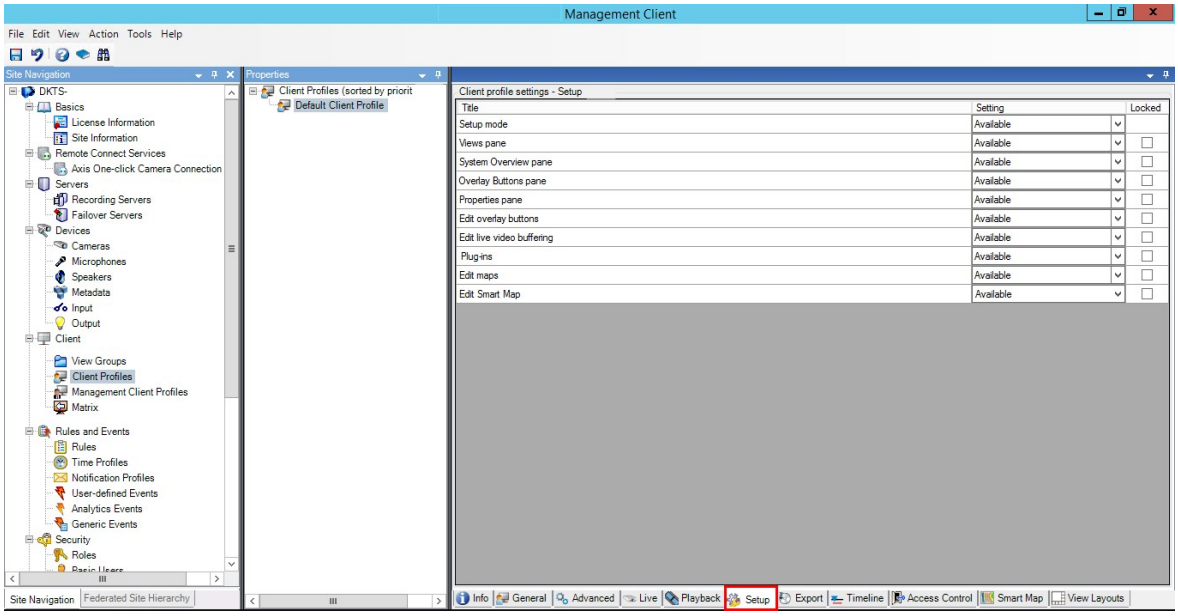
4. 在 **OpenStreetMap 服务器**字段中，输入拼贴图服务器地址。
5. 要在 XProtect Smart Client 中实施此设置，请选中**锁定**复选框。这样，XProtect Smart Client 操作员将无法更改地址。
6. 保存更改。

启用 智能地图 编辑

仅当在 XProtect Smart Client 中启用编辑时，操作员才能在设置模式下，在 Management Client 中编辑智能地图。如果尚未启用，则需要为每个相关的 Smart Client 配置文件启用编辑。

步骤：

1. 在**站点导航**窗格中，展开**客户端**节点。
2. 单击 **Smart Client 配置文件**。



3. 在总览窗格中，选择相关 Smart Client 配置文件。
4. 在**属性**面板中，单击**设置**选项卡。
5. 在**编辑智能地图**列表中，选择**可用**。
6. 为每个相关 Smart Client 配置文件重复以上步骤。
7. 保存更改。下次将用户分配给所选的SmartClient配置文件时，登录至XProtectSmartClient即可编辑智能地图。

要禁用编辑，请在**编辑智能地图**列表中选择**不可用**。

在智能地图上启用编辑设备

您必须启用每个角色的设备编辑，以允许操作员执行以下操作：

- 在智能地图上放置输入设备或麦克风
- 在智能地图上调整摄像机的视野

可以允许操作员在智能地图上编辑以下设备类型：

- 摄像机
- 输入设备
- 麦克风

要求

在开始前，请确保已启用智能地图编辑(请参阅 第 280 页上的启用 智能地图 编辑)。您在与操作员角色关联的 Smart Client 配置文件上执行此操作。

步骤：

1. 展开**安全**节点 > **角色**。
2. 在**角色**窗格中，选择与操作员关联的角色。
3. 要提供角色编辑权限，请执行以下操作：
   - 选择**整体安全**选项卡，然后在**角色设置**窗格中选择设备类型(例如**摄像机**或**输入**)
   - 在**允许**列，选中**完全控制**或**编辑**复选框
4. 保存更改。

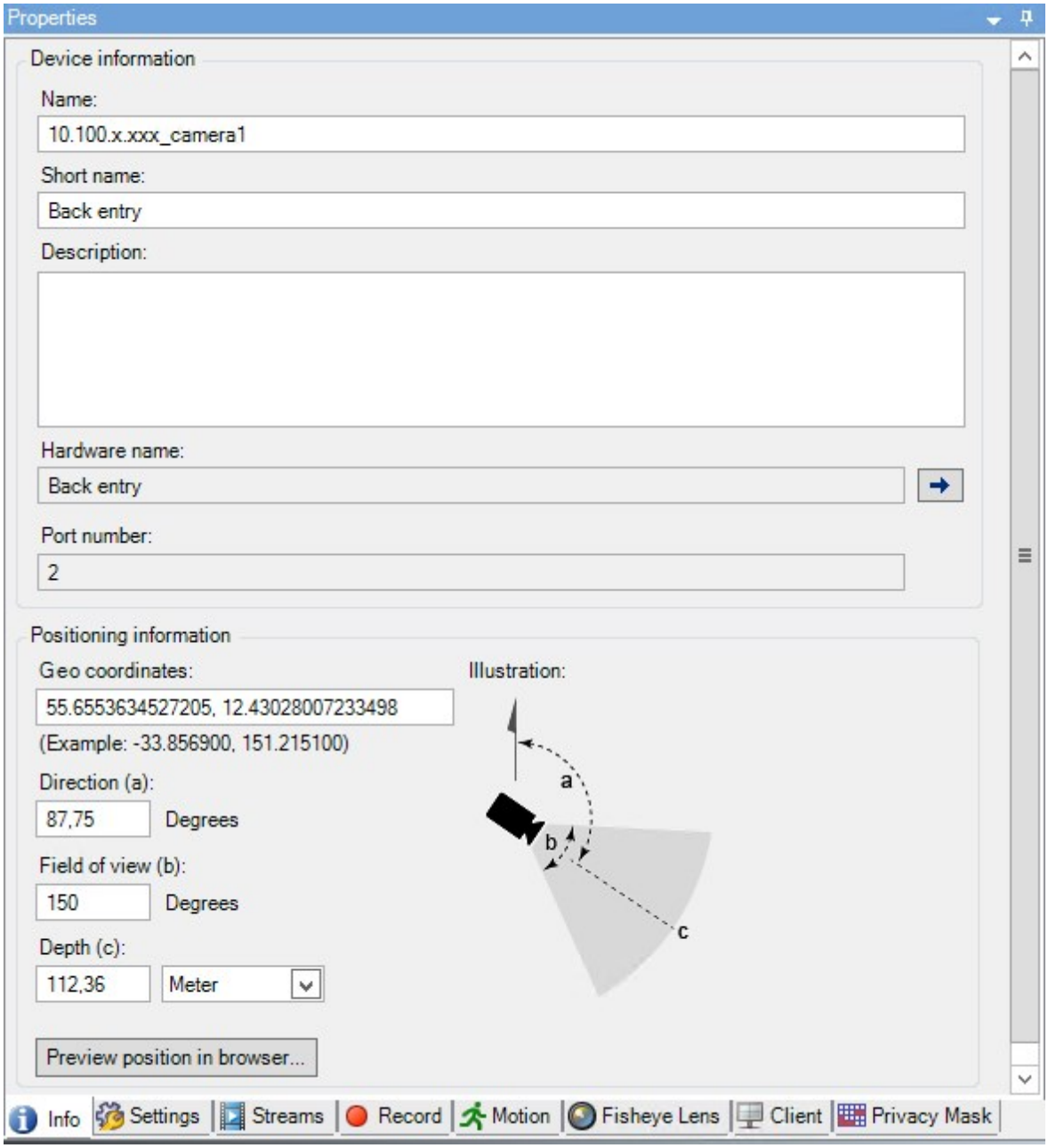
要为单个设备启用编辑功能，请转至**设备**选项卡，然后选择相关设备。

定义设备位置和摄像机方向、视野、深度(智能地图)

为确保摄像机处于智能地图上的正确位置，您可以设置设备的地理坐标。对于摄像机，您还可以设置方向、视野和视野深度。进行上述任何设置后，下一次操作员在 XProtect Smart Client 中加载智能地图时，都会自动将设备添加到智能地图中。

步骤：

1. 在 Management Client 中，展开**设备**节点，然后选择设备类型（例如，**摄像机**或**输入**）。
2. 在**设备**窗格中，选择相关设备。
3. 在**信息**选项卡中，向下滚动到**位置信息**。



4. 在**地理坐标**字段中，按顺序指定纬度和经度坐标。使用句点作为小数点分隔符，并使用逗号分隔纬度和经度。

- 对于摄像机：
    1. 在**方向**字段，输入 0 至 360 度范围内的值。
    2. 在**视野**字段，输入 0 至 360 度范围内的值。
    3. 在**深度**字段，输入视野深度(以米或英尺为单位)。

5. 保存更改。

您也可以在记录服务器上设置属性。

使用 Milestone Federated Architecture 配置智能地图

当您使用 Milestone Federated Architecture 中的智能地图时，所有来自互联站点的设备都出现在智能地图上。请按照以下步骤在联合体系结构中设置智能地图。

有关 Milestone Federated Architecture 的详细信息，请参阅 第 81 页上的正在配置 Milestone Federated Architecture。

1. 在将顶层站点与子站点连接之前，请确保已在各个站点的所有设备上指定了地理坐标。当在 XProtect Smart Client 中在智能地图上定位设备时，地理坐标会自动添加，但是您也可以在设备属性的 Management Client 中手动添加。有关详细信息，请参阅 第 282 页上的定义设备位置和摄像机方向、视野、深度(智能地图)。
2. 您必须将 Smart Client 操作员作为 Windows 用户添加在父站点和所有联合点上。至少在顶层站点上，Windows 用户必须具有智能地图编辑权限。这使用户能够为顶层站点和所有子站点编辑智能地图。接下来，您需要确定子站点上的 Windows 用户是否需要智能地图编辑权限。在 Management Client 中，首先您在**角色**下创建 Windows 用户，然后您启用智能地图编辑。有关详细信息，请参阅 第 280 页上的启用 智能地图 编辑。
3. 在顶层站点上，您必须将子站点作为 Windows 用户添加到具有管理员权限的角色中。当您指定对象类型时，选择**计算机**复选框。
4. 在每个子站点上，您必须将顶层站点作为 Windows 用户添加到顶层站点上使用的相同管理员角色。当您指定对象类型时，选择**计算机**复选框。
5. 在顶层站点上，确保您能看到**联合站点分层**窗口。在 Management Client 中，前往**视图**，然后选择**联合站点分层**。将每个子站点添加到顶层站点。有关详细信息，请参阅 第 269 页上的将站点添加至层次结构。
6. 现在您可以测试MilestoneFederatedArchitecture是否在XProtectSmartClient中有效。以管理员或操作员的身份登录顶层站点，并打开包含智能地图的视图。如果设置正确，那么来自顶层站点和各个子站点的所有设备都会出现在智能地图上。如果登录至其中一个子站点，您将只看到来自该站点及其子站点的设备。

若要在智能地图上编辑设备，例如摄像机的位置和角度，则用户需要设备编辑权限。有关详细信息，请参阅 第 281 页上的在智能地图上启用编辑设备。

维护

备份和还原系统配置

Milestone建议您定期对系统配置进行备份，作为一项灾难恢复措施。

尽管配置丢失很少发生，但在某些令人遗憾的情况下仍会出现。通过技术或组织措施保护备份非常重要。

关于备份和还原系统配置(已解释)

Management Client 系统提供了内置功能，用于备份可在中定义的所有系统配置。日志服务器数据库和日志文件(包括审核日志文件)不包含在该备份中。

如果系统较大，Milestone 建议定义计划备份。使用第三方工具完成：Microsoft® SQL Server Management Studio。该备份包含与手动备份相同的数据。

备份期间，系统会保持联机状态。

备份系统配置可能需要一定时间。备份时间取决于：

- 您的系统配置
- 您的硬件
- 您是否在一台服务器或多台服务器上安装了 SQL Server、Event Server 和 Management Server 组件

每次进行手动或计划备份时，SQL Server 数据库的交易日志文件都会刷新。有关如何刷新交易日志文件的其他信息，请参阅 第 115 页上的SQL Server 数据库交易日志(已解释)。

> 创建备份时，请确保您知道系统配置密码设置。

> 对于符合 FIPS 140-2 的系统，如果使用不符合 FIPS 的密码对 2017 R1 之前版本的 XProtect VMS 导出和存档媒体数据库进行了加密，则需要将数据存档在启用 FIPS 之后仍可访问的位置。有关如何配置 XProtect VMS 以在符合 FIPS 140-2 的模式下运行的详细信息，请参阅强化指南中的FIPS 140-2 合规部分。

选择共享备份文件夹

在备份和还原任何系统配置之前，必须为该目的建立备份文件夹。

1. 右键单击通知区域的 Management Server 服务图标，然后选择**选择共享备份文件夹**。
2. 在出现的窗口中，浏览至所需文件位置。
3. **单击**确定两次。

4. 如果询问是否要删除当前备份文件夹中的文件，根据需求单击**是**或**否**。

手动备份系统配置

1. 从菜单栏中选择**文件 > 备份配置**。
2. 阅读对话框中的注释，然后单击**备份**。
3. 输入 .cnf 文件的文件名。
4. 输入文件夹目标，然后单击**保存**。
5. **等待直到备份完成**，然后单击关闭。

所有相关的系统配置文件都会组合为保存在特定位置的一个.cnf文件。备份期间，所有备份文件都会首先导出至管理服务器上的临时系统备份文件夹。您可以通过右键单击通知区域的ManagementServer服务图标，然后选择“选择共享备份文件夹”来选择其他临时文件夹。

从手动备份中恢复系统配置

重要信息

- 进行安装的用户和进行还原的用户都必须是管理服务器**和** SQL Server 上的系统配置 SQL Server 数据库的本地管理员
- 在还原期间，除了记录服务器外，您的系统会完全关闭，这需要一些时间
- 备份只能在创建该备份的系统安装上还原。确保设置与制作备份时的设置尽可能相似。否则，还原可能失败
- 如果在还原过程中提示您输入系统配置密码，您必须提供在创建备份时有效的系统配置密码。没有此密码，您将无法从备份中恢复配置
- 如果您生成 SQL Server 数据库的备份并在干净的 SQL Server 上还原它，则从 SQL Server 数据库中引发的错误将不工作，并且您将只会从 SQL Server 收到一条常规错误消息。为避免这种情况，请首先使用干净的 XProtect 重新安装您的 SQL Server 系统，然后在此基础上还原备份
- 如果在验证阶段还原失败，您可以再次启动旧配置，因为您未作任何更改
  如果在流程其他地方还原失败，您无法回滚到旧配置
  只要备份文件未损坏，您就可以执行其他还原
- 还原会替换当前配置。这意味着自上次备份起的所有配置更改都会丢失
- 不会还原任何日志，包括审核日志
- 还原一旦启动便无法取消

还原

1. 右键单击通知区域的 Management Server 服务图标，然后选择**还原配置**。
2. 阅读重要注释，然后单击**还原**。
3. 在打开文件对话框中，浏览至系统配置备份文件的位置，选择该文件，然后单击**打开**。

   备份文件位于 Management Client 计算机上。如果 Management Client 安装在不同服务器上，则在选择目标之前，将备份文件复制到该服务器。

4. **还原配置**窗口即会打开。等待还原完成，然后单击**关闭**。

系统配置密码(已解释)

选择通过分配系统配置密码来对整体系统配置进行保护。分配系统配置密码后，备份将受此密码保护。密码设置存储在运行管理服务器的计算机上的一个安全文件夹中。您将需要此密码来：

- 从使用与当前密码设置不同的密码设置创建的配置备份中还原配置
- 由于硬件故障(恢复)在另一台计算机上移动或安装管理服务器
- 在具有集群的系统中配置其他管理服务器

可以在安装过程中或安装后分配系统配置密码。密码必须符合 Windows 密码策略定义的 Windows 复杂性要求。

系统管理员必须保存此密码并确保其安全，这一点非常重要。如果为您分配了系统配置密码，并且正在还原备份，则可能会要求您提供系统配置密码。没有此密码，您将无法从备份中恢复配置。

系统配置密码设置

可以更改系统配置密码设置。在系统配置密码设置中，您有以下选项：

- 选择通过分配系统配置密码来对系统配置进行密码保护
- 更改系统配置密码
- 选择删除系统配置密码，不对系统配置进行密码保护

更改系统配置密码设置

更改密码时，系统管理员必须保存与不同备份关联的密码，并确保密码的安全。如果要还原备份，可能会要求您提供在创建备份时有效的系统配置密码。没有此密码，您将无法从备份中恢复配置。

更改密码后，如果您的管理服务器和事件服务器安装在不同的计算机上，则还必须在事件服务器上输入当前的系统配置密码。有关详细信息，请参阅输入当前系统配置密码(事件服务器)。

要应用更改，必须重启管理服务器服务。

1. 找到管理服务器托盘图标，并确保该服务正在运行。
2. 右键单击通知区域的 Management Server 服务图标，然后选择**更改系统配置密码设置**。
3. 随即出现“更改系统配置密码设置”窗口。

分配密码

1. 在**新密码**字段中输入新密码。
2. 在**确认**字段中输入新密码，然后选择 **Enter**。
3. 阅读通知，然后单击**是**接受更改。
4. 等待更改确认，然后选择**关闭**。
5. 要应用更改，必须重启管理服务器服务。
6. 重启后，确保管理服务器正在运行。

删除密码保护

如果不需要密码保护，您可以选择退出：

1. 选中复选框：**我选择不使用系统配置密码，并且了解系统配置不会被加密**，然后单击 **Enter**。
2. 阅读通知，然后单击**是**接受更改。
3. 等待更改确认，然后选择**关闭**。
4. 要应用更改，必须重启管理服务器服务。
5. 重启后，确保管理服务器正在运行。

输入系统配置密码设置(恢复)

如果由于硬件故障或其他原因删除了保存密码设置的文件,您将需要提供系统配置密码设置才能访问保存系统配置的数据库。在新计算机上安装期间,将要求您输入系统配置密码设置。

但是,如果保存密码设置的文件已删除或损坏,并且运行管理服务器的计算机没有其他问题,则可以选择输入系统配置密码设置:

1. 找到管理服务器托盘图标。
2. 右键单击通知区域的 Management Server 服务图标,然后选择**输入系统配置密码**。
3. 随即出现"输入系统配置密码设置"窗口。

系统配置采用密码保护

1. 在**密码**字段中输入密码,然后选择 **Enter**。
2. 等待密码被接受。选择**关闭**。
3. 确保管理服务器正在运行。

系统配置不采用密码保护

1. 选中复选框:**该系统不使用系统配置密码**,选择**Enter**。
2. 等待设置被接受。选择**关闭**。
3. 确保管理服务器正在运行。

手动备份系统配置(已解释)

如果要对包含系统配置的管理服务器的数据库执行手动备份,请确保系统保持联机状态。管理服务器的数据库默认名称是 **Surveillance**。

启动备份之前要考虑这些事项:

- 不能使用 SQL Server 数据库的备份将系统配置复制到其他系统
- 备份 SQL Server 数据库可能需要一些时间。它取决于系统配置、硬件,以及 SQL Server、管理服务器和 Management Client 是否安装在相同计算机上
- 由于日志(包括审核日志)存储在日志服务器的数据库中,因此它们**不是**管理服务器的数据库备份的一部分。日志服务器的数据库默认名称是 **SurveillanceLogServerV2**。您以相同的方式备份这两个 SQL Server 数据库。

备份和还原事件服务器配置(已解释)

备份和还原系统配置时,事件服务器配置的内容会包含在内。

首次运行事件服务器时，会自动将其全部配置文件移动到 SQL Server 数据库。可以将还原后的配置应用到事件服务器，而无需重新启动事件服务器，并且在加载配置还原时事件服务器能够启动和停止所有外部通信。

系统配置的计划备份和还原(已解释)

管理服务器会在 SQL Server 数据库中存储系统配置。Milestone 建议您定期对此数据库进行计划备份，作为一项灾难恢复措施。尽管系统配置丢失很少发生，但在某些令人遗憾的情况下仍会出现。幸运的是，它只需要一分钟，而且备份还有一个额外的好处，那就是刷新 SQL Server 数据库的事务日志。

如果具有小型安装，并且不需要计划备份，则可以手动备份系统配置。有关说明，请参阅 第 290 页上的手动备份系统配置(已解释)。

在备份/还原管理服务器时，确保将具有系统配置的 SQL Server 数据库包含在备份/还原中。

使用计划备份和还原的要求

Microsoft® SQL Server Management Studio，该工具可从其网站 (https://www.microsoft.com/downloads/) 免费下载。

除了管理 SQL Server 及其数据库以外，该工具还包括一些简单易用的备份和还原功能。在管理服务器上下载和安装该工具。

通过计划备份来备份系统配置

1. 从 Windows 的“开始”菜单，启动 Microsoft® SQL Server Management Studio。
2. 在连接时，指定所需 SQL Server 的名称。使用用于创建 SQL Server 数据库的帐户。
    1. 找到包含整个系统配置(包括事件服务器、记录服务器、摄像机、输入、输出、用户、规则、巡视配置文件等)的 SQL Server 数据库。此 SQL 数据库的默认名称是 **Surveillance**。
    2. 制作 SQL Server 数据库的备份，并确保：
        - 验证所选 SQL Server 数据库为正确的数据库
        - 验证备份类型为**全部**
        - 设置重复备份的计划。您可以在 Microsoft 网站 (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017) 上阅读有关计划备份和自动备份的详细信息
        - 验证建议的路径是否合乎需求或选择其他路径
        - 选择**完成后验证备份**和**写入媒体前检查校验和**
3. 遵循工具中的说明操作到最后步骤。

还考虑使用相同方法备份日志服务器的数据库(包含日志)。日志服务器的 SQL Server 数据库默认名称为 **SurveillanceLogServerV2**。

从计划备份恢复系统配置

要求

要避免在还原系统配置数据库时对系统配置进行更改，请停止：

- Management Server 服务（请参阅 第 303 页上的管理服务器服务）
- Event Server 服务（可从 Windows **服务**（在您的计算机上搜索 **services.msc**。在**服务**中，定位 **Milestone XProtect Event Server**）完成）
- 万维网发布服务，也称为 Internet 信息服务 (IIS)。了解关于如何停止 IIS (https://technet.microsoft.com/library/cc732317(WS.10).aspx/) 的信息

从 Windows 的**开始**菜单打开 Microsoft® SQL Server Management Studio。

在该工具中执行以下操作：

1. 在连接时，指定 SQL Server 的名称。使用用于创建 SQL Server 数据库的用户帐户。
2. 找到包含整个系统配置（包括事件服务器、记录服务器、摄像机、输入、输出、用户、规则、巡视配置文件等）的 SQL Server 数据库（默认名称为 **Surveillance**）。
3. 制作 SQL Server 数据库的还原，并确保：
   - 选择从**设备备份**
   - 选择备份媒体类型**文件**
   - 找到并选择备份文件 (**.bak**)
   - 选择**改写现有数据库**
4. 遵循工具中的说明操作到最后步骤。

使用相同的方法还原日志服务器的 SQL Server 数据库（包含日志）。日志服务器的 SQL Server 数据库默认名称为 **SurveillanceLogServerV2**。

> 当 Management Server 服务停止时，系统也不工作。记住在完成数据库还原后要立即再次启动所有服务，这一点很重要。

备份日志服务器的数据库

使用处理系统配置的相同方法（如上文所述）处理日志服务器的数据库。日志服务器的数据库包含您的所有系统日志，其中包括记录服务器和摄像机报告的错误。日志服务器的数据库默认名称是 **SurveillanceLogServerV2**。

SQL Server数据库位于日志服务器的 SQL Server 上。通常，日志服务器和管理服务器在相同的 SQL Server 上都具有其 SQL Server 数据库。由于日志服务器数据库不包含任何系统配置，因此对其进行备份并非至关重要，但是您可能会意识到在管理服务器备份/还原之前访问其中的系统日志的好处。

备份和还原失败与问题情境(已解释)

- 如果在上次系统配置备份后,移动了eventserver或其他已注册服务(如logserver),则必须为新系统选择需要哪个已注册服务配置。可以决定在将系统还原至旧版本后保持新配置。通过查看服务的主机名进行决定。
- 如果由于 event server 未位于指定目标(例如,选择旧的已注册服务安装时)而导致系统配置的还原失败,则进行其他还原。
- 如果要还原配置备份并输入了错误的系统配置密码,则必须提供在创建备份时有效的系统配置密码。

移动管理服务器

管理服务器会在 SQL Server 数据库中存储系统配置。如果将管理服务器从一个物理服务器移动到另一个物理服务器,则务必确保新管理服务器也能访问该 SQL Server 数据库。系统配置可通过下列两种不同的方式存储:

- **网络 SQL Server**:如果将系统配置存储在网络上 SQL Server 的 SQL Server 数据库中,则在新的管理服务器上安装管理服务器软件时,可以指向 SQL Server 上该数据库的位置。在这种情况下,只有以下关于管理服务器主机名和 IP 地址的段落适用,您应该忽略本主题的其余部分:

  管理服务器主机名 和 IP 地址:当您将管理服务器从一台物理服务器移动到另一台物理服务器时,目前最简单的方法是为新服务器分配与旧服务器相同的主机名和 IP 地址。这是因为录制服务器会自动连接到旧管理服务器的主机名和 IP 地址。如果为新的管理服务器提供新的主机名和/或 IP 地址,则录制服务器无法找到管理服务器,您必须手动停止系统中的每项 Recording Server 服务,更改其管理服务器 URL,再次注册录制服务器,并在完成后,启动 Recording Server 服务。
- **本地 SQL Server**:如果在管理服务器上 SQL Server 的 SQL Server 数据库中存储您的系统配置,则需要在移动之前备份现有管理服务器的系统配置数据库。通过备份 SQL Server 数据库,随后将其还原到新管理服务器上的 SQL Server,您可以避免在移动后重新配置摄像机、规则、时间配置文件等

> 如果移动管理服务器,则需要当前的系统配置密码才能还原备份,请参阅 第 288 页上的系统配置密码(已解释)。

要求

- **用于在新管理服务器上进行安装的软件安装文件**
- 您在购买系统和最初安装系统时收到的**软件许可证文件 (.lic)**。不应使用在手动脱机激活许可证后收到的已激活的软件许可证文件。已激活的软件许可证文件中包含有关安装系统的特定服务器的信息。因此,在移动到新服务器时,无法重复使用已激活的软件许可证文件

如果您还要升级与该移动相关的系统软件,您应已收到新的软件许可证文件。只需使用该文件即可。

- **Microsoft® SQL Server Management Studio**
- 在管理服务器不可用时会出现什么情况? 第 294 页上的不可用的管理服务器(已解释))
- 复制日志服务器数据库(请参阅 第 292 页上的备份日志服务器的数据库)

不可用的管理服务器(已解释)

- **录制服务器仍可录制**:当前正在工作的任何录制服务器都会从管理服务器接收到其配置的副本,从而可以在管理服务器关闭时自行使用和存储记录。因此,计划的录制和移动触发的录制都会工作,事件触发的录制也会工作(除非它们所基于的、与管理服务器或其他任何录制服务器相关的事件进入管理服务器)
- **录制服务器将暂时在本地存储日志数据**:在录制服务器重新变为可用时,它们会自动将日志数据发送到管理服务器:
  - **客户端无法登录**:客户端访问权通过管理服务器授权。没有管理服务器,客户端便无法登录
  - **已登录的客户端可以在最长四小时内保持登录状态**:在客户端登录后,它们已通过管理客户端授权,可以与录制服务器在最长四小时内进行通信。如果可以在四小时内使新管理服务器上线并运行,大多数用户都不会受到影响
  - **无法配置系统**:如果没有管理服务器,便无法更改系统配置

Milestone 建议您将在管理服务器中断时可能丢失与监控系统的联系这一风险通知给用户。

移动系统配置

移动系统配置包含三个步骤:

1. 制作系统配置备份。这与进行计划备份相同。另请参阅 第 291 页上的通过计划备份来备份系统配置。
2. 在新服务器上安装新管理服务器。请参阅计划备份,步骤 2。
3. 将系统配置还原到新系统。另请参阅 第 292 页上的从计划备份恢复系统配置。

更换记录服务器

如果记录服务器出现故障,并且您希望使用继承旧记录服务器设置的新服务器进行更换:

1. 从旧的记录服务器检索记录服务器 ID:
   1. 选择**记录服务器**,然后在**总览**窗格中选择旧记录服务器。
   2. 选择**存储**选项卡。
   3. 在按住键盘上 CTRL 键的同时选择**信息**选项卡。
   4. 复制**信息**选项卡靠下部分中的记录服务器 ID 编号。不要复制文字 *ID*,而是仅复制编号本身。

2. 替换新记录服务器上的记录服务器 ID:

1. 停止旧记录服务器上的 Recording Server 服务，然后在 Windows 的**服务**中将服务的**启动类型**设置为**已禁用**。

   > 不同时启动两台具有相同 ID 的记录服务器很重要。

2. 在新的记录服务器上，打开资源管理器并转至 `C:\ProgramData\Milestone\XProtect Recording Server` 或您的记录服务器所在的路径。
3. 打开文件 `RecorderConfig.xml`。
4. 删除在标签 *<id>* 和 *</id>* 之间声明的 ID。

5. 在 *<id>* 和 *</id>* 标签之间粘贴复制的记录服务器 ID。保存 *RecorderConfig.xml* 文件。
6. 转到注册表：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`.
7. 打开 **RecorderIDOnMachine** 并使用新 ID 更改旧记录服务器 ID。

3. 在管理服务器上注册新的记录服务器。为此，请用右键单击 Recording Server Manager 托盘图标，然后单击**注册**。有关详细信息，请参阅 第 168 页上的注册记录服务器。
4. 重启 Recording Server 服务。在新的 Recording Server 服务启动时，它会继承旧记录服务器的所有设置。

移动硬件

可以在属于同一个站点的记录服务器之间移动硬件。移动后，硬件及其设备将在新记录服务器上运行，并且新记录将存储在该服务器上。此移动对于客户端用户是透明的。

旧记录服务器上的记录将保存，直到：

- 系统在保留时间到期时删除它们。已由某用户使用证据锁定（请参阅 第 65 页上的证据锁定（已解释））保护的记录不会被删除，除非证据锁定的保留时间到期。在创建证据锁定时，需为它们定义保留时间。保留时间可能永远不会到期
- 您可在**录制**选项卡上从每个设备的新记录服务器中删除它们

如果尝试删除仍包含记录的记录服务器，您会收到警告。

> 如果将硬件移动到当前尚未向其添加硬件的记录服务器，客户端用户必须注销并登录才能从设备接收数据。

您可以使用硬件移动功能执行以下操作：

- **负载平衡**:例如,如果记录服务器上的磁盘过载,您可以添加新记录服务器并移动一些硬件
- **升级**:例如,如果必须将用于托管记录服务器的服务器更换为更新的型号,您可以安装新记录服务器,并将硬件从旧服务器移动到新服务器
- **更换损坏的记录服务器**:例如,如果服务器处于脱机状态并且将永远不再联机,则您可以将硬件移动到其他记录服务器,从而使系统保持运行。您将无法访问旧记录。有关详细信息,请参阅 第 294 页上的更换记录服务器。

远程记录

当将硬件移动到另一个记录服务器时,系统会从摄像机上的互连站点或边缘存储取消正在进行或计划进行的检索。记录不会删除,但数据不会如预期那样被检索和保存在数据库中。在这种情况下,您会收到警告。对于在您启动硬件移动时已开始执行检索的 XProtect Smart Client 用户,检索会失败。XProtect Smart Client 用户将得到通知,并且可稍后重试。

如果他人已在远程站点上移动硬件,则您必须使用**更新硬件**选项手动同步中央站点,以反映远程站点的新配置。如果不同步,移动的摄像机会保持与中央站点断开连接。

移动硬件(向导)

要将硬件从一个记录服务器移动到另一个记录服务器,请运行**移动硬件**向导。该向导将引导您执行必要步骤以完成一个或多个硬件设备的移动。

要求

启动向导之前:

- 确保新记录服务器可以通过网络访问物理摄像机
- 安装要向其移动硬件的记录服务器(请参阅 第 139 页上的通过 Download Manager 安装(已解释) 或 第 146 页上的以静默方式安装 recording server)
- 在新记录服务器上安装与现有服务器上所运行的设备软件包版本相同的设备软件包版本(请参阅 第 124 页上的设备驱动程序(已解释))

要运行向导:

1. 在**站点导航**窗格中,选择**记录服务器**。
2. 在**总览**窗格中,右键单击要从中移动硬件的记录服务器,或右键单击某个特定硬件设备。
3. 选择**移动硬件**。

> 如果您要从中移动硬件的记录服务器已断开连接,将出现错误消息。只有在您确信已断开的记录服务器永不重新联机时,才选择从此记录服务器移动硬件。如果随便地移动硬件,且服务器重新联机,则系统可能会发生异常行为,因为一段时间内会在两个记录服务器上运行相同的硬件。例如,可能的问题包括许可证错误或者事件未发送到正确的记录服务器。

4. 如果您已从记录服务器级别启动此向导，将显示**选择您要移动的硬件**页面。选择您要移动的硬件设备。
5. 在**选择您要将硬件移动到的记录服务器**页面中，从此站点上已安装的记录服务器的列表中选择。
6. 在**选择要用于将来的记录的存储**页面中，存储使用情况条栏表示记录数据库中仅用于实时记录而不用于存档的可用空间。总保留时间是记录数据库和存档的保留期限。
7. 系统将处理您的请求。
8. 如果移动成功，单击**关闭**。如果在 Management Client 中选择新记录服务器，您可以查看移动的硬件，并且记录现在将存储在此服务器上。

   如果移动失败，您可以在下面对问题进行故障排除。

   > 在互连系统中，您必须在远程站点上移动硬件后手动同步中央站点，以反映您或其他系统管理员在远程站点进行的更改。

硬件移动故障排除

如果移动未成功，可能是由下列原因之一导致：

错误类型	故障排除
记录服务器未连接或处于故障转移模式。	确保记录服务器已联机。您可能需要注册它。 如果服务器处于故障转移模式，则等待并重试。
记录服务器不是最新版本。	更新录制服务器，以便它运行与管理服务器相同的版本。
在配置中找不到记录服务器。	确保记录服务器尚未被删除。
更新配置失败，或与配置数据库的通信失败。	确保您的 SQL Server 和数据库已连接并正在运行。
在当前记录服务器上停止硬件失败	可能另一个进程已锁定记录服务器，或记录服务器处于错误模式。 确保记录服务器正在运行，然后重试。
硬件不存在。	确保您尝试移动的硬件未同时被其他用户从系统中删除。不太可能出现该情况。
已从其移动硬件的记录服务器重新联机，但您已在其处于脱机状态时选择忽略它。	最有可能的是，您已经在启动**移动设备**向导时接受了将永不联机的旧记录服务器，但在移动过程中该服务器变为联机状态。

错误类型	故障排除
	再次启动向导，并在系统要求您确认服务器是否重新联机时选择**否**。
源记录存储不可用。	您试图移动的硬件设备配置了记录存储，而记录存储目前处于脱机状态。 如果硬盘脱机或不可用，则记录存储脱机。 确保记录存储处于联机状态，然后重试。
目标记录服务器上的所有记录存储必须可用。	您试图将硬件移动到一个或多个记录存储目前脱机的硬件。 请确保目标记录服务器上的所有记录存储都处于联机状态。 如果硬盘脱机或不可用，则记录存储脱机。

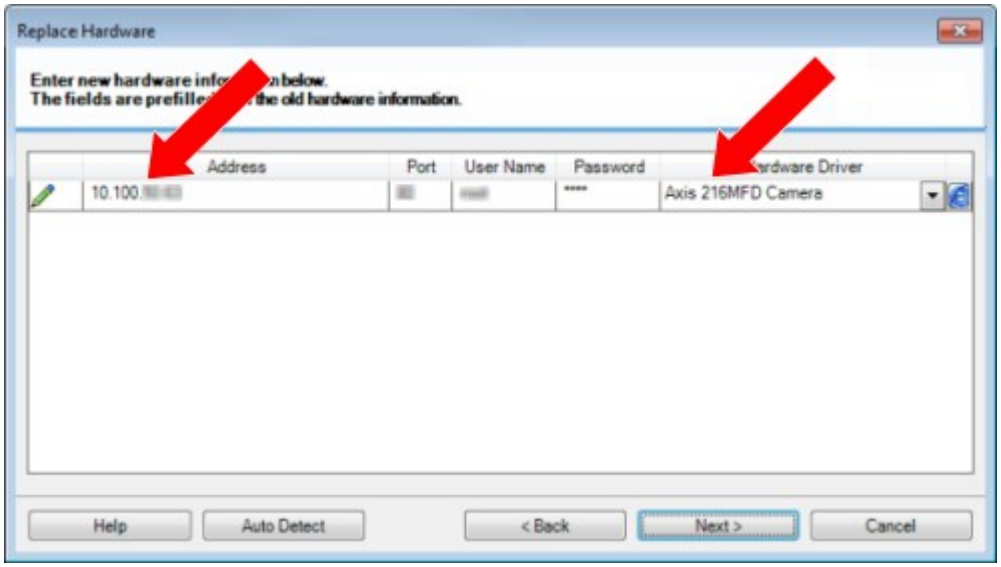
更换硬件

如果将网络上的硬件设备更换为其他硬件设备，则必须知道新硬件设备的 IP 地址、端口、用户名和密码。

如果尚未启用自动许可证激活(请参阅 第 100 页上的自动在线激活序列号(已解释))，并且已使用所有无需激活的设备变更(请第 101 页上的无需激活的设备变更(已解释)参阅)，则必须在更换硬件设备**之后**手动激活许可证。如果新硬件设备数量超出设备许可证总数，则必须购买新的设备许可证。

1. 展开所需的记录服务器，右键单击要更换的硬件。
2. 选择**更换硬件**。
3. 出现**更换硬件**向导。单击**下一步**。

4. 在向导中的**地址**字段(用图像中的红色箭头标记),输入新硬件的 IP 地址。在已知的情况下,可从**硬件驱动程序**下拉列表中选择相关的驱动程序。否则选择**自动检测**。如果端口、用户名或密码数据对于新硬件不同,请在**启动自动检测过程之前**进行修正(如果需要)。



向导会使用来自现有硬件的数据进行预填充。如果用相似的硬件设备进行更换,可重新使用这些数据中的一些,例如端口和驱动程序信息。

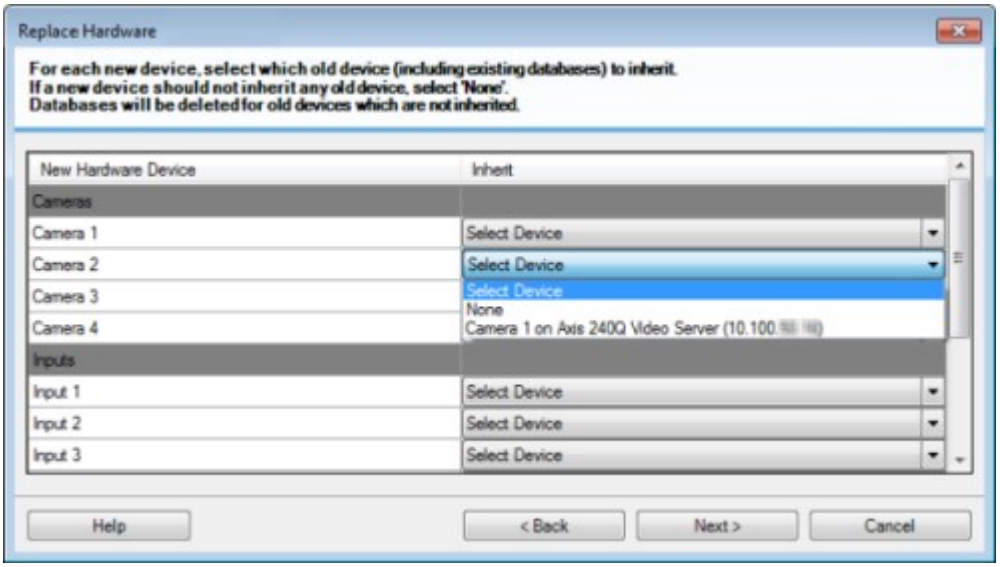
5. 进行以下操作之一：

   - 如果直接从列表选择了所需的硬件设备驱动程序，则单击**下一步**
   - 如果在列表中选择了**自动侦测**，则单击**自动侦测**，等待流程成功(用最左端的✓标记)，然后单击**下一步**

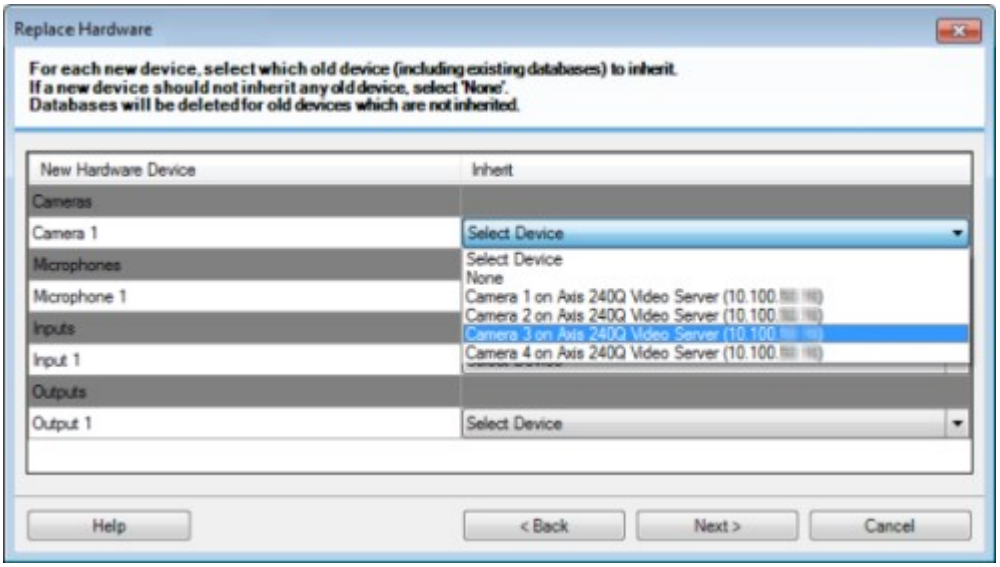
     该步骤旨在帮助您映射设备及其数据库，具体取决于分别连接至旧硬件设备和新硬件设备的摄像机、麦克风、输入、输出等的数目。

     考虑**如何**将数据库从旧硬件设备映射至新硬件设备的数据库很重要。通过在右侧列中选择相应摄像机、麦克风、输入、输出或**无**，可进行各设备的实际映射。

     > ⚠ 确保映射**所有**摄像机、麦克风、输入、输出等。内容已映射到**无**，则为**丢失**。



旧硬件设备拥有的独立设备超过新硬件设备的示例：



单击**下一步**。

6. 您将看到要添加、替换或删除的硬件的列表。**单击**确认。
7. 最后一步是已添加、更换和继承的设备及其设置的摘要。单击**复制到剪贴板**将内容复制到 Windows 剪贴板和/或单击**关闭**以结束向导。

更新您的硬件数据

为确保您的硬件设备和系统使用的是相同的固件版本，您需要手动更新 Management Client 中硬件设备的硬件数据。Milestone建议您在每次固件升级后更新硬件数据，以便更新您的硬件设备。

若要获取最新的硬件数据：

1. 在**站点导航**窗格中，选择**记录服务器**。
2. 展开所需的记录服务器，然后选择您想要获取最新信息的硬件。
3. 在**信息**选项卡的**属性**窗格上，单击**上次更新的硬件数据**字段中的**更新**按钮。
4. 向导会检查系统是否在运行硬件的最新固件。

   选择**确认**以更新 Management Client 中的信息。更新完成后，系统侦测到的硬件设备当前固件版本会出现在**信息**选项卡的**固件版本**字段内。

更改 SQL Server 数据库的位置和名称

管理服务器、事件服务器、日志服务器、Identity Provider 和 XProtect Incident Manager 使用连接字符串连接不同的 SQL Server 数据库。这些连接字符串存储在 Windows 注册表中。如果更改了 SQL Server 数据库的位置或名称，则必须编辑指向该 SQL Server 数据库的所有连接字符串。

数据库	使用者
Surveillance 数据库	• Management Server 服务 • Event Server 服务 • VideoOS Management Server 应用程序池 • VideoOS Report Server 应用程序池
Surveillance_IDP .	• VideoOS IDP 应用程序池
Surveilance_IM	• VideoOS IM 应用程序池
Surveillance_LogServerV2	• Log Server 服务

继续之前：

- 备份 SQL Server 数据库和 Windows 注册表。
- 确保运行相关服务和应用程序池的用户是数据库的所有者。
- 完成从旧 SQL Server 数据库到新数据库的内容迁移。

若要使用 SQL Server 数据库的新位置和名称更新连接字符串：

1. 停止所有使用 SQL Server 数据库的 XProtect VMS 服务和应用程序池。

   根据您的系统架构，服务和应用程序池可能在不同的计算机上运行。您必须停止所有连接到同一 SQL Server 数据库的应用程序池和服务。

2. 在注册表编辑器中，转到 `HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString`。

3. 使用 SQL Server 数据库的新位置和名称更新连接字符串。

   所有 SQL Server 数据库的默认连接字符串为：

   - **ManagementServer**:`Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **EventServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ServerService**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ReportServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IDP**:`Data Source=localhost;Initial Catalog=Surveillance_IDP;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IncidentManager**:`Data Source=localhost;Initial Catalog=Surveillance_IM;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **LogServer**: `Data Source=localhost;Initial Catalog=SurveillanceLogServerV2;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`

4. 启动您在步骤 1 中停止的所有 XProtect 服务和应用程序池。

管理服务器服务

在运行服务器服务的计算机上，可以在通知区域中找到服务器管理器托盘图标。通过这些图标，您可以获取有关服务的信息并执行某些任务。例如，其中包括检查服务的状态、查看日志或状态消息，以及启动和停止服务。

服务器管理器托盘图标(已解释)

表中的托盘图标显示管理服务器、记录服务器、故障转移记录服务器和事件服务器上运行的服务的不同状态。它们在安装了服务器的计算机上可见，位于通知区域中：

Management Server Manager 托盘图标	Recording Server Manager 托盘图标	Event Server Manager 托盘图标	Failover Recording Server Manager 托盘图标	说明
				**运行中** 启用并启动服务器服务时出现。

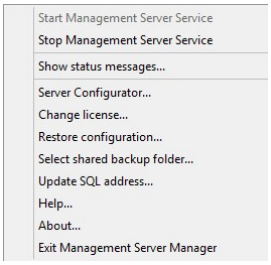
Management Server Manager 托盘图标	Recording Server Manager 托盘图标	Event Server Manager 托盘图标	Failover Recording Server Manager 托盘图标	说明
				如果 Failover Recording Server 服务在运行，则在标准记录服务器出现故障时它可以接管。
				**已停止** 服务器服务已停止运行时出现。 如果 Failover Recording Server 服务停止运行，则在标准记录服务器出现故障时它无法接管。
				**启动** 服务器服务正在启动时出现。在正常情况下，托盘图标会在短时间后变为**正在运行**。
				**停止** 服务器服务正在停止运行时出现。在正常情况下，托盘图标会在短时间后变为**已停止**。
				**处于不确定状态** 初次加载服务器服务时出现，直到收到第一条信息，在此基础上，托盘图标在正常情况下会更改为**启动**，然后更改为**运行**。

Management Server Manager 托盘图标	Recording Server Manager 托盘图标	Event Server Manager 托盘图标	Failover Recording Server Manager 托盘图标	说明
				**脱机运行** 通常在记录服务器或故障转移记录服务正在运行但 Management Server 服务未运行时出现。

启动或停止 Management Server 服务

Management Server Manager 托盘图标指示 Management Server 服务的状态，例如**运行中**。通过该图标，您可以启动或停止 Management Server 服务。如果停止 Management Server 服务，您将无法使用 Management Client。

1. 在通知区域中，右键单击 Management Server Manager 托盘图标。随即显示上下文菜单。



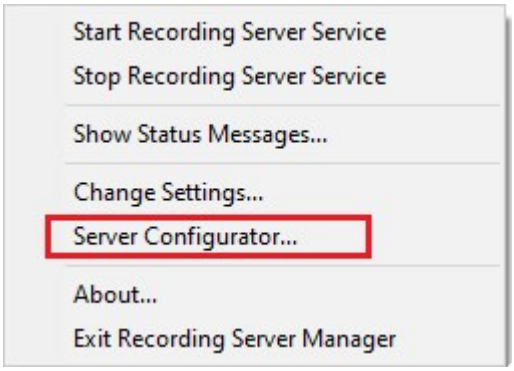
2. 如果该服务已停止，请单击**启动ManagementServer服务**来启动它。托盘图标将会更改以反映新的状态。
3. 要停止服务，请单击**停止 Management Server 服务**。

有关托盘图标的详细信息，请参阅 第 303 页上的服务器管理器托盘图标(已解释)。

启动或停止 Recording Server 服务

Recording Server Manager 托盘图标指示 Recording Server 服务的状态，例如**运行中**。通过该图标，您可以启动或停止 Recording Server 服务。如果您停止 Recording Server 服务，系统将无法与连接到服务器的设备进行交互。这意味着无法查看实时视频或记录视频。

1. 在通知区域中，右键单击 Recording Server Manager 托盘图标。随即显示上下文菜单。

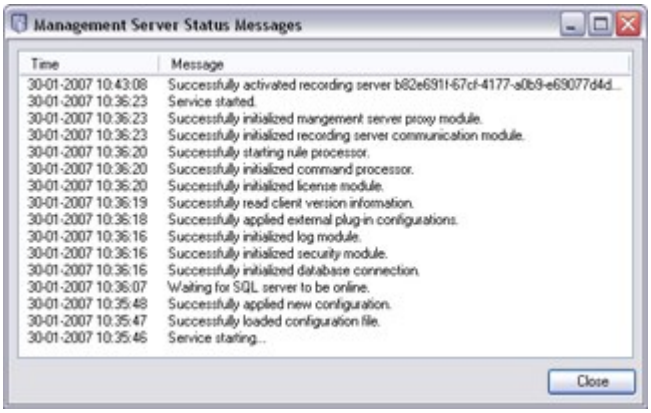


2. 如果该服务已停止，请单击**启动 Recording Server 服务**来启动它。托盘图标将会更改以反映新的状态。
3. 要停止服务，请单击**停止 Recording Server 服务**。

有关托盘图标的详细信息，请参阅 第 303 页上的服务器管理器托盘图标(已解释)。

查看管理服务器或录制服务器的状态消息

1. 在通知区域中，右键单击相关的托盘图标。随即显示上下文菜单。
2. **选择**显示状态消息。根据服务器类型，会出现**管理服务器状态消息**或**录制服务器状态消息**窗口，其中会列出添加有时间戳的状态消息：



管理加密使用的是 Server Configurator

使用 Server Configurator 来选择本地服务器上的证书以进行加密通信，并注册服务器服务以使其有资格与服务器进行通信。

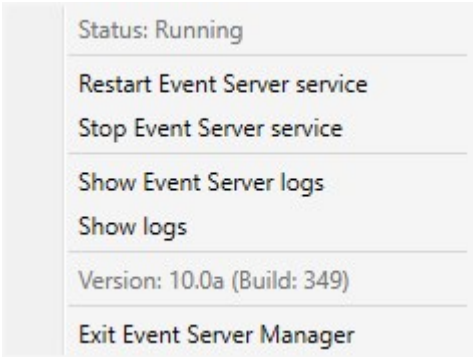
从 Windows 开始菜单、管理服务器托盘图标或者录制服务器托盘图标打开 Server Configurator。请参阅 第 347 页上的Server Configurator(实用工具)。

有关详细信息，请参阅有关如何保护 XProtect VMS 安装的证书指南。

启动、停止和重启 Event Server 服务

Event Server Manager 托盘图标指示 Event Server 服务的状态，例如**运行中**。通过该图标，您可以启动、停止或重启 Event Server 服务。如果您停止该服务，系统的某些部分将不会工作，包括事件和警报。但是，您仍然可以查看和记录视频。有关详细信息，请参阅 第 307 页上的停止 Event Server 服务。

1. 在通知区域中，右键单击 Event Server Manager 托盘图标。随即显示上下文菜单。



2. 如果该服务已停止，请单击**启动 Event Server 服务**来启动它。托盘图标将会更改以反映新的状态。
3. 要重启或停止服务，请单击**重启 Event Server 服务**或**停止 Event Server 服务** 。

有关托盘图标的详细信息，请参阅 第 303 页上的服务器管理器托盘图标(已解释)。

停止 Event Server 服务

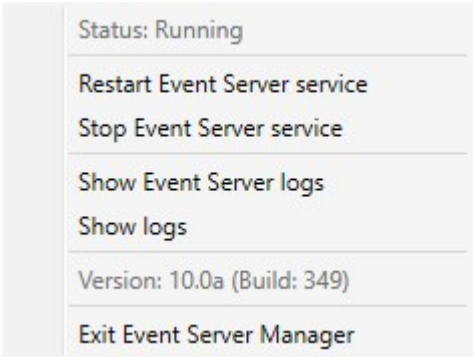
在 Event Server 上安装 MIP 插件时，首先必须停止 Event Server 服务，然后重新启动它。在停止该服务后，视频管理软件系统的许多区域将不会工作：

- 不会将事件或警报存储在事件服务器上。但是，系统和设备事件仍会触发动作，如开始录制
- XProtect 扩展在 XProtect Smart Client 中不工作，也无法从 Management Client 进行配置。
- 分析事件不会工作
- 常规事件不会工作
- 不会触发警报
- 在 XProtect Smart Client 中，地图视图项目、警报列表视图项目和警报管理器工作区不会工作
- 事件服务器上的 MIP 插件无法运行
- MIP 和 Management Client 中的 XProtect Smart Client 插件无法正常运行

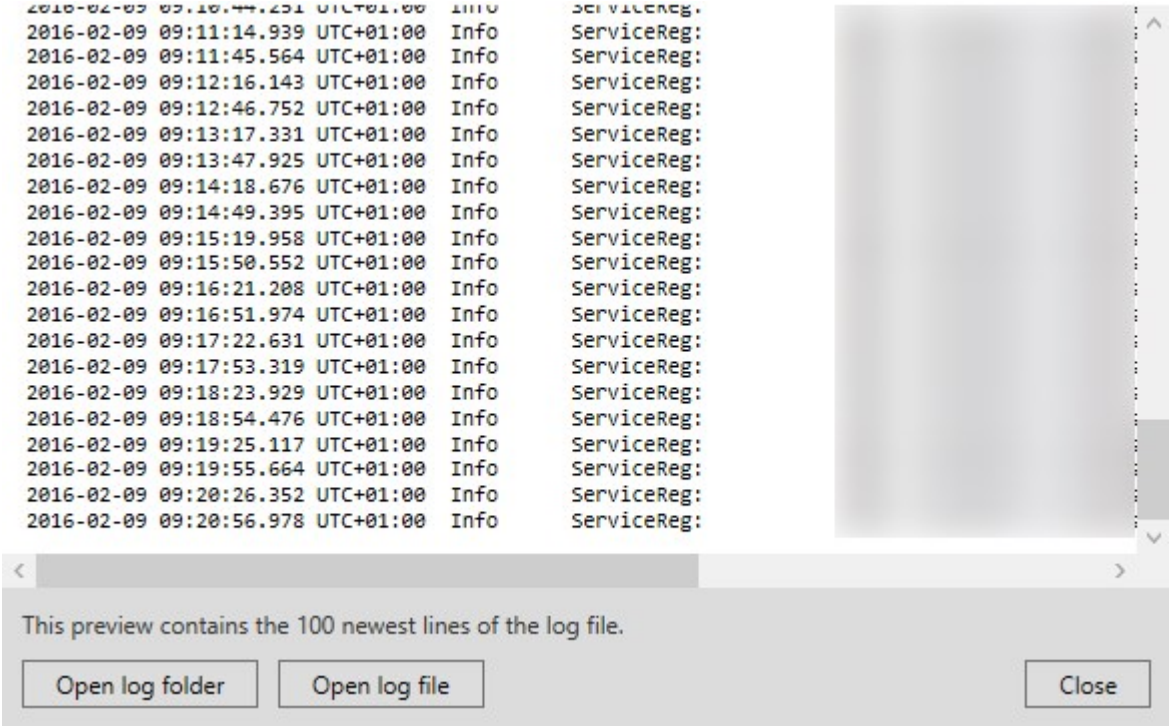
查看事件服务器或 MIP 日志

您可以在 Event Server 日志中查看有关 Event Server 活动的时间标记信息。在**事件服务器**文件夹的子文件夹的 MIP 日志中记录了有关第三方集成的信息。

1. 在通知区域中，右键单击 Event Server Manager 托盘图标。随即显示上下文菜单。



2. 要查看 Event Server 日志中最新的 100 行，请单击**显示事件服务器日志**。显示日志查看器。



   1. 要查看日志文件，请单击**打开日志文件**。
   2. 要打开日志文件夹，请单击**打开日志文件夹**。

3. 要查看 MIP 日志中最新的 100 行，请返回到上下文菜单，然后单击**显示 MIP 日志**。显示日志查看器。

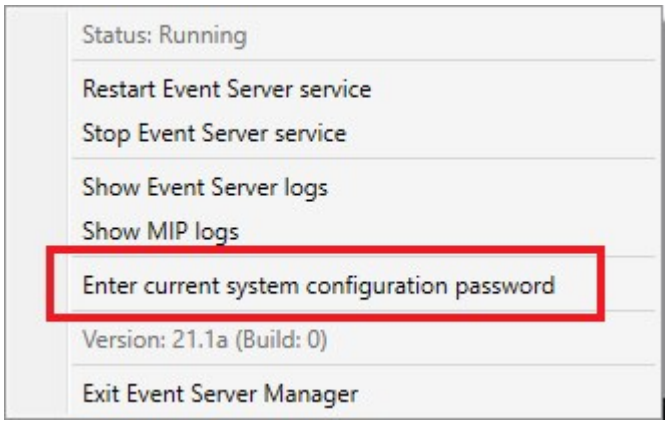
> 如果有人从日志目录删除了日志文件，则菜单项将变灰。要打开日志查看器，首先需要将日志文件复制回到其文件夹中：`C:\ProgramData\Milestone\XProtect Event Server\logs` 或 `C:\ProgramData\Milestone\XProtect Event Server\logs\MIP Logs`。

输入当前的系统配置密码

如果在管理服务器中更改了系统配置密码，则也必须在事件服务器中输入当前的系统配置密码。

> ⚠ 如果您未在事件服务器中输入当前密码，则系统组件（例如访问控制）将停止工作。

1. 在通知区域中，右键单击 Event Server Manager 托盘图标。随即显示上下文菜单。



2. 要输入当前的系统配置密码，请单击**输入当前的系统配置密码**。会显示一个窗口。
3. 输入与管理服务器中输入的相同的系统配置密码。

管理已注册服务

有时可能需要能够与系统通信的服务器和/或服务，即使它们并不直接是系统的一部分。某些服务（但并非所有）可自动在系统中注册自己。可自动注册的服务有：

- Event Server 服务
- Log Server 服务

自动注册的服务显示在已注册服务列表中。

可在 Management Client 中手动将服务器/服务指定为已注册服务。

添加和编辑已注册服务

1. 在**添加/删除已注册服务**窗口中，根据需求单击**添加**或**编辑**。
2. 在**添加已注册服务**或**编辑已注册服务**窗口中（根据之前的选择），指定或编辑设置。
3. 单击**确定**。

管理网络配置

利用网络配置设置，可指定管理服务器的服务器 LAN 和 WAN 地址，以便管理服务器和受信任服务器能够通信。

1. 在**添加/删除已注册服务**窗口中，单击**网络**。
2. 指定管理服务器的 LAN 和/或 WAN IP 地址。

   如果所有相关服务器(管理服务器和受信任服务器)位于本地网络，只需指定 LAN 地址。如果一台或多台相关服务器通过互联网连接访问系统，则必须还指定 WAN 地址。

3. 单击**确定**。

已注册服务属性

在**添加已注册服务**或**编辑已注册服务**窗口中，指定以下内容：

组件	要求
类型	已预填充的字段。
名称	已注册服务的名称。Management Client 名称仅用于在中显示的目的。
URL	**单击**添加来添加已注册服务的 IP 地址或主机名。如果指定主机名作为 URL 的一部分，则主机必须在网络上存在并且可用。URL 必须以 *http://* 或 *https://* 开始，并且不得包含以下任意字符：*< > & ' " * ?	[ ]*。 典型 URL 格式的**示例**：*http://ipaddress:port/directory*(端口和目录是可选的)。您可以根据需要添加一个以上的 URL。
受信任	如果应立即信任已注册服务，则选择该项(这是通常出现的情况，但利用该选项可以灵活地添加已注册服务，然后通过稍后编辑已注册服务将其标记为已注册)。 如果更改受信任状态，也会更改共享为相关已注册服务定义的一个或多个 URL 的其他已注册服务的状态。
说明	已注册服务的说明。Management Client 说明仅用于在中显示的目的。
高级	如果是高级服务，它将具有需要为您定义的每个主机地址设置的特定 URI 方案(例如 HTTP、HTTPS、TCP 或 UDP)。因此，主机地址有多个端点，每个端点均具有自己的方案，以及该方案的主机地址和 IP 端口。

删除设备驱动程序(已解释)

如果您的计算机上不再需要设备驱动程序，可从系统中删除设备软件包。遵循删除程序的标准Windows步骤即可。

如果您已安装多个设备软件包，并且无法删除安装文件，那么您可以使用设备软件包安装文件夹中的脚本来彻底删除文件。

如果删除了设备驱动程序，记录服务器和摄像机设备将无法再通信。在升级时请勿删除设备软件包，可在旧版本基础上安装新版本。只有卸载了整个系统时，才可以删除设备软件包。

删除记录服务器

如果删除记录服务器，将删除在 Management Client 中为记录服务器指定的**所有**配置，包括记录服务器的所有相关硬件(摄像机、输入设备等)。

1. 右键单击**总览**窗格中想要删除的记录服务器。
2. 选择**删除记录服务器**。
3. 如果确定，单击**是**。
4. 记录服务器及其所有相关硬件即会被删除。

删除记录服务器上的所有硬件

删除硬件时，所有与硬件相关的录制数据将会被永久性删除。

1. 右键单击想要删除所有硬件的记录服务器。
2. **选择**删除所有硬件。
3. 确认删除。

更改管理服务器计算机的主机名

如果管理服务器是通过其完全限定的域名 (FQDN) 或主机名寻址的，则对计算机主机名的更改将在 XProtect 中具有必须考虑和处理的含义。

通常，应谨慎计划更改管理服务器的主机名，因为此后可能需要进行大量清理。

在以下各部分中，您可以查看更改主机名的含义总览。

证书的有效性

证书用于加密服务之间的通信，并且证书安装在运行一项或多项 XProtect 服务的所有计算机上。

根据证书的创建方式，证书可以与安装它们的计算机相关联，并且只有在计算机名称保持不变的情况下才有效。

有关如何创建证书的详细信息，请参阅证书简介。

如果更改计算机名称，则使用的证书可能会失效，并且 XProtect VMS 无法启动。要使系统重新启动并运行，请完成以下步骤：

- 创建新证书，然后将其重新安装到环境中的所有计算机上。
- 在每个计算机上使用 Server Configurator 来应用新证书，以启用使用新证书进行的加密。

这将触发新证书的注册，并使系统重新启动和运行。

注册服务的客户数据属性丢失

如果您在更改管理服务器地址等操作后使用 Server Configurator 完成注册，则对注册服务信息的任何编辑都将被覆盖。因此，如果您更改了已注册服务的信息，则必须对使用更改后的名称注册到计算机的管理服务器上的所有服务再次应用此更改。

可以为注册服务编辑的信息位于**工具 > 注册服务 > 编辑**下：

- 受信任
- 高级
- 外部标记
- 任何手动添加的 URL

在 Milestone Customer Dashboard 中，主机名将保持不变

Milestone Customer Dashboard 是供 Milestone 合作伙伴、经销商及 XProtect 视频管理软件用户对 Milestone 软件的安装和许可证进行管理和监控的免费在线工具。

连接到 Milestone Customer Dashboard 的系统上的管理服务器名称的更改不会自动反映在 Milestone Customer Dashboard 中。

直到完成新的许可证激活，旧的主机名才会显示在 Milestone Customer Dashboard 中。但是，名称更改不会破坏 Milestone Customer Dashboard 中的任何内容，一旦进行了新的激活，该记录就会在数据库中使用新的主机名进行更新。有关 Milestone Customer Dashboard 的详细信息，请参阅 Milestone Customer Dashboard(已作说明) 。

主机名更改可以触发 SQL Server 地址更改

如果 SQL Server 与管理服务器位于同一个计算机上，并且此计算机的名称已更改，则 SQL Server 的地址也将更改。这意味着，对于位于不同计算机上的组件以及本地计算机上使用计算机名而不是连接到 SQL Server 的本地主机的组件，必须更新 SQL Server 地址。这特别适用于使用与 Event Server 相同的数据库的 Management Server。它也可能适用于使用不同数据库但很可能在同一 SQL Server 上的 Log Server。

请参阅 第 301 页上的更改 SQL Server 数据库的位置和名称。

在 中进行主机名更改Milestone Federated Architecture

对位于 Milestone Federated Architecture 设置中的计算机名称进行更改将产生以下影响，这适用于在工作组内部和跨域连接站点时。

站点的主机是架构中的根节点

如果更改架构中运行中央站点的计算机的名称，则所有子节点将自动重新附加到新地址。因此，在此情况下，重命名不需要任何操作。

站点的主机是架构中的子节点

为避免在更改运行一个或多个联合站点的计算机名称时出现连接问题，您必须在重命名计算机之前向受影响的站点添加备用地址。受影响的站点是将重命名其主机的节点。有关由于未准备或不可预测的主机名更改而导致的连接问题以及如何解决此类问题的更多信息，请参阅问题：Milestone Federated Architecture 设置中的父节点无法连接到子节点。

必须在**站点导航**或**联合站点分层**窗格的**属性**窗格中添加备用地址。必须满足以下先决条件：

- 必须添加备用地址才能重命名主机计算机
- 备用地址必须反映主机计算机的未来名称(重命名时)

有关如何访问**属性**窗格的信息，请参阅设置站点属性。

> 为确保尽可能顺利地进行更新，请在主机名将更改的节点的父节点上停止 Management Client。否则，请在计算机重命名后停止并重新启动客户端。有关详细信息，请参阅开始或停止 Management Server 服务。

> 此外，请确保您提供的备用地址反映在中央站点的**联合站点分层**窗格中，如果没有，请停止并重新启动 Management Client。

主机被重命名并且您重新启动了计算机后，联合站点将自动切换到新地址。

管理服务器日志

以下是服务器日志的类型：

- 系统日志
- 审核日志
- 规则触发日志

这些用于记录系统的使用情况。这些日志位于 Management Client 中的**服务器日志**下。

有关用于故障排除和调查软件错误的日志的信息，请参阅 第 318 页上的调试日志(已作说明)。

识别用户活动、事件、操作和错误

使用日志可获取系统中用户活动、事件、操作和错误的详细记录。

要查看 Management Client 中的日志，请转到**网站导航**窗格，然后选择**服务器日志**。

日志类型	记录了什么？
系统日志	记录系统相关信息。
审核日志	用户活动
规则触发日志	记录用户指定**创建新 <日志条目>** 操作的规则。有关 <日志条目> 操作的详细信息，请参阅操作和停止操作。

要查看其他语言的日志，请参阅**选项**下的 第 331 页上的“常规”选项卡(选项)。

要将日志导出为逗号分隔值(.csv)文件，请参见导出日志。

要更改日志设置，请参阅 第 333 页上的“服务器日志”选项卡(选项)。

筛选日志

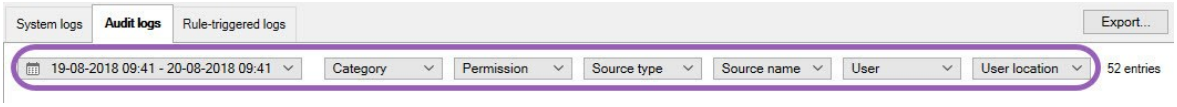
在每个日志窗口中，您可以应用筛选器以查看日志条目，例如，特定时间范围、设备或用户。

> 根据用户界面中当前可见的日志条目生成筛选器。

1. 在**站点导航**窗格中，选择**服务器日志**。默认会出现**系统日志**选项卡。

   要在日志类型之间导航，请选择其他选项卡。

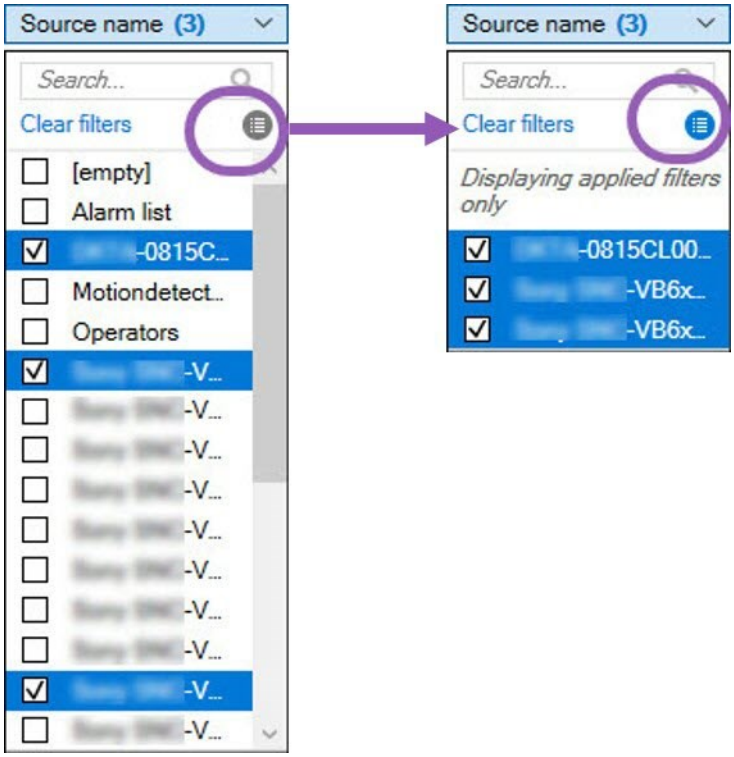
2. 在选项卡下，选择一个过滤器组，例如**类别**、**源类型**或**用户**。



   出现筛选器列表。过滤器列表最多显示 1000 个筛选器。

3. 选择要应用它的过滤器。再次选择过滤器以将其删除。

   可选:在过滤器列表中,选择**仅显示应用的过滤器**以仅查看您应用的过滤器。



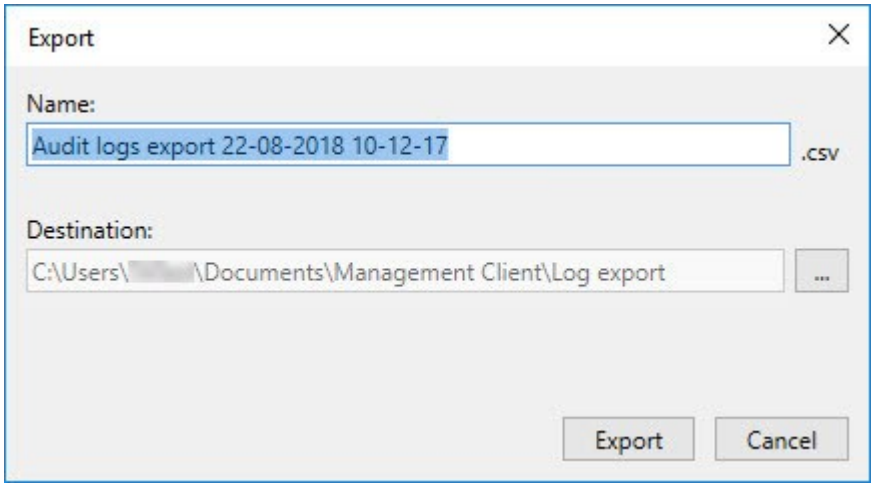
导出日志时,导出内容的变化取决于您应用的筛选器。有关导出的信息,请参阅导出日志。

导出日志

例如,导出日志可帮助您将日志条目保存到日志保留期之外。您可以将日志导出为逗号分隔值(.csv)文件。

导出日志:

1. 选择右上角的**导出**。出现**导出**窗口。



2. 在**导出**窗口的**名称**字段中，指定日志文件的名称。
3. 默认情况下，导出的日志文件保存在**Logexport**文件夹中。要指定一个不同的位置，选择 ... 到右侧**目标**字段。
4. 选择**导出**以导出日志。

> 导出内容的变化取决于您应用过滤器。有关导出的信息，请参阅 筛选日志。

搜索日志

要搜索日志，请使用“日志”窗格顶部的**搜索条件**：

1. 从列表中指定搜索条件。
2. 单击**刷新**以使日志页面反映您的搜索条件。要清除搜索条件，然后返回查看所有日志内容，请单击**清除**。

您可以双击任一行以在**日志详细信息**窗口中显示所有详细信息。这样，还可以读取内容比单行显示的文本更多的日志条目。

更改日志语言

1. 在日志窗格的底部，在**日志显示语言**列表中，选择所需的语言。

2. 日志将以所选语言显示。下次打开日志时，它将重置为默认语言。

允许 2018 R2 和更早版本的组件写入日志

2018 R3 版本的日志服务器引入了身份验证以增强安全性。这可以防止 2018 R2 和更早版本的组件将日志写入日志服务器。

受影响的组件：

- XProtect Smart Client
- XProtect LPR 插件
- LPR Server
- 访问控制插件
- 事件服务器
- 警报插件

如果您使用的是上面列出的任何组件的2018R2或更早版本，则必须决定是否允许组件将日志写入新日志服务器：

1. 选择**工具 > 选项**。
2. 在**选项**对话框的**服务器日志**选项卡的底部，找到**允许 2018 R2 和更早版本的组件写入日志**复选框。
    - 选中该复选框以允许 2018 R2 及更早版本的组件写入日志
    - 清除该复选框以禁止 2018 R2 和早期组件写入日志

故障排除

调试日志(已作说明)

调试日志用于识别系统中的缺陷和瑕疵。

有关用于系统使用的日志的信息，请参阅 第 313 页上的管理服务器日志。

以下是 XProtect 安装中日志文件的位置：

- C:\ProgramData\Milestone\IDP\Logs

  只有 IIS 用户和管理员可以访问此项。如果更改了 IIS 用户，则必须更新这些权限。

- C:\ProgramData\Milestone\MIPSDK
- C:\ProgramData\Milestone\XProtect Data Collector Server\Logs
- C:\ProgramData\Milestone\XProtect Event Server\Logs
- C:\ProgramData\Milestone\XProtect Log Server
- C:\ProgramData\Milestone\XProtect Management Server\Logs
- C:\ProgramData\Milestone\XProtect Mobile Server\Logs
- C:\ProgramData\Milestone\XProtect Recording Server\Logs
- C:\ProgramData\Milestone\XProtect Report Web Server\Logs

问题：更改 SQL Server 和数据库位置可防止访问数据库

如果 SQL Server 和视频管理软件数据库的位置发生更改，例如更改了运行 SQL Server 的计算机的主机名，则录制服务器对数据库的访问将丢失。

解决方案：更改连接字符串以反映 SQL Server 和数据库的更改。请参阅 第 301 页上的更改 SQL Server 数据库的位置和名称。

问题：由于端口冲突，记录服务器启动失败

此问题只有在简单邮件传输协议 (SMTP) 服务正在运行时才会出现，因为它使用端口 25。如果端口 25 已在使用，则可能无法启动 Recording Server 服务。端口号 25 可用于记录服务器的 SMTP 服务非常重要。

SMTP 服务：验证和解决方案

要验证是否已安装 SMTP 服务，请执行以下操作：

1. 从 Windows 的**开始**菜单，选择**控制面板**。
2. 在**控制面板**中，双击**添加或删除程序**。
3. 在**添加或删除程序**窗口的左侧，单击**添加/删除 Windows 组件**。
4. 在 **Windows 组件**向导中，选择 **Internet 信息服务 (IIS)**，然后单击**详细信息**。
5. 在 **Internet 信息服务 (IIS)** 窗口中，验证是否已选中 **SMTP 服务**复选框。如果是这样，则安装 SMTP 服务。

如果安装了 SMTP 服务，请选择以下解决方案之一：

解决方案 1：禁用 SMTP 服务，或将其设置为手动启动

此解决方案让您可以启动记录服务器，而无需每次都停止 SMTP 服务：

1. 从 Windows 的**开始**菜单，选择**控制面板**。
2. 在**控制面板**中，双击**管理工具**。
3. 在**管理工具**窗口中，双击**服务**。
4. 在**服务**窗口中，双击**简单邮件传输协议 (SMTP)**。
5. 在 **SMTP 属性**窗口中，单击**停止**，然后将**启动类型**设置为**手动**或**已禁用**。

   设置为**手动**时，可以从**服务**窗口手动启动 SMTP 服务，也可以使用命令 *net start SMTPSVC* 从命令提示符启动 SMTP 服务。
6. 单击**确定**。

解决方案 2：删除 SMTP 服务

删除 SMTP 服务可能会影响使用 SMTP 服务的其他应用程序。

1. 从 Windows 的**开始**菜单，选择**控制面板**。
2. 在**控制面板**窗口中，双击**添加或删除程序**。
3. 在**添加或删除程序**窗口的左侧，单击**添加/删除 Windows 组件**。
4. 在 **Windows 组件**向导中，选择 **Internet 信息服务 (IIS)**项，然后单击**详细信息**。
5. 在 **Internet 信息服务 (IIS)** 窗口中，清除 **SMTP 服务**复选框。
6. 单击**确定**、**下一步**和**完成**。

问题：Recording Server 在切换 Management Server 群集节点时会脱机

如果设置 Microsoft 群集以实现 Management Server 冗余，则在群集节点之间切换 Recording Server 时，Recording Server 或 Management Server 可能会脱机。

要更正此问题，请执行以下操作：

在进行配置更改时，在 Microsoft 故障转移群集管理器上，暂停对服务的控制和监视，以便 Server Configurator 可以进行更改并启动和/或停止 Management Server 服务。如果将故障转移群集服务启动类型更改为手动，则不应导致与 Server Configurator 的任何冲突。

在 Management Server 计算机上：

1. 在安装了管理服务器的每个计算机上启动 Server Configurator。
2. 转到**注册**页面。
3. 单击铅笔 () 符号以使管理服务器地址可编辑。
4. 将管理服务器地址更改为群集的 URL，例如 `http://MyCluster`。
5. 单击**注册**。

在具有使用ManagementServer(例如RecordingServer、MobileServer、EventServer、APIGateway) 的组件的计算机上：

1. 在每个计算机上启动 Server Configurator。
2. 转到**注册**页面。
3. 将管理服务器地址更改为群集的 URL，例如 `http://MyCluster`。
4. 单击**注册**。

问题：MilestoneFederatedArchitecture设置中的父节点无法连接到子节点

如果您重命名了在 Milestone Federated Architecture 中作为子节点的站点的主机，则父节点将无法连接到它。充当中子节点的站点的主机，则父节点将无法连接到它。

重新建立父节点与站点之间的连接

- 将受影响的站点从其父站点分离。有关详细信息，请参阅将站点从层级分离。
- 使用主机的新名称重新连接该站点。有关更多信息，请参见将站点添加至分层。

为确保更改生效，您可能需要在主机名已更改的节点的父节点上停止并重新启动 Management Client。有关详细信息，请参阅开始或停止 Management Server 服务。

有关 Milestone Federated Architecture 设置中主机名更改含义的详细信息，请参阅 Milestone Federated Architecture 中的主机名更改。

问题：Azure SQL 数据库服务不可用

如果您使用 Azure SQL 数据库，但在安装过程中或正常操作过程中遇到连接问题，原因可能是 Azure SQL 数据库服务暂时不可用。

Azure SQL 数据库是一项服务，其中大多数传统数据库维护由 Microsoft 负责。该服务可能在短时间内不可用，但可以在不需要用户交互的情况下恢复到一定程度。

数据库错误会写入 XProtect VMS 日志文件，并带有相关事件 ID，在 Azure SQL 数据库长时间不可用的情况下，可将该 ID 提供给 Microsoft 支持。

有关详细信息，请参阅排查 Azure SQL 数据库的常见连接问题。

升级

升级(已解释)

升级时,计算机上当前安装的所有组件都会进行升级。升级期间无法删除已安装的组件。如果要删除已安装的组件,请在升级之前或之后使用 Windows 的**添加和删除程序**功能。在升级过程中,将自动移除和替换所有组件(管理服务器数据库除外)。这将包括设备软件包的驱动程序。

管理服务器数据库包含完整的系统配置(记录服务器配置、摄像机配置、规则等)。只要不移除管理服务器数据库,就无需重新配置系统配置(即使您可能想要在新版本中配置一些新功能)。

对于早于当前版本的 XProtect 版本,与记录服务器的向后兼容性受到限制。您仍可访问这些较旧记录服务器上的记录,但要更改其配置,它们必须与当前记录服务器的版本相同。Milestone 建议您升级本系统中的所有 recording server。

在进行包括记录服务器的升级时,系统会提示您是要升级还是保持视频设备驱动程序。如果选择升级,在重新启动系统后,硬件设备可能需要数分钟时间才能与新的视频设备驱动程序取得联系。这是由于会在新安装的驱动程序上执行多个内部检查。

如果您从 2017 R3 或更旧版本升级到 2018 R1 或更新版本,并且您的系统使用的是旧摄像机,则必须从我们网站 (https://www.milestonesys.com/downloads/) 的下载页面手动下载包含旧驱动程序的设备软件包。要查看是否有摄像机使用的是旧设备软件包中的驱动程序,请访问我们网站 (https://www.milestonesys.com/community/business-partner-tools/device-packs/) 上的此页面。

如果您从 2018 R1 版本或更早版本升级至 2018 R2 版本或以后的版本,那么在升级之前,您需要使用安全补丁在系统中更新所有记录服务器。没有安全补丁的升级将导致记录服务器出现故障。

在我们的网站 https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/ 上可以找到关于在记录服务器上安装安全补丁的说明。

如果要加密管理服务器与记录服务器之间的连接,则所有记录服务器必须升级到 2019 R2 或更高版本。

有关建议升级片段的概述，请参阅 第 324 页上的升级最佳实践

升级要求

- 准备好软件许可证文件(请参阅 第 98 页上的许可证(已解释))(.lic):
  - **服务包升级**:在安装管理服务器期间，向导可能会要求您指定软件许可证文件的位置。您可以同时使用在购买系统(或最新升级)后获得的软件许可证文件，以及在您最后一次许可证激活后获得的已激活软件许可证文件
  - **版本升级**:在您购买新版本之后，您会收到新的软件许可证文件。在安装管理服务器期间，向导会要求您指定新软件许可证文件的位置

  系统会先验证软件许可证文件，然后您才能继续操作。要求许可证的已添加的硬件设备和其他设备将进入宽限期。如果尚未启用自动许可证激活(请参阅第 104 页上的启用自动许可证激活)，请记住在宽限期到期之前手动激活许可证。如果您没有软件许可证文件，请联系 XProtect 经销商。
- 准备好**新的产品版本**软件。您可以从 Milestone 网站上的下载页面进行下载。
- 请确保您已备份系统配置(请参阅 第 286 页上的关于备份和还原系统配置(已解释))

  管理服务器会在 SQL Server 数据库中存储系统配置。SQL Server 数据库可以位于管理服务器自身计算机上的 SQL Server 实例中或网络上的 SQL Server 实例中。

  如果您使用您的网络上 SQL Server 实例中的 SQL Server 数据库，当您想要创建、移动或升级 SQL Server 数据库时，管理服务器必须在 SQL Server 实例上拥有管理员权限。对于 SQL Server 数据库的常规使用和维护，管理服务器只需要是数据库所有者。
- 如果您计划在安装期间启用加密，您需要在相关计算机上安装并信任相应证书。有关详细信息，请参阅第 124 页上的安全通信(已解释)。

在做好开始升级的准备后，请遵循 第 324 页上的升级最佳实践 中的程序操作。

升级 XProtect VMS 以在 FIPS 140-2 兼容模式下运行

从版本 2020 R3 开始，XProtect VMS 配置为运行，使其仅使用 FIPS 140-2 认证的算法实例。

有关如何配置XProtectVMS以在符合FIPS140-2的模式下运行的详细信息，请参阅强化指南中的FIPS140-2合规部分。

> 对于符合 FIPS 140-2 的系统，如果使用不符合 FIPS 的密码对 2017 R1 之前版本的 XProtect VMS 导出和存档媒体数据库进行了加密，则需要将数据存档在启用 FIPS 之后仍可访问的位置。

以下过程描述了配置 XProtect VMS 以在 FIPS 140-2 兼容模式下运行所需的条件:

1. 在属于视频管理软件的所有计算机(包括托管 SQL Server 的计算机)上禁用 Windows FIPS 安全策略。

   升级时,如果在 Windows 操作系统上启用了 FIPS,将无法安装 XProtect VMS。

2. 确保独立的第三方集成可以在启用 FIPS 的 Windows 操作系统上运行。

   如果独立集成不符合FIPS140-2,则在将Windows操作系统设置为在FIPS模式下运行后,它将无法运行。

   为防止发生这种情况:

   - 列出以下项的所有独立集成的清单:XProtect VMS
   - 联系这些集成的提供商,并询问集成是否符合 FIPS 140-2
   - 部署符合 FIPS 140-2 的独立集成

3. 确保驱动程序以及与设备的通信均符合 FIPS 140-2 要求。

   XProtect VMS如果满足以下条件,则可以保证 并强制执行 FIPS 140-2 兼容操作模式:

   - 设备仅使用兼容的驱动程序连接到 XProtect VMS

     有关确保和强制执行合规性的驱动程序的详细信息,请参阅强化指南中的 FIPS 140-2 合规部分。

   - 设备使用设备软件包版本 11.1 或更高版本

     旧版驱动程序设备包中的驱动程序不能保证获得符合 FIPS 140-2 的连接。

   - 设备通过 HTTPS 以及视频流的 HTTPS 上的安全实时传输协议 (SRTP) 或 Real Time Streaming Protocol (RTSP) 连接

     > 驱动程序模块不能保证通过 HTTP 的连接符合 FIPS 140-2。连接可能符合要求,但不能保证一定符合要求。

   - 运行记录服务器的计算机在启用 FIPS 模式的情况下运行 Windows 操作系统

4. 确保使用兼容 FIPS 140-2 的密码对媒体数据库中的数据进行加密。

   这是通过运行媒体数据库升级工具来完成的。有关如何配置 XProtect VMS 以在符合 FIPS 140-2 的模式下运行的详细信息,请参阅强化指南中的FIPS 140-2 合规部分。

5. 在 Windows 操作系统上启用 FIPS 之前,以及在配置完 XProtect VMS 系统并确保所有组件和设备都可以在启用 FIPS 的环境中运行之后,请在 XProtect Management Client 中更新现有的硬件密码。

   为此,在 Management Client 中,从**录制服务器**节点的所选录制服务器中,右键单击并选择**添加硬件**。通过**添加硬件**向导进行。这将更新所有当前凭据并对其进行加密以符合 FIPS。

只有在升级了整个视频管理软件(包括所有客户端)之后,才能启用 FIPS。

升级最佳实践

请先阅读包括 SQL Server 数据库备份在内的升级要求(请参阅 第 323 页上的升级要求),然后再开始正式升级。

现在，设备驱动程序分为两个设备软件包：包含较新驱动程序的常规设备软件包和包含较旧驱动程序的旧设备软件包。常规设备软件包始终会自动安装更新或升级。如果您的旧摄像机使用的是旧设备软件包中的旧设备驱动程序和，则您还没有安装旧设备软件包，系统不会自动安装旧设备软件包。

如果您的系统使用旧摄像机，Milestone 建议您检查摄像机是否使用此页面 (https://www.milestonesys.com/community/business-partner-tools/device-packs/) 中旧设备软件包的驱动程序。要检查是否已安装旧软件包，请查看 XProtect 系统文件夹。如果您需要下载旧版设备软件包，请前往下载页面 (https://www.milestonesys.com/downloads/)。

如果您的系统为**单台计算机**系统，则可以在现有安装基础上安装新软件。

在MilestoneInterconnect或MilestoneFederatedArchitecture系统中，您必须开始升级中央站点，然后升级远程站点。

在分布式系统中，按以下顺序执行升级：

1. 使用安装程序（请参阅 第 134 页上的安装本系统 - 自定义选项）中的**自定义**选项升级管理服务器。
    1. 在用于选择组件的向导页面上，所有管理服务器组件均已预先选中。
    2. 指定 SQL Server 和数据库。决定是否要保留已使用的 SQL Server 数据库以及是否要将现有数据保留在数据库中。

        当您开始安装时，您将丢失故障转移记录服务器功能（请参阅 第 36 页上的故障转移记录服务器（已作说明））。

        如果您在管理服务器上启用了加密，记录服务器会处于离线状态，直到它们升级完毕，而且您启用了对管理服务器的加密（请参阅 第 124 页上的安全通信（已解释））。

2. 升级故障转移记录服务器。在管理服务器的下载网页（由 Download Manager 控制）安装 Recording Server。

    如果您计划在故障转移记录服务器上启用加密，并且希望保留故障转移功能，请在不加密的情况下升级故障转移记录服务器，并在升级记录服务器后启用。

    此时，故障转移服务器的功能将重新可用。

3. 如果您计划从记录服务器或故障转移记录服务器到客户端启用加密，并且客户端在升级期间可以检索数据非常重要，则请在升级记录服务器之前升级从记录服务器检索数据流的所有客户端和服务。这些客户端和服务是：
   - XProtect Smart Client
   - Management Client
   - Management Server
   - XProtect Mobile 服务器
   - XProtect Event Server
   - DLNA Server Manager
   - Milestone Open Network Bridge
   - 通过从记录服务器检索数据流的站点Milestone Interconnect
   - 一些第三方 MIP SDK 集成
4. 升级 recording server。您可以使用安装向导来安装记录服务器（请参阅 第 140 页上的安装记录服务器，通过 Download Manager）或默认安装（请第 146 页上的以静默方式安装 recording server参阅）。静默安装的优点在于您可以执行远程操作。

   > 如果启用加密，并且在运行的所有相关计算机上的所选服务器身份验证证书都不受信任，则它们将丢失连接。有关详细信息，请参阅第124页上的安全通信（已解释）。

继续为您系统中的其他站点执行这些步骤。

在群集中升级

在更新群集之前，确保制作相关数据库的备份。

1. 停止群集中所有管理服务器上的Management Server服务。
2. 卸载群集中所有服务器上的管理服务器。
3. 根据“在群集中安装”所述，使用在群集中安装多台管理服务器的步骤。请参阅第153页上的在群集中安装。

> 安装时，请确保重用现有 SQL Server 和当前存储系统配置的现有 SQL Server 数据库。系统配置会自动升级。

用户界面详情

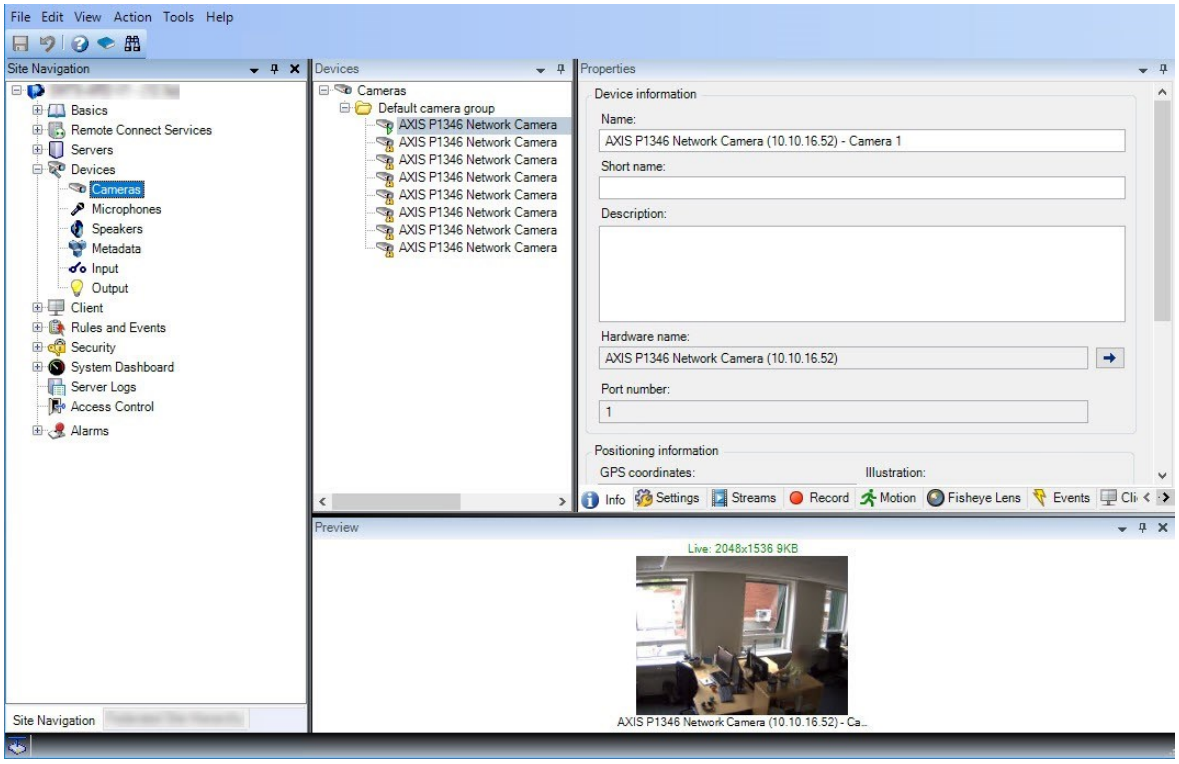
主窗口和窗格

Management Client 窗口分为两个窗格。窗格数和布局取决于：

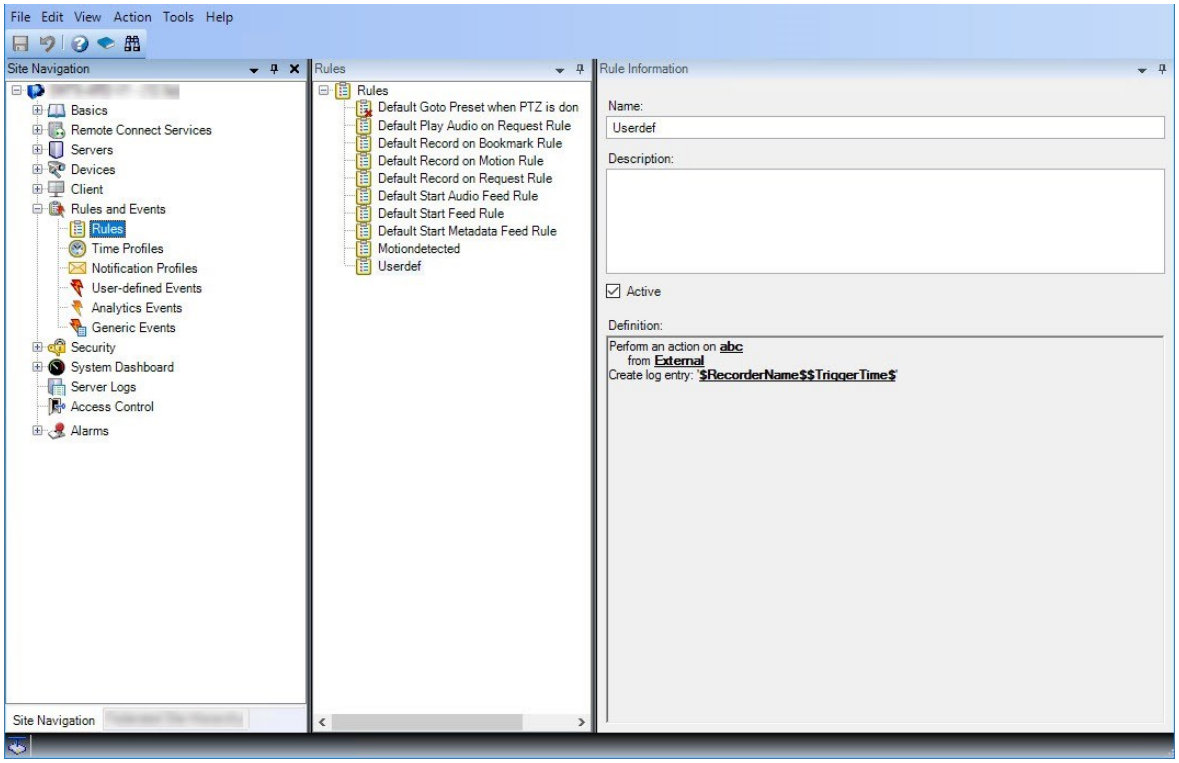
- 系统配置
- 任务
- 可用的功能

以下为一些典型布局的示例：

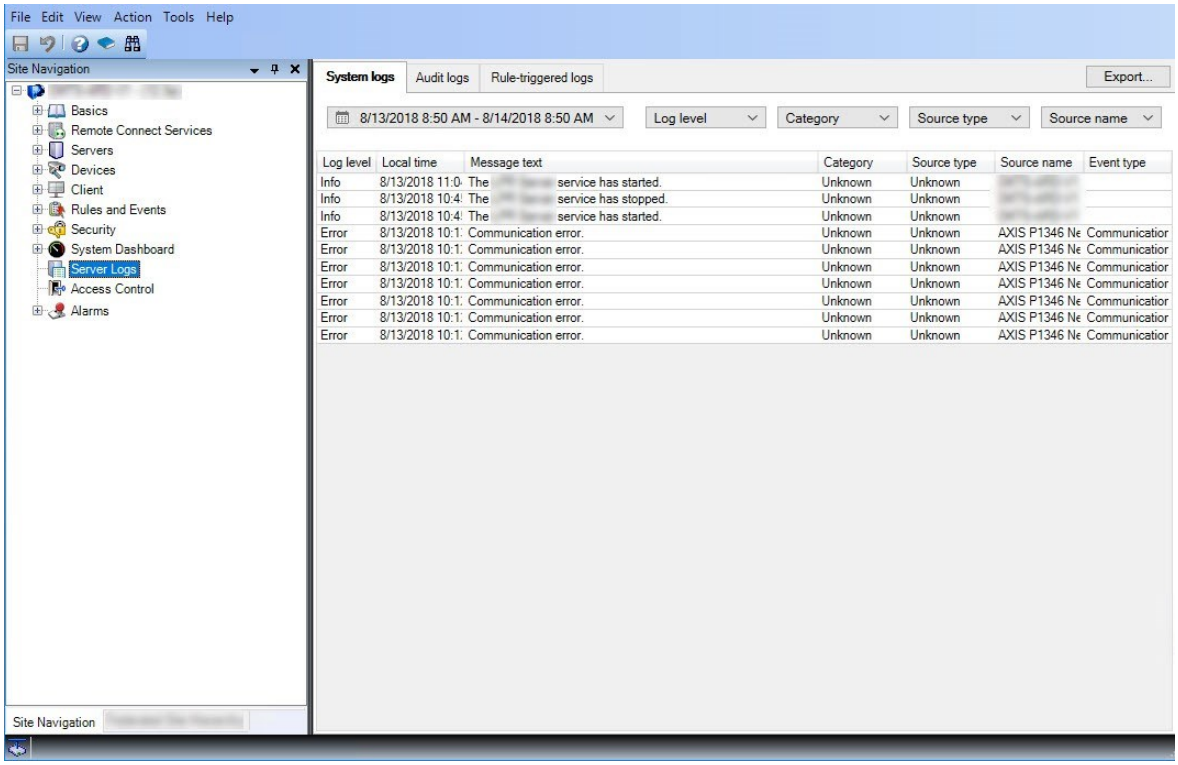
- 使用记录服务器和设备：



- 使用规则、时间和通知配置文件、用户、角色：

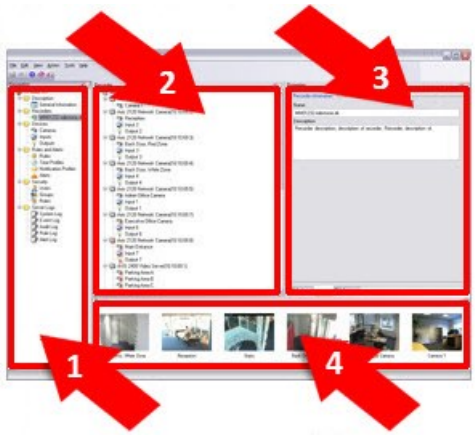


- 查看日志：



窗格布局

图示大致列出了典型的窗口布局。可自定义布局，因此其可能与您计算机上的布局看起来有所不同。



1. “站点导航”窗格和“联合站点层级”窗格
2. 总览窗格
3. 属性窗格
4. 预览窗格

站点导航窗格

这是您在 Management Client 中的主导航元素。其中显示了您所登录的站点的名称、设置和配置。站点名称显示在窗格的顶部。功能按反映软件功能的类别分组。

在**站点导航**窗格中，您可以根据自己的需求来配置和管理系统。如果您的系统不是单站点系统，而是包括联合点，请注意，您可以在**联合站点分层**窗格管理这些站点。

可用的功能取决于正在使用的系统。请参阅 Milestone 网站 (https://www.milestonesys.com/products/software/product-index/) 上产品总览页中的完整功能列表。

“联合站点层级”窗格

该导航元素用于以父项/子项站点层次结构显示所有 Milestone Federated Architecture 站点。

您可以选择任何站点，登录该站点和ManagementClient以使该站点启动。您登录的站点始终位于层次结构的顶部。

总览窗格

提供您在**站点导航**窗格中所选择元素的总览，例如以详细列表的形式显示总览信息。在**总览**窗格中选择了某个元素后，其通常在**属性**窗格中显示属性。右键单击**总览**窗格中的元素即可访问管理功能。

属性窗格

显示在**总览**窗格中所选择元素的属性。这些属性显示在多个专用选项卡中：

预览窗格

使用记录服务器和设备时会出现**预览**窗格。显示来自所选摄像机的预览图像，或显示关于设备状态的信息。示例显示了摄像机预览图像，其中包含关于摄像机实时流分辨率和数据速率的信息。

默认情况下，随预览图像一起显示的信息涉及实时流。它以绿色文本显示在预览上方。**如果想要记录流信息(**红色文本)，则在菜单中选择视图显示记录流。

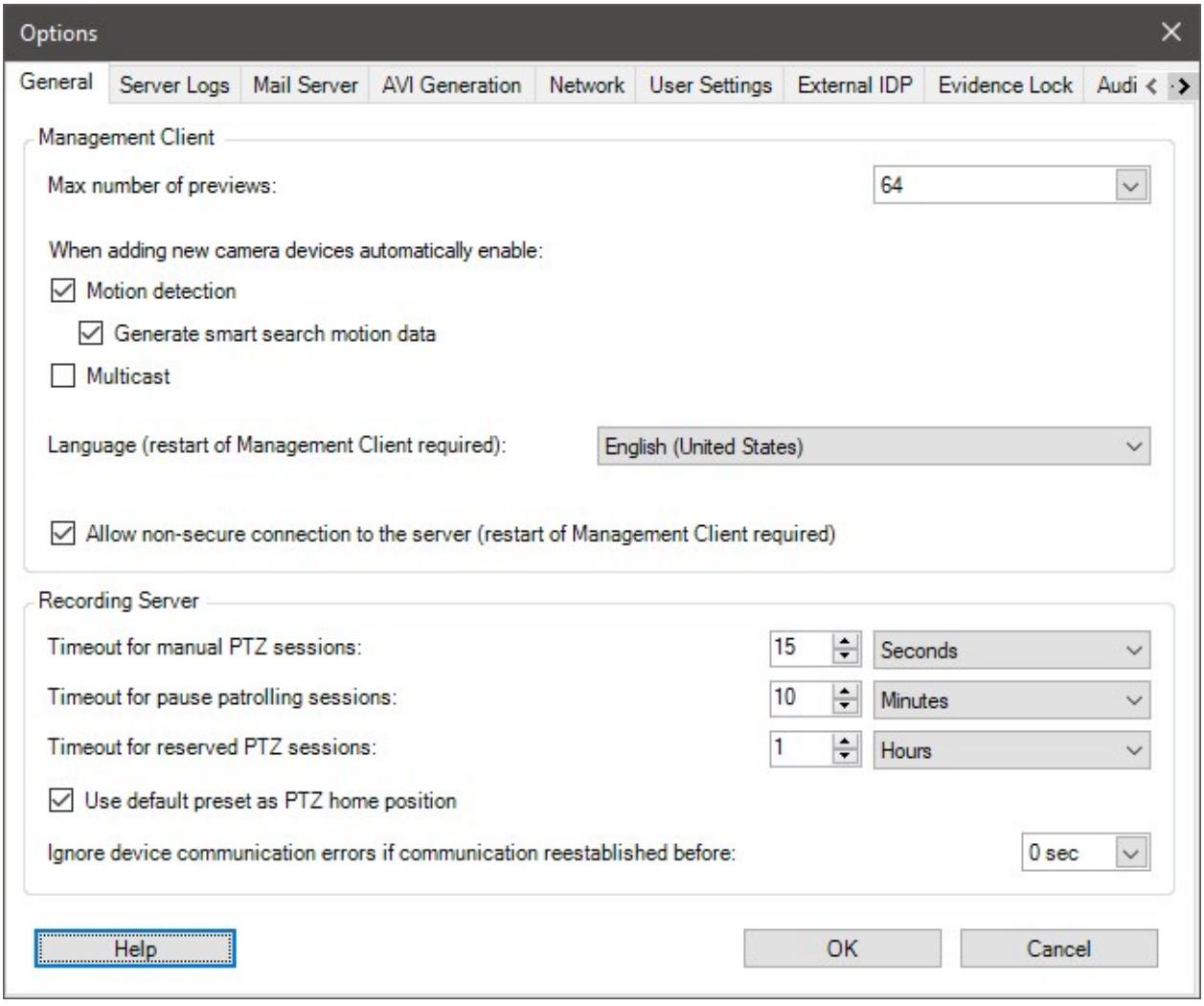
如果**预览**窗格以高帧速率显示多个摄像机的预览图像，则性能会受到影响。**要控制预览图像的数量及其帧速率，**请在菜单中选择选项常规。

系统设置(“选项”对话框)

在**选项**对话框中，可指定与系统的总体外观和功能相关的许多设置。

可用的功能取决于正在使用的系统。请参阅 Milestone 网站 (https://www.milestonesys.com/products/software/product-index/) 上产品总览页中的完整功能列表。

选择**工具 > 选项**即可进入对话框。



“常规”选项卡(选项)

在“常规”选项卡上，您可以指定 Management Client 和记录服务器的常规设置。

Management Client

名称	说明
最大预览数量	**选择**预览窗格中显示的缩略图图像最大数量。默认为 64 个缩略图图像。 从菜单中选择**动作 > 刷新**以使更改生效。 如果将大量缩略图图像与高帧速率结合，则可能降低系统速度。
添加新摄像机设备时自动启用：移动侦测	使用**添加硬件**向导将新摄像机添加至系统时，选中该复选框，可在这些新摄像机上启用移动侦测。 该设置不会影响现有摄像机上的移动侦测设置。 在**移动**选项卡上为摄像机设备启用或禁用摄像机移动侦测。
添加新摄像机设备时自动启用：生成智能搜索的移动数据	要生成智能搜索移动数据，需要启用摄像机的移动侦测功能。 使用**添加硬件**向导将新摄像机添加至系统时，选中该复选框，可在这些新摄像机上启用智能搜索移动数据生成。 该设置不会影响现有摄像机上的移动侦测设置。 在**移动**选项卡上为摄像机设备启用或禁用摄像机的智能搜索移动数据生成。
添加新摄像机设备时自动启用：多播	使用**添加硬件**向导将新摄像机添加至系统时，选中该复选框，可在这些新摄像机上启用多播。 该设置不会影响现有摄像机上的多播设置。 在**客户端**选项卡上为摄像机设备启用或禁用摄像机实时多播。
语言	选择 Management Client 的语言。 重新启动 Management Client 即可使用新语言。
允许与服务器的非安全连接	选中该复选框以允许通过 HTTP 协议进行非安全服务器连接。(不会提示用户允许非安全服务器连接)。 重新启动 Management Client 以使用此设置。

记录服务器

名称	说明
手动 PTZ 会话的超时	具有必需用户权限的客户端用户可手动中断 PTZ 摄像机的巡视。选择在手动中断后恢复常规巡视之前的等待时间。该设置将应用于本系统上的所有 PTZ 摄像机。默认设置为 15 秒。 如果您需要摄像机上的单独超时，可在摄像机的**预设**选项卡中进行此指定。
暂停巡视会话的超时	具有足够高 PTZ 优先级的客户端用户可以在 PTZ 摄像机上暂停巡视。选择在暂停后恢复常规巡视之前的等待时间。该设置将应用于本系统上的所有 PTZ 摄像机。默认设置为 10 分钟。 如果您需要摄像机上的单独超时，可在摄像机的**预设**选项卡中进行此指定。
保留的 PTZ 会话的超时	设置针对保留 PTZ 会话的默认超时时间。当用户运行保留 PTZ 会话时，在 PTZ 摄像机被手动释放或在时间超时之前，PTZ 摄像机无法由其他人使用。默认设置为 1 小时。 如果您需要摄像机上的单独超时，可在摄像机的**预设**选项卡中进行此指定。
使用默认预设作为 PTZ 初始位置	选中此复选框可在客户端中激活**初始位置**按钮时使用默认预设位置而非 PTZ 摄像机的初始位置。 必须为摄像机定义默认预设位置。如果未定义默认预设位置，则在客户端中激活**初始位置**按钮时不会发生任何改变。 默认情况下取消选中此复选框。 要指定默认预设位置，请参阅 第 212 页上的指定摄像机的预设位置作为默认值
如果在以下事件之前重新建立通信，则忽略设备通信错误	系统会记录硬件和设备上的所有通信错误，但您可以在此处选择在规则引擎触发**通信错误**事件之前通信错误必须存在多长时间。

“服务器日志”选项卡(选项)

在服务器日志选项卡上，可指定系统管理服务器日志的设置。

有关详细信息，请参阅识别用户活动、事件、操作和错误。

名称	说明
日志	选择要配置的日志类型： • 系统日志 • 审核日志 • 规则触发日志
设置	禁用或启用日志，并指定保留期限。 允许 2018 R2 和更早版本的组件写入日志。有关详细信息，请参阅允许 2018 R2 和更早版本的组件写入日志。 对于**系统**日志，请指定想要记录的消息级别： • 所有(包括未定义的消息) • 信息、警告和错误 • 警告和错误 • 错误(默认设置) 对于**审核**日志，如果您希望系统记录 XProtect Smart Client 上的所有用户动作，请启用用户访问记录。这些动作包括导出、触发输出、摄像机实时查看或播放等。 指定： • 播放片段的长度 这意味着用户如果在此时段内播放，系统只会生成一个日志条目。如果在此时段外播放，系统则会创建新的日志条目。 • 系统创建日志条目前用户已观看的录像数(帧数)

“邮件服务器”选项卡(选项)

在**邮件服务器**选项卡上，您可以指定系统邮件服务器的设置。
有关详细信息，请参阅通知配置文件(已解释)。

名称	说明
发件人电子邮件地	输入对于所有通知配置文件要显示为电子邮件通知发件人的电子邮件地址。示例：**sender@organization.org**。

名称	说明
址	
邮件服务器地址	输入用于发送电子邮件通知的 SMTP 邮件服务器的地址。示例：**mailserver.organization.org**。
邮件服务器端口	用于连接到邮件服务器的 TCP 端口。对于未加密的连接，默认端口为 25，加密的连接通常使用端口 465 或 587。
将与服务器的连接加密	如果要保护管理服务器与 SMTP 邮件服务器之间的通信，请选中此复选框。 使用 STARTTLS 电子邮件 协议命令保护连接。在此模式下，会话在未加密的连 接上开始，然后 SMTP 邮件 服务器向管理服务器发出 STARTTLS 命令，以切换到使用 SSL 的安全通信。
服务器需要登录	如果启用，您必须指定用户用于登录邮件服务器的用户名和密码。

“AVI 生成”选项卡（选项）

在 **AVI 生成**选项卡上，可指定生成 AVI 视频剪辑文件的压缩设置。如果要将 AVI 文件包含在由规则触发的通知配置文件发送的电子邮件通知中，则需要这些设置。

另请参阅从规则触发电子邮件通知。

名称	说明
压缩程序	选择您想要应用的编码解码器（压缩/解压缩技术）。为了使列表中有更多编码解码器可用，请在管理服务器中先安装这些编码解码器。 并非所有摄像机都支持所有编码解码器。
压缩质量	（并非对于所有编码解码器都可用）。使用滑块选择编码解码器所执行的压缩率 (**0-100**)。 **0** 表示不压缩，这通常会导致图像质量高但文件大小很大。**100** 表示最高压缩，这通常会导致图像质量低但文件大小很小。 如果滑块不可用，则压缩质量完全由所选编码解码器确定。
关键帧频率	（并非对于所有编码解码器都可用）。如果要使用关键帧，则选中该复选框，然后指定关键帧之间的所需帧数。 关键帧是以指定间隔存储的单帧。关键帧是以指定间隔存储的单帧。这样可以大幅缩小文件的大

名称	说明
	小。 如果复选框不可用或者未选中，则每个帧将包含摄像机的整个视图。
数据速率	(并非对于所有编码解码器都可用)。如果要使用特定数据速率，则选中该复选框，然后指定每秒千字节数。 数据速率用于指定所附加 AVI 文件的大小。 如果该复选框不可用或未选中，则数据速率由所选编码解码器确定。

“网络”选项卡(选项)

在**网络**上，如果本地客户端通过互联网连接到记录服务器，可指定该客户端的 IP 地址。监控系统随后将其识别为来自本地网络。

还可指定系统的 IP 版本：IPv4 或 IPv6。默认值为 IPv4。

“书签”选项卡(选项)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

在**书签**选项卡上，您可指定书签的设置、其 ID 以及在 XProtect Smart Client 中的功能。

名称	说明
书签 ID 前缀	指定 XProtect Smart Client 用户制作的所有书签的前缀。
默认书签时间	将书签的默认开始和结束时间指定为在 XProtect Smart Client 中进行设置。 该设置需要与这些内容一致： • 默认的书签规则，请参阅规则(“规则和事件”节点)。 • 有关每个摄像机的预缓冲期间，请参阅管理预缓冲。

要指定角色的书签权限，请参阅 第 456 页上的“设备”选项卡(角色)。

“用户设置”选项卡(选项)

在**用户设置**选项卡上，可指定用户首选项设置，如在启用远程记录时是否显示消息。

外部 IDP 选项卡(选项)

在 Management Client 中的**外部 IDP** 选项卡上，您可以添加和配置外部 IDP 并从外部 IDP 登记索赔。

名称	说明
已启用	外部 IDP 默认启用。
名称	外部 IDP 的名称。这里输入的名称会出现在客户端窗口日志里的**身份验证**字段。
身份验证机构	外部 IDP 的 URL。
添加	添加和配置外部 IDP。当选择**添加**时，**外部 IDP** 对话框会打开，您可以输入配置信息，请参阅表下方的**配置**。
编辑	编辑外部 IDP 配置。
删除	删除外部 IDP 配置。 如果您移除外部 IDP 配置，则通过该配置进行身份验证的用户将无法登录到 XProtect 视频管理软件。如果再次添加，由于外部 IDP 的 ID 已更改，将在登录时创建新用户。

配置外部 IDP

- 若要添加外部 IDP，请在**外部 IDP**部分中选择**添加**，并输入下表中的信息：

名称	说明
名称	这里输入的外部 IDP 名称会出现在客户端窗口中日志里的**身份验证**字段。
客户端 ID 和客户端密	必须从外部 IDP 获取。需要客户端 ID 和客户端密钥才能与外部 IDP 安全通信。

名称	说明
钥	
回拨路径	身份验证 URL 的一部分重定向流量以使用户登录。 用户从外部 IDP 托管的登录页面登录。身份验证过程完成后，将调用此路径，并将用户重定向到 XProtect VMS。 默认值为“/signin-oidc”。 重定向格式 回调路径的URI由管理服务器 FQID 与 /idp/ 一起构建，回调路径配置在外部提供商上。 示例： • XProtect Smart Client 和 XProtect Management Client 的重定向URI格式：[schema]://[management server address]/idp/[callback path] • XProtect Web Client 和 XProtect Mobile 客户端的重定向URI格式：[重定向 Uri 无“/index.html”]/idp/[回调路径] 请注意，回调路径的 "idp" 部分区分大小写，必须以小写字母输入。
提示登录	如果用户应保持登录状态或如果需要对用户进行验证，则指定外部 IDP。根据外部 IDP，验证可以包含密码验证或完整登录。
用于创建用户名的索赔	可选择指定应使用外部 IDP 中的哪个索赔来为 VMS 中自动配置的用户生成唯一的用户名。有关索赔生成的唯一用户名的详细信息，请参阅 外部 IDP 用户的唯一用户名。
范围	或者，使用范围限制您从外部 IDP 获得的索赔数量。如果知道与您的 VMS 相关的索赔处于特定范围内，则可以用范围来限制可以从外部 IDP 获得的索赔数量。

注册索赔

当您注册了来自外部 IDP 的索赔时，可以将索赔映射到 VMS 中的角色，以决定 VMS 中的用户特权。有关详细信息，请参阅映射来自外部 IDP 的索赔。

- 若要注册来自外部 IDP 的索赔，请在**已注册索赔**部分中选择**添加**，并输入下表中的信息：

名称	说明
外部 IDP	外部 IDP 的名称。

名称	说明
声明名称	自由文本的索赔名称。名称将在选择角色时可用。
显示名称	索赔的显示名称。
区分大小写	表明索赔的值是否区分大小写。 通常区分大小写的值示例： - ID 的文本再现，如 GUID：F951B1F0-2FED-48F7-88D3-49EB5999C923 或 OadFgrDesdFesff= 通常不区分大小写的值示例： - 电子邮件地址 - 角色名称 - 组名称 .
添加、编辑、移除	注册和保持索赔。 如果您在外部 IDP 网站修改索赔，用户需要重新登录 XProtect 客户端。比如说，用户 Bob 需要成为，例如，操作员。索赔随后会在外部 IDP 网站添加给 Bob，但如果 Bob 已经登录至 XProtect，他必须完成新的登录才能使更改生效。

添加 Web 客户端的重定向 URI

重定向 URI 是用户成功登录后重定向的位置。重定向 URI 必须与 Web 客户端的地址完全匹配。例如，如果您从 **https://localhost:8082/index.html** 打开 XProtect Web Client 并且您添加的 Web 客户端的重定向 URI 是 **https://127.0.0.1:8082/index.html**，您将无法通过外部 IDP 登录。

名称	说明
URI	格式为 **https://[mobile server]:[port]/index.html** 的 XProtect Web Client URI。重定向 URI 不区分大小写。
添加、编辑、移除	注册和维护重定向 URI。 移除 URI 时，必须至少保留一个重定向 URI，系统才能正常工作。

“客户仪表板”选项卡(选项)

在**客户仪表板**选项卡上,您可以启用或禁用 Milestone Customer Dashboard。

客户仪表板是一个在线监控服务,用于向系统管理员或具有系统安装相关信息访问权限的其他人员提供系统当前状态(包括可能的技术问题,如摄像机故障)的图形总览。

可随时选中或清除复选框以更改“客户仪表板”设置。

“证据锁定”选项卡(选项)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

在**证据锁定**选项卡上,定义和编辑证据锁定配置文件以及客户端用户可以选择来使数据保持保护状态的持续时间。

名称	说明
证据锁定配置文件	包含已定义证据锁定配置文件的列表。 可以添加和删除现有证据锁定配置文件。无法删除默认证据锁定配置文件,但可以更改其时间选项和名称。
锁定时间选项	客户端用户可以选择的、锁定证据的持续时间。 可用时间选项为小时、天、周、月、年、无限或用户定义。

若要指定角色的证据锁定访问权限,请参阅角色设置的 第 456 页上的“设备”选项卡(角色)。

“音频消息”选项卡(选项)

在**音频消息**选项卡上,您可以上传包含用于广播消息并由规则触发的音频消息的文件。

最多可上传 50 个文件,每个文件的大小不超过 1 MB。

名称	说明
名称	提供消息的名称。在添加消息时输入名称。要将消息上传到系统,请单击**添加**。

名称	说明
说明	提供消息的说明。 在添加消息时输入说明。您可以使用“说明”字段说明目的或实际消息。
添加	可用于将音频消息上传至系统。 支持标准 Windows 音频文件格式： • .wav • .wma • .flac
编辑	可用于修改名称和说明，或者可以更换实际文件。
删除	从列表中删除音频消息。
播放	单击此按钮可从运行 Management Client 的计算机中听取音频消息。

要创建触发音频消息播放的规则，请参阅添加规则。

要详细了解可以在规则中采用的大致动作，请参阅操作和停止操作。

“隐私设置”选项卡

在**隐私设置**选项卡上，您可以启用或禁用 XProtect Mobile Server、XProtect Mobile 客户端、XProtect Web Client 和 XProtect Smart Client 中的使用数据收集。然后单击**确定**。

> 启用使用数据收集，即表示您同意 Milestone Systems 使用 Google 作为第三方技术提供商，不能排除在美国进行数据处理。有关数据保护和使用数据收集的更多信息，请参阅 GDPR 隐私指南。

“访问控制设置”选项卡(选项)

> 要使用 XProtect Access，您必须购买允许访问此功能的基本许可证。

名称	说明
显示开发属性面板	如果选中，会为 **访问控制 > 常规设置**显示额外的开发人员信息。 此设置只能由访问控制系统集成的开发人员使用。

“分析事件”选项卡(选项)

在**分析事件**选项卡上，可启用并指定分析事件功能。

名称	说明
启用	指定您是否要使用分析事件。默认情况下，禁用该功能。
端口	指定此功能使用的端口。默认端口号是 9090。 确保相关 VCA 工具提供商也使用此端口号。如果您更改端口号，请确保提供商也更改其端口号。
所有网络地址或**指定的网络地址**	指定是允许来自所有 IP 地址/主机名的事件，还是只允许来自**地址列表**中指定 IP 地址/主机名的事件(请参阅以下内容)。
地址列表	指定受信任 IP 地址/主机名的列表。该列表可筛选输入数据，从而只允许来自特定 IP 地址/主机名的事件。可使用域名系统 (DNS)、IPv4 和 IPv6 地址格式。 您可以通过手动输入每个 IP 地址或主机名或者通过导入外部地址列表来将地址添加到列表中。 • **手动输入**：在地址列表中输入 IP 地址/主机名。对每个所需地址重复上述步骤 • **导入**：单击**导入**以浏览外部地址列表。外部列表必须是 .txt 文件，并且每个 IP 地址或主机名必须在单独的行上

“警报和事件”选项卡(选项)

在**警报和事件**选项卡上，您可指定警报、事件和日志的设置。与这些设置相关，另请参阅 第 110 页上的限制数据库的大小。

名称	说明
保留其已关闭警报	指定对数据库中状态为**关闭**的警报进行存储的天数。若将该值设为 **0**，则该警报在关闭后即遭删除。 警报始终具有时间标记。如果警报由摄像机触发，则时间标记具有来自警报时间的图像。警报信息本身存储在事件服务器中，对应于附加图像的视频记录则存储在相关监控系统服务器中。 为了能够查看警报图像，视频记录的保留时间应至少为将在事件服务器上保留警报的时间。
保留其所有其他警报	指定对数据库中状态为**新建**、**正在进行**或**保持**的警报进行存储的天数。若将该值设为 0，则警报会显示在系统中，但不会存储。 警报始终具有时间标记。如果警报由摄像机触发，则时间标记具有来自警报时间的图像。警报信息本身存储在事件服务器中，对应于附加图像的视频记录则存储在相关监控系统服务器中。 为了能够查看警报图像，视频记录的保留时间应至少为将在事件服务器上保留警报的时间。
保留日志	指定保留事件服务器日志的天数。若您要长期保留日志，请确保安装事件服务器的机器具有足够的磁盘空间。
启用详细日志记录	若要保留事件服务器通信更详细的日志，请选中该复选框。系统会将其存储**保留日志**字段中指定的天数。
事件类型	指定在数据库中存储事件的天数。有两种定位方式： • 您可以指定整个事件组的保留时间。值为**关注组**的事件类型将继承事件组的值 • 即使已设置事件组的值，也可以指定各事件类型的保留时间。 若该值是 **0**，则事件不会存储在数据库中。 外部事件(用户定义的事件、常规事件和输入事件)默认设置为 **0**，该值无法更改。因为这些事件类型的出现频率极高，将它们存储在数据库中可能会导致性能问题。

“常规事件”选项卡(选项)

在**常规事件**选项卡上,可指定与常规事件和数据源相关的设置。

有关如何配置实际常规事件的详细信息,请参阅常规事件(已解释)。

名称	说明
数据源	可在两种默认数据源之间进行选择,也可定义自定义数据源。具体选择取决于第三方程序和/或您想要联接的硬件或软件: **兼容性**:启用出厂默认设置,回显所有字节,TCP 和 UDP,仅 IPv4,端口 1234,无分隔符,仅本地主机,当前代码页编码 (ANSI)。 **国际**:启用出厂默认设置,仅回显统计信息,仅 TCP,IPv4+6,端口 1235,<CR><LF> 作为分隔符,仅本地主机,UTF-8 编码。(<CR><LF> = 13,10)。 [数据源 A] [数据源 B] 等等。
新建	单击以定义新数据源。
名称	数据源的名称。
已启用	数据源默认禁用。选中该复选框可启用数据源。
重设	单击以重设所选数据源的所有设置。在**名称**字段中输入的名称将保持。
端口	数据源的端口号。
协议类型选择器	系统应监听并分析以用来侦测常规事件的协议: **任何**:TCP 及 UDP。 **TCP**:仅 TCP。 **UDP**:仅 UDP。 在用于常规事件的 TCP 和 UDP 数据包中,可以包含特殊字符,如 @、#、+、~ 等。
IP 类型选择器	可选择的 IP 地址类型:IPv4、IPv6 或两者皆可。
分隔符字节	选择用于分隔各个常规事件录像的分隔符字节。数据源类型**国际**(请参阅前面的**数据源**)的

名称	说明
	默认值为 **13,10**。(13,10 = <CR><IF>)。
回声类型选择器	可用的回声返回格式： • **回显统计信息**：回显以下格式：**[X],[Y],[Z],[常规事件的名称]** **[X]** = 请求编号。 **[Y]** = 字符数。 **[Z]** = 匹配常规事件的数量。 **[常规事件的名称]** = 在**名称**字段中输入的名称。 • **回显所有字节**：回显所有字节 • **无回显**：抑制所有回显
编码类型选择器	默认情况下，列表仅显示最相关的选项。选中**全部显示**复选框可显示所有可用编码。
允许的外部 IPv4 地址	指定 IP 地址，管理服务器必须能够与该地址通信才能管理外部事件。也可使用此功能排除您不希望从中获取数据的 IP 地址。
允许的外部 IPv6 地址	指定 IP 地址，管理服务器必须能够与该地址通信才能管理外部事件。也可使用此功能排除您不希望从中获取数据的 IP 地址。

组件节点

Management Client 菜单

文件菜单

可将更改保存到配置并退出应用程序。您还可以备份您的配置，请参阅 第 286 页上的关于备份和还原系统配置(已解释)。

编辑菜单

可撤销更改。

查看菜单

名称	说明
重设应用程序布局	将 Management Client 中不同窗格的布局重设为其默认设置。
预览窗口	**在使用记录服务器和设备时开启和关闭**预览窗格。
显示记录流	**默认情况下**，预览窗格中随预览图像一起显示的信息涉及摄像机的实时流。**如果需要关于记录流的信息**，请选择显示记录流。
联合站点层级	**默认情况下**，启用联合站点层级窗格。
站点导航	**默认情况下**，启用站点导航窗格。

动作菜单

动作菜单的内容根据您在**站点导航**窗格中所选的元素而有所不同。可选择的动作与右键单击元素时的动作相同。

有关每个摄像机的预缓冲期间，请参阅管理预缓冲。

名称	说明
刷新	始终可用，用于从管理服务器重新载入请求的信息。

工具菜单

名称	说明
已注册服务	管理已注册服务。 请参阅 第 309 页上的管理已注册服务。
有效角色	用于查看所选用户或组的所有角色。
选项	用于打开“选项”对话框，可在其中定义和编辑全局系统设置。有关详细信息，请参阅 第 331 页上的系统设置(“选项”对话框)。

帮助菜单

可访问帮助系统和关于 Management Client 版本的信息。

Server Configurator(实用工具)

“加密”选项卡属性

此选项卡允许您指定以下属性:

> 在群集环境中,在为群集环境中的所有计算机创建证书之前,必须设置群集并确保其正在运行。之后,您可以安装证书并使用 Server Configurator 进行群集中所有节点的注册。有关详细信息,请参阅有关如何保护 XProtect VMS 安装的证书指南。

名称	说明	任务
服务器证书	选择要用于对管理服务器、Data Collector server、日志服务器和录制服务器之间的双向连接进行加密的证书。	从管理服务器启用加密或将加密应用到管理服务器 为记录服务器或远程服务器启用服务器加密
事件服务器和扩展	选择用于以对事件服务器和与事件服务器 通信的组件之间的双向连接进行加密的证书,包括 LPR Server。	第 263 页上的启用事件服务器加密
流媒体证书	选择要用来加密记录服务器与从记录服务器检索数据流的所有客户端、服务器和集成之间的通信的证书。	对客户端和服务器启用加密
移动流媒体证书	选择证书以加密移动设备服务器与从移动设备服务器检索数据流的 移动客户端和 Web 客户端之间的通信。	在移动设备服务器上启用加密

注册服务器

名称	说明	任务
管理	管理服务器的地址通常包括计算机的主机名或完全限	有关从安装了管理服务器的计算机更改

名称	说明	任务
服务器地址	定域名 (FQDN)。 默认情况下，此地址仅在计算机上未安装管理服务器的 XProtect VMS 中处于活动状态。 根据经验，不应从安装了管理服务器的计算机上更改管理服务器地址。 但是，例如，如果在故障转移设置中使用 Server Configurator，则可能必须从管理服务器计算机更改地址。这项操作可以在群集故障转移环境中，也可以在其他故障转移设置方案中。 • 要从安装了管理服务器的计算机激活**管理服务器地址**字段，请单击钢笔 ( ) 符号。 ⚠ 如果更新管理服务器地址，则需要访问已安装组件的每个计算机并使用新地址信息更新管理服务器地址。	管理服务器地址的含义的详细信息，请单击： 更改管理服务器计算机的主机名
注册	向指定的管理服务器注册计算机上正在运行的服务器。	注册记录服务器

语言选择

使用此选项卡选择 Server Configurator 语言。Server Configurator 的语言集对应于 Management Client 的语言集。

名称	说明
选择语言	选择用户界面的语言。

如果您在故障转移群集环境中工作，建议您在 Server Configurator 中启动任务。这是因为在应用更改时 Server Configurator 可能需要停止服务，并且故障转移群集环境可能会干扰此操作。

托盘图标状态

表格中的托盘图标显示了 XProtect VMS 中运行在服务器上的服务的不同状态。这些图标可在安装了服务器的计算机上使用：

Management Server Manager 托盘图标	Recording Server Manager 托盘图标	Event Server Manager 托盘图标	Failover Recording Server Manager 托盘图标	说明
				**运行中** 启用并启动服务器服务时出现。 如果 Failover Recording Server 服务在运行，则在标准记录服务器出现故障时它可以接管。
				**已停止** 服务器服务已停止运行时出现。 如果 Failover Recording Server 服务停止运行，则在标准记录服务器出现故障时它无法接管。
				**启动** 服务器服务正在启动时出现。在正常情况下，托盘图标会在短时间后变为**正在运行**。
				**停止** 服务器服务正在停止运行时出现。在正常情况下，托盘图标会在短时间后变为**已停**

Management Server Manager 托盘图标	Recording Server Manager 托盘图标	Event Server Manager 托盘图标	Failover Recording Server Manager 托盘图标	说明
				止。
				**处于不确定状态** 初次加载服务器服务时出现，直到收到第一条信息，在此基础上，托盘图标在正常情况下会更改为**启动**，然后更改为**运行**。
				**脱机运行** 通常在记录服务器或故障转移记录服务正在运行但 Management Server 服务未运行时出现。

从托盘图标开始和停止服务

右键单击通知区域中的图标以打开托盘图标，您可以在其中启动和停止服务。

- 启动或停止 Management Server 服务
- 启动或停止 Recording Server 服务

Management Server Manager(托盘图标)

使用 Management Server Manager 托盘图标上的菜单项从 Management Server Manager 中执行任务。

名称	说明
开始Management Server和停止Management Server	单击适当的菜单项以启动或停止 Management Server 服务。如果停止 Management Server 服务，您将无法使用 Management Client。 服务状态由托盘图标反映。有关托盘图标的状态的详细信息，请参阅服务器管理器托盘图标(已作说明) 。
显示状态消息	查看带有时间戳的状态消息列表。
更改系统配置密码设置	分配或更改系统配置密码。您还可以选择删除系统配置密码，不对系统配置进

名称	说明
	行密码保护。 更改系统配置密码设置
输入系统配置密码	输入密码。例如，如果保存密码设置的文件被删除或损坏，则适用此规则。有关详细信息，请参阅输入系统配置密码设置。
配置故障转移管理服务器	启动故障转移管理服务器配置向导或打开**管理您的配置**页面以管理您现有的配置。有关故障转移群集的详细信息，请参阅 第 35 页上的XProtect Management Server Failover 。
Server Configurator	打开 **Server Configurator** 以注册服务器并管理加密。有关管理加密的详细信息，请参阅使用 Server Configurator 管理加密。
更改许可证	在管理服务器计算机上，更改软件许可证号。您将需要输入新的许可证代码，例如，在升级您的 XProtect 系统时。有关详细信息，请参阅更改软件许可证号。
还原配置	打开一个对话框，您可以在其中还原系统配置。请确保已阅读对话框中的信息，然后单击**还原**。有关详细信息，请参阅从手动备份中恢复系统配置。
选择共享备份文件夹	在备份任何系统配置之前，请设置一个备份文件夹以存储备份。有关详细信息，请参阅选择共享备份文件夹。
更新 SQL 地址	打开向导以更改 SQL Server 地址。在主机名更改的极少数情况下，可能需要使 SQL Server 地址符合更改。有关详细信息，请参阅 主机名更改可以触发 SQL 服务器地址更改。

基本节点

许可证信息(“基本”节点)

在**许可证信息**窗口中，您可以跟踪在此站点和所有其他站点上共享相同软件许可证文件的所有许可证、您的 Milestone Care 订阅，并确定要如何激活许可证。

要了解更多有关**许可证信息**窗口中可用的各种信息和功能的详情，请参阅 第 107 页上的“许可证信息”窗口。

站点信息(“基本”节点)

在具有许多子站点的大型 Milestone Federated Architecture 设置中，很容易失去总览，并且可能很难找到每个子站点的管理员的联系信息。

因此，您可以将附加信息添加到每个子站点，然后该信息可供中央站点上的管理员使用。

可以添加以下信息：

- 站点名
- 地址/位置
- 管理员
- 其他信息

远程连接服务节点

Axis One-click 摄像机连接(“远程连接服务”节点)

这些是 Axis One-Click 摄像机连接属性。

名称	说明
摄像机密码	输入/编辑。购买时随摄像机一起提供。有关更多详细信息，请参阅摄像机手册或访问 Axis 网站 (https://www.axis.com/)。
摄像机用户	查看详细信息以获取**摄像机密码**。
说明	输入/编辑摄像机的说明。
外部地址	输入/编辑摄像机连接的 ST 服务器的网址。
内部地址	输入/编辑录制服务器连接的 ST 服务器的网址。
名称	如果需要，请编辑项目的名称。
所有者身份验证密钥	请参阅**摄像机密码**。
密码(用于分派服务器)	输入密码。必须与从系统提供商处收到的密码相同。
密码(用于 ST 服务器)	输入密码。必须与安装 Axis One-Click Connection 组件时输入的用户名相同。
在 Axis 分派服务上注册/注销	指明您是否希望将 Axis 摄像机注册到 Axis 分派服务。可以在安装之时或之后完成。
序列号	由制造商指定的硬件序列号。序列号通常但并非总是与 MAC 地址一致。

名称	说明
使用凭据	如果您决定在安装 ST 服务器期间使用凭据，请选中该复选框。
用户名(用于分派服务器)	输入用户名。该用户名必须与从系统提供商处收到的用户名相同。
用户名(用于 ST 服务器)	输入用户名。必须与安装 **Axis One-Click Connection 组件时**输入的用户名相同。

服务器节点

服务器(节点)

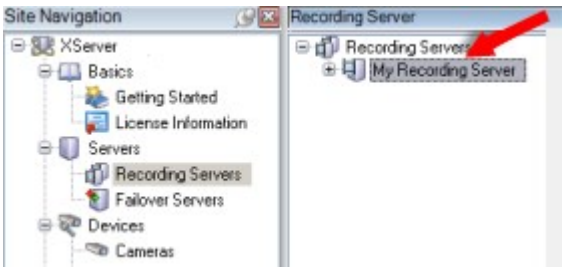
本节将介绍如何安装和配置记录服务器和故障转移记录服务器。您还将学习如何将新硬件添加到系统以及如何互连其他站点。

- 第 353 页上的记录服务器(“服务器”节点)
- 第 364 页上的故障转移服务器(“服务器”节点)

记录服务器(“服务器”节点)

该系统使用记录服务器记录视频馈送，并与摄像机和其他设备通信。监控系统通常由多个记录服务器组成。

记录服务器是已安装 Recording Server 软件并将其配置为与管理服务器通信的计算机。当您展开**服务器**文件夹然后选择**记录服务器**时，可以在**总览**窗格中看到您的记录服务器。



对于早于此管理服务器版本的版本，与录制服务器的向后兼容性将受到限制。您仍可访问旧版本记录服务器上的记录；但如果要更改其配置，请确保它们与该管理服务器版本匹配。Milestone 建议将系统中的所有记录服务器升级至与您的管理服务器相同的版本。

“记录服务器设置”窗口

右键单击 Recording Server Manager 托盘图标并选择**更改设置**时，可以指定以下内容：

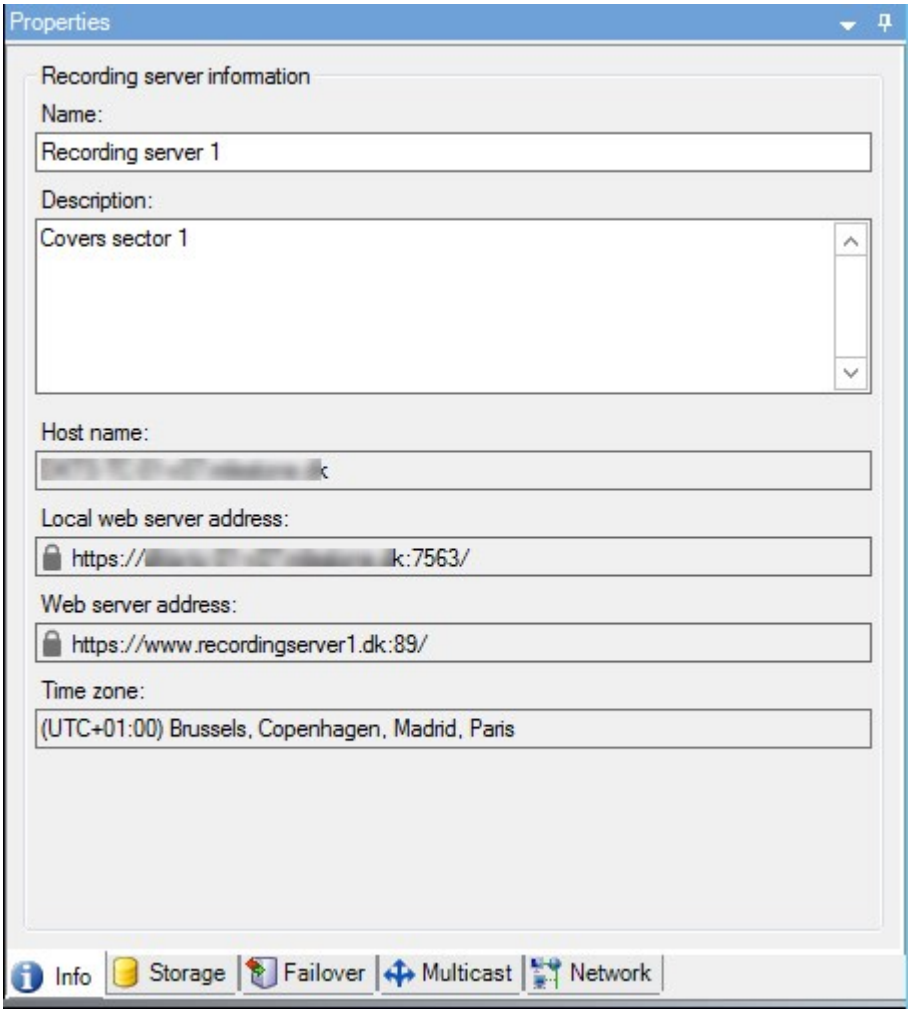
名称	说明
地址	IP 地址(示例:记录服务器应连接的管理服务器的 123.123.123.123) 或主机名(示例:ourserver)。该信息是必需的,以便记录服务器可以与管理服务器通信。
端口	在与管理服务器通信时要使用的端口号。默认为端口 9000。可根据需要进行更改。
Web 服务器端口	用于处理 Web 服务器请求的端口号,例如,处理 PTZ 摄像机控制命令以及来自 XProtect Smart Client 的浏览和实时请求。默认为端口 7563。可根据需要进行更改。
提醒服务器端口	记录服务器监听 TCP 信息时要使用的端口号(某些设备使用 TCP 发送事件消息)。默认为端口 5432(默认为禁用状态)。可根据需要进行更改。
SMTP 服务器端口	记录服务器监听简单邮件传输协议 (SMTP) 信息时使用的端口号。SMTP 是在服务器之间发送电子邮件的标准。某些设备使用 SMTP 通过电子邮件将事件消息或图像发送到监控系统服务器。默认为端口 25,您可以启用和禁用该端口。可根据需要更改端口号。
将从管理服务器到录制服务器的连接加密	在启用加密并从列表中选择服务器身份验证证书之前,请确保首先在管理服务器上启用加密,并且管理服务器证书在记录服务器上受信任。 有关详细信息,请参阅 第 124 页上的安全通信(已解释)。
加密流式传输数据的客户端和服务的连接	在启用加密并从列表中选择服务器身份验证证书之前,请确保该证书在运行从记录服务器检索数据流的服务的所有计算机上都是受信任的。 XProtect Smart Client 和所有服务(从记录服务器检索数据流)必须升级 2019 R1 或更高版本。使用 2019 R1 之后的 MIP SDK 版本创建的某些第三方解决方案可能需要更新。 有关详细信息,请参阅 第 124 页上的安全通信(已解释)。 要验证您的记录服务器是否使用加密,请参阅 第 251 页上的查看客户端的加密状态。
详细信息	查看有关所选证书的 Windows 证书存储信息。

记录服务器属性

“信息”选项卡(记录服务器)

在**信息**选项卡上,您可以验证或编辑记录服务器的名称和说明。

您可以查看主机名和地址。Web 服务器地址前面的挂锁图标表示与从该记录服务器检索数据流的客户端和服务的通信已经过加密。



名称	说明
名称	您可以选择输入记录服务器的名称。列出记录服务器时，将在系统和客户端中使用该名称。名称不要求是唯一的。 重命名记录服务器时，名称将在 Management Client 中全局更改。
说明	您可以选择输入系统内多个列表中显示的说明。说明不是必填项。
主机名称	显示记录服务器的主机名。
本地 Web 服务器地址	显示记录服务器的 Web 服务器的本地地址。例如，您可以使用本地地址来处理 PTZ 摄像机控制命令，并处理来自 XProtect Smart Client 的浏览和实时请求。 该地址包括用于 Web 服务器通信的端口号（通常为端口 7563）。

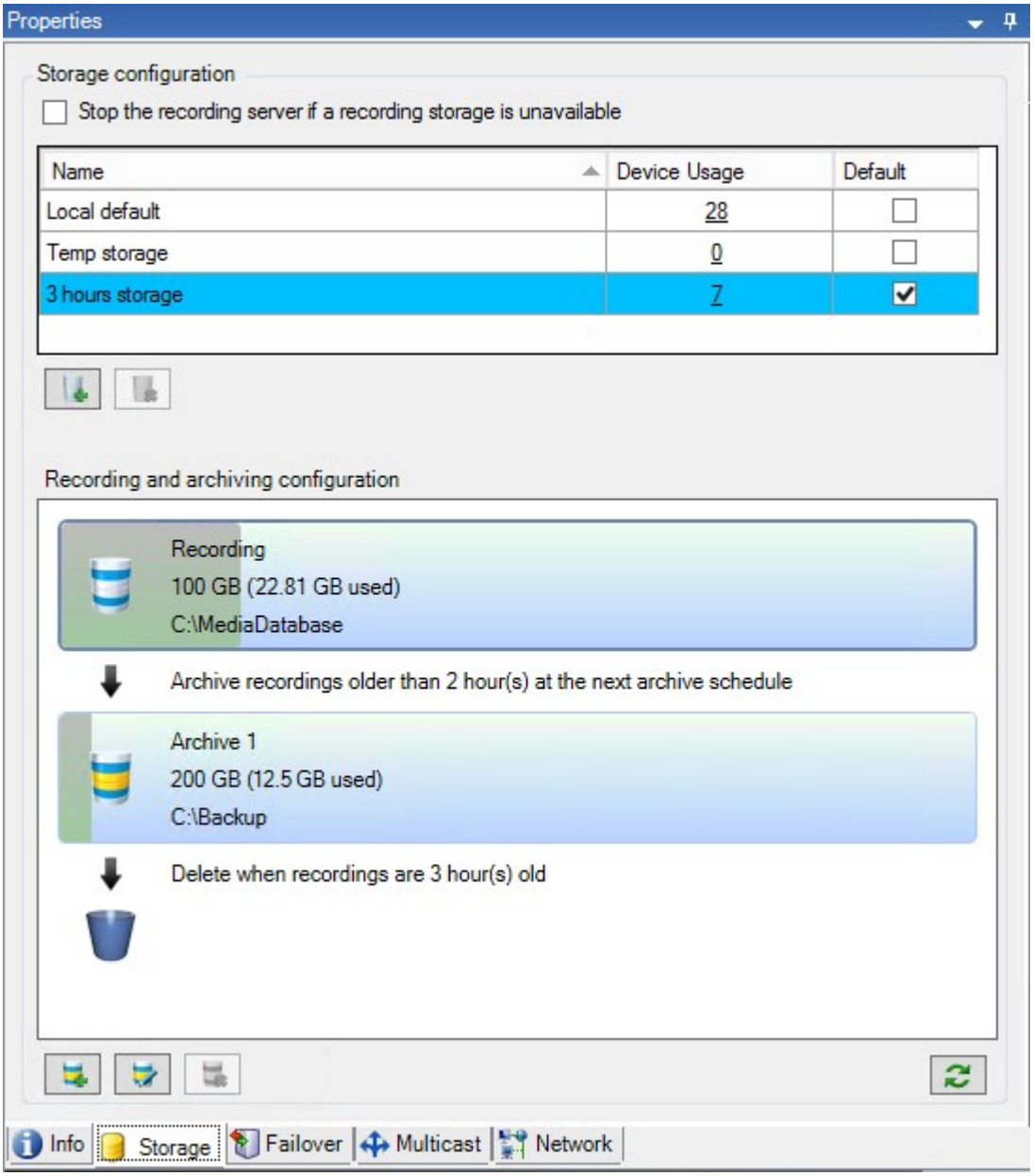
名称	说明
	如果对从记录服务器检索数据流的客户端和服务器启用加密，则会显示挂锁图标，并且地址包括 **https**，而非 **http**。
Web 服务器地址	显示 Internet 上记录服务器的 Web 服务器的公共地址。 如果您的安装使用防火墙或 NAT 路由器，请输入防火墙或 NAT 路由器的地址，以便在 Internet 上访问监控系统的客户端可以连接到记录服务器。 您可以在**网络**选项卡上指定公共地址和端口号。 如果对从记录服务器检索数据流的客户端和服务器启用加密，则会显示挂锁图标，并且地址包括 **https**，而非 **http**。
时区	显示记录服务器所在的时区。

“存储”选项卡(记录服务器)

在**存储**选项卡上，您可以设置、管理和查看所选记录服务器的存储。

对于记录存储和存档，横条显示当前的可用空间量。如果记录存储不可用，您可以指定记录服务器的行为。如果您的系统包含故障转移服务器，这最为常用。

如果您正在使用**证据锁定**，则会显示一条垂直的红线，指明证据锁定脚本使用的空间。



存储和记录设置属性

可用的功能取决于正在使用的系统。请参阅 Milestone 网站 (https://www.milestonesys.com/products/software/product-index/) 上产品总览页中的完整功能列表。

在**存储和记录设置**对话框中，指定以下内容：

名称	说明
名称	如果需要，重命名存储。名称必须是唯一的。
路径	指定在该存储中保存记录的目录的路径。存储不必位于记录服务器计算机上。 如果目录不存在，可自行创建。必须使用 UNC（通用命名约定）格式指定网络驱动器，例如：`\\server\volume\directory\`。
保留时间	指定记录在被删除或移动至下一存档（具体取决于存档设置）之前应在存档中保留多长时间。 保留时间必须始终长于上个存档或默认记录数据库的保留时间。这是因为指定的存档保留天数包含之前在该过程中声明的所有保留时间。
最大大小	选择有关记录数据库中保存的记录数据的最大吉字节数 (GB)。 超出指定吉字节数的记录数据将自动移动至列表中的第一个存档（如果已指定）或被删除。 ⚠ 如果空闲空间小于 5GB，系统始终会将数据库中最旧的数据自动存档（如果未定义下一个存档，则将其删除）。如果空闲的空间不到 1GB，则会将数据删除。数据库始终需要 250MB 的空闲空间。达到此限制的情况下（如果未能足够快地删除数据），在释放足够的空间之前，不会将更多数据写入数据库。数据库的实际最大大小是您指定的吉字节数减去 5GB。
登录	对记录启用数字签名。这意味着，例如，系统会确认导出的视频在播放时未被修改或篡改。 系统采用 SHA-2 算法进行数字签名。
加密	选择记录的加密等级： • 无 • 弱（使用较少 CPU） • 强（使用较多 CPU） 系统采用 AES-256 算法加密。 如果您选择**弱**，则会加密部分录制内容。如果您选择**强**，则会加密整个录制内容。 如果您选择启用加密，还必须在下方指定密码。
密码	为允许查看加密数据的用户输入密码。 Milestone 建议您使用强密码。强密码不包含任何能在字典中找到或属于用户姓名一部分的字词。它们包括八个或更多的字母数字字符、大小写和特殊字符。

存档设置属性

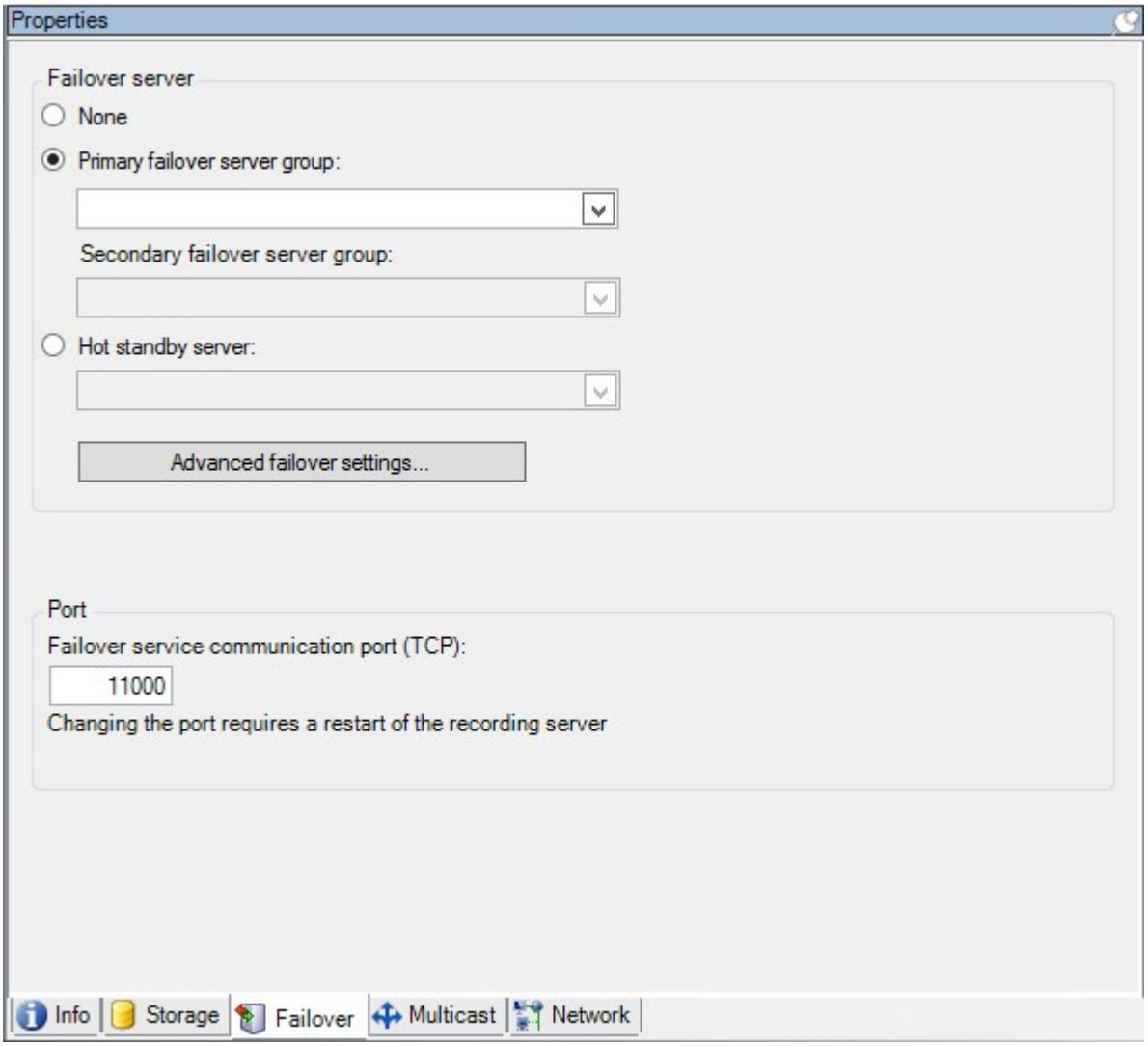
在**存档设置**对话框中，指定以下内容：

名称	说明
名称	如果需要，重命名存储。名称必须是唯一的。
路径	指定在该存储中保存记录的目录的路径。存储不必位于记录服务器计算机上。 如果目录不存在，可自行创建。必须使用 UNC（通用命名约定）格式指定网络驱动器，例如：\\server\volume\directory\.
保留时间	指定记录在被删除或移动至下一存档（具体取决于存档设置）之前应在存档中保留多长时间。 保留时间必须始终长于上个存档或默认记录数据库的保留时间。这是因为指定的存档保留天数包含之前在该过程中声明的所有保留时间。
最大大小	选择有关记录数据库中保存的记录数据的最大吉字节数 (GB)。 超出指定吉字节数的记录数据将自动移动至列表中的第一个存档（如果已指定）或被删除。 如果空闲空间小于 5GB，系统始终会将数据库中最旧的数据自动存档（如果未定义下一个存档，则将其删除）。如果空闲的空间不到 1GB，则会将数据删除。数据库始终需要 250MB 的空闲空间。达到此限制的情况下（如果未能足够快地删除数据），在释放足够的空间之前，不会将更多数据写入数据库。数据库的实际最大大小是您指定的吉字节数减去 5GB。
时间表	指定阐明存档过程的启动间隔的存档计划。存档的频率可以很高（原则上为全年每小时一次），也可以很低（例如，每 36 个月的第一个星期一）。
降低帧速率	要在存档时降低 FPS，请选中**降低帧速率**复选框，并设置每秒帧数 (FPS)。 按选择的 FPS 数降低帧速率将使记录占用较少的存档空间，但这同样会降低存档的质量。MPEG-4/H.264/H.265 会自动缩减至关键帧（最小）。 0.1 = 每 10 秒 1 帧。

“故障转移”选项卡（记录服务器）

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

如果贵组织使用故障转移记录服务器，则使用**故障转移**选项卡来将故障转移服务器分配到记录服务器；请参阅“故障转移”选项卡属性。



有关故障转移记录服务器、安装和设置、故障转移组及其设置的详细信息，请参阅 第 36 页上的故障转移记录服务器(已作说明)。

“故障转移”选项卡属性

名称	说明
无	选择没有故障转移记录服务器的设置。

名称	说明
主要故障转移服务器组/次要故障转移服务器组	选择使用一个主要故障转移服务器组和可能的一个次要故障转移服务器组的常规故障转移设置。
热后备服务器	选择使用一台专用记录服务器作为热后备服务器的热后备设置。
高级故障转移设置	打开**高级故障转移设置**窗口： • **全力支持**：为设备启用完全故障转移支持 • **仅实时**：仅为设备上的实时流启用故障转移支持 • **禁用**：为设备禁用故障转移支持
故障转移服务通信端口 (TCP)	默认情况下，端口号为 11000。该端口用于记录服务器和故障转移记录服务器之间的通信。如果更改端口，则记录服务器**必须**正在运行，同时**必须**连接到管理服务器。

“多播”选项卡（记录服务器）

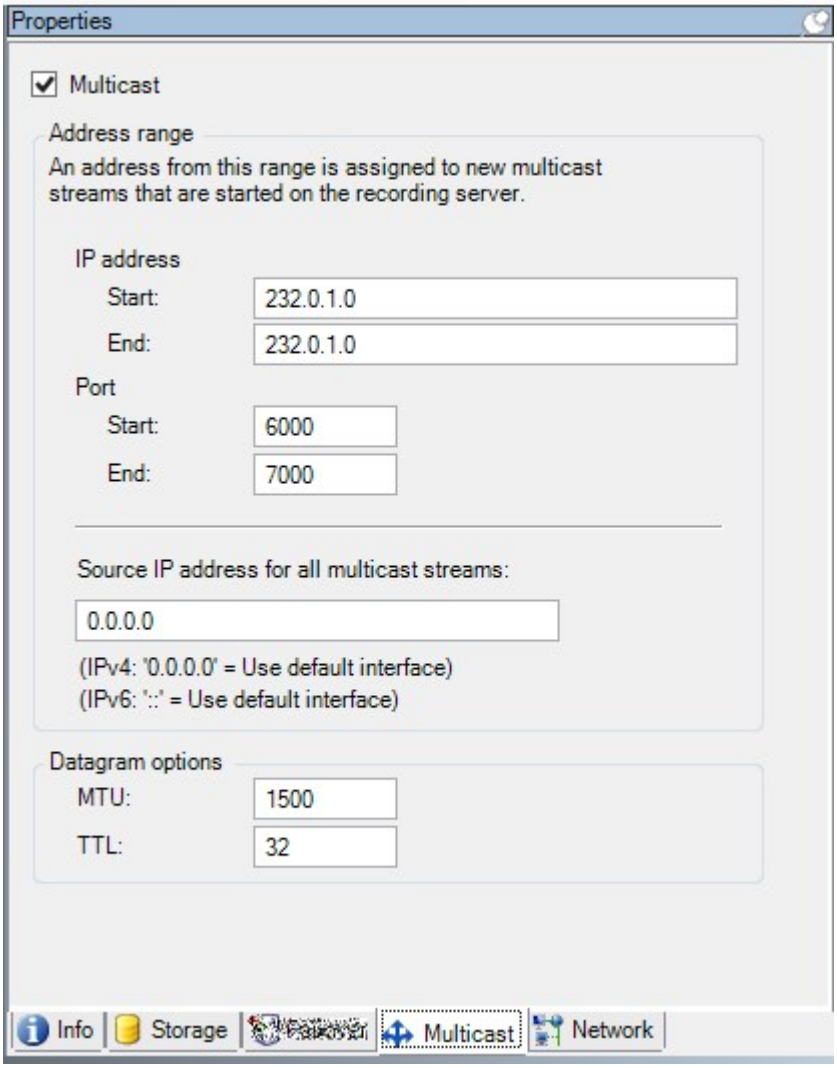
本系统支持来自记录服务器的实时流的多播。当多个 XProtect Smart Client 用户需要查看来自同一摄像机的实时视频时，多播可帮助节省大量系统资源。当使用 Matrix 功能且多个客户端要求来自相同摄像机的实时视频时，多播特别有用。

只有实时流才可使用多播，记录的视频/音频则不可使用多播。

如果记录服务器有一个以上的网络接口卡，则只可能在其中一个上使用多播。您可以通过 Management Client 来指定使用其中哪一个。

如果您正在使用故障转移服务器，请记住指定故障转移服务器中网络接口卡的 IP 地址（请参阅 第 366 页上的多播选项卡（故障转移服务器））。

要成功实现多播，还要求已将网络设备设置为仅将多播数据包中继至所需的接收方组。否则，多播可能与广播没有差异，从而可能显著降低网络通信速度。



指定 IP 地址范围

指定您要为来自所选记录服务器的多播流分配地址的范围。当用户查看来自记录服务器的多播视频时，客户端将连接到这些地址。

对于各多播摄像机馈送，IP 地址与端口的组合（IPv4 示例：232.0.1.0:6000）必须是唯一的。您可以使用一个 IP 地址和多个端口，或多个 IP 地址和较少的端口。默认情况下，本系统建议使用单个 IP 地址和 1000 个端口范围，但是您可以根据需要进行更改。

多播的 IP 地址必须位于 IANA 为动态主机分配所定义的范围内。IANA 是监督全球 IP 地址分配的机构。

名称	说明
IP 地址	在开始字段中，指定所需范围内的第一个 IP 地址。然后在**结束**字段中指定所需范围内的最后一个 IP 地址。
端口	在**开始**字段中，指定所需范围内的第一个端口号。然后在**结束**字段中指定所需范围内的最后一个端口号。
所有多播流的来源 IP 地址	仅可以在一个网络接口卡上进行多播，因此，如果记录服务器有一个以上的网络接口卡或者它的网络接口卡有一个以上的 IP 地址，则该字段有重要意义。 要使用记录服务器的默认接口，在该字段中使用值 0.0.0.0 (IPv4) 或 :: (IPv6)。如果您希望使用另一个网络接口卡，或在相同的网络接口卡上使用不同的 IP 地址，请指定所需接口的 IP 地址。 • IPv4：224.0.0.0 至 239.255.255.255。 • IPv6 的范围在 IANA 网站 (https://www.iana.org/) 上有介绍。

指定数据报选项

指定通过多播传输的数据包(数据报)的设置。

名称	说明
MTU	最大传输单元，允许的最大物理数据包大小(以字节来度量)。大于指定 MTU 的消息在发送前将被拆分为较小的包。默认值为 1500，这也是大多数 Windows 计算机和以太网上的默认值。
TTL	生存时间，数据包在被丢弃或返回之前的传输期间所允许的最大跳跃数。跳跃是两个网络设备之间的点，通常为路由器。默认值为 128。

“网络”选项卡(记录服务器)

如果您需要在公共或不可信网络中以 XProtect Smart Client 访问 VMS，Milestone 建议您通过 VPN 使用安全连接。这能帮助确保 XProtect Smart Client 和 VMS 服务器之间的通信得到保护。

在网络选项卡上定义记录服务器的公共 IP 地址。

为什么使用公共地址?

客户端可能从本地网络以及从互联网连接,在这两种情况下,监控系统都必须提供适当的地址以使得客户端可从记录服务器访问实时和记录的视频:

- 当客户端从本地连接时,监控系统应使用本地地址和端口号回复
- 当客户端从互联网连接时,监控系统应回复记录服务器的公共地址。这是防火墙或 NAT(网络地址转换)路由器的地址,通常也有不同的端口号。地址和端口随后可转发到服务器的本地地址和端口。

故障转移服务器(“服务器”节点)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

故障转移记录服务器是在常规记录服务器变得不可用时进行接管的额外记录服务器。您可以采用两种方式来配置故障转移记录服务器,将其作为**冷后备服务器**或作为**热后备服务器**。

故障转移记录服务器的安装类似于标准记录服务器(请参阅 第 143 页上的安装故障转移记录服务器,通过 Download Manager)。安装了故障转移记录服务器之后,便可在 Management Client 中看到它们。Milestone 建议您将所有故障转移记录服务器安装在单独的计算机上。确保使用管理服务器的正确 IP 地址/主机名配置故障转移记录服务器。在安装过程中,将提供运行故障转移服务器服务所使用的用户帐户的用户权限。它们是:

- 用于启动或停止故障转移记录服务器的启动/停止权限
- 用于读取或写入 RecorderConfig.xml 文件的读取和写入访问权限

如果选择了证书进行加密,则管理员必须在所选证书私钥上向故障转移用户授予读取访问权限。

如果故障转移记录服务器从使用加密的记录服务器接管,Milestone 还建议您准备使用加密的故障转移记录服务器。有关详细信息,请参阅 第 124 页上的安全通信(已解释) 和 第 143 页上的安装故障转移记录服务器,通过 Download Manager。

可在设备级别指定您想要的故障转移支持类型。对于记录服务器上的每台设备,选择全力、仅实时或无故障转移支持。这有助于对故障转移资源进行优先级排序,例如,为视频而不为音频设置故障转移,或仅在重要的摄像机而不在较不重要的摄像机上设置故障转移。

在系统处于故障转移模式时,您无法更换或移动硬件、更新记录服务器或更改设备配置(如存储设置或视频流设置)。

冷后备故障转移记录服务器

在热后备故障转移记录服务器设置中，您可以将多播故障转移记录服务器分到故障转移组中。整个故障转移组专门用于在多台预选的记录服务器中的任意一台变得不可用时进行接管。您可以根据需求创建任意数量的组(请参阅 第 183 页上的为冷后备故障转移记录服务器分组)。

分组具有明显的好处:在之后指定哪些故障转移记录服务器应接管记录服务器时，您可以选择一组故障转移记录服务器。如果所选组包含一台以上的故障转移记录服务器，这样便可使一台以上故障转移记录服务器做好在记录服务器不可用时进行接管的准备，从而确保安全。您可以指定第二组故障转移服务器，当第一组中的所有记录服务器都繁忙时，第二组就接管第一组。故障转移记录服务器一次只能为一个组的成员。

故障转移组中的故障转移记录服务器按顺序排列。该顺序决定了故障转移记录服务器接管记录服务器的顺序。默认情况下，该顺序反映您将故障转移记录服务器加入故障转移组时的顺序:最先放入的就排在最前面。可根据需要进行更改。

热后备故障转移记录服务器

在热后备记录服务器设置中，您可以专门指定一台故障转移记录服务器只接管**一台**记录服务器。因此，系统可使该故障转移记录服务器保持“后备”模式，这意味着它与相应记录服务器的正确/当前配置同步，可以比常规故障转移记录服务器更快地进行接管。如上文所述，热后备服务器仅分配给一台记录服务器，无法进行分组。您无法将已经属于某个故障转移组的故障转移服务器选为热后备记录服务器。

故障转移记录服务器验证

要验证从故障转移服务器到记录服务器的视频数据合并，您必须通过停止记录服务器服务或关闭记录服务器计算机来使记录服务器不可用。

通过拔出网线或使用测试工具阻塞网络而导致的任何手动网络中断都不是有效的方法。

“信息”选项卡属性(故障转移服务器)

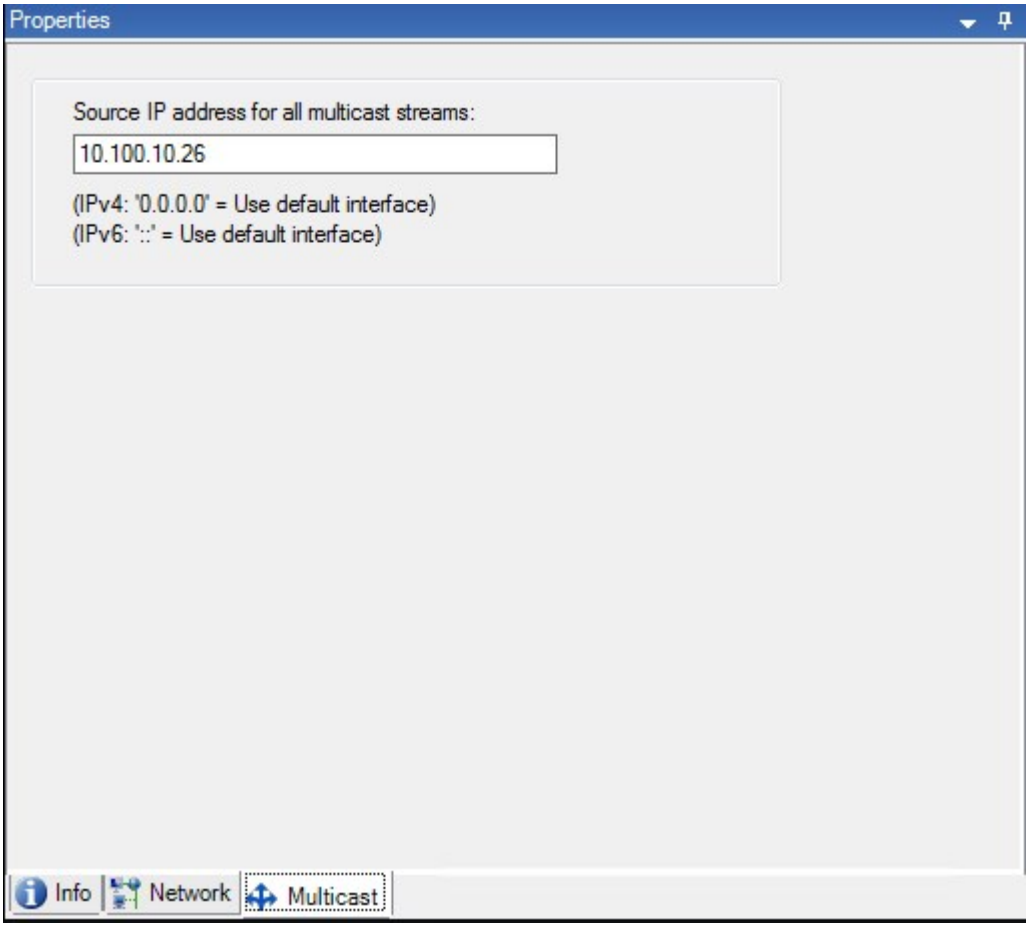
指定以下故障转移记录服务器属性:

名称	说明
名称	显示在 Management Client 和日志等中的故障转移记录服务器的名称。
说明	这是一个可选字段，用于描述故障转移记录服务器，例如它从哪台记录服务器进行接管。

名称	说明
主机名称	显示故障转移记录服务器的主机名。该属性不能更改。
本地 Web 服务器地址	显示故障转移记录服务器的 Web 服务器的本地地址。例如，您可以使用本地地址来处理 PTZ 摄像机控制命令，并处理来自 XProtect Smart Client 的浏览和实时请求。 该地址包括用于 Web 服务器通信的端口号(通常为端口 7563)。 如果故障转移记录服务器从使用加密的记录服务器接管，则还需要准备故障转移记录服务器以使用加密。 如果对从记录服务器检索数据流的客户端和服务器启用加密，则会显示挂锁图标，并且地址包括 **https**，而非 **http**。
Web 服务器地址	显示 Internet 上故障转移记录服务器的 Web 服务器的公共地址。 如果您的安装使用防火墙或 NAT 路由器，请输入防火墙或 NAT 路由器的地址，以便在 Internet 上访问监控系统的客户端可以连接到故障转移记录服务器。 您可以在**网络**选项卡上指定公共地址和端口号。 如果对从记录服务器检索数据流的客户端和服务器启用加密，则会显示挂锁图标，并且地址包括 **https**，而非 **http**。
UDP 端口	用于在故障转移记录服务器之间进行通信的端口号。默认端口为 8844。
数据库位置	指定故障转移记录服务器存储记录的数据库路径。 在故障转移记录服务器从记录服务器接管时，不能更改数据库路径。系统会在故障转移记录服务器不再从记录服务器接管时应用更改。
启用此故障转移服务器	清除该框会禁用故障转移记录服务器(默认情况下为选中状态)。您必须先禁用故障转移记录服务器，然后它们才能从记录服务器接管。

多播选项卡(故障转移服务器)

如果您正在使用故障转移服务器，并且您已经启用视频直播中的多播，那么您必须在记录服务器和故障转移服务器上指定您所使用的网络接口卡的 IP 地址。



有关多播的详细信息，请参阅 第 180 页上的为记录服务器启用多播。

“信息”选项卡属性（故障转移组）

字段	说明
名称	显示在 Management Client 和日志等中的故障转移组名称。
说明	可选的说明，例如服务器的物理位置。

片段选项卡属性（故障转移组）

字段	说明
指定故障转移顺序	可使用**向上**和**向下**来设置组中常规故障转移记录服务器的所需顺序。

Milestone Interconnect 的远程服务器

Milestone Interconnect™允许您将一些物理上分散的较小远程 XProtect 安装与一个 XProtect Corporate 中央站点集成。这些小型站点称为远程站点，可安装在船舶、公共汽车或火车等移动设备上。这意味着此类站点无需永久性地连接到网络。

“信息”选项卡(远程服务器)

名称	说明
名称	只要远程服务器在系统和客户端中列出，系统便会使用该名称。名称不要求是唯一的。 重命名服务器时，名称将在 Management Client 中全局更改。
说明	输入远程服务器的说明(可选)。 说明将出现在系统中的多个列表中。例如，在将鼠标指针悬停在**总览**窗格中的硬件名称上时，会出现说明。
型号	显示远程站点上安装的 XProtect 产品。
版本	显示远程系统的版本。
软件许可证号	远程系统的软件许可证号。
驱动程式	标识处理远程服务器连接的驱动程序。
地址	硬件的主机名或 IP 地址。
IE	打开硬件供应商的默认主页。可以使用此页面管理硬件或系统。
远程系统 ID	用于 XProtect(例如)管理许可证的远程站点的唯一系统 ID。

设置选项卡(远程服务器)

在**设置**选项卡上，您可以查看远程系统的名称。

“事件”选项卡(远程服务器)

可以将远程系统中的事件添加至中央站点，以便创建规则，从而立即响应远程系统的事件。事件的数量取决于远程系统中配置的事件。默认事件无法删除。

如果列表显示不完整：

1. 右键单击**总览**窗格中的相关远程服务器，然后选择**更新硬件**。
2. 此对话框中列出了自 Milestone Interconnect 设置建立或最后一次刷新以来远程系统中的所有更改(设备移除、更新和添加)。单击**确认**可使用这些更改更新中央站点。

远程检索选项卡

在 Milestone Interconnect 远程检索选项卡上，可以处理设置中远程站点的远程记录检索设置：

指定以下属性：

名称	说明
检索最高以下速率的记录	确定用于从远程站点检索记录的最高带宽(单位为 Kbits/s)。选中此复选框可启用对检索的限制。
检索以下范围内的记录	确定从远程站点检索记录限于特定的时间间隔。 已到结束时间但尚未完成的作业会继续执行直至最终完成，因此，如果结束时间处于临界状态，需要将其设置得更早一些，以便继续执行未完成的作业。 如果系统在时间间隔之外收到自动检索或从 XProtect Smart Client 进行检索的请求，系统将接受检索请求，但会在到达选择的时间间隔之后才开始检索。 可从**系统仪表板 -> 当前任务**查看由用户启动的搁置中的远程记录检索作业。
在并行设备上检索	确定同时检索其记录的设备的最大数量。如果根据系统的功能需要更多或更少的容量，请更改默认值。

更改设置时，可能需要数分钟，更改才会反映在系统中。

以上任何选项均不会应用于远程记录的直接播放。
所有设置为直接播放的摄像机在直接播放时均可用，并可根据需要使用带宽。

设备节点

设备("设备"节点)

使用 Management Client 添加硬件**向导时将在**中显示设备。请参阅 第 185 页上的添加硬件。

如果设备具有相同的属性，您可通过设备组管理这些设备，请参阅 第 50 页上的设备组(已解释)。

也可分别管理设备。

启用/禁用以及重命名单独的摄像机可在记录服务器硬件上进行。请参阅通过设备组启用/禁用设备。

对于摄像机的其他所有配置和管理，请在"站点导航"窗格中展开**设备**，然后选择一个设备：

- **摄像机**
- **麦克风**
- **扬声器**
- **元数据**
- **输入**
- **输出**

在总览窗格中，可将摄像机分组以便轻松总览摄像机。**初始分组将作为**添加硬件向导的一部分完成。

> 有关受支持硬件的信息，请参阅 Milestone 网站 (https://www.milestonesys.com/support/tools-and-references/supported-devices/) 上关于受支持硬件的页面。

设备的状态图标

选择了某台设备后，当前状态信息将显示在预览窗格中。
以下图标用于显示设备的状态：

摄像机	麦克风	扬声器	元数据	输入	输出	说明
						**设备已启用并检索数据**：设备已启用，并且您正在检索实时流。
						**设备正在记录**：设备正在系统上记录数据。
						**设备暂时停止或没有馈送**：设备停止后，不会有信息传输至系统。如果是摄像机，则无法查看实时视频。停止的设备仍能够就检索事件、设定设置等与记录服务器通信，这一点与设备被禁用时相反。
						**设备被禁用**：无法通过规则自动启动，并且无法与记录服务器通信。如果摄像机被禁用，则无法查看实时视频和记录的视频。
						**正在修复设备数据库**。

摄像机	麦克风	扬声器	元数据	输入	输出	说明
						**设备需要注意**:设备的运行不正常。将鼠标指针悬停在设备图标上以在工具提示中取得关于问题的说明。
						**状态未知**:设备的状态未知,例如,在记录服务器离线时。
						可以组合某些图标,如此例中,**设备已启用并检索数据**与**设备正在记录**组合。

摄像机(“设备”节点)

在您将硬件添加至系统时,摄像机设备会自动添加,并默认启用。

系统附带默认启动馈送规则,该规则确保来自所有已连接摄像机的视频馈送均自动馈送到系统。可以根据需要停用和/或修改默认规则。

遵循该配置顺序,完成与摄像机设备配置相关的最典型任务:

1. 配置摄像机设置,请参阅“设置”选项卡(设备)。
2. 配置流,请参阅“流”选项卡(设备)。
3. 配置移动,请参阅“移动”选项卡(设备)。
4. 配置记录,请参阅“记录”选项卡(设备)和监视设备的数据库。
5. 依照需要配置其余设置。

麦克风(“设备”节点)

在您将硬件添加至系统时,麦克风设备会自动添加。默认情况下会禁用它们,因此必须在使用前启用,可以在**添加硬件**向导中启用,也可以之后启用。麦克风不需要单独的许可证。您可以在系统上使用任意所需数量的麦克风。

麦克风的使用可以完全独立于摄像机。

系统附带默认启动音频馈送规则,该规则确保来自所有已连接麦克风的音频馈送均自动馈送到系统。可以根据需要停用和/或修改默认规则。

可在这些选项卡上配置麦克风设备:

- “信息”选项卡,请参阅“信息”选项卡(设备)
- “设置”选项卡,请参阅“设置”选项卡(设备)
- “记录”选项卡,请参阅“记录”选项卡(设备)
- “事件”选项卡,请参阅“事件”选项卡(设备)

扬声器(“设备”节点)

在您将硬件添加至系统时，扬声器设备会自动添加。默认情况下会禁用它们，因此必须在使用前启用，可以在**添加硬件**向导中启用，也可以之后启用。扬声器不需要单独的许可证。您可以在系统上使用任意所需数量的扬声器。

扬声器的使用可以完全独立于摄像机。

系统附带默认启动音频馈送规则，该规则会启动设备，以使设备准备好将用户激活的音频发送至扬声器。可以根据需要停用和/或修改默认规则。

可在这些选项卡上配置扬声器设备：

- “信息”选项卡，请参阅“信息”选项卡(设备)
- “设置”选项卡，请参阅“设置”选项卡(设备)
- “记录”选项卡，请参阅“记录”选项卡(设备)

元数据(“设备”节点)

系统附带默认启动馈送规则，该规则确保来自支持元数据的所有已连接硬件的元数据馈送均自动馈送到系统。可以根据需要停用和/或修改默认规则。

可在这些选项卡上配置元数据设备：

- “信息”选项卡，请参阅“信息”选项卡(设备)
- “设置”选项卡，请参阅“设置”选项卡(设备)
- “记录”选项卡，请参阅“记录”选项卡(设备)

输入(“设备”节点)

输入设备的使用可以完全独立于摄像机。

指定在设备上使用外部输入单元之前，请验证以确保设备自身能识别传感器操作。大部分设备都能在其配置界面中或通过通用网关接口 (CGI) 脚本命令显示此信息。

在您将硬件添加至系统时，输入设备会自动添加。默认情况下会禁用它们，因此必须在使用前启用，可以在**添加硬件**向导中启用，也可以之后启用。输入设备不需要单独的许可证。您可以在系统上使用任意所需数量的输入设备。

可在这些选项卡上配置输入设备：

- “信息”选项卡，请参阅“信息”选项卡(设备)
- “设置”选项卡，请参阅“设置”选项卡(设备)
- “事件”选项卡，请参阅“事件”选项卡(设备)

输出(“设备”节点)

输出也可以从 Management Client 和 XProtect Smart Client 手动触发。

> 指定在设备上使用外部输出单元之前,请验证以确保设备自身能控制连接至输出的设备。大部分设备都能在其配置界面中或通过通用网关接口 (CGI) 脚本命令显示此信息。

在您将硬件添加至系统时,输出设备会自动添加。默认情况下会禁用它们,因此必须在使用前启用,可以在**添加硬件**向导中启用,也可以之后启用。输出设备不需要单独的许可证。您可以在系统上使用任意所需数量的输出设备。

可在这些选项卡上配置输出设备:

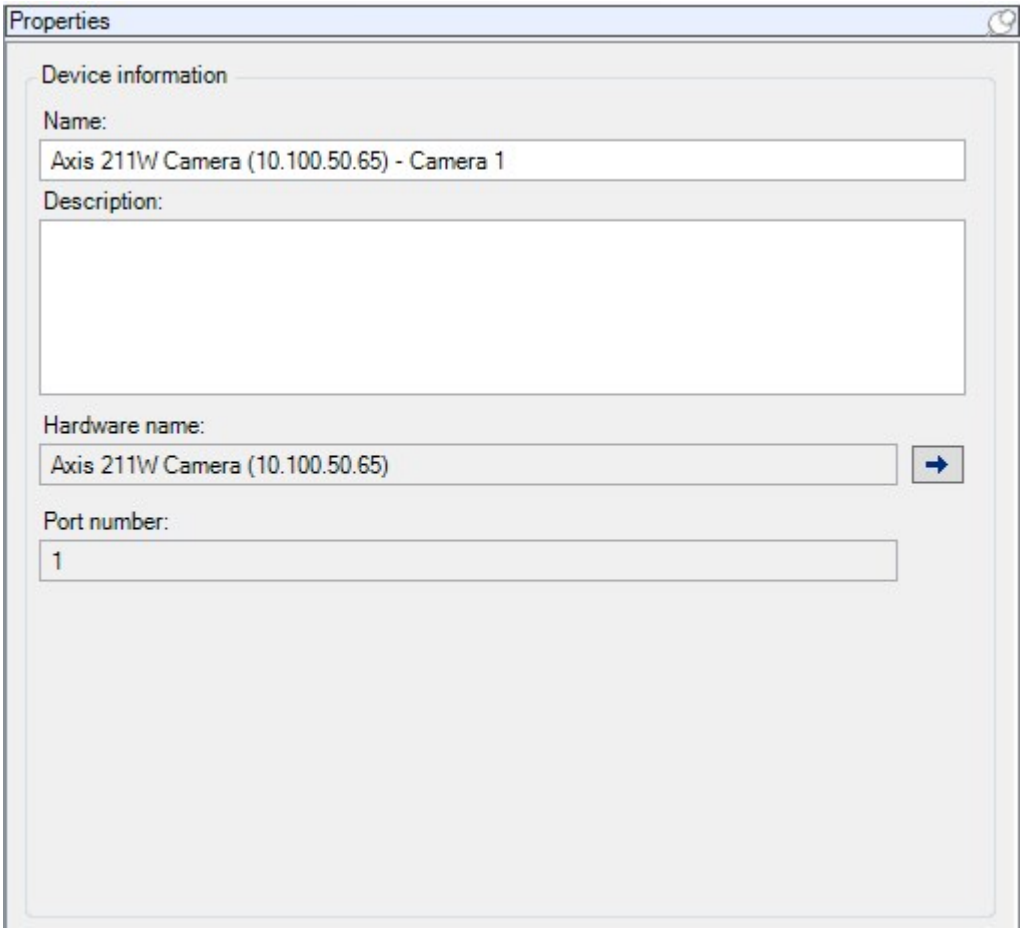
“信息”选项卡,请参阅

- “信息”选项卡,请参阅“信息”选项卡(设备)
- “设置”选项卡,请参阅“设置”选项卡(设备)

“设备”选项卡

“信息”选项卡(设备)

在**信息**选项卡上,可以在多个字段中查看和编辑关于设备的基本信息。
所有设备都拥有**信息**选项卡。



“信息”选项卡属性

名称	说明
名称	在系统和客户端中列出设备时将使用该名称。 重命名设备时，名称将在 Management Client 中全局更改。
说明	输入设备的说明(可选)。 说明将出现在系统中的多个列表中。例如，在将鼠标指针悬停在**总览**窗格中的名称上时，会出现说明。
硬件名称	显示设备所连接硬件的名称。该字段不可在此处编辑，但您可通过单击字段旁边的**转到**进行更改。这会让您前往硬件信息，以便在其中更改名称。

名称	说明
端口号	显示硬件上连接设备的端口。 对于单设备硬件，端口号通常为 **1**。对于多设备硬件(例如具有数个通道的视频服务器)，端口号通常指示设备所连接的通道(例如 **3**)。
简称	要应用摄像机的简称，请在此处输入。字符的最大长度为 128。 如果您正在使用智能地图，系统会自动显示简称，并在智能地图上显示摄像机。否则，则会显示全称。
地理坐标	以**latitude, longitude**的格式输入摄像机的地理位置。您输入的值将确定摄像机图标在 XProtect Smart Client 和 XProtect Mobile 客户端 智能地图上的位置。 该字段主要针对智能地图和第三方集成。
方向	输入从垂直轴上的正北点测量的摄像机的查看方向。您输入的值将确定摄像机图标在 XProtect Smart Client 和 XProtect Mobile 客户端 智能地图上的方向。 默认值为 0.0。 该字段主要针对智能地图和第三方集成。
视野	输入视野宽度(以度为单位)。您输入的值决定了 XProtect Smart Client 和 XProtect Mobile 客户端 中智能地图上摄像机图标的视野角度。 默认值为 0.0。 该字段主要针对智能地图和第三方集成。
深度	输入视野的深度(以米或英尺为单位)。您输入的值决定了 XProtect Smart Client 和 XProtect Mobile 客户端 中智能地图上摄像机图标的视野长度。 默认值为 0.0。 该字段主要针对智能地图和第三方集成。
在浏览器中预览位置	要确认您是否输入了正确的地理坐标，请单击此按钮。Google Maps 将在您标配的 Internet 浏览器中打开，并显示您指定的位置。 该字段主要针对智能地图和第三方集成。

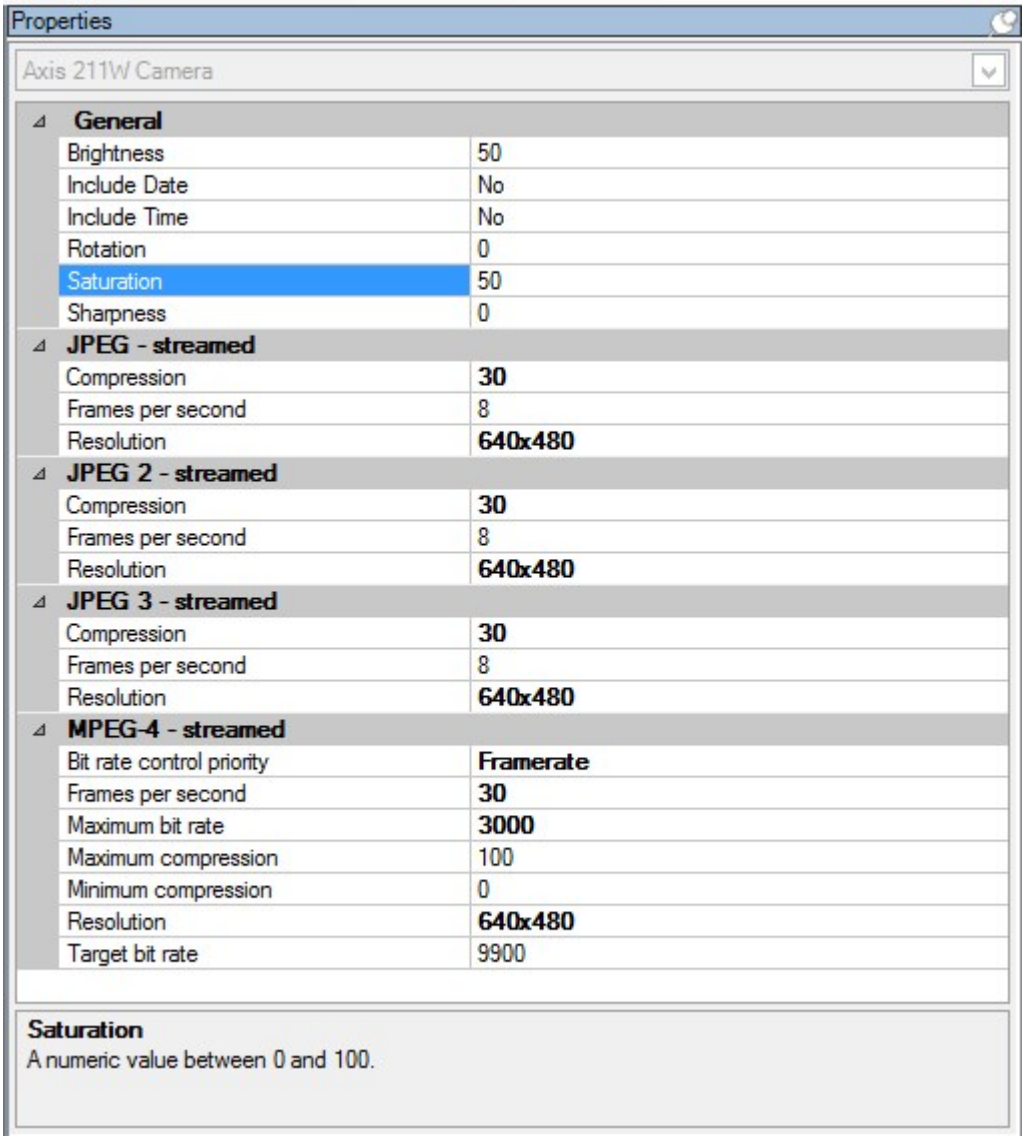
“设置”选项卡(设备)

在设置选项卡上,可以在多个字段中查看和编辑设备的设置。
所有设备都拥有设置选项卡。

表格中显示的值可更改或为只读。将设置更改为非默认值时,值会以粗体显示。

表格的内容取决于设备驱动程序。

允许的范围显示于设置表格下方的信息框中:



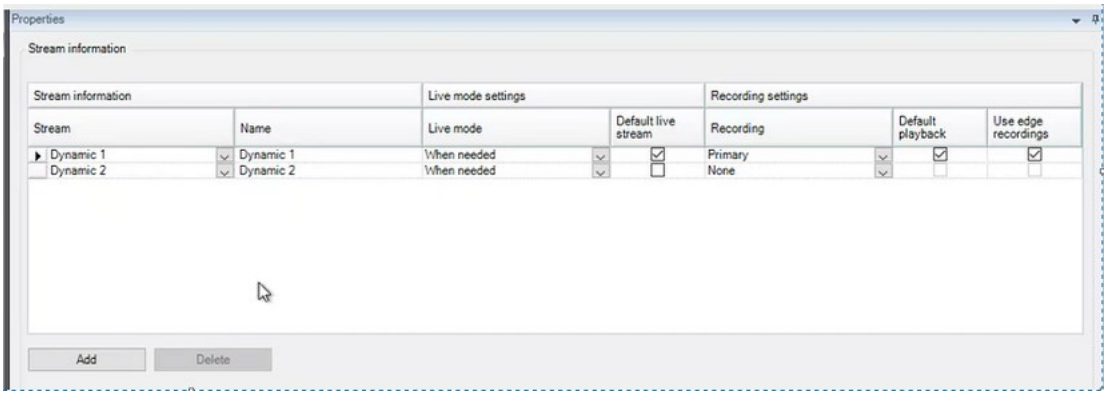
有关摄像机设置的详细信息,请参阅查看或编辑摄像机设置。

“数据流”选项卡(设备)

以下设备拥有数据流选项卡:

- 摄像机

数据**流**选项卡会默认列出单个数据流。即选定摄像机的默认数据流，用于实时视频和记录的视频。若您使用自适应播放，必须创建两个流。



“流”选项卡上的任务

名称	说明
添加	单击以将流添加到列表。 添加数据流

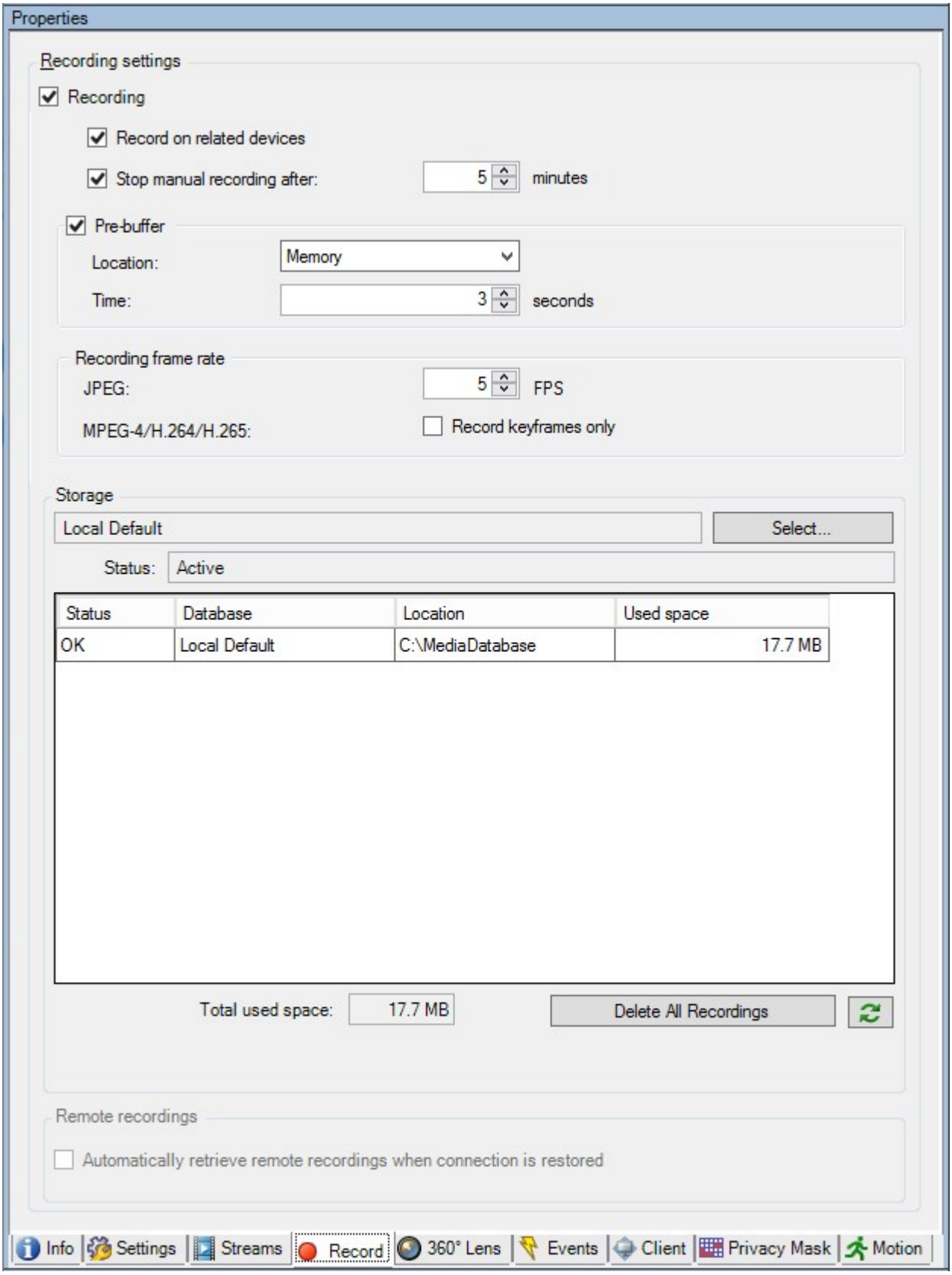
“记录”选项卡(设备)

以下设备具有**记录**选项卡：

- 摄像机
- 麦克风
- 扬声器
- 元数据

只有在启用了记录且符合记录相关的规则条件时，才会将来自设备的记录保存在数据库中。

设备无法配置的参数以灰色显示。


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

“记录”选项卡上的任务

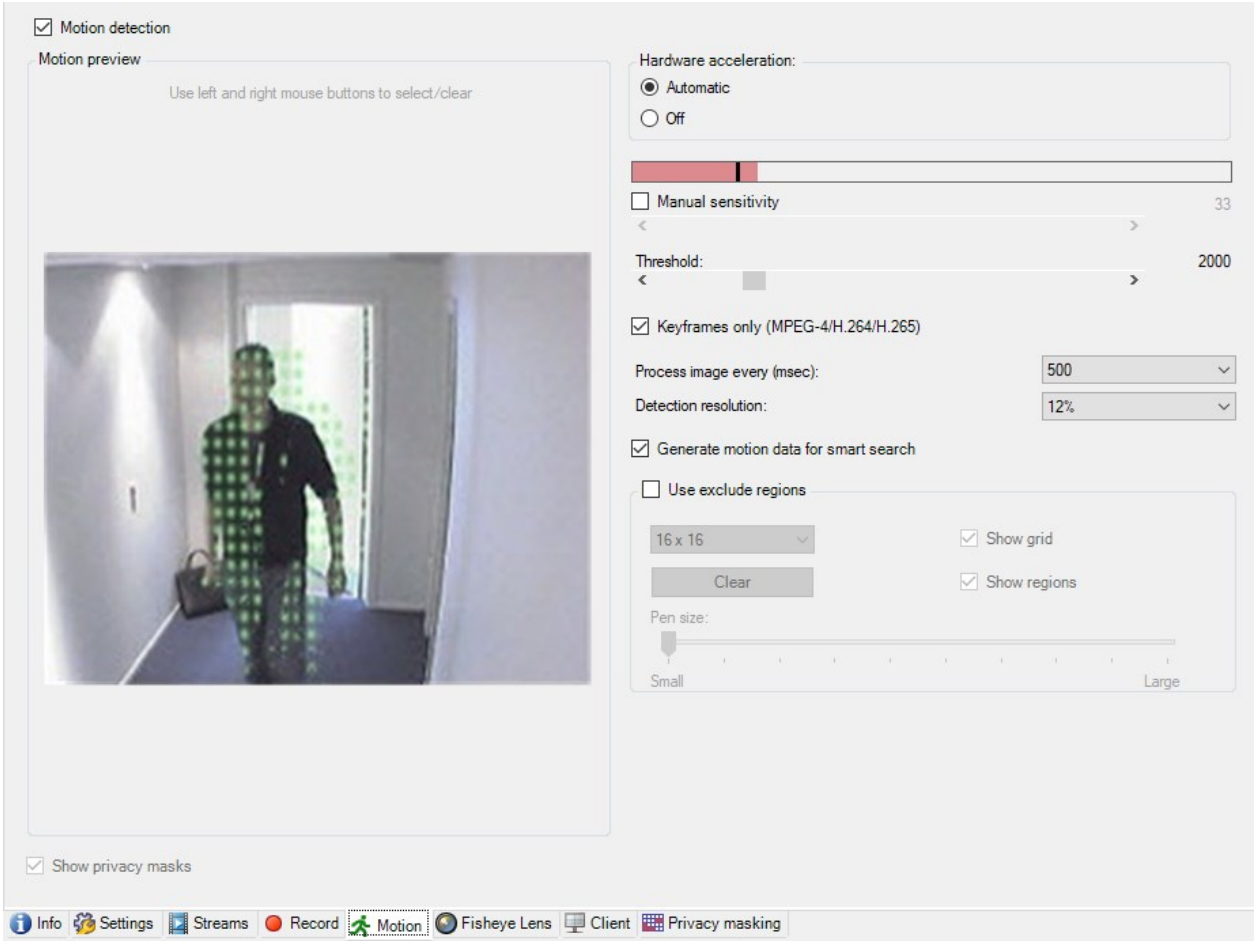
名称	说明
记录	启用/禁用记录 启用相关设备上的记录
预缓冲	预缓冲记录的预缓冲和存储(已作说明) 管理预缓冲 管理手动记录
记录帧速率	指定记录帧速率 启用关键帧记录
存储	监视设备的数据库状态
选择	将设备从一个存储移到另一个存储
删除所有记录	如果已将组中的所有设备添加到同一服务器，请使用此按钮： 删除记录
连接恢复时自动检索远程记录	保存和检索远程记录

“移动”选项卡(设备)

以下设备拥有移动选项卡：

- 摄像机

在移动选项卡上，可以启用和配置所选摄像机的移动侦测。



“移动”选项卡上的任务

名称	说明
移动侦测	启用和禁用移动侦测
硬件加速	选择**自动**以启用硬件加速，或选择**关闭**以禁用设置。有关详细信息，请参阅启用或禁用硬件加速。
隐私屏蔽	如果您定义了带有永久隐私屏蔽的区域，则可以选中**隐私屏蔽**复选框以在**移动**选项卡上显示隐私屏蔽。您可以在 第 391 页上的隐私屏蔽选项卡(设备) 中定义隐私屏蔽区域。 在永久隐私屏蔽遮盖的区域没有移动侦测。

名称	说明
手动灵敏度	决定图像中的**每个像素必须变化多少**才能被视为移动。 启用手动灵敏度以定义移动
阈值	决定图像中的**每个像素必须变化多少**才能被视为移动。 指定阈值以定义移动
仅限关键帧 (MPEG-4/H.264/H.265)	选中此复选框以仅对关键帧而不是对整个视频流进行移动侦测。仅适用于 MPEG-4/H.264/H.265。 对关键帧进行移动侦测会减少执行分析的处理能力用量。
每(毫秒)处理图像	在此列表中选择一个图像处理间隔，以确定系统执行移动侦测分析的频率。 例如，每 1000 毫秒即每秒一次。默认值为每隔 500 毫秒。 该间隔在实际帧速率高于您此处所设间隔的情况下应用。
侦测分辨率	在此列表中选择侦测分辨率以优化移动侦测性能。 仅分析图像的选定百分比，例如 25%。分析 25% 表示只分析图像中四分之一的像素，而不是所有像素。 使用优化的侦测可减少进行分析的处理能力用量，但同时也意味着降低移动侦测精度。
生成智能搜索的移动数据	启用此复选框后，系统会生成移动侦测所使用图像的移动数据。例如，如果选择仅对关键帧进行移动侦测，那么将只生成关键帧的移动数据。 如果有更多移动数据，客户端用户就能通过智能搜索功能根据图像选定区域的移动进行相关记录的快速搜索。系统不会生成永久隐私屏蔽遮盖区域的移动数据，只会生成可解除隐私屏蔽遮盖区域的移动数据(请参阅“移动侦测”选项卡(已作说明))。 移动侦测阈值和排除区域不会影响到生成的移动数据。 • 在**工具 > 选项 > 常规**下指定生成摄像机智能搜索数据的默认设置。
使用排除区域	在摄像机视图的特定区域中禁用移动侦测： 指定移动侦测的排除区域

“预设”选项卡(设备)

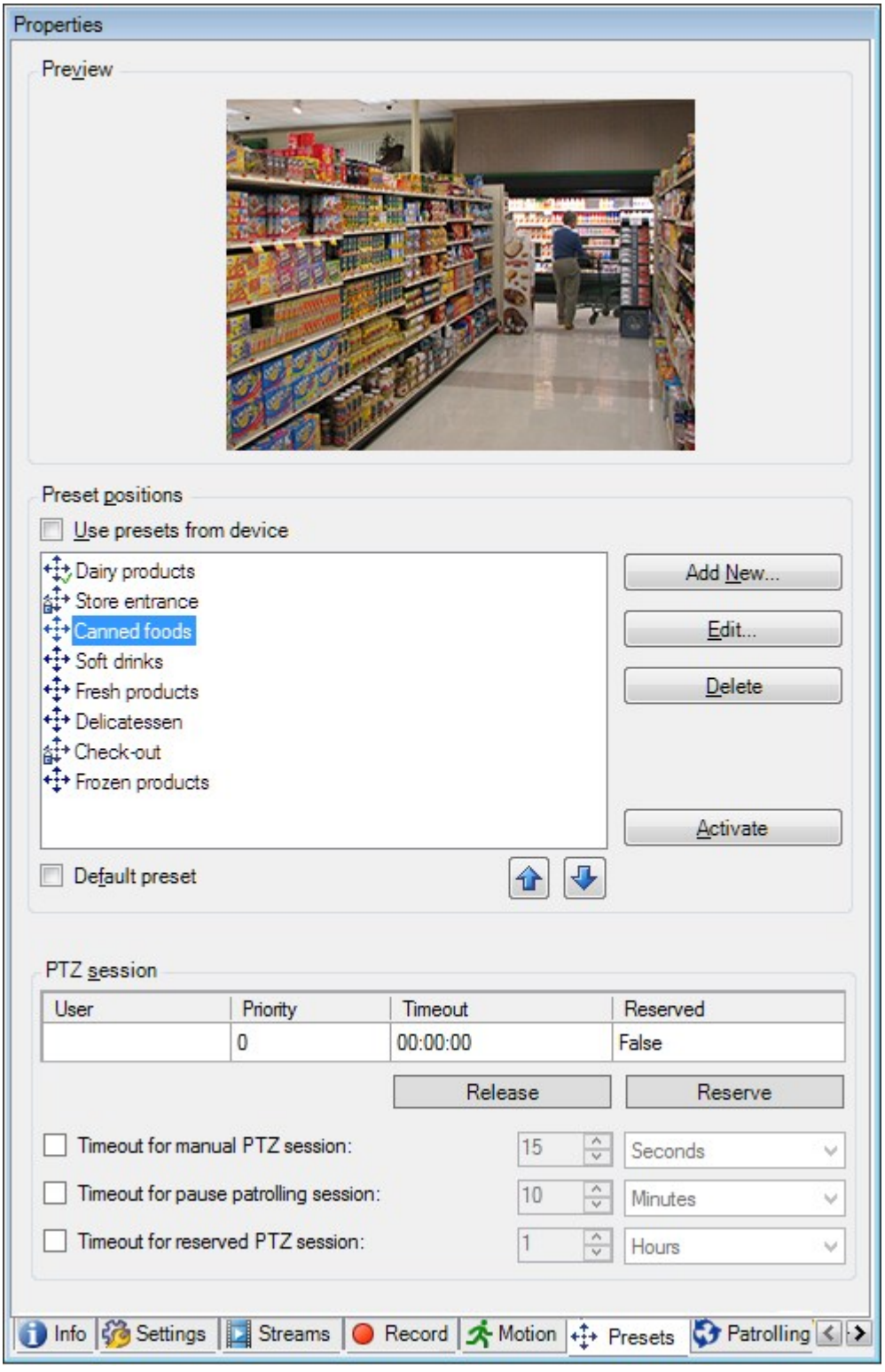
以下设备拥有**预设**选项卡：

- 支持预设位置的 PTZ 摄像机

在**预设**选项卡上，您可以在以下对象中创建或导入预设位置，例如：

- 将 PTZ（全景-倾斜-变焦）摄像机设置为在事件发生后移动至特定预设位置的规则
- 用于 PTZ 摄像机在多个预设位置之间自动移动的巡视
- 由 XProtect Smart Client 用户执行的手动激活

您可以在“整体安全”选项卡上为角色分配 PTZ 权限（请参阅 第 433 页上的“整体安全”选项卡（角色））或“PTZ”选项卡（请第 465 页上的PTZ 选项卡（角色）参阅）。


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

“预设”选项卡上的任务

名称	说明
新建	在系统中为摄像机添加预设位置： 添加预设位置(类型 1)
使用设备的预设	在摄像机本身上为 PTZ 摄像机添加一个预设位置： 使用摄像机的预设位置(类型 2)
默认预设	指定 PTZ 摄像机的其中一个预设位置作为摄像机的默认预设位置： 将摄像机的预设位置指定为默认位置
编辑	编辑系统中定义的现有预设位置： 编辑摄像机的预设位置(仅类型 1) 编辑在摄像机中定义的预设位置的名称： 重命名摄像机的预设位置(仅类型 2)
已锁定	选择此复选框以锁定预设位置。如果要阻止XProtect Smart Client中的用户或拥有受限安全权限的用户更新或删除预设，可锁定预设位置。锁定的预设由该图标  表示。 在添加(参阅添加预设位置(类型 1))和编辑(参阅编辑预设位置(仅类型 1))过程中锁定预设。
激活	单击此按钮以测试摄像机预设位置： 测试预设位置(仅类型 1)。
保留和释放	防止其他用户控制摄像机并释放保留。 有运行保留 PTZ 会话的安全权限的管理员可在此模式下运行 PTZ 摄像机。这可阻止其他用户控制摄像机。具有足够的权限，您可以释放其他用户的保留的 PTZ 会话： 保留和释放 PTZ 会话。
PTZ 会话	监视系统当前是否正在巡视或用户已控制： 第 385 页上的PTZ 会话属性。 查看 PTZ 摄像机的状态并管理摄像机的超时： 指定 PTZ 会话超时。

PTZ 会话属性

PTZ 会话表显示了 PTZ 摄像机的当前状态。

名称	说明
用户	显示已按下**保留**按钮并且当前正在控制 PTZ 摄像机的用户。 如果巡视会话由系统启动，它将显示**巡视**。
优先级	显示用户的 PTZ 优先级。您只能从优先级低于您的用户接管 PTZ 会话。
超时	显示当前 PTZ 会话的剩余时间。
保留	指示当前会话是否为保留 PTZ 会话： • **真**：保留 • **假**：未保留

PTZ 会话部分中的复选框使您可以更改每个 PTZ 摄像机的以下超时。

名称	说明
手动 PTZ 会话的超时	指定此摄像机上的手动 PTZ 会话的超时时间(如果您希望此超时不同于默认时间)。可以在**工具**菜单的**选项**下指定默认时间。
暂停巡视 PTZ 会话的超时	指定此摄像机上的暂停巡视 PTZ 会话的超时时间(如果您希望此超时不同于默认的时间)。可以在**工具**菜单的**选项**下指定默认时间。
保留的 PTZ 会话的超时	指定此摄像机上的保留 PTZ 会话的超时时间(如果您希望此超时不同于默认的时间)。可以在**工具**菜单的**选项**下指定默认时间。

"巡视"选项卡(设备)

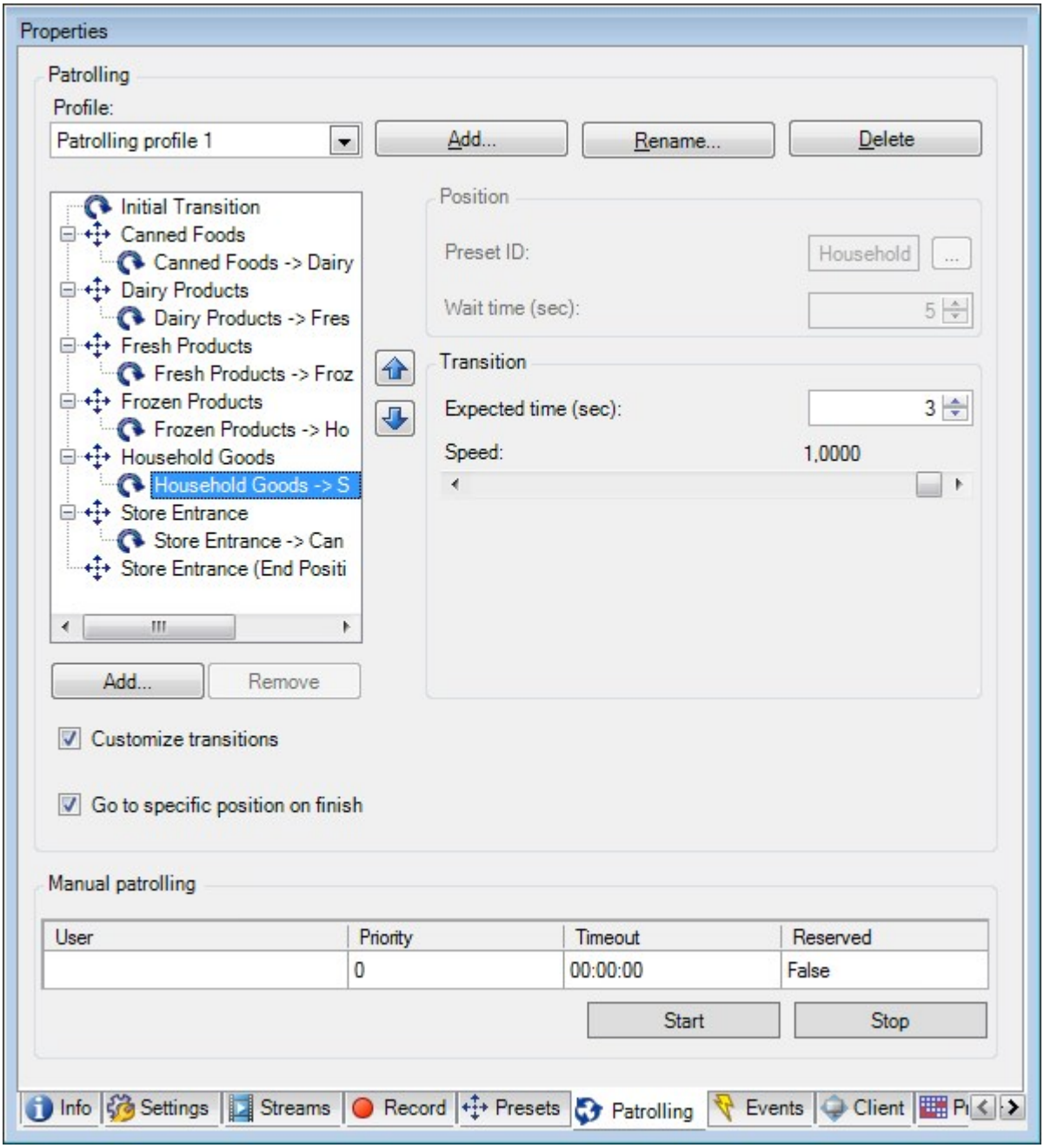
以下设备拥有巡视选项卡：

- PTZ 摄像机

在**巡视**选项卡上，可以创建巡视配置文件，这是 PTZ（全景/倾斜/变焦）摄像机在大量预设位置之间的自动移动。

必须先在**预设**选项卡中为摄像机指定至少两个预设位置才能使用巡视功能，请参阅添加预设位置（类型 1）。

巡视选项卡，显示使用了自定义转换的巡视配置文件：



“巡视”选项卡上的任务

名称	说明
添加	添加巡视配置文件
预设 ID	指定巡视配置文件中的预设位置
等待时间(秒)	指定各预设位置的时间
自定义转换	自定义转换 (PTZ)
完成时转到特定位置	指定巡视时的结束位置
手动巡视	监视系统当前是否正在巡视或用户已控制。
开始和**停止**	可使用**开始**和**停止**按钮启动和停止手动巡视。 有关如何指定在恢复所有或单个 PTZ 摄像机的常规巡视之前应该经过多少时间的信息，请参阅指定 PTZ 会话超时。

手动巡视属性

手动巡视表显示了 PTZ 摄像机的当前状态。

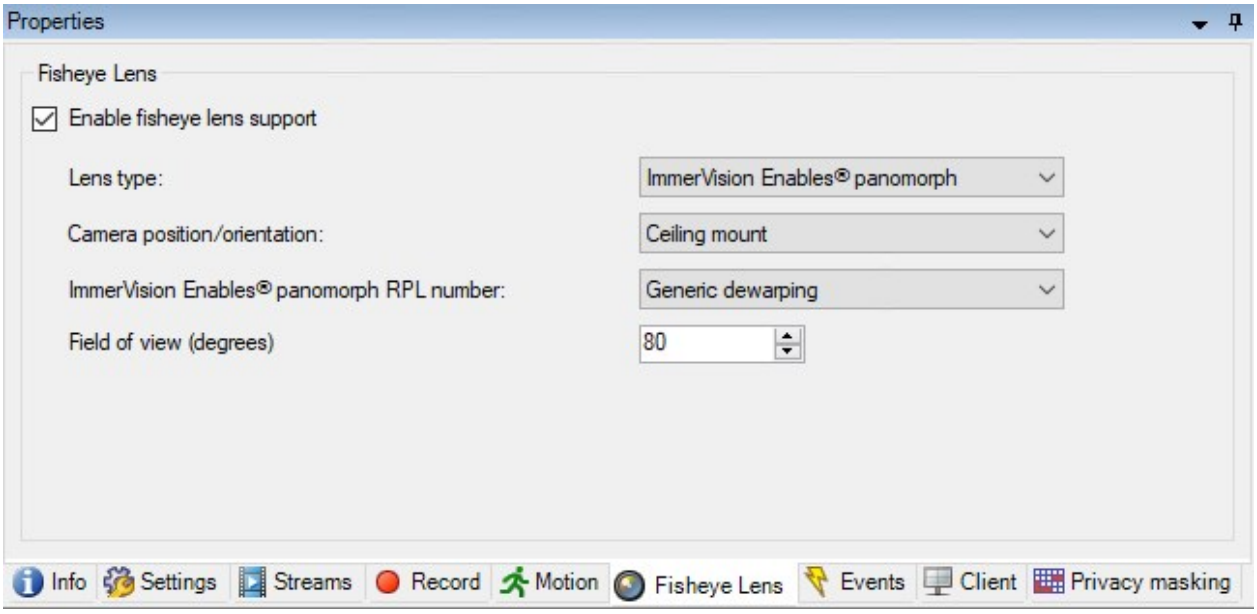
名称	说明
用户	显示已保留了 PTZ 会话或启动手动巡视且当前正在控制摄像机的用户。 如果巡视会话由系统启动，它将显示**巡视**。
优先级	显示用户的 PTZ 优先级。您只能从优先级低于您的用户或巡视配置文件接管 PTZ 会话。
超时	显示当前保留会话或手动 PTZ 会话的剩余时间。
保留	指示当前会话是否为保留 PTZ 会话。 • **真**：保留 • **假**：未保留

“鱼眼镜头”选项卡(设备)

以下设备具有**鱼眼镜头**选项卡：

- 配有鱼眼镜头的固定摄像机

在**鱼眼镜头**选项卡上，您可以为所选摄像机启用和配置鱼眼镜头支持。



“鱼眼镜头”选项卡上的任务

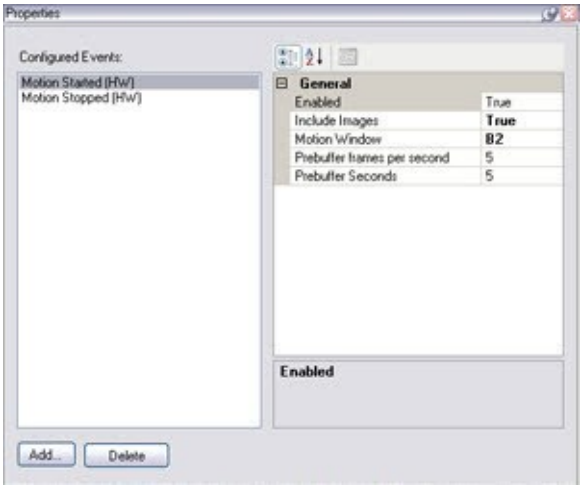
名称	说明
启用鱼眼镜头支持	启用和禁用鱼眼镜头支持

“事件”选项卡(设备)

以下设备拥有事件选项卡：

- 摄像机
- 麦克风
- 输入

除了系统的事件外，某些设备也可配置为触发事件。在系统中创建基于事件的规则时可以使用这些事件。从技术层面而言，这些事件发生于实际摄像机/硬件上而非监控系统上。



“事件”选项卡上的任务

名称	说明
添加和**删除**	添加或删除设备的事件

“事件”选项卡(属性)

名称	说明
配置的事件	**可以在**配置的事件列表中选择和添加的事件完全取决于设备及其配置。对于一些类型的设备，该列表为空。
常规	属性的列表取决于设备和事件。为了使事件按预期工作，必须在设备以及在该选项卡上以同样方式指定部分或全部属性。

“客户端”选项卡(设备)

以下设备拥有客户端选项卡：

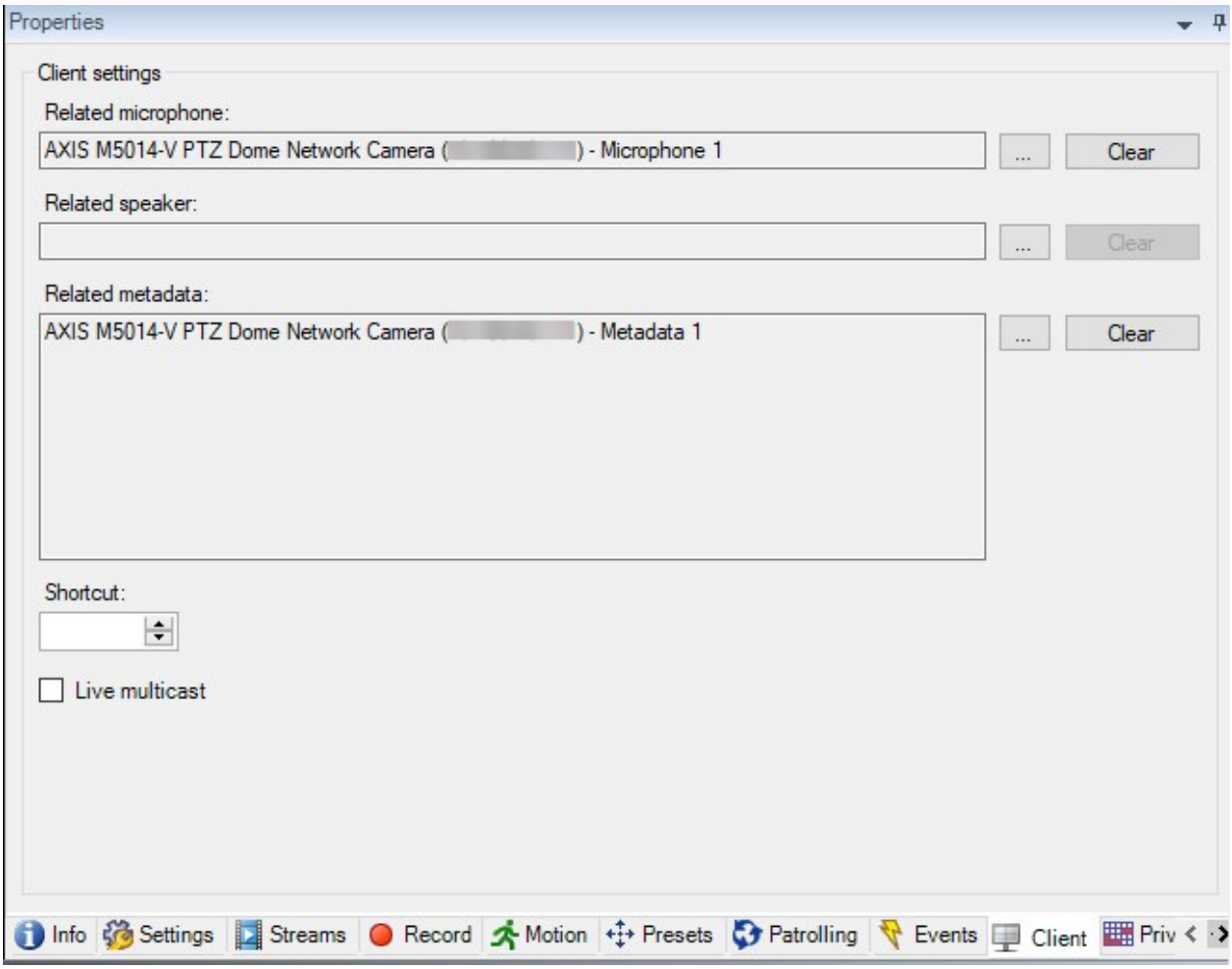
- 摄像机

在**客户端**选项卡上，可以指定当使用 XProtect Smart Client 中的摄像机时查看和听取其他哪些设备。

摄像机进行记录时，相关元数据设备会进行记录，请参阅 第 199 页上的启用相关设备上的记录。

您还可以在摄像机上启用**实时多播**。这意味着摄像机通过记录服务器将实时流多播到客户端。

即使记录服务器使用加密，也不会加密多播流。



“客户端”选项卡属性

名称	说明
相关麦克风	指定 XProtect Smart Client 用户默认从摄像机的哪个麦克风接收音频。XProtect Smart Client 用户可根据需要手动选择监听另一个麦克风。 指定与用于视频流和音频流传输的手机视频推送摄像机相关的麦克风。

名称	说明
	摄像机进行记录时，相关麦克风会进行记录。
相关扬声器	指定 XProtect Smart Client 用户默认使用摄像机的哪一个扬声器讲话。XProtect Smart Client 用户可根据需要手动选择其他扬声器。 摄像机进行记录时，相关扬声器会进行记录。
相关元数据	指定摄像机上，XProtect Smart Client 用户从其接收数据的一个或多个元数据设备。 摄像机进行记录时，相关元数据设备会进行记录。
快捷方式	为使 XProtect Smart Client 用户可以简便地选择摄像机，请为摄像机定义键盘快捷键。 • 创建每个快捷键，使其唯一识别摄像机 • 摄像机快捷键数字不得长于四位数
实时多播	系统支持将来自记录服务器的实时流多播到 XProtect Smart Client。要从摄像机启用实时流的多播，请选中该复选框。 实时多播仅适用于您在**流**选项卡上指定为摄像机默认流的流。 还必须为记录服务器配置多播。请参阅 第 180 页上的为记录服务器启用多播。 即使记录服务器使用加密，也不会加密多播流。

隐私屏蔽选项卡(设备)

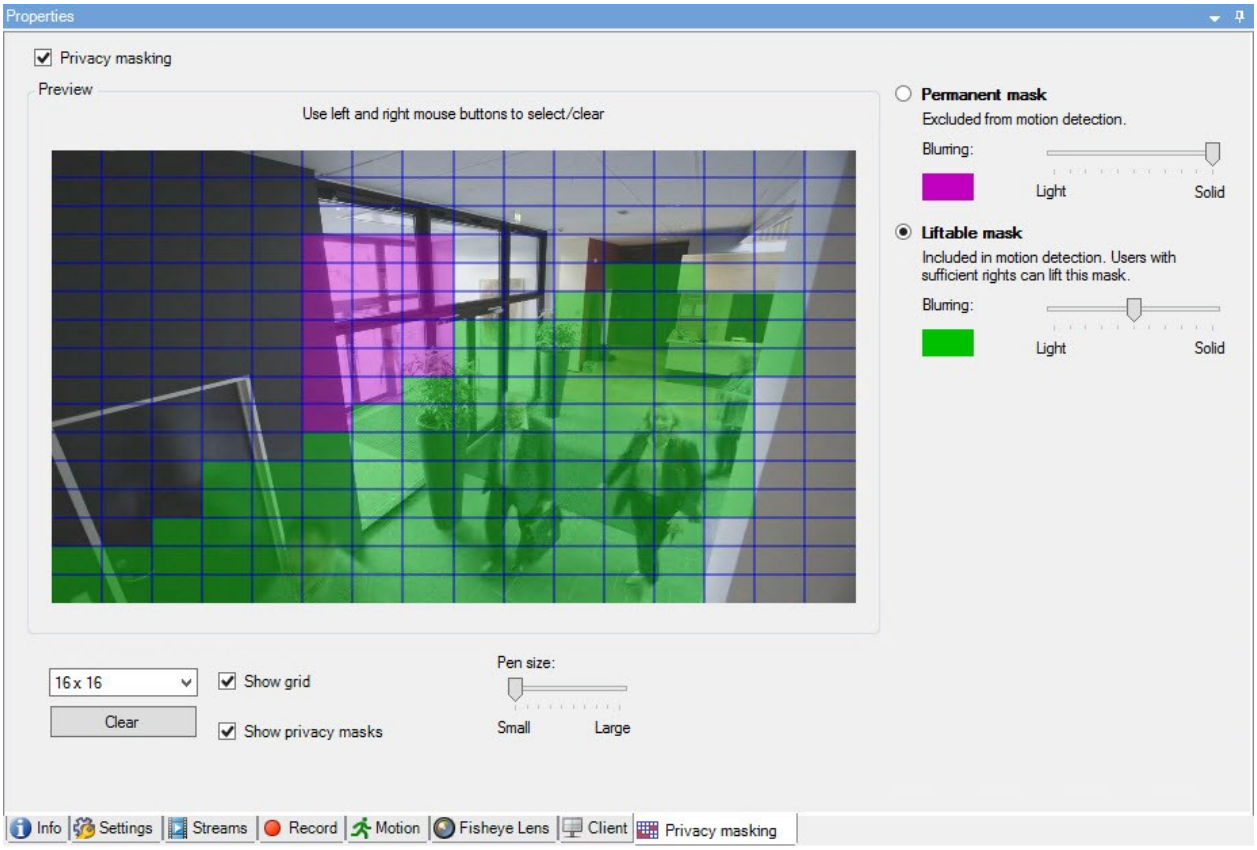
可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

XProtectEssential+2018R1及以上版本不支持隐私屏蔽，所以如果要升级应用了隐私屏蔽的系统，屏蔽将被删除。

以下设备拥有**隐私屏蔽**选项卡：

- 摄像机

在**隐私屏蔽**选项卡上，您可以启用和配置所选摄像机的隐私保护。



“隐私屏蔽”选项卡上的任务

名称	说明
隐私屏蔽	启用/禁用隐私屏蔽 隐私屏蔽(已作说明)
永久屏蔽和**可解除屏蔽**	定义您想用永久的还是可解除的隐私屏蔽： 定义隐私屏蔽

与隐私屏蔽相关的任务

任务	说明
为与有权解除隐私屏蔽的角色相关联的 Smart Client 配置文件更改解除隐私屏蔽的超时。	更改可解除隐私屏蔽的超时时间
启用或禁用为角色解除隐私屏蔽的权限。	授予用户解除隐私屏蔽的权限
创建一个设备报告，其中包含有关摄像机当前隐私屏蔽设置的信息。	创建隐私屏蔽配置报告

“隐私屏蔽”选项卡(属性)

名称	说明
栅格尺寸	选择的栅格尺寸决定栅格的密度，而不考虑栅格是否会显示出来。 可选择的值为 8×8、16×16、32×32 或 64×64。
清除	清除您指定的**所有**隐私屏蔽。
显示栅格	选中**显示栅格**复选框即可显示栅格。
显示隐私屏蔽	选择**显示隐私屏蔽**复选框(默认)时，永久隐私屏蔽在预览中以紫色显示，可解除隐私屏蔽以绿色显示。 Milestone 建议保持选中**显示隐私屏蔽**复选框，以便您和您的同事可以看到当前的隐私保护配置。
笔大小	使用**笔大小**滑块来指示当单击并拖动栅格以选择区域时希望的选择大小。默认设置为小，等同于栅格中的一个方块。
永久屏蔽	在此选项卡的预览中以及在**移动**选项卡上以紫色显示。 永久隐私屏蔽在 XProtect Smart Client 中始终可见，不能解除。可用于遮盖从不需要监视的视频区域，如不允许监视的公共区域。永久隐私屏蔽是排除在移动侦测之外的。 您可以将隐私屏蔽遮盖指定为实体或某种模糊级别。遮盖设置适用于实时和记录视频。
可解	在此选项卡的预览中以绿色显示。

名称	说明
除屏蔽	具有足够用户权限的用户可以在 XProtect Smart Client 中解除可解除隐私屏蔽。默认情况下，隐私屏蔽会解除 30 分钟，或直到用户再次应用。请注意，用户有权访问的所有摄像机的视频都将解除隐私屏蔽。 如果 XProtect Smart Client 用户没有解除隐私屏蔽的权限，系统会要求有权授权的用户进行授权。 您可以将隐私屏蔽指定为实体或某种模糊级别。遮盖设置适用于实时和记录视频。
模糊	使用滑块选择客户端中隐私屏蔽的模糊级别，或将遮盖设置为实体。 默认情况下，永久隐私屏蔽区域的遮盖是实体的(不透明的)。默认情况下，可解除隐私屏蔽为中等模糊级别。 您可以通知客户端用户永久和可解除隐私屏蔽的外观，以便区分。

“硬件属性”窗口

有多个选项可用于为系统中的每台记录服务器添加硬件。

> 如果硬件位于已启用 NAT 的路由器或防火墙之后，您可能需要指定不同的端口号并配置路由器/防火墙，使其映射硬件使用的端口和 IP 地址。

添加硬件向导可帮助您检测网络上的硬件(例如摄像机和视频编码器)，并将它们添加至本系统上的记录服务器。该向导还可帮助您为 Milestone Interconnect 设置添加远程记录服务器。**一次仅为**一台记录服务器添加硬件。

“信息”选项卡(硬件)

有关远程服务器**信息**选项卡的信息，请参阅 第 368 页上的“信息”选项卡(远程服务器)。

名称	说明
名称	输入名称。只要硬件在系统和客户端中列出，系统便会使用该名称。名称不要求是唯一的。 重命名硬件时，名称将在 Management Client 中全局更改。
说明	输入硬件的说明(可选)。说明将出现在系统中的多个列表中。例如，在将鼠标指针移动到**总览**窗格中的硬件名称上时，会出现说明：

名称	说明
	
型号	标识硬件型号。
序列号	由制造商指定的硬件序列号。序列号通常但并非总是与 MAC 地址一致。
驱动程式	标识处理硬件连接的驱动程序。
IE	打开硬件供应商的默认主页。可以使用此页面管理硬件。
地址	硬件的主机名或 IP 地址。
MAC 地址	指定系统硬件的媒体访问控制 (MAC) 地址。MAC 地址由 12 个十六进制字符组成，是网络上每个硬件的唯一标识。
固件版本：	硬件设备的固件版本。要确保系统显示当前版本，请在每次固件更新后运行**更新硬件数据**向导。
上次更改密码	**密码上次更改**字段根据更改密码的计算机的本地时间设置显示最新密码更改的时间戳。
上次更新的硬件数据：	硬件数据上次更新的时间和日期。

“设置”选项卡(硬件)

在设置选项卡上，可以检查或编辑硬件的设置。

> **设置**选项卡的内容取决于所选硬件，可能会因为硬件类型不同而有所差异。**对于某些类型的硬件**，设置选项卡不会显示任何内容或仅显示只读内容。

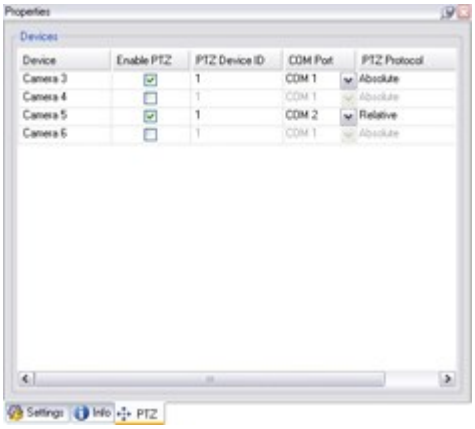
有关远程服务器**设置**选项卡的信息，请参阅 第 368 页上的设置选项卡(远程服务器)。

“PTZ”选项卡(视频编码器)

在 **PTZ** 选项卡上，可以为视频编码器启用 PTZ(全景/倾斜/变焦)。该选项卡只在所选设备为视频编码器或驱动程序同时支持 PTZ 及非 PTZ 摄像机时可用。

必须在 PTZ 选项卡中对视频编码器的每个通道单独启用 PTZ 使用，然后才可使用视频编码器所连接 PTZ 摄像机的 PTZ 功能。

> 并非所有视频编码器都支持使用 PTZ 摄像机。即使视频编码器支持 PTZ 摄像机的使用，也可能需要在使用 PTZ 摄像机前进行相应配置。通常是通过访问设备的 IP 地址进入基于浏览器的配置界面来安装额外的驱动程序。



PTZ 选项卡，为视频编码器的两个通道启用了 PTZ。

客户端节点

客户端(节点)

本文将介绍如何为 XProtect Smart Client 中的操作员和 Management Client 中的系统管理员自定义用户界面。

Smart Wall(“客户端”节点)

Smart Wall 属性

“信息”选项卡

在 Smart Wall 定义的 **信息** 选项卡上，可添加和编辑 Smart Wall 属性。

名称	说明
名称	Smart Wall 定义的名称。在 XProtect Smart Client 中显示为 Smart Wall 视图组名称。

名称	说明
说明	Smart Wall 定义的说明。说明仅在 XProtect Management Client 内部使用。
状态文本	在摄像机视图项目中显示摄像机和系统状态信息。
无标题栏	在电视墙上的所有视图项目上隐藏标题栏。
标题栏	在电视墙上的所有视图项目上显示标题栏。

“预设”选项卡

在 Smart Wall 定义的**预设**选项卡上，可添加和编辑 Smart Wall 预设[1]。

名称	说明
新增	向您的 Smart Wall 定义添加预设。 输入新预设的名称和说明。
编辑	编辑预设的名称或说明。
删除	删除预设。
激活	在配置为使用预设的 Smart Wall 监视器上应用预设。要自动应用预设，必须创建使用预设的规则。

“布局”选项卡

在 Smart Wall 定义的 **布局** 选项卡上定位监视器，使其位置与电视墙上物理监视器的安装相似。XProtect Smart Client 中也会使用该布局。

名称	说明
编辑	调整监视器的位置。
移动	要将监视器移动至新位置，请选择监视器然后将其拖动至所需位置，或者单击其中一个箭头按钮沿所选方向移动监视器。

[1]XProtect Smart Client 中一个或多个 Smart Wall 监视器的预定义布局。预设决定了显示哪些摄像机，以及电视墙上每个监视器的内容结构。

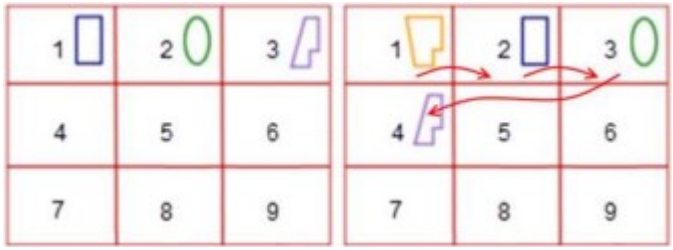
名称	说明
变焦按钮	放大或缩小 Smart Wall 布局预览，确保正确放置监视器。
名称	监视器的名称。名称显示在 XProtect Smart Client 中。
大小	电视墙上物理监视器的尺寸。
纵横比	电视墙上物理监视器的高/宽关系。

监视器属性

"信息"选项卡

在 Smart Wall 预设中监视器的 **信息** 选项卡上，可以添加监视器并编辑监视器的设置。

名称	说明
名称	监视器的名称。名称显示在 XProtect Smart Client 中。
说明	监视器的说明。XProtect Management Client 说明仅在内部使用。
大小	电视墙上物理监视器的尺寸。
纵横比	电视墙上物理监视器的高/宽关系。
空预设	定义在 Smart Wall 中触发或选择了新 XProtect Smart Client 预设时，对于空预设布局，应在监视器上显示的内容： • **选择** 保留会保持监视器上的当前内容。 • 选择**清除** 会清除所有内容，从而使监视器上不显示任何内容。
空预设项目	定义在 Smart Wall 中触发或选择了新 XProtect Smart Client 预设时，应在空预设项目中显示的内容： • 选择 **保留** 会保持布局项目中的当前内容。 • 选择 **清除** 会清除内容，从而使布局项目中不显示任何内容。
元素	定义在 XProtect Smart Client 中查看时，应如何将摄像机插入监视器的布局：

名称	说明
插入	• **独立** - 只有受影响的布局项目的内容会变化，布局中的其余内容保持不变。 • **已链接** - 会将布局项目的内容从左侧推动到右侧。例如，如果摄像机插入位置 1，则会将位置 1 的原有摄像机推动到位置 2，将位置 2 的原有摄像机推动到位置 3，以此类推，如该示例中所示： 

“预设”选项卡

在 Smart Wall 预设中监视器的 **预设** 选项卡上，可以编辑所选 Smart Wall 预设中监视器的视图布局和内容。

名称	说明
预设	所选 Smart Wall 定义的 Smart Wall 预设的列表。
编辑	**单击**编辑可编辑所选监视器的布局和内容。 双击摄像机可将其删除。 单击 **清除** 可定义新布局或排除 Smart Wall 预设中的监视器，从而使监视器可用于不受 Smart Wall 预设控制的其他内容。 单击  以选择监视器要用的布局，然后单击 **确定**。

Smart Client 配置文件(“客户端”节点)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

在以下选项卡上，您可以指定每个 Smart Client 配置文件的属性。您可以根据需要在 Management Client 中锁定设置，使 XProtect Smart Client 用户无法更改它们。

若要创建或编辑 Smart Client 配置文件，请展开**客户端**，然后选择 **Smart Client 配置文件**。

“信息”选项卡（Smart Client 配置文件）

此选项卡允许您指定以下属性：

制表符	说明
信息	名称和说明、现有配置文件的优先级以及使用配置文件的角色总览。 如果用户是多个角色的成员，每个角色都有各自的 Smart Client 配置文件，则用户将获得具有最高优先级的 Smart Client 配置文件。

“常规”选项卡（Smart Client 配置文件）

此选项卡允许您指定以下属性：

制表符	说明
常规	显示/隐藏和最小化与最大化菜单设置之类的设置、登录/注销、启动、超时、信息和消息传递选项以及启用或禁用 XProtect Smart Client 中某些选项卡的设置。 **摄像机错误消息**、**服务器错误消息**和**实时视频错误消息**设置可让您控制这些错误消息是显示为覆盖层、带有覆盖层的黑色图像还是隐藏。 当摄像机实时馈送停止时，**中会显示**实时视频已停止消息XProtect Smart Client。例如，如果摄像机已停止发送图像，即使它仍然连接。 ⚠ 如果**隐藏**摄像机错误消息，可能会导致操作员忽略与摄像机的连接丢失的风险。 **搜索期间允许的摄像机**设置可让您控制操作员可以添加到 XProtect Smart Client 中的搜索的摄像机数量。设置摄像机限制可以帮助您防止系统过载。 **联机帮助**设置让您可以禁用 XProtect Smart Client 中的帮助系统。 **视频教程**设置让您可以禁用 XProtect Smart Client 中的**视频教程**按钮。该按钮将操作员重定向到视频教程页面：https://www.milestonesys.com/support/help-yourself/video-tutorials/

“高级”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性:

制表符	说明
高级	高级设置,例如最大解码线程、去交错和时区设置。 **最大解码线程**控制用于解码视频流的解码线程数量。此设置有助于在实时模式及播放模式中提高多核计算机的性能。具体性能改善取决于视频流。该设置主要用于高度编码的高分辨率视频流,如 H.264/H.265(对于此类视频,潜在性能改善非常显著),而在使用如 JPEG 或 MPEG-4 等编码时,该设置的作用较小。 **去交错**可以将视频转换为非隔行的格式。隔行处理决定图像在屏幕上如何刷新。刷新的方式是,先扫描图像中的奇数行,然后扫描偶数行。因为每次扫描过程中需要处理的信息较少,所以这种方式的刷新率较高。但是,隔行扫描会导致闪烁,或者明显察觉一半的图像行会改变。 **自适应流媒体传输**使 XProtect Smart Client 能够自动选择与视图项目所请求的流具有最佳分辨率匹配的实时视频流。这会减少 CPU 和 GPU 的负载,从而提高计算机的解码能力和性能。这需要配置具有不同分辨率的实时视频流的多流,请参阅管理多流。可以将自适应流应用于实时模式和播放模式。在播放模式中,自适应流称为自适应播放。自适应播放需要将两个流设置为记录。如需有关如何添加流以进行自适应流(在实时模式中)和自适应播放的更多信息,请参阅 第 201 页上的添加数据流。

“实时”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性:

制表符	说明
实时	实时模式/其他实时功能、摄像机播放按钮、摄像机覆盖按钮、边界框和实时相关的 MIP 插件的可用性。

“播放”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性:

制表符	说明
播放	播放模式和其他播放功能、打印报告布局、独立播放、书签、边界框和播放相关的 MIP 插件的可用性。

“设置”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性:

制表符	说明
设置	常规设置/窗格/按钮,与设置相关的 MIP 插件的可用性以及编辑地图和编辑实时视频缓冲的权限。

“导出”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性:

制表符	说明
导出	路径、隐私屏蔽、视频和静态图像格式以及导出时要包含的内容、XProtect Smart Client - Player 的导出格式以及更多设置。

“时间轴”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性:

制表符	说明
时间轴	是否包括音频、时间和移动指示的可见性以及处理播放空白部分的方式。 您还可以选择是否显示其他来源的其他数据或其他标记。

“访问控制”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性:

制表符	说明
访问控制	选择在由事件触发访问请求通知时，是否在 XProtect Smart Client 屏幕上弹出该通知。

“警报管理器”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性：

制表符	说明
警报管理器	指定是否： • 将在安装了 XProtect Smart Client 的计算机上显示警报的桌面通知。通知仅在 XProtect Smart Client 运行时显示(即使已最小化) 仅当警报具有特定优先级(例如**中**或**高**)时，才会显示警报的桌面通知。要配置触发通知的警报优先级，请转到**警报 > 警报数据设置 > 警报数据级别**。对于每个必需的警报优先级，请选中**启用桌面通知**复选框。请参阅警报数据设置(“警报”节点) • 警报应在安装 XProtect Smart Client 的计算机上播放声音通知。声音通知仅在 XProtect Smart Client 运行时播放(即使已最小化) 警报的声音通知仅在声音与警报关联时播放。要将声音与警报关联，请转到**警报 > 警报数据设置 > 警报数据级别**。对于每个所需的警报优先级，选择要与警报关联的声音。请参阅警报数据设置(“警报”节点)

“智能地图”选项卡(Smart Client 配置文件)

此选项卡允许您指定以下属性：

制表符	说明
智能	指定智能地图功能的设置。

制表符	说明
地图	您可以指定是否： • Milestone Map Service 可用作地理背景 • OpenStreetMaps 可用作地理背景 • 当用户向智能地图添加自定义叠加层时，XProtect Smart Client 会自动创建位置。 您还可以指定系统从计算机中删除与智能地图相关的数据的频率。为了帮助 XProtect Smart Client 更快地显示智能地图，客户端将地图数据保存在计算机的缓存中。随着时间的推移，这可能会降低计算机的速度。 缓存不适用于 Google Maps。 如果您要使用 Bing Maps 或 Google Maps 作为地理背景，请输入 Bing Maps API 的密钥，或 Google Static Maps API 的密钥。

Management Client 配置文件(“客户端”节点)

此功能仅在 XProtect Corporate 中可用。

“信息”选项卡(Management Client 配置文件)

在**信息**选项卡上，可以为 Management Client 配置文件设置以下内容：

组件	要求
名称	输入 Management Client 配置文件的名称。
优先级	使用上下箭头设置 Management Client 配置文件的优先级。
说明	输入配置文件的说明。这是可选的。
使用 Management Client 配置文件的角色	该字段显示与 Management Client 配置文件关联的角色。不可对其进行编辑。

“配置文件”选项卡(Management Client配置文件)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

在**配置文件**选项卡上,可以启用或禁用以下元素在 Management Client 用户界面上的可见性:

导航

在该部分,决定是否允许与ManagementClient配置文件关联的管理员用户查看位于**导航**窗格中的各个功能和操作。

导航元素	说明
基本信息	允许与 Management Client 配置文件关联的管理员用户查看**许可证信息**和**站点信息**。
远程连接服务	允许与 Management Client 配置文件关联的管理员用户查看 **Axis One-click 摄像机连接**。
服务器	允许与 Management Client 配置文件关联的管理员用户查看**记录服务器**和**故障转移服务器**。
设备	允许与 Management Client 配置文件关联的管理员用户查看**摄像机**、**麦克风**、**扬声器**、**元数据**、**输入**和**输出**。
客户端	允许与 Management Client 配置文件关联的管理员用户查看 **Smart Wall**、**视图组**、**Smart Client 配置文件**、**Management Client 配置文件**和 **Matrix**。
规则和事件	允许与 Management Client 配置文件关联的管理员用户查看**规则**、**时间配置文件**、**通知配置文件**、**用户定义事件**、**分析事件**和**常规事件**。
安全	允许与 Management Client 配置文件关联的管理员用户查看**角色**和**基本用户**。
系统仪表板	允许与 Management Client 配置文件关联的管理员用户查看**系统监视器**、**系统监视器阈值**、**证据锁定**、**当前任务**和**配置报告**。
服务器日志	允许与 Management Client 配置文件关联的管理员用户查看系统、审核和规则触发的日志。
访问控制	允许与 Management Client 配置文件关联的管理员用户查看**访问控制**功能(如果已将任何访问控制系统集成或插件添加至您的系统)。

详细信息

在该部分，决定是否允许与 Management Client 配置文件关联的管理员用户查看特定设备通道的各个选项卡，如摄像机的**设置**选项卡或**记录**选项卡。

设备通道	说明
摄像机	允许与 Management Client 配置文件关联的管理员用户查看部分或全部与摄像机相关的设置和选项卡。
麦克风	允许与 Management Client 配置文件关联的管理员用户查看部分或全部与麦克风相关的设置和选项卡。
扬声器	允许与 Management Client 配置文件关联的管理员用户查看部分或全部与扬声器相关的设置和选项卡。
元数据	允许与 Management Client 配置文件关联的管理员用户查看部分或全部与元数据相关的设置和选项卡。
输入	允许与 Management Client 配置文件关联的管理员用户查看部分或全部与输入相关的设置和选项卡。
输出	允许与 Management Client 配置文件关联的管理员用户查看部分或全部与输出相关的设置和选项卡。

工具菜单

在该部分，决定是否允许与 Management Client 配置文件关联的管理员用户查看属于**工具**菜单的元素。

工具菜单选项	说明
已注册服务	允许与 Management Client 配置文件关联的管理员用户查看**已注册服务**。
有效角色	允许与 Management Client 配置文件关联的管理员用户查看**有效角色**。
选项	允许与 Management Client 配置文件关联的管理员用户查看**选项**。

联合站点

在该部分，决定是否允许与 Management Client 配置文件关联的管理员用户查看**联合站点层级**窗格。

规则和事件节点

规则(“规则和事件”节点)

本系统包含大量默认规则，无需进行任何设置即可使用基本功能。您可以根据需要取消激活或修改默认规则。如果您修改或取消激活默认规则，本系统可能不会按预期工作，并且可能无法保证视频或音频自动馈送到本系统。

默认规则	说明
当 PTZ 完成时回到预设	确保当 PTZ 摄像机经过手动操作后回到各自默认的预设位置。默认情况下，未启用该规则。 即使启用了此规则，也必须为相关 PTZ 摄像机定义默认预设位置才能使该规则工作。**可在**预设选项卡上执行该操作。
根据请求播放音频	确保在出现外部请求时自动录制视频。 请求始终由与系统外部集成的系统触发，并且此规则主要供外部系统或插件集成商使用。
根据书签进行记录	确保当操作员在 XProtect Smart Client 中设置书签时自动记录视频。要使用该功能，应启用相关摄像机的记录。默认情况下，会启用记录。 此规则的默认记录时间是设置书签之前的 3 秒和设置书签之后的 30 秒。可编辑规则中的默认记录时间。您在“记录”选项卡上设置的预缓冲必须等于或大于预记录时间。
移动记录	确保如果为相应摄像机启用了记录，只要在摄像机视频中侦测到移动，就会记录视频。默认情况下，会启用记录。 虽然默认规则指定了基于侦测到的移动的记录，但这并不能保证系统记录视频，因为您可能对一台或多台摄像机单独禁用了摄像机记录。即使启用了记录，仍需牢记，记录的质量可能会受各台摄像机的记录设置影响。
根据请求进行记录	确保在发生外部请求时自动记录视频，前提是已经为相关摄像机启用了记录。默认情况下，会启用记录。 请求始终由与系统外部集成的系统触发，并且此规则主要供外部系统或插件集成商使用。
启动音频馈送	确保来自所有已连接麦克风和扬声器的音频馈送均自动馈送到系统。 虽然安装系统后，默认规则会立即启用对已连接麦克风和扬声器的音频馈送的访问，但这并不能保证会记录音频，因为您必须单独指定记录设置。
启动馈	确保来自所有已连接摄像机的视频馈送均自动馈送到系统。

默认规则	说明
送	虽然安装系统后，默认规则会立即启用对已连接摄像机的视频馈送的访问，但这并不能保证会记录视频，因为必须单独指定摄像机的记录设置。
启动元数据馈送	确保来自所有已连接摄像机的数据馈送均自动馈送到系统。 虽然安装系统后，默认规则会立即启用对已连接摄像机的数据馈送的访问，但这并不能保证会记录数据，因为必须单独指定摄像机的记录设置。
显示访问请求通知	确保分类为“访问请求”的所有访问控制事件都会导致在 XProtect Smart Client 中弹出访问请求通知，除非在 Smart Client 配置文件中禁用了通知功能。

重新创建默认规则

如果意外删除了任何默认规则，可通过输入以下内容重新创建它们：

默认规则	要输入的文本
当 PTZ 完成时回到预设	在 PTZ 手动会话停止时从所有摄像机执行动作 立即移动到发生事件的设备上的默认预设
根据请求播放音频	从外部请求播放音频消息时执行动作 从设备上具有优先级 1 的元数据中播放音频消息
根据书签进行记录	对所有摄像机、所有麦克风、所有扬声器的书签引用请求执行动作，在事件发生前三秒在发生事件的设备上启动记录 停止记录 30 秒后立即执行动作
移动记录	在移动开始时执行动作且所有摄像机从设备上发生事件前三秒启动记录 在移动停止时执行停止动作且所有摄像机三秒后停止记录
根据请求进行记录	对“请求从外部开始记录”执行动作，在来自元数据的设备上立即开始记录 对“请求从外部停止记录”执行动作，立即停止记录
启动音频馈送	在时间间隔内执行动作且始终启动所有麦克风和所有扬声器上的馈送 在时间间隔结束时执行操作且立即停止馈送

默认规则	要输入的文本
启动馈送	在时间间隔内执行动作且始终启动所有摄像机上的馈送 在时间间隔结束时执行操作且立即停止馈送
启动元数据馈送	在时间间隔内执行动作且始终启动所有元数据上的馈送 在时间间隔结束时执行操作且立即停止馈送
显示访问请求通知	在发生访问请求(访问控制类别)时从系统 [+ 单元] 执行动作 显示内置访问请求通知

通知配置文件("规则和事件"节点)

为通知配置文件指定以下属性:

组件	要求
名称	输入通知配置文件的描述性名称。在创建规则的过程中,每当您选择通知配置文件,该名称稍后都会出现。
说明(可选)	输入通知配置文件的说明。当鼠标指针暂停在"总览"窗格的**通知配置文件**列表中的通知配置文件上时,会出现说明。
接收方	输入通知配置文件的电子邮件通知应该发往的电子邮件地址。要输入一个以上电子邮件地址,请以分号将地址隔开。例如:aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
主题	输入您希望作为电子邮件通知的主题出现的文本。 您可以在主题和消息文本字段中插入系统变量,例如**设备名称**。要插入变量,在字段下的框中单击所需的变量链接。
邮件文本	输入您希望出现在电子邮件通知正文部分中的文本。除消息文本外,各电子邮件通知的中文会自动包含这些信息: • 触发电子邮件通知的来源 • 任何附带静态图像或 AVI 视频剪辑的来源
电子邮件间隔时间	指定发送各电子邮件通知之间需要经过的最短间隔时间(以秒为单位)。示例:

组件	要求
	• 如果指定值为 **120120**，则即使通知配置文件在经过 2 分钟之前被规则再次触发，发送各电子邮件通知之间至少也要经过 2 分钟 • **如果指定值为** 0，每当通知配置文件被规则触发，就会发送电子邮件通知。这可能导致发送大量的电子邮件通知。如果使用值 **0**，因此应仔细考虑是否希望使用规则中可能经常被触发的通知配置文件
图像数	指定您希望包含在通知配置文件的各电子邮件通知中的静态图像的最大数量。默认为 5 个图像。
图像间隔时间(毫秒)	指定希望出现在包含的图像上的记录之间间隔的毫秒数。示例：对于默认值 500 毫秒，包含的图像显示记录的时间间隔为 0.5 秒。
事件前时间(秒)	该设置用于指定 AVI 文件的开始。默认情况下，AVI 文件包含从触发通知配置文件前 2 秒开始的记录。您可以将该值更改为所需秒数。
事件后时间 (秒):	该设置用于指定 AVI 文件的结束。默认情况下，AVI 文件在通知配置文件触发 4 秒后结束。您可以将该值更改为所需秒数。
帧速率	指定希望 AVI 文件包含的每秒帧数。默认为每秒 5 帧。帧速率越高，图像质量和 AVI 文件大小越高。
电子邮件中嵌入的图像	如果选择(默认)，图像会被插入电子邮件通知的正文部分。如果不选择，图像会作为附带的文件包含在电子邮件通知中。

事件总览

在**管理规则**向导中添加基于事件的规则时，可以在大量不同事件类型间选择。为了便于总览，根据可选择的事件是否为以下内容将其分组列出：

硬件：

某些硬件本身可以创建事件，例如侦测移动。可以将它们作为事件使用，但必须先在硬件上进行配置，然后才能在系统中使用。有可能只能使用一些硬件上列出的事件，因为并非所有类型的摄像机都能侦测干预或温度变化。

硬件 - 可配置事件：

硬件的可配置事件将从设备驱动程序自动导入。这意味着它们对于各个硬件不尽相同，因此本文不进行介绍。在将可配置事件添加至系统并在硬件的**事件**选项卡上配置之前，不会触发这些可配置事件。某些可配置事件还需要您配置摄像机(硬件)本身。

硬件 - 预定义事件：

事件	说明
通信错误(硬件)	在硬件连接丢失时发生。
通信已开始(硬件)	与硬件成功建立了通信时发生。
通信已停止(硬件)	在成功停止了与硬件的通信时发生。

设备 - 可配置事件：

设备的可配置事件将从设备驱动程序自动导入。这意味着它们对于各个设备不尽相同，因此本文不进行介绍。在将可配置事件添加至系统并在设备的**事件**选项卡上配置之前，无法触发这些可配置事件。

设备 - 预定义事件：

事件	说明
书签引用请求	在客户端的实时模式下生成书签时发生。此外，还需要使用“默认根据书签进行录制”规则。
通信错误(设备)	与设备的连接断开时，或尝试与设备通信不成功时发生。
通信已开始(设备)	与设备成功建立了通信时发生。
通信已停止(设备)	成功停止与设备的通信时发生。
证据锁定已更改	由客户端用户或通过 MIP SDK 更改了设备的证据锁定时发生。
证据已锁定	由客户端用户或通过 MIP SDK 创建了设备的证据锁定时发生。

事件	说明
证据已取消锁定	由客户端用户或通过 MIP SDK 删除了设备的证据锁定时发生。
馈送溢出启动	在记录服务器不能以在配置中指定的速度处理接收到的数据，因此被迫丢弃部分录制时发生馈送溢出(媒体溢出)。 如果服务器状态良好，馈送溢出的发生通常都是由于磁盘写入速度太慢。可通过减少数据写入量或提高存储系统性能来解决此问题。通过降低摄像机帧速率、分辨率或图像质量减少数据写入量，但这可能降低录制质量。如果不想使用此方法，可以选择安装额外的驱动器以分担负载或者安装更快速的磁盘或控制器，从而提高存储系统的性能。 可以使用该事件触发操作，帮助避免问题，例如，降低录制帧速率。
馈送溢出停止	当数据源溢出(请参阅 第 412 页上的馈送溢出启动)结束时发生。
实时客户端馈送请求	客户端用户请求从设备获得实时流时发生。 在请求时发生事件，即使客户端用户的请求随后不成功，例如由于客户端用户没有查看请求的实时馈送的权限或者由于馈送出于某种原因而停止。
实时客户端馈送终止	客户端用户不再请求从设备获得实时流时发生。
手动记录已开始	在客户端用户启动摄像机的录制会话时发生。 即使设备正在通过规则操作录制，也会触发该事件。
手动记录已停止	在客户端用户停止摄像机的录制会话时发生。 如果规则系统还启动了录制会话，即使在手动录制停止后，它仍会继续录制。
已请求标记数据参考	在客户端中或通过 MIP SDK 在播放模式下生成了证据锁定时发生。 会创建您可以在规则中使用的事件。
操作启动	系统在接收自摄像机的视频中侦测到移动时发生。 此事件类型要求为事件所链接的摄像机启用系统的移动侦测。 除了系统的移动侦测之外，某些摄像机本身就能侦测移动并触发**操作启动(硬件)**事件，但这取决于摄像机硬件和系统中的配置。另请参阅 第 410 页上的硬件 - 可配置事件:。

事件	说明
操作停止	在接收的视频中不再侦测到移动时发生。另请参阅 第 412 页上的操作启动。 此事件类型要求为事件所链接的摄像机启用系统的移动侦测。 除了系统的移动侦测之外，某些摄像机本身就能侦测移动并触发“操作停止(硬件)”事件，但这取决于摄像机硬件和系统中的配置。另请参阅 第 410 页上的硬件 - 可配置事件:。
输出已激活	设备上的外部输出端口被激活时发生。 此事件类型要求系统中至少有一个设备支持输出端口。
输出已更改	设备上的外部输出端口的状态改变时发生。 此事件类型要求系统中至少有一个设备支持输出端口。
输出已取消激活	设备上的外部输出端口被取消激活时发生。 此事件类型要求系统中至少有一个设备支持输出端口。
PTZ 手动会话启动	手动操作的 PTZ 会话(与基于预定巡视的或由事件自动触发的 PTZ 会话相反)在摄像机上启动时发生。 此事件类型要求事件所链接的摄像机为 PTZ 摄像机。
PTZ 手动会话停止	手动操作的 PTZ 会话(与基于预定巡视的或由事件自动触发的 PTZ 会话相反)在摄像机上停止时发生。 此事件类型要求事件所链接的摄像机为 PTZ 摄像机。
录制开始	只要录制启动便会发生。已启动的手动录制有单独的事件。
录制已停止	只要录制停止便会发生。已停止的手动录制有单独的事件。
设置更改	设备的设置成功获得更改时发生。
设置更改错误	尝试更改设备的设置不成功时发生。

外部事件 - 预定义事件：

事件	说明
请求播放音频消息	通过 MIP SDK 请求播放音频消息时激活。 通过 MIP SDK 第三方供应商为您的系统开发自定义插件，例如，集成到外部访问控制系统或类似功能。
请求开始记录	通过 MIP SDK 请求开始记录时激活。 通过 MIP SDK 第三方供应商为您的系统开发自定义插件，例如，集成到外部访问控制系统或类似功能。
请求停止记录	通过 MIP SDK 请求停止记录时激活。 通过 MIP SDK 第三方供应商为您的系统开发自定义插件，例如，集成到外部访问控制系统或类似功能。

外部事件 - 常规事件：

常规事件应允许通过 IP 网络向系统发送简单字符串，从而在系统中触发操作。常规事件的目的是允许尽可能多的外部资源与系统交互。

外部事件 - 用户定义事件：

也可以选择进行多个事件自定义以符合系统要求。可为以下目的使用此类用户定义事件：

- 使得客户端用户能够在客户端中查看实时视频时手动触发事件
- 很多其他用途。例如，可以创建当从设备接收到特定类型的数据时发生的用户定义事件

  另请参阅 第 71 页上的用户定义事件(已解释)。

记录服务器：

事件	说明
存档可用	当记录服务器的存档从不可用变为可用时发生。另请参阅 第 414 页上的存档不可用。
存档不可用	在记录服务器的存档变得不可用时(如到网络驱动器上的存档的连接丢失时)发生。在这种情况下，无法为记录存档。

事件	说明
	例如，您可以使用事件来触发警报或通知配置文件，使得自动发送电子邮件通知到组织中的相关人员。
存档未完成	当记录服务器的存档尚未完成上一轮存档却已计划开始下一轮时发生。
设置保留大小之前数据库会删除录制	在达到数据库大小限值之前达到保留时间限值。
设置保留时间之前数据库会删除录制	在达到保留时间限值之前达到数据库大小限值。
数据库磁盘已满 - 正在自动存档	在数据库磁盘已满时发生。数据库磁盘剩余空间低于 5GB 时便被视为已满： 如果空闲空间小于 5GB，总是会将数据库中最旧的数据自动存档（或在未定义下一个存档时删除）。
数据库磁盘已满 - 正在删除	当数据库磁盘已满并有小于 1 GB 的空间可用时出现。即使已定义下一个存档，数据也会被删除。数据库始终需要 250MB 的空闲空间。如果达到此限制（如果未能足够快地删除数据），则在释放足够的空间之前，不会将更多数据写入数据库。数据库的实际最大大小是您指定的吉字节数减去 5GB。
数据库已满 - 自动存档	在记录服务器的存档已满却需要自动存档至存储中的存档时发生。
数据库修复	数据库出现问题时发生，这种情况下，系统会自动尝试两种不同的数据库修复方法：快速修复和完全修复。
数据库存储可用	当记录服务器的存储从不可用变为可用时发生。另请参阅 第 415 页上的数据库存储不可用。 例如，如果录制已被**数据库存储不可用**事件停止，则可以使用该事件来启动录制。
数据库存储不可用	在记录服务器的存储变得不可用时（如到网络驱动器上的存储的连接丢失时）发生。在这种情况下，无法为记录存档。 例如，您可以使用事件来停止录制、触发警报或通知配置文件，使得自动发送电子邮件通知到组织中的相关人员。
故障转移加密的通信错误	故障转移服务器与受监控的记录服务器之间存在 SSL 通信错误时发生。
故障转移启动	在故障转移记录服务器从记录服务器进行接管时发生。另请参阅故障转移服务器（节点）。
故障转移停止	在记录服务器重新可用并且可以从故障转移记录服务器进行接管时发生。

系统监视器事件

系统监视器事件是由**系统监测阈值**节点中配置的超阈值触发的。另请参阅 第 254 页上的查看硬件的当前状态，并在需要时进行故障排除。

> 此功能要求 Data Collector 服务正在运行。

系统监视器 - 服务器：

事件	说明
CPU 使用率处于临界状态	当 CPU 使用率超过临界 CPU 阈值时发生。
CPU 使用率处于正常状态	当 CPU 使用率回到警告 CPU 阈值以下时发生。
CPU 使用率处于警告状态	当 CPU 使用率超过警告 CPU 阈值或低于临界 CPU 阈值时发生。
内存使用率处于临界状态	当内存使用率超过临界内存阈值时发生。
内存使用率处于正常状态	当内存使用量下降到警告内存阈值以下时发生。
内存使用率处于警告状态	当内存使用率超过警告内存阈值，或者下降到临界内存使用阈值以下时发生。
NVIDIA 解码临界	当 NVIDIA 解码使用率超过临界 NVIDIA 解码阈值时发生。
NVIDIA 解码正常	当 NVIDIA 解码使用率下降到低于警告的 NVIDIA 解码阈值时发生。
NVIDIA 解码警告	当 NVIDIA 的解码使用率超过了警告 NVIDIA 解码阈值或低于临界 NVIDIA 解码阈值时发生。
NVIDIA 内存临界	当 NVIDIA 内存率使用超过临界 NVIDIA 内存阈值时发生。
NVIDIA 内存正常	当 NVIDIA 内存使用率下降到警告 NVIDIA 内存阈值以下时发生。
NVIDIA 内存警告	当 NVIDIA 内存使用率超过警告 NVIDIA 内存阈值，或者下降到临界 NVIDIA 内存阈值以下时发生。

事件	说明
NVIDIA 渲染临界	当 NVIDIA 渲染使用率超过临界 NVIDIA 渲染阈值时发生。
NVIDIA 渲染正常	当 NVIDIA 渲染使用率下降到警告 NVIDIA 渲染阈值以下时发生。
NVIDIA 渲染警告	当 NVIDIA 渲染使用率超过警告 NVIDIA 渲染阈值，或者下降到临界 NVIDIA 渲染阈值以下时发生。
可用服务处于临界状态	当服务器服务停止运行时发生。 此事件没有阈值。
可用服务处于正常状态	当服务器服务状态更改为运行时发生。 此事件没有阈值。

系统监视器 - 摄像机：

事件	说明
实时 FPS 处于临界状态	当实时 FPS 率低于临界实时 FPS 阈值时发生。
实时 FPS 处于正常状态	当实时 FPS 率超过警告的实时 FPS 阈值时发生。
实时 FPS 处于警告状态	当实时 FPS 率低于警告的实时 FPS 阈值或超过临界的实时 FPS 阈值时发生。
录制 FPS 处于临界状态	当录制 FPS 率低于临界录制 FPS 阈值时发生。
录制 FPS 处于正常状态	当录制 FPS 率超过警告的录制 FPS 阈值时发生。
录制 FPS 处于警告状态	当录制 FPS 率低于警告录制 FPS 阈值或超过临界录制 FPS 阈值时发生。
已用空间处于临界状态	当用于特定摄像机录制的存储空间超过临界使用空间阈值时发生。
已用空间处于正常状态	当用于特定摄像机录制的存储空间低于警告使用空间阈值时发生。
已用空间处于警告状态	当用于特定摄像机录制的存储空间超过警告使用空间阈值或低于临界使用空间阈值时发生。

系统监视器 - 磁盘：

事件	说明
可用空间处于临界状态	当磁盘空间使用超过临界可用空间阈值时发生。
可用空间处于正常状态	当磁盘空间使用低于警告可用空间阈值时发生。
可用空间处于警告状态	当磁盘空间使用超过警告可用空间阈值或低于临界可用空间阈值时发生。

系统监视器 - 存储：

事件	说明
保留时间处于临界状态	当系统预测存储将比临界保留时间阈值更快地填满时发生。例如，当来自视频流的数据以比预期更快地填充存储时。
保留时间处于正常状态	当系统预测存储将比警告保留时间阈值更慢地填满时发生。例如，当来自视频流的数据以预期速率填充存储时。
保留时间处于警告状态	当系统预测存储将以比警告保留时间阈值更快速度，或者比临界保留时间阈值更慢的速度填充时发生。例如，由于被配置为录制运动的摄像机所检测到的更多运动，当来自视频流的数据以比预期更快的速率填充存储时。

其他：

事件	说明
自动在线激活序列号失败	当自动在线激活序列号失败时发生。 对于此事件，没有阈值。
已开始进行计划好的密码更改	开始进行计划好的密码更改时发生。
已成功完成了计划好的密码更改	完成计划好的密码更改而且不出错时发生。
已完成了计划好的密码更改，但出现错误	完成计划好的密码更改但出错时发生。

来自 XProtect 扩展和集成的事件：

来自 XProtect 扩展和集成的事件可用于规则系统，例如：

- 分析事件也可在规则系统中使用

操作和停止操作

一组操作和停止操作可用于**管理规则**向导中的规则创建。如果本系统安装使用 XProtect 扩展或特定于供应商的插件，则可能有更多操作可用。对于每种操作类型，列出了相关停止操作信息。

管理规则向导

动作	说明
在 <设备> 上开始记录	开始录制，并将数据保存在所选设备的数据库中。 选择此类型操作时，**管理规则**向导将提示您指定： 应开始录制的时间。这应在要发生操作的设备上立即或于触发事件/触发时间间隔开始之前数秒发生。 此操作类型要求操作所链接的设备上已启用录制。仅当为相关设备启用了预缓冲时，才能保存事件或时间间隔之前的数据。可在**录制**选项卡上启用录制和指定设备的预缓冲设置。 **需要停止动作**：此动作类型需要一个或多个停止动作。在以下步骤之一中，向导将自动提示您指定停止动作：**停止录制**。 没有此停止操作，录制可能会无限期继续下去。还可以选择指定更多停止操作。
在 <设备> 上开始馈送	开始从设备向本系统进行数据馈送。开始从设备馈送时，数据将从设备传送到本系统，这样就可根据数据类型查看和录制。 选择此操作类型时，**管理规则**向导将提示您指定在哪些设备上启动馈送。本系统包括确保始终在所有摄像机上启动馈送的默认规则。 **需要停止动作**：此动作类型需要一个或多个停止动作。在以下步骤之一中，向导将自动提示您指定停止动作：**停止馈送**。 还可以指定更多停止操作。 使用强制停止操作**停止馈送**停止设备的馈送意味着不再从该设备传送数据到本系统，这样就(例如)无法再进行实时查看和录制视频。然而，已停止馈送的设备仍然可以与记录服务器通信，并且可通过规则自动重新启动馈送(与手动禁用设备后的情况相反)。

动作	说明
	当此操作类型启用了对选定设备的数据馈送的访问时，并不能保证会录制数据，因为必须单独指定录制设置。
将 <Smart Wall> 设置为 <预设>	将 XProtect Smart Wall 设置为所选预设。指定 **Smart Wall 预设**选项卡上的预设。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
设置 <Smart Wall> <监视器> 以显示 <摄像机>	设置特定 XProtect Smart Wall 监视器以显示本站点或在 Milestone Federated Architecture 中配置的任何子站点上的所选摄像机的实时视频。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
将 <Smart Wall> <监视器> 设置为显示文本 <消息>	设置特定的 XProtect Smart Wall 监视器，以显示用户定义的最大长度为 200 个字符的文本消息。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
从 <Smart Wall> 监视器 <监视器> 删除 <摄像机>	停止显示特定摄像机的视频。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
在 <设备> 上设置实时帧速率	设置系统显示选定摄像机的实时视频时使用的特定帧速率(用于替代摄像机的默认帧速率)。在**设置**选项卡上进行该指定。 选择此操作类型时，**管理规则**向导将提示您指定在哪些设备上设置哪个帧速率。始终确认指定的帧速率在相关摄像机上可用。 **需要停止动作**：此动作类型需要一个或多个停止动作。在以下步骤之一中，向导将自动提示您指定停止动作：**恢复默认实时帧速率**。 没有此停止操作，可能始终不会恢复默认帧速率。还可以选择指定更多停止操作。
在 <设备> 上设置记录帧速率	设置系统在数据库中保存选定摄像机的录制视频时使用的特定帧速率(不使用摄像机的默认录制帧速率)。 选择此操作类型时，**管理规则**向导将提示您指定在哪些摄像机上设置哪个录制帧速率。 只能针对 JPEG 指定录制帧速率，JPEG 是一种视频编码解码器，它将每个帧分别压缩为 JPEG 图像。此操作类型还要求操作所链接的摄像机上已启用录制。可在**录制**选

动作	说明
	项卡上启用摄像机录制。可以指定的最大帧速率取决于相应摄像机类型及其选定图像分辨率。 **需要停止动作**:此动作类型需要一个或多个停止动作。在以下步骤之一中,向导将自动提示您指定停止动作:**恢复默认录制帧速率**。 没有此停止操作,可能始终不会恢复默认录制帧速率。还可以选择指定更多停止操作。
设置 <设备> 上所有 MPEG-4/H.264/H.265 帧的记录帧速率	设置系统在数据库中保存选定摄像机的录制视频时,帧速率为录制所有帧,而不是仅关键帧。在**录制**选项卡上启用"只录制关键帧"功能。 选择此操作类型时,**管理规则**向导将提示您选择应该应用操作的设备。 只可以为 MPEG-4/H.264/H.265 启用关键帧录制。此操作类型还要求操作所链接的摄像机上已启用录制。可在**录制**选项卡上启用摄像机录制。 **需要停止动作**:此动作类型需要一个或多个停止动作。在以下步骤之一中,向导将自动提示您指定停止动作: **恢复 MPEG-4/H.264/H.265 关键帧的默认录制帧速率** 如果没有此停止操作,可能始终不会恢复默认设置。还可以选择指定更多停止操作。
使用带 PTZ 优先级 <优先级> 的 <配置文件> 开始巡视 <设备>	为具有特定优先级的特定 PTZ 摄像机根据特定巡视配置文件开启 PTZ 巡视。这是有关巡视执行方式的准确定义,包括预设位置的顺序、时间设置等。 如果自较早版本的系统升级系统,旧的值(**非常低**、**低**、**中**、**高**和**非常高**)已经转换为以下值: • 非常低 = 1000 • 低 = 2000 • 中 = 3000 • 高 = 4000 • 非常高 = 5000 选择此操作类型时,**管理规则**向导将提示您选择巡视配置文件。只能在一个设备上选择一个巡视配置文件,不能选择多个巡视配置文件。 此动作类型要求动作所链接的设备为 PTZ 设备。

动作	说明
	必须为设备定义至少一个巡视配置文件。可在**巡视选项卡**上定义 PTZ 摄像机的巡视配置文件。 **需要停止动作**:此动作类型需要一个或多个停止动作。在以下步骤之一中,向导将自动提示您指定停止动作: **停止巡视** 没有此停止操作,巡视可能永远不会停止。还可以指定更多停止操作。
暂停巡视 <设备>	暂停 PTZ 巡视。选择此操作类型时,**管理规则**向导将提示您指定在哪些设备上暂停巡视。 此动作类型要求动作所链接的设备为 PTZ 设备。 必须为设备定义至少一个巡视配置文件。可在**巡视选项卡**上定义 PTZ 摄像机的巡视配置文件。 **需要停止动作**:此动作类型需要一个或多个停止动作。在以下步骤之一中,向导将自动提示您指定停止动作:**恢复巡视** 没有此停止操作,巡视可能会无限期暂停。还可以选择指定更多停止操作。
将 <设备> 移至有 PTZ 优先级 <优先级> 的 <预设> 位置	将特定摄像机移至(然而始终根据优先级)特定预设位置。选择此操作类型时,**管理规则**向导将提示您选择预设位置。在一个摄像机上只能选择一个预设位置。无法选择多个预设位置。 此动作类型要求动作所链接的设备为 PTZ 设备。 该动作要求为这些设备定义了至少一个预设位置。可在**预设选项卡**上定义 PTZ 摄像机的预设位置。 **无强制停止动作**:此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。

动作	说明
移至有 PTZ 优先级 <优先级> 的 <设备> 默认预设	将一个或多个特定摄像机移至(然而始终根据优先级)各自的默认预设位置。选择此操作类型时，**管理规则**向导将提示您选择应该应用操作的设备。 此动作类型要求动作所链接的设备为 PTZ 设备。 该动作要求为这些设备定义了至少一个预设位置。可在**预设选项卡**上定义 PTZ 摄像机的预设位置。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
将设备输出设置为 <状态>	将设备输出设置为特定状态(已激活或已取消激活)。选择此操作类型时，**管理规则**向导将提示您指定在哪些设备上设置何种状态。 此操作类型要求操作所链接的每个设备至少有一个连接到输出端口的外部输出单元。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
在 <设备> 上创建书签	在选定设备的实时流或录制上创建书签。使用书签可方便追溯特定事件或时间段。书签设置在**选项**对话框中进行控制。选择此操作类型时，**管理规则**向导将提示您指定书签详细信息并选择设备。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
播放<设备>上<优先级>的音频<消息>	在所选设备上播放由事件触发的音频消息。设备大多为扬声器或摄像机。 这类动作需要您已在**工具 > 选项 > 音频消息**选项卡上将消息上传至系统。 您可以为同一事件创建多个规则，并向每台设备发送不同消息，但要始终符合优先级。控制顺序的优先级是在规则上设置以及通过**语音**选项卡在设备上为角色设置的优先级： • 如果已播放一条消息，并且将另一条具有相同优先级的消息发送至同一扬声器，将在完成第一条消息后继续播放第二条 • 如果已播放一条消息，并且将另一条具有更高优先级的消息发送至同一扬声器，将中断第一条消息，立即播放第二条
发送通知到 <配置文件>	使用特定通知配置文件发送通知。选择此操作类型时，**管理规则**向导将提示您选择通知配置文件以及包含预警报图像的来源设备。只能选择一个通知配置文件，而不能选择多个通知配置文件。单个通知配置文件可能包含多个接收方。

动作	说明
	还可以为相同事件创建更多规则，并向每个通知配置文件发送不同通知。可以通过在**规则**列表中右键单击规则来复制和重用规则内容。 该操作类型要求定义了至少一个通知配置文件。仅当为相关通知配置文件启用了**包含图像**选项时，才会包含预警报图像。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
新建 <日志条目>	在规则日志中生成条目。选择此操作类型时，**管理规则**向导将提示您为日志条目指定文本。指定日志文本时，可以在日志消息中插入变量，例如：**$DeviceName$**、**$EventName$**。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
在 <设备> 上启动插件	启动一个或多个插件。选择此操作类型时，**管理规则**向导将提示您选择所需插件以及要启动插件的设备。 此操作类型要求在系统上安装至少一个或多个插件。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
在 <设备> 上停止插件	停止一个或多个插件。选择此操作类型时，**管理规则**向导将提示您选择所需插件以及要停止插件的设备。 此操作类型要求在系统上安装至少一个或多个插件。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
在 <设备> 上应用新设置	更改一个或多个设备上的设备设置。选择此操作类型时，**管理规则**向导将提示您选择相关设备，并且您可以在指定的设备上定义相关设置。 如果为一个以上设备定义设置，则只能更改可用于所有指定设备的设置。 **示例**：指定操作应链接到设备 1 和设备 2。设备 1 具有设置 A、B 和 C，而设备 2 具有设置 B、C 和 D。在这种情况下，只能更改同时可用于两个设备的设置，即设置 B 和 C。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。

动作	说明
设置 Matrix，以查看 <设备>	使得选定摄像机的视频显示在能够显示 Matrix 所触发视频的计算机上，如安装了 XProtect Smart Client 的计算机。 选择此动作类型时，**管理规则**向导将提示您选择 Matrix 接收方以及在所选 Matrix 接收方上显示视频的一个或多个来源设备。 此动作类型仅允许您每次选择一个 Matrix 接收方。如果要使选定设备的视频显示在一个以上 Matrix 接收方，则应为每个所需 Matrix 接收方创建规则或使用 XProtect Smart Wall 功能。通过在**规则**列表中右键单击规则，可复制和重用规则内容。这样，就不必从头创建几乎相同的规则。 作为 Matrix 接收方自身配置的一部分，用户必须指定 Matrix 通信所需的端口号和密码。确保用户有权访问此信息。用户通常还必须定义允许的主机（接受显示 Matrix 所触发视频相关命令的来源主机）的 IP 地址。在这种情况下，用户还必须知道管理服务器或所用任何路由器或防火墙的 IP 地址。
发送 SNMP 陷阱	在选定设备上生成录制事件的小型消息。SNMP 陷阱的文本是自动生成的，无法自定义。可以包含已发生事件所在的设备的来源类型和名称。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
从 <设备> 检索并存储远程记录	检索和存储（支持边缘录制的）选定设备在触发事件前后的指定时间段内的远程录制。 此规则与连接恢复时**自动检索远程记录**设置无关。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
从 <设备> 检索并存储 <开始时间和结束时间> 之间的远程记录	检索和存储（支持边缘录制的）选定设备在指定时间段内的远程录制。 此规则与连接恢复时**自动检索远程记录**设置无关。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
保存附加的图像	确保收到来自“图像接收”事件的图像（摄像机通过 SMTP 电子邮件发送）时会将其保存以供将来使用。将来，其他事件也可能触发此操作。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。

动作	说明
在 <存档> 上激活存档	启动一个或多个存档上的存档操作。选择此操作类型时，**管理规则**向导将提示您选择相关存档。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
在 <站点> 触发器上 <用户定义的事件>	最常用于 Milestone Federated Architecture 中，但也可在单站点安装中使用它。使用该规则在站点（通常为联合分层中的远程站点）上触发用户定义事件。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
显示 <访问请求通知>	允许在满足触发事件的条件时，在 XProtect Smart Client 屏幕上弹出访问请求通知。Milestone 建议使用访问控制事件作为该动作的触发事件，因为访问请求通知通常配置用于相关访问控制命令和摄像机上的操作。 此操作类型要求在系统上安装至少一个访问控制插件。 **无强制停止动作**：此操作类型不需要停止操作。可指定在事件发生时或一段时间后执行可选停止动作。
更改硬件设备上的密码	根据该特定硬件设备的密码要求，将所选硬件设备的密码更改为随机生成的密码。有关受支持的硬件设备的列表，请参阅查找硬件。 只有在使用**对 <recurring time> 执行操作**规则类型设置规则时，此操作才可用。 以下事件可用于该操作： • 第 418 页上的已开始进行计划好的密码更改 • 第 418 页上的已成功完成了计划好的密码更改 • 第 418 页上的已完成了计划好的密码更改，但出现错误 此动作类型不具有停止动作。 您可以在**当前任务**节点中查看此操作的进度。有关详细信息，请参阅第 252 页上的查看记录服务器上当前正在进行的任务。 要查看操作结果 - 转到**系统日志**选项卡上的**服务器日志**节点。有关详细信息，请参阅第 333 页上的“服务器日志”选项卡（选项）。 有关详细信息，请参阅系统日志（选项卡）。

测试分析事件(属性)

测试分析事件的要求时，会出现一个窗口，用于检查四个条件，并提供可能的错误描述和解决方案。

条件	说明	错误消息和解决方案
更改已保存	如果是新事件，该事件是否已保存？或者如果事件名称有所更改，这些更改是否已保存？	**测试分析事件之前保存更改**。解决方案/说明：保存变更。
分析事件已启用	分析事件功能是否已启用？	**分析事件尚未启用**。解决方案/说明：启用分析事件功能。为此，单击**工具 > 选项 > 分析事件**，然后选中**已启用**复选框。
允许地址	发送事件的计算机的 IP 地址/主机名是否已被允许(在分析事件地址列表中列出)？	**本地主机名必须添加为 Analytics Event 服务允许的地址**。解决方案/说明：将您的计算机添加到允许的 IP 地址或主机名的分析事件地址列表。 **解析本地主机名时出错**。解决方案/说明：计算机的 IP 地址或主机名无法找到或无效。
发送分析事件	是否将测试事件成功发送到事件服务器？	请参阅下表。

每个步骤标记为失败：✗或成功：✓.

条件**发送分析事件**的错误消息和解决方案：

错误消息	解决方案
事件服务器未找到	无法在注册服务列表中找到事件服务器。
连接到事件服务器时出错	无法连接到声明端口上的事件服务器。发生错误很可能是由于网络问题或 Event Server 服务已停止。
发送分析事件时出错	已建立与事件服务器的连接，但无法发送事件。发生错误很可能是由于网络问题，如超时。
从事件服务器接收响应时出错	已将事件发送到事件服务器，但没有收到回复。发生错误很可能是因为网络问题或端口正忙。

错误消息	解决方案
	请查看通常位于 ProgramData\Milestone\XProtect Event Server\Logs\ 的事件服务器日志。
事件服务器不知道分析事件	Event Server 服务不知道事件。发生错误很可能是因为没有保存事件或对事件所作的更改。
事件服务器接收到无效分析事件	事件格式不正确。
发件人未经事件服务器授权	很可能您的计算机不在允许的 IP 地址或主机名列表中。
事件服务器中的内部错误	事件服务器错误。 请查看通常位于 ProgramData\Milestone\XProtect Event Server\Logs\ 的事件服务器日志。
从事件服务器接收到无效响应	响应无效。可能是因为端口正忙或出现网络问题。 请查看通常位于 ProgramData\Milestone\XProtect Event Server\Logs\ 的事件服务器日志。
来自事件服务器的响应未知	响应有效但无法理解。发生错误可能是因为网络问题或端口正忙。 请查看通常位于 ProgramData\Milestone\XProtect Event Server\Logs\ 的事件服务器日志。
意外错误	请联系 Milestone 支持部门以获取帮助。

常规事件和数据来源(属性)

该功能仅在安装 XProtect 事件服务器后才能工作。

常规事件(属性)

组件	要求
名称	常规事件的唯一名称。名称必须在所有类型的事件中都唯一，例如用户定义事件、分析事件等。

组件	要求
已启用	常规事件默认是启用的。清除该复选框可禁用事件。
表达式	在分析数据包时本系统应查找的表达式。可使用以下运算符： • ( )：用来确保将相关术语作为逻辑单位一起处理。可使用它们在分析中强制执行特定的处理顺序 **示例**：搜索条件“(User001 OR Door053) AND Sunday”会首先处理括号中的两个术语，然后将结果与字符串的最后一部分结合。因此，系统首先查找包含术语 User001 或 Door053 的任何数据包，然后再运行结果来查看哪些数据包还包含术语 Sunday。 • AND：通过使用 AND 运算符，可指定必须包含 AND 运算符两边的术语 **示例**：搜索条件“User001 AND Door053 AND Sunday”只有在术语 User001、Door053 和 Sunday 均包括在表达式中时才会返回结果。仅包含其中一个或两个术语并不够。使用 AND 结合的术语越多，检索到的结果就越少。 • OR：可通过 OR 运算符指定必须包括的一个或其他术语 **示例**：搜索条件“"User001" OR "Door053" OR "Sunday"”会返回包含 User001、Door053 或 Sunday 的所有结果。使用 OR 结合的术语越多，检索到的结果就越多。
表达式类型	表示本系统在分析接收到的数据包时的特定行为。选项如下所示： • **搜索**：为了使事件发生，已接收的数据包必须包含在**表达式**字段中指定的文本，但还可包含更多内容 **示例**：如果已指定接收到的数据包应包含术语 User001 和 Door053，则如果接收到的数据包包含术语User001和Door053 以及 Sunday，将会触发事件，因为所需的两个术语已包含在接收到的数据包中。 • **匹配**：他内容为了使事件发生，接收到的数据包必须包含与**表达式**字段中指定的文本一样的内容，不得包含其 • **正则表达式**：为了使事件发生，在**表达式**字段中指定的文本必须能够识别接收到的数据包中的特定模式 如果从**搜索**或**匹配**切换至**正则表达式**，**表达式**字段中的文本会自动翻译为正则表达式。
优先级	必须将优先级指定为 0(最高优先级) 和 999999(最低优先级) 之间的一个数字。 可能针对不同事件分析同一数据包。通过为每个事件指定优先级，可管理当已接收的软件包匹配多个事件的条件时，应触发哪个事件。 当本系统接收到 TCP 和/或 UDP 数据包时，数据包分析过程将首先分析具有最高优先级的事件。这样，就可以在数据包符合若干事件的条件时，仅触发具有最高优先级的事件。如果数据包符合几个具有相同优先级事件的条件，例如，两个事件的优先级都是 999，则系统会自动触发具

组件	要求
	有此优先级的所有事件。
检查表达式是否与事件字符串匹配	根据在**表达式**字段中输入的表达式来测试事件字符串。

Webhooks(规则和事件节点)

在 **Webhook** 节点中，您可以创建、编辑和删除 Webhook 端点。

创建和编辑 Webhook 时，以下字段可用：

字段	说明
名称	输入 Webhook 端点的唯一名称。 主机名不能为空。
地址	您要向其发送事件数据的 Web 服务器或应用程序的 URL。如果 Web 服务器的 URL 已更新，则必须在 Webhook 节点中更新 Webhook URL。 通过不安全的网络(如开放互联网)使用 HTTP，会以纯文本形式暴露所有事件。
令牌	输入一个用于通过验证 HTTP POST 来源的令牌，以帮助确保与其他应用程序的通信安全。 使用令牌进行安全通信是可选的，但建议使用。
API 版本	用于 Webhook 功能的 Webhook 插件和 API 的版本。

安全节点

角色(“安全性”节点)

“信息”选项卡(角色)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

在角色的**信息**选项卡上,可以进行以下设置:

名称	说明
名称	输入角色的名称。
说明	输入角色的说明。
Management Client 配置文件	选择要与角色关联的 Management Client 配置文件。 不能将它应用至默认**管理员**角色。 需要在管理服务器上管理安全性的权限。
Smart Client 配置文件	选择要与角色关联的 Smart Client 配置文件。 需要在管理服务器上管理安全性的权限。
默认时间配置文件	选择要与角色关联的默认时间配置文件。 不能将它应用至默认**管理员**角色。
证据锁定配置文件	选择要与角色关联的证据锁定配置文件。
时间配置文件内的 **Smart Client 登录**	选择与该角色关联的 XProtect Smart Client 用户被允许登录的时间配置文件。 如果 XProtect Smart Client 用户在期限到期时登录,该用户将被自动注销。 不能将它应用至默认**管理员**角色。
允许 Smart Client 登录	选中复选框以允许与此角色关联的用户登录 XProtect Smart Client。

名称	说明
	默认不允许访问 Smart Client。取消选中复选框拒绝访问 XProtect Smart Client。
允许 XProtect Mobile 客户端登录	选中复选框以允许与此角色关联的用户登录 XProtect Mobile 客户端。 默认不允许访问 XProtect Mobile 客户端。取消选中复选框拒绝访问 XProtect Mobile 客户端。
允许 XProtect Web Client 登录	选中复选框以允许与此角色关联的用户登录 XProtect Web Client。 默认不允许访问 XProtect Web Client。取消选中复选框拒绝访问 XProtect Web Client。
需要登录授权	选中该复选框可将登录授权与角色关联。这意味着在用户登录时，XProtect Smart Client 或 Management Client 会请求二次授权，通常由超级用户或管理员进行。 要使管理员能够为用户授权，请在**整体安全**选项卡上配置管理服务器的**为用户授权**权限。 不能将它应用至默认**管理员**角色。
在 PTZ 会话期间使用户匿名	如果选中该复选框，可在与该角色关联的用户控制 PTZ 会话时隐藏其名称。

“用户和组”选项卡(角色)

在**用户和组**选项卡上，将用户和组分配给角色(请参阅 第 249 页上的将用户和组分配至角色/从角色删除)。您可以分配 Windows 用户和组或基本用户(请参阅 第 57 页上的用户(已解释))。

外部 IDP(角色)

在**外部 IDP**选项卡上，您可以查看现有声明并向角色添加新声明。

名称	说明
外部 IDP	外部 IDP 的名称。
声明名称	在外部 IDP 中定义的变量。
声明值	可以用于分配适当角色到用户的索赔值，比如组名称。

“整体安全”选项卡(角色)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

在**整体安全**选项卡上设置角色的整体权限。对于系统中的每个可用组件,通过设置**允许**或**拒绝**来定义角色的访问权限。如果拒绝某个角色访问组件,则该角色的用户在**整体安全**选项卡中看不到该组件。

总体安全选项卡在免费 XProtect Essential+ 中不可用。

您可以为 XProtect Corporate 定义比其他 XProtect 视频管理软件产品更多的权限。这是因为在 XProtect Corporate 中只能设置不同的管理员权限,而您可以在所有产品中为使用 XProtect Smart Client、XProtect Web Client 或 XProtect Mobile 客户端的角色设置整体权限。

整体安全设置仅应用于当前站点。

如果将一个用户与多个角色关联,并为一个角色的安全设置选择**拒绝**,而为另一个角色选择**允许**,则**拒绝**权限会驳回**允许**权限。

下文的描述将介绍在为相关角色选择**允许**时,不同系统组件的每个权限会发生的情况。如果使用 XProtect Corporate,则可以在每个系统组件下看到**只有**您的系统可以使用的设置。

对于每个系统组件或功能,具有完整系统权限的管理员可以使用**允许**或**拒绝**复选框设置角色的安全权限。您在此处设置的任何安全权限都是为整个系统组件或功能设置的。(例如)如果选中**摄像机**上的**拒绝**复选框,则添加至系统的所有摄像机对于该角色均不可用。相反,如果选中**允许**复选框,角色可以看到添加到系统中的所有摄像机。在摄像机上选择**允许**或**拒绝**的结果是**设备**选项卡上的摄像机设置继承了**整体安全**选项卡上的选择,以便所有摄像机可用或不可用于特定角色。

如果要为**单独**的摄像机或相似设备设置安全权限,则当您在**整体安全**选项卡上**没有为系统组件或功能设置任何整理权限**的情况下,只能在相关系统组件或功能的选项卡上设置这些单独权限。

以下描述还适用于可以通过 MIP SDK 配置的权限。

如果您想将基本许可证从 XProtect Corporate 切换得到其他产品,请确保删除仅可用于 XProtect Corporate 的所有安全权限。如果您没有删除这些权限,您就无法完成切换。

管理服务器

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
连接	让用户能够连接到 Management Server。 默认情况下会启用此权限。 出于维护目的，您可以暂时拒绝角色的连接权限，然后重新应用对系统的访问权限。 必须选择此权限才能访问系统。
读取	此权限是一个高度特权的管理权限，它为 XProtect VMS 提供重要的访问权限，包括访问敏感数据，例如系统中配置的凭据。 启用对广泛功能的访问权限，其中包括： • 使用 Management Client 登录 • 当前任务的列表 • 服务器日志 它还可以访问： • 远程连接服务 • Smart Client 配置文件 • Management Client 配置文件 • Matrix • 时间配置文件 • 已注册服务器和服务注册 API 此权限还会向客户透露一些敏感信息： • 任何已配置的外部 IDP 的凭据 • ...中所有摄像机的凭据、IP 地址和其他信息XProtect VMS

安全权限	说明
	• 已配置邮件服务器的凭据 • 任何已配置矩阵的凭据 • 为互连功能配置的凭据 • 为许可证激活配置的凭据 此权限不会显示 XProtect VMS 用户的凭据。这包括基本用户、Windows用户和来自外部 IDP 的用户。
编辑	启用对广泛功能的数据的修改权限，其中包括： • 选项 • 许可证管理 它还使用户能够创建、删除和编辑以下内容： • 远程连接服务 • 设备组 • Matrix • 时间配置文件 • 通知配置文件 • 已注册服务器 启用在记录服务器上配置网络时配置本地 IP 范围的权限。
系统监视器	启用查看系统监视器的数据的权限。
状态 API	启用对位于记录服务器上的状态 API 执行查询的权限。这意味着启用此权限的角色有权读取位于记录服务器上的项目的状态。
管理联合站点层级	启用将当前站点添加至联合站点层级中的其他站点以及从其中分离的权限。 如果将该权限设置为仅在子站点上允许，则用户仍然可以从父站点分离站点。
备份配置	启用使用系统的备份和还原功能创建系统配置备份的权限。
为用户授权	启用在 XProtect Smart Client 或 Management Client 中用户被要求二次登录时为用户授

安全权限	说明
	权的权限。您在**信息**选项卡上定义角色是否需要登录授权。
管理安全	启用管理管理服务器的权限的权限。 并为用户创建、删除和编辑启用以下功能： • 角色 • 基本用户 • Smart Client 配置文件 • Management Client 配置文件

记录服务器

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
编辑	启用编辑记录服务器上的属性的权限，需要管理服务器上的编辑权限的网络配置设置除外。
删除	启用删除记录服务器的权限。为此，还必须在以下对象上为用户赋予删除权限： • 硬件安全组(如果已将硬件添加至记录服务器) 如果记录服务器上的任何设备包含证据锁定，则只能在记录服务器脱机时将其删除。
管理硬件	启用在记录服务器上添加硬件的权限。
管理存储	启用管理记录服务器上的存储容器(即创建、删除、移动和清空存储容器)的权限。
管理安全	启用管理记录服务器的安全权限的权限。

故障转移服务器

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在 Management Client 中查看和访问故障转移服务器的权限。
编辑	启用在 Management Client 中创建、更新、删除、移动和启用或禁用故障转移服务器的权限。
管理安全	启用管理故障转移服务器的安全权限的权限。

Mobile 服务器

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在 Management Client 中查看和访问移动服务器的权限。
编辑	启用在 Management Client 中编辑和删除移动服务器的权限。
管理安全	启用管理移动服务器的安全权限的权限。
创建	启用向系统添加移动服务器的权限。

硬件

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
编辑	启用编辑硬件上的属性的权限。
删除	启用删除硬件的权限。 如果任何硬件设备包含证据锁定，则只能在记录服务器脱机时删除硬件。
驱动程序命令	启用将特殊指令发送到驱动器从而管理功能和配置的权限。 这里的**驱动程序命令**权限仅适用于客户端中专门开发的 MIP 插件。它不控制标准配置任务。
查看密码	启用在**编辑硬件**对话框中查看硬件设备上的密码的权限。
管理安全	启用管理硬件的安全权限的权限。

摄像机

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端和 Management Client 中查看摄像机设备的权限。

安全权限	说明
编辑	启用编辑 Management Client 中摄像机属性的权限。它还允许用户启用或禁用摄像机。
查看实时信息	启用在客户端和 Management Client 中查看摄像机的实时视频的权限。
查看受限的实时	启用在客户端与 Management Client 中对摄像机的实时受限视频进行查看的权限。
播放	启用在所有客户端中播放摄像机的记录视频的权限。
播放受限记录	启用在所有客户端中对摄像机中录制的受限视频进行播放的权限。
检索远程记录	启用在客户端中从远程站点上的摄像机检索记录的权限，或启用从摄像机上的边缘存储检索记录的权限。
读取片段	启用在客户端中读取片断信息(例如，与播放记录视频相关的片断信息)的权限。
智能搜索	启用在客户端中使用智能搜索功能的权限。
导出	启用从客户端导出记录的权限。
创建书签	启用在客户端中的记录和实时视频中创建书签的权限。
读取书签	启用在客户端中搜索和读取书签详细信息的权限。
编辑书签	启用在客户端中编辑书签的权限。
删除书签	启用在客户端中删除书签的权限。
创建和扩展证据锁定	启用在客户端中创建和扩展证据锁定的权限。
读取证据锁定	启用在客户端中搜索和读取证据锁定的权限。
删除和减少证据锁定	启用在客户端中删除或减少证据锁定的权限。
创建和扩展实时和播放限制	启用在客户端中对限制进行创建和扩展的权限。
读取实时和播放限制	启用在客户端中对既有限制的列表进行查看的权限。
删除和减少实时和播放限制	启用在客户端中对限制进行删除和缩减的权限。

安全权限	说明
开始手动记录	启用在客户端中启动视频的手动记录的权限。
停止手动记录	启用在客户端中启动视频的手动记录的权限。
AUX 命令	启用从客户端在摄像机上使用辅助 (AUX) 命令的权限。 **AUX 命令**为用户提供对通过视频编码器连接的摄像机上的刮水器的控制。通过辅助连接所连接的摄像机相关设备通过客户端受到控制。
手动 PTZ	启用在客户端和 Management Client 中使用 PTZ 摄像机上的 PTZ 功能的权限。
激活 PTZ 预设或巡视配置文件	启用在客户端和 Management Client 中将 PTZ 摄像机移到预设位置、启动和停止巡视配置文件以及暂停巡视的权限。 要允许此角色在摄像机上使用其他 PTZ 功能，请启用**手动 PTZ** 权限。
管理 PTZ 预设或巡视配置文件	启用在客户端和 Management Client 中对 PTZ 摄像机添加、编辑和删除 PTZ 预设和巡视配置文件的权限。 要允许此角色在摄像机上使用其他 PTZ 功能，请启用**手动 PTZ** 权限。
锁定/解锁 PTZ 预设	启用在 Management Client 中锁定和解锁 PTZ 预设的权限。这可以防止或允许其他用户更改客户端和 Management Client 中的预设位置。
保留 PTZ 会话	启用在客户端和 Management Client 中保留 PTZ 会话模式中设置 PTZ 摄像机的权限。 在保留 PTZ 会话中，具有更高 PTZ 优先级的其他用户无法接管控制权。 要允许此角色在摄像机上使用其他 PTZ 功能，请启用**手动 PTZ** 权限。
释放 PTZ 会话	启用从 Management Client 释放其他用户的 PTZ 会话的权限。 您始终可以释放自己的 PTZ 会话(不需要此权限)。
删除记录	启用通过 Management Client 从系统删除存储的视频记录的权限。
解除隐私屏蔽	启用临时解除 XProtect Smart Client 中隐私屏蔽的权限。它也有权授权其他 XProtect Smart Client 用户解除隐私屏蔽。 可解除隐私屏蔽仅适用于在 Management Client 中配置为可解除隐私屏蔽的隐私屏蔽。
管理安全	启用在 Management Client 中管理摄像机的安全权限的权限。

麦克风

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端和 Management Client 中查看麦克风设备的权限。
编辑	启用在 Management Client 中编辑麦克风属性的权限。它还允许用户启用或禁用麦克风。
监听实时信息	启用在客户端和 Management Client 中监听扬声器的实时音频的权限。
收听受限的实时音频	启用在客户端与 Management Client 中对扬声器的实时受限音频进行收听的权限。
播放	启用在客户端中播放麦克风的记录音频的权限。
播放受限记录	启用在客户端中对麦克风中录制的受限音频进行播放的权限。
检索远程记录	启用在客户端中从远程站点上的麦克风检索记录的权限，或启用从摄像机上的边缘存储检索记录的权限。
读取片段	启用在客户端中读取片断信息(例如，与**播放**相关的片断信息)的权限。
导出	启用从客户端导出记录的权限。
创建书签	启用在客户端中创建书签的权限。
读取书签	启用在客户端中搜索和读取书签详细信息的权限。
编辑书签	启用在客户端中编辑书签的权限。
删除书签	启用在客户端中删除书签的权限。
创建和扩展证据锁定	启用在客户端中创建或扩展证据锁定的权限。
读取证据锁定	启用在客户端中搜索和读取证据锁定详细信息的权限。
删除和减少证据锁	启用在客户端中删除或减少证据锁定的权限。

安全权限	说明
定	
创建和扩展实时和播放限制	启用在客户端中对麦克风所受的限制进行创建和扩展的权限。
读取实时和播放限制	启用在客户端中对麦克风所受既有限制的列表进行查看的权限。
删除和减少实时和播放限制	启用在客户端中对麦克风所受限制进行删除和缩减的权限。
开始手动记录	启用在客户端中启动音频的手动记录的权限。
停止手动记录	启用在客户端中停止音频的手动记录的权限。
删除记录	启用从系统删除存储的记录的权限。
管理安全	启用在 Management Client 中管理麦克风的安全权限的权限。

扬声器

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端和 Management Client 中查看扬声器设备的权限。
编辑	启用编辑 Management Client 中扬声器属性的权限。它还允许用户启用或禁用扬声器。
监听实时信息	启用在客户端和 Management Client 中监听扬声器的实时音频的权限。
收听受限的实时音频	启用在客户端与 Management Client 中对扬声器的实时受限音频进行收听的权限。

安全权限	说明
话语	启用在客户端中通过扬声器说话的权限。
播放	启用在客户端中播放扬声器的记录音频的权限。
播放受限记录	启用在客户端中播放扬声器的记录音频的权限。
检索远程记录	启用在客户端中从远程站点上的扬声器检索记录的权限，或启用从摄像机上的边缘存储检索记录的权限。
读取片段	启用在客户端中于浏览扬声器记录音频的同时使用片断功能的权限。
导出	启用在客户端中导出扬声器的记录音频的权限。
创建书签	启用在客户端中创建书签的权限。
读取书签	启用在客户端中搜索和读取书签详细信息的权限。
编辑书签	启用在客户端中编辑书签的权限。
删除书签	启用在客户端中删除书签的权限。
创建和扩展证据锁定	启用在客户端中创建或扩展证据锁定，保护记录音频的的权限。
读取证据锁定	启用在客户端中查看受证据锁定保护的记录音频的的权限。
删除和减少证据锁定	启用在客户端中删除或减少受保护音频上的证据锁定的权限。
创建和扩展实时和播放限制	启用在客户端中对扬声器所受限制进行创建和扩展的权限。
读取实时和播放限制	启用在客户端中对扬声器所受既有限制的列表进行查看的权限。
删除和减少实时和播放限制	启用在客户端中对扬声器所受限制进行删除和缩减的权限。
开始手动记录	启用在客户端中启动音频的手动记录的权限。
停止手动记录	启用在客户端中停止音频的手动记录的权限。
删除记录	启用从系统删除存储的记录的权限。
管理安全	启用在 Management Client 中管理扬声器的安全权限的权限。

元数据

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端中接收元数据的权限。
编辑	启用在 Management Client 中编辑元数据属性的权限。它还允许用户启用或禁用元数据设备。
实时	启用在客户端中接收元数据设备的实时元数据的权限。
查看受限的实时	启用在客户端中对元数据设备的实时受限元数据进行接收的权限。
播放	启用在客户端中播放元数据设备的记录数据的权限。
播放受限记录	启用在客户端中对元数据设备中录制的受限数据进行播放的权限。
检索远程记录	启用在客户端中从远程站点上的元数据设备检索记录的权限，或启用从摄像机上的边缘存储检索记录的权限。
读取片段	启用在客户端中读取片断信息(例如，与**播放**相关的片断信息)的权限。
导出	启用在客户端中导出记录的权限。
创建和扩展证据锁定	启用在客户端中创建证据锁定的权限。
读取证据锁定	启用在客户端中查看证据锁定的权限。
删除和减少证据锁定	启用在客户端中删除或减少证据锁定的权限。
创建和扩展实时和播放限制	启用在客户端中对元数据所受限制进行创建和扩展的权限。
读取实时和播放限制	启用在客户端中对元数据所受既有限制的列表进行查看的权限。

安全权限	说明
删除和减少实时和播放限制	启用在客户端中对元数据所受限制进行删除和缩减的权限。
开始手动记录	启用在客户端中启动元数据的手动记录的权限。
停止手动记录	启用在客户端中停止元数据的手动记录的权限。
删除记录	启用从系统删除存储的记录的权限。
管理安全	启用在 Management Client 中管理元数据的安全权限的权限。

输入

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端和 Management Client 中查看输入设备的权限。
编辑	启用在 Management Client 中编辑输入设备的属性的权限。它还允许用户启用或禁用输入设备。
管理安全	启用在 Management Client 中管理输入设备的安全权限的权限。

输出

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端中查看输出设备的权限。
编辑	启用在 Management Client 中编辑输出设备的属性的权限。它还允许用户启用或禁用输出设备。
激活	启用在客户端中触发输出的权限。
管理安全	启用在 Management Client 中对输出设备的安全进行管理的权限。

Smart Wall

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	在 XProtect Management Client 中启用管理所有安全权限这一权限。
读取	启用在 XProtect Smart Client 中查看电视墙的权限。
编辑	启用在 XProtect Management Client 中编辑 Smart Wall 定义的属性这一权限。
删除	启用在 XProtect Management Client 中删除现有 Smart Wall 定义这一权限。
操作	启用在 XProtect Smart Client 和 XProtect Management Client 中激活和修改 Smart Wall 定义(例如，以更改和激活预设或在视图上应用摄像机)这一权限。 您可以将**操作**与定义何时应用用户权限的时间配置文件相关联。
创建 Smart Wall	启用在 XProtect Management Client 中创建新 Smart Wall 定义这一权限。
管理安全	启用在 XProtect Management Client 定义中管理 Smart Wall 的安全权限这一权限。
播放	启用在 XProtect Smart Client 的电视墙中播放记录数据的权限。 您可以将**播放**与定义何时应用用户权限的时间配置文件相关联。

视图组

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端和 Management Client 中查看视图组的权限。查看在 Management Client 中创建的组。
编辑	启用在 Management Client 中编辑视图组的属性的权限。
删除	启用在 Management Client 中删除视图组的权限。
操作	启用在 XProtect Smart Client 中使用视图组(即创建和删除子组和视图)的权限。
创建视图组	启用在 Management Client 中创建视图组的权限。
管理安全	启用在 Management Client 中管理视图组的安全权限的权限。

用户定义的事件

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端中查看用户定义事件的权限。
编辑	启用在 Management Client 中编辑用户定义事件的属性的权限。
删除	启用在 Management Client 中删除用户定义事件的权限。

安全权限	说明
触发	启用在客户端中触发用户定义事件的权限。
管理安全	启用在 Management Client 中管理用户定义事件的安全权限的权限。
创建用户定义事件	启用在 Management Client 中创建新的用户定义事件的权限。

分析事件

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在 Management Client 中查看分析事件的权限。
编辑	启用在 Management Client 中编辑分析事件的属性的权限。
管理安全	启用在 Management Client 中管理分析事件的安全权限的权限。

常规事件

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在客户端和 Management Client 中查看常规事件的权限。
编辑	启用在 Management Client 中编辑常规事件的属性的权限。
管理安全	启用在 Management Client 中管理常规事件的安全权限的权限。

Matrix

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用从客户端选择视频并将视频发送至 Matrix 接收方的权限。
编辑	启用编辑 Matrix 中 Management Client 的属性的权限。
删除	启用在 Matrix 中删除 Management Client 的权限。
创建 Matrix	启用在 Matrix 中创建新 Management Client 的权限。
管理安全	启用在 Management Client 中管理所有 Matrix 的安全权限的权限。

规则

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在 Management Client 中查看现有规则的权限。
编辑	启用在 Management Client 中编辑规则属性和定义规则行为的权限。 它还要求用户在受该规则影响的所有设备上具有读权限。
删除	启用从 Management Client 中删除规则的权限。 它还要求用户在受该规则影响的所有设备上具有读权限。
创建规则	启用在 Management Client 中创建新的规则的权限。

安全权限	说明
	它还要求用户在受该规则影响的所有设备上具有读权限。
管理安全	启用在 Management Client 中管理所有规则的安全权限的权限。

站点

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在 Management Client 中查看其他站点的权限。连接的站点通过 Milestone Federated Architecture 进行连接。 要编辑属性，您需要在每个站点上的管理服务器中具有“编辑”权限。
管理安全	启用在所有站点上管理安全权限的权限。

系统监视器

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。

安全权限	说明
读取	启用在 XProtect Smart Client 中查看系统监视器的权限。
编辑	启用在 Management Client 中编辑系统监视器的属性的权限。
管理安全	启用在 Management Client 中管理所有系统监视器的安全权限的权限。

元数据搜索

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用查看 Management Client 及其相关设置中的**元数据使用**功能的权限，但不启用更改设置的权限。
编辑元数据搜索配置	启用在 Management Client 中启用或禁用元数据搜索类别(例如，人员或车辆的元数据)的权限。
管理安全	启用管理元数据搜索的安全权限的权限。

搜索

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
读取公共搜索	启用在 XProtect Smart Client 中查看和打开已保存公共搜索的权限。

安全权限	说明
创建公共搜索	启用在 XProtect Smart Client 中将新配置的搜索另存为公共搜索的权限。
编辑公共搜索	启用在 XProtect Smart Client 中编辑已保存公共搜索的详细信息或配置的权限，例如名称、说明、摄像机和搜索类别。
删除公共搜索	启用删除已保存公共搜索的权限。
管理安全	启用在 Management Client 中管理搜索的安全权限的权限。

警报

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
管理	启用在 Smart Client 中管理警报的权限。例如，更改警报的优先级、将警报重新分配给其他用户、确认警报、更改多个警报的警报状态(例如，从**新建**更改为**已分配**)。要编辑警报设置，您还需要**编辑警报设置**权限。 只有当您将此项设置为允许时，**选项**对话框中的**警报和事件**选项卡才会出现。
视图	启用在 XProtect Smart Client 中查看**警报管理器**选项卡，并通过 API 检索警报和警报设置的权限。 要在 XProtect Smart Client 中查看警报，必须为至少一个警报定义启用**查看**权限。默认情况下，您可以查看来自第三方解决方案的警报。
禁用警报	启用禁用警报的权限。

安全权限	说明
接收通知	启用在 XProtect Mobile 客户端和 XProtect Web Client 中接收有关警报的通知的权限。
管理安全	启用管理所有警报的安全权限的权限。
编辑警报设置	启用编辑警报定义、警报状态、警报类别、警报声音、警报保留和事件保留的权限。要编辑警报设置，您还需要拥有**管理**权限。

警报定义

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
视图	启用查看警报定义、警报状态、警报类别、警报声音、警报保留和事件保留的权限。
写入	启用**查看**权限。
管理安全	启用管理警报定义的安全权限的权限。

服务器日志

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取系统日志条目	启用查看系统日志条目的权限。
读取审核日志条目	启用查看审核日志条目的权限。

安全权限	说明
读取规则触发的日志条目	启用查看规则触发的日志条目的权限。
读取日志配置	启用读取**工具 > 选项 > 服务器日志**中的日志设置的权限。
更新日志配置	启用更改**工具 > 选项 > 服务器日志**中的日志设置的权限。
管理安全	启用管理所有警报的安全权限的权限。

访问控制

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
编辑	启用在 Management Client 中编辑访问控制系统的属性的权限。
用户访问控制	允许用户在客户端中使用任何与访问控制有关的功能。
查看持卡人列表	允许用户在客户端中的**访问控制**选项卡上查看持卡人列表。
接收通知	允许用户在客户端中接受有关访问请求的通知。
管理安全	启用管理所有访问控制系统的安全权限的权限。

LPR

如果您的系统是用 XProtect LPR 运行，请向用户指定以下权限：

安全权限	说明
完全控制	启用管理系统该部分上的所有安全条目这一权限。

安全权限	说明
使用 LPR	启用在客户端中使用任何 LPR 相关功能这一权限
管理匹配列表	启用在 Management Client 中添加、导入、修改、导出和删除匹配列表的权限。
读取匹配列表	启用查看匹配列表的权限。
管理安全	启用在 Management Client 中管理所有交易定义的安全权限这一权限。

交易来源

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在 Management Client 中查看交易来源的属性的权限。
编辑	启用在 Management Client 中编辑交易来源的属性的权限。
删除	启用在 Management Client 中删除交易来源这一权限。
创建	启用在 Management Client 中创建新的交易来源这一权限。
管理安全	启用在 Management Client 中管理所有交易来源的安全权限这一权限。

交易定义

安全权限	说明
完全控制	启用管理系统该部分上所有安全条目的权限。
读取	启用在 Management Client 中查看交易定义的属性这一权限。
编辑	启用在 Management Client 中编辑交易定义的属性这一权限。
删除	启用在 Management Client 中删除交易定义这一权限。
创建	启用在 Management Client 中创建新的交易定义这一权限。
管理安全	启用在 Management Client 中管理所有交易定义的安全权限这一权限。

MIP 插件

通过 MIP SDK，第三方供应商可以为您的系统开发自定义插件，例如，集成到外部访问控制系统或类似功能。

"设备"选项卡(角色)

可用的功能取决于正在使用的系统。请参阅Milestone网站(https://www.milestonesys.com/products/software/product-index/)上产品总览页中的完整功能列表。

使用**设备**选项卡可指定具有所选角色的用户/组可以为 XProtect Smart Client 中的各设备(如摄像机)或设备组使用哪些功能。

请记住为各个设备重复这一过程。还可以选择设备组，并一次为整个组中的所有设备指定角色权限。

您仍然可以选择或清除此类方块填充的复选框，但是请注意，在该情况下，您的选择将应用于设备组内的**所有**设备。或者，选择设备组内的单个设备以确定相关权限将应用于具体哪些相关设备。

摄像机相关权限

为摄像机设备指定以下权限：

名称	说明
读取	所选摄像机在客户端中可见。
查看实时信息	允许在客户端中实时查看所选摄像机的视频。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权限是作为应用程序权限的一部分授予的。指定时间配置文件或保留默认值。
查看受限的实时	允许在客户端中对所选摄像机的受限视频进行实时查看。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权限是作为应用程序权限的一部分授予的。指定时间配置文件或保留默认值。
播放 > 在时间配置文件内	允许在客户端中播放所选摄像机的记录视频。指定时间配置文件或保留默认值。
播放 > 限制播放	允许在客户端中播放所选摄像机的记录视频。指定播放限制或不应用任何限制。
播放受限记录	允许在客户端中对所选摄像机中录制的受限视频进行播放。指定时间配置文件或保留默认值。

名称	说明
读取片段	允许在客户端中读取片断信息(例如与片段资源管理器相关的片断信息)。
智能搜索	允许用户在客户端中使用智能搜索功能。
导出	允许用户从客户端导出记录。
开始手动记录	允许在客户端中启动所选摄像机的视频的手动记录。
停止手动记录	允许在客户端中停止所选摄像机的视频的手动记录。
读取书签	允许在客户端中搜索和读取书签详细信息。
编辑书签	允许在客户端中编辑书签。
创建书签	允许在客户端中添加书签。
删除书签	允许在客户端中删除书签。
AUX 命令	允许从客户端使用辅助命令。
创建和扩展证据锁定	允许客户端用户: • 将摄像机添加至新的或现有的证据锁定 • 延长现有证据锁定的过期时间 • 延长现有证据锁定的受保护间隔 需要包含在证据锁定中的所有设备的用户权限。
删除和减少证据锁定	允许客户端用户: • 将摄像机从现有证据锁定删除 • 删除现有证据锁定 • 缩短现有证据锁定的过期时间 • 缩短现有证据锁定的受保护间隔 需要包含在证据锁定中的所有设备的用户权限。

名称	说明
读取证据锁定	允许客户端用户搜索和读取证据锁定详细信息。
创建和扩展实时和播放限制	允许客户端用户： • 针对摄像机而创建实时限制 • 针对摄像机记录而创建播放限制 • 将新摄像机添加到实时或播放限制 • 延长摄像机记录的限制期 需要限制中所含所有设备的用户权限。
读取实时和播放限制	允许客户端用户： • 查看摄像机所受既有实时限制和播放限制的列表 • 筛选和搜索摄像机所受实时限制和播放限制的列表
删除和减少实时和播放限制	允许客户端用户： • 移除摄像机所受的实时限制 • 移除摄像机记录所受的播放限制 • 缩短摄像机记录的限制期 • 更改实时或播放限制的设置 需要限制中所含所有设备的用户权限。

麦克风相关权限

为麦克风设备指定以下权限：

名称	说明
读取	所选麦克风在客户端中可见。
监听实时信息	允许在客户端中监听所选麦克风的实时音频。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权

名称	说明
	限是作为应用程序权限的一部分授予的。指定时间配置文件或保留默认值。
收听受限的实时音频	允许在客户端中对所选麦克风中的实时受限视频进行收听。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权限是作为应用程序权限的一部分授予的。指定时间配置文件或保留默认值。
播放 > 在时间配置文件内	允许在客户端中播放所选麦克风的记录音频。指定时间配置文件或保留默认值。
播放 > 限制播放	允许在客户端中播放所选麦克风的记录音频。指定播放限制或不应用任何限制。
播放受限记录	允许在客户端中对所选麦克风中录制的受限音频进行播放。指定时间配置文件或保留默认值。
读取片段	允许在客户端中读取片断信息(例如与片段资源管理器相关的片断信息)。
导出	允许用户从客户端导出记录。
开始手动记录	允许在客户端中启动所选麦克风的音频的手动记录。
停止手动记录	允许在客户端中停止所选麦克风的音频的手动记录。
读取书签	允许在客户端中搜索和读取书签详细信息。
编辑书签	允许在客户端中编辑书签。
创建书签	允许在客户端中添加书签。
删除书签	允许在客户端中删除书签。
创建和扩展证据锁定	允许客户端用户： • 将麦克风添加至新的或现有的证据锁定 • 延长现有证据锁定的过期时间 • 延长现有证据锁定的受保护间隔 需要包含在证据锁定中的所有设备的用户权限。
删除和减少证据	允许客户端用户：

名称	说明
锁定	• 将麦克风从现有证据锁定删除 • 删除现有证据锁定 • 缩短现有证据锁定的过期时间 • 缩短现有证据锁定的受保护间隔 需要包含在证据锁定中的所有设备的用户权限。
读取证据锁定	允许客户端用户搜索和读取证据锁定详细信息。
创建和扩展实时和播放限制	允许客户端用户： • 针对麦克风而创建实时限制 • 针对音频记录而创建播放限制 • 将新麦克风添加到实时或播放限制 • 延长音频记录的限制期 需要限制中所含所有设备的用户权限。
读取实时和播放限制	允许客户端用户： • 查看麦克风所受既有实时限制和播放限制的列表 • 筛选和搜索麦克风所受实时限制和播放限制的列表
删除和减少实时和播放限制	允许客户端用户： • 移除麦克风所受的实时限制 • 移除音频记录所受的播放限制 • 缩短音频记录的限制期 • 更改实时或播放限制的设置 需要限制中所含所有设备的用户权限。

扬声器相关权限

为扬声器设备指定以下权限：

名称	说明
读取	所选扬声器在客户端中可见。
监听实时信息	允许在客户端中监听所选扬声器的实时音频。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权限是作为应用程序权限的一部分授予的。指定时间配置文件或保留默认值。
收听受限的实时音频	允许在客户端中对所选扬声器中的实时受限视频进行收听。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权限是作为应用程序权限的一部分授予的。指定时间配置文件或保留默认值。
播放 > 在时间配置文件内	允许在客户端中播放所选扬声器的记录音频。指定时间配置文件或保留默认值。
播放 > 限制播放	允许在客户端中播放所选扬声器的记录音频。指定播放限制或不应用任何限制。
播放受限记录	允许在客户端中对所选扬声器中录制的受限音频进行播放。指定时间配置文件或保留默认值。
读取片段	允许在客户端中读取片断信息(例如与片段资源管理器相关的片断信息)。
导出	允许用户从客户端导出记录。
开始手动记录	允许在客户端中启动所选扬声器的音频的手动记录。
停止手动记录	允许在客户端中停止所选扬声器的音频的手动记录。
读取书签	允许在客户端中搜索和读取书签详细信息。
编辑书签	允许在客户端中编辑书签。
创建书签	允许在客户端中添加书签。
删除书签	允许在客户端中删除书签。
创建和扩展证据锁定	允许客户端用户： • 将扬声器添加至新的或现有的证据锁定 • 延长现有证据锁定的过期时间 • 延长现有证据锁定的受保护间隔

名称	说明
	需要包含在证据锁定中的所有设备的用户权限。
删除和减少证据锁定	允许客户端用户： • 将扬声器从现有证据锁定删除 • 删除现有证据锁定 • 缩短现有证据锁定的过期时间 • 缩短现有证据锁定的受保护间隔 需要包含在证据锁定中的所有设备的用户权限。
读取证据锁定	允许客户端用户搜索和读取证据锁定详细信息。
创建和扩展实时和播放限制	允许客户端用户： • 针对扬声器而创建实时限制 • 针对音频记录而创建播放限制 • 将新麦克风添加到实时或播放限制 • 延长音频记录的限制期 需要限制中所含所有设备的用户权限。
读取实时和播放限制	允许客户端用户： • 查看扬声器所受既有实时限制和播放限制的列表 • 筛选和搜索扬声器所受实时限制和播放限制的列表
删除和减少实时和播放限制	允许客户端用户： • 移除扬声器所受的实时限制 • 移除音频记录所受的播放限制 • 缩短音频记录的限制期 • 更改实时或播放限制的设置 需要限制中所含所有设备的用户权限。

元数据相关权限

为元数据设备指定以下权限：

名称	说明
读取	启用在客户端中查看元数据设备和检索其数据的权限。
编辑	启用编辑元数据属性的权限。它还允许用户在 Management Client 中并通过 MIP SDK 启用或禁用元数据设备。
查看实时信息	启用在客户端中查看摄像机的实时元数据的权限。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权限是作为应用程序权限的一部分授予的。
查看实时限制	启用在客户端中对摄像机的实时受限元数据进行查看的权限。 对于 XProtect Smart Client，它要求角色被授予查看客户端的**实时**选项卡的权限。该权限是作为应用程序权限的一部分授予的。
播放	启用在客户端中播放元数据设备的记录数据的权限。
播放受限记录	启用在客户端中对受限元数据设备中录制的数据进行播放的权限。
读取片段	启用在客户端中于浏览元数据设备记录数据的同时使用片断功能的权限。
导出	启用在客户端中导出元数据设备的记录音频的权限。
创建和扩展证据锁定	启用在客户端中创建和扩展元数据上的证据锁定的权限。
读取证据锁定	启用在客户端中查看元数据上证据锁定的权限。
删除和减少证据锁定	启用在客户端中删除或减少元数据上证据锁定的权限。
开始手动记录	启用在客户端中启动元数据的手动记录的权限。
停止手动记录	启用在客户端中停止元数据的手动记录的权限。
创建和扩展实时和播放限制	允许客户端用户： • 针对元数据设备而创建实时限制 • 针对元数据设备而创建播放限制

名称	说明
	• 将新元数据添加到实时或播放限制 • 延长元数据设备的限制期 需要限制中所含所有设备的用户权限。
读取实时和播放限制	允许客户端用户： • 查看元数据设备所受既有实时限制和播放限制的列表 • 筛选和搜索元数据设备所受实时限制和播放限制的列表
删除和减少实时和播放限制	允许客户端用户： • 移除元数据设备所受的实时限制 • 移除元数据设备所受的播放限制 • 缩短元数据设备的限制期 • 更改实时或播放限制的设置 需要限制中所含所有设备的用户权限。

输入相关权限

为输入设备指定以下权限：

名称	说明
读取	所选输入将在客户端中可见。

输出相关权限

为输出设备指定以下权限：

名称	说明
读取	所选输出在客户端中可见。如果可见，输出将在客户端中的列表上可选。
激活	所选输出可从 Management Client 和客户端触发。指定时间配置文件或保留默认值。

PTZ 选项卡(角色)

在 **PTZ** 选项卡上设置全景/倾斜/变焦 (PTZ) 摄像机的权限。可以指定用户/组可以在客户端中使用的功能。可以选择独立的 PTZ 摄像机或包含 PTZ 摄像机的设备组。

为 PTZ 指定以下权限:

名称	说明
手动 PTZ	确定所选角色是否可以在选定摄像机上使用 PTZ 功能以及暂停巡视。 指定时间配置文件,选择**始终**,或保留默认值(其采用在该角色的**信息**选项卡中定义的默认时间配置文件)。
激活 PTZ 预设或巡视配置文件	确定所选角色是否可将选定摄像机移动到预设位置、启动和停止巡视配置文件以及暂停巡视。 指定时间配置文件,选择**始终**,或保留默认值(其采用在该角色的**信息**选项卡中定义的默认时间配置文件)。 要允许此角色在摄像机上使用其他 PTZ 功能,请启用**手动 PTZ** 权限。
PTZ 优先级	决定 PTZ 摄像机的优先级。当监控系统上的多个用户需要同时控制同一台 PTZ 摄像机时,可能引发冲突。 通过按照具有所选角色的用户/组为所选 PTZ 摄像机的使用指定优先级,可以避免这种情况。可指定的优先级范围为 1 至 32,000,其中 1 是最低优先级。默认优先级为 3,000。优先级数字最高的角色是可以控制 PTZ 摄像机的人员。
管理 PTZ 预设或巡视配置文件	确定在 Management Client 和 XProtect Smart Client 中对选定摄像机添加、编辑和删除 PTZ 预设和巡视配置文件所需的权限。 要允许此角色在摄像机上使用其他 PTZ 功能,请启用**手动 PTZ** 权限。
锁定/解锁 PTZ 预设	确定角色是否可以锁定和解锁选定摄像机的预设位置。
保留 PTZ 会话	确定在保留 PTZ 会话模式下设置选定摄像机的权限。 在保留 PTZ 会话中,具有更高 PTZ 优先级的其他用户或巡视会话无法接管控制权。 要允许此角色在摄像机上使用其他 PTZ 功能,请启用**手动 PTZ** 权限。
释放 PTZ 会话	确定所选角色是否可从 Management Client 释放其他用户的 PTZ 会话。 您始终可以释放自己的 PTZ 会话(不需要此权限)。

“语音”选项卡(角色)

仅当在系统上使用扬声器时才相关。为扬声器指定以下权限:

名称	说明
话语	确定是否允许用户通过所选扬声器讲话。指定时间配置文件或保留默认值。
话语优先级	当多个客户端用户同时要通过相同的扬声器讲话时可能引发冲突。 通过按照具有所选角色的用户/组为所选扬声器的使用指定优先级，可以解决该问题。在**非常低**到**非常高**的范围内指定优先级。优先级最高的角色可以在其他角色之前使用扬声器。 如果具有相同角色的两个用户同时希望讲话，则适用先到先得的原则。

“远程记录”选项卡(角色)

为远程记录指定以下权限：

名称	说明
检索远程记录	启用在客户端中从远程站点上的摄像机、麦克风、扬声器和元数据设备检索记录的权限，或启用从摄像机上的边缘存储检索记录的权限。

Smart Wall 选项卡(角色)

通过角色，可以为客户端用户授予 Smart Wall 相关用户权限：

名称	说明
读取	允许用户查看 XProtect Smart Client 中选定的 Smart Wall。
编辑	允许用户在 Smart Wall 中编辑选定的 Management Client。
删除	允许用户在 Smart Wall 中删除选定的 Management Client。
操作	允许用户在 XProtect Smart Client 的所选 Smart Wall 中应用布局并激活预设。
播放	允许用户在 XProtect Smart Client 的选定 Smart Wall 中播放记录数据。

“外部事件”选项卡(角色)

指定以下外部事件权限：

名称	说明
读取	允许用户在客户端和 Management Client 中搜索和查看选定的外部系统事件。
编辑	允许用户在 Management Client 中编辑选定的外部系统事件。
删除	允许用户在 Management Client 中删除选定的外部系统事件。
触发	允许用户在客户端中触发选定的外部系统事件。

“视图组”选项卡(角色)

在**视图组**选项卡上,指定具有所选角色的用户和用户组能够在客户端中使用哪些视图组。

为视图组指定以下权限:

名称	说明
读取	启用在客户端和 Management Client 中查看视图组的权限。查看在 Management Client 中创建的组。
编辑	启用在 Management Client 中编辑视图组的属性的权限。
删除	启用在 Management Client 中删除视图组的权限。
操作	启用在 XProtect Smart Client 中使用视图组(即创建和删除子组和视图)的权限。

“服务器”选项卡(角色)

仅当系统在 Milestone Federated Architecture 设置中工作时,在**服务器**选项卡上指定角色权限才相关。

名称	说明
站点	启用在 Management Client 中查看选定站点的权限。连接的站点通过 Milestone Federated Architecture 进行连接。 要编辑属性,您需要在每个站点上的管理服务器中具有“编辑”权限。

有关详细信息,请参阅 第 81 页上的正在配置 Milestone Federated Architecture。

Matrix 选项卡(角色)

如果在系统上配置了 Matrix 接收方,则可以配置 Matrix 角色权限。可以从客户端发送视频至所选 Matrix 接收方。在 Matrix 选项卡上选择可以接收该视频的用户。

以下权限可用:

名称	说明
读取	确定具有所选角色的用户和组是否能够从客户端选择视频并将视频发送至 Matrix 接收方。

"警报"选项卡(角色)

在系统设置中使用警报来提供对安装(包括任何其他 XProtect 服务器)的集中总览和控制时,可以使用**警报**选项卡来指定具有所选角色的用户和组应具有哪些警报权限(例如,如何在客户端中处理警报)。

在**警报**中,您可以指定警报的权限:

安全权限	说明
管理	启用在 Smart Client 中管理警报的权限。例如,更改警报的优先级、将警报重新分配给其他用户、确认警报、更改多个警报的警报状态(例如,从**新建**更改为**已分配**)。要编辑警报设置,您还需要**编辑警报设置**权限。 只有当您将此项设置为允许时,**选项**对话框中的**警报和事件**选项卡才会出现。
视图	启用在 XProtect Smart Client 中查看**警报管理器**选项卡,并通过 API 检索警报和警报设置的权限。 要在 XProtect Smart Client 中查看警报,必须为至少一个警报定义启用**查看**权限。默认情况下,您可以查看来自第三方解决方案的警报。
禁用警报	启用禁用警报的权限。
接收通知	启用在 XProtect Mobile 客户端和 XProtect Web Client 中接收有关警报的通知的权限。
编辑警报设置	启用编辑警报定义、警报状态、警报类别、警报声音、警报保留和事件保留的权限。要编辑警报设置,您还需要拥有**管理**权限。

在**警报定义**中，您可以指定特定警报定义的权限：

名称	说明
视图	启用查看警报定义、警报状态、警报类别、警报声音、警报保留和事件保留的权限。
写入	启用**查看**权限。

“访问控制”选项卡(角色)

在添加或编辑基本用户、Windows 用户或组时，指定访问控制设置：

名称	说明
用户访问控制	允许用户在客户端中使用任何与访问控制有关的功能。
查看持卡人列表	允许用户在客户端中的**访问控制**选项卡上查看持卡人列表。
接收通知	允许用户在客户端中接受有关访问请求的通知。

“LPR”选项卡(角色)

如果您的系统是用 XProtect LPR 运行，请向用户指定以下权限：

名称	说明
使用 LPR	启用在客户端中使用任何 LPR 相关功能的权限。
管理匹配列表	启用在 Management Client 中添加、导入、修改、导出和删除匹配列表的权限。
读取匹配列表	启用查看匹配列表的权限。

“事件”选项卡(角色)

如果您有 XProtect Incident Manager，您可以为您的角色指定以下权限。

若要给一个 Management Client 管理员角色提供管理或查看事件属性的权限，请选择**事件属性**节点。

要授予操作员查看您定义的事件属性的 XProtect Smart Client 权限，请选择**事件属性**并授予**查看**权限。要授予管理或查看事件项目的一般权限，请选择**事件项目**节点。展开**事件项目**节点并选择一个或更多子节点，以便为这些额外的具体功能或能力提供权限。

名称	说明
管理	为角色提供管理(查看、创建、编辑和删除)与某个功能有关的设置和属性,或查看由 Management Client 或 XProtect Smart Client 中选定节点代表的用户界面元素的权限。
视图	授予角色权限以查看(但不能创建、编辑和删除)与功能相关的设置和属性、查看定义的事件属性,或查看由 Management Client 或 XProtect Smart Client 中选定节点代表的用户界面元素。

MIP 选项卡(角色)

通过 MIP SDK,第三方供应商可以为您的系统开发自定义插件,例如,集成到外部访问控制系统或类似功能。第三方插件在各个选项卡上有自己的设置。

您更改的设置取决于实际插件。在 **MIP** 选项卡上查找插件的自定义设置。

基本用户(安全性节点)

Milestone XProtect VMS 中有两类用户帐户:基本用户和 Windows 用户。

基本用户是您在 Milestone XProtect VMS 中创建的用户帐户。它是专用的系统用户帐户,会进行个人用户的基本用户名和密码身份验证。

Windows 用户是您通过 Microsoft 的 Active Directory 而添加的用户帐户。

基本用户与 Windows 用户之间的一些区别如下:

- 基本用户通过用户名与密码的组合进行身份验证,并且特定于一个系统/站点。请注意,即便在不同的联合站点上创建的两个基本用户具有彼此相同的名称和密码,基本用户也只能访问创建自己的站点。
- Windows 用户根据 Windows 登录进行身份验证,并且特定于计算机。

"系统仪表板"节点

"系统仪表板"节点

在**系统仪表板**节点下,您可以找到不同的功能来监控您的系统及其各种系统组件。

名称	说明
当前任务	获得所选记录服务器上正在进行的任务的总览。
系统监视器	根据您定义的参数监视服务器和摄像机的状态。

名称	说明
系统监视阈值	为用于系统监视器中的服务器和监视器拼贴图设置监视参数的阈值。
证据锁定	获取系统中所有受保护数据的总览。
配置报告	使用系统配置打印报告。您可以决定在报告中包含哪些内容。

当前任务(“系统仪表板”节点)

当前任务窗口显示所选记录服务器上正在进行的任务的总览。如果启动的任务需要很长时间并且在后个运行，则可以打开**当前任务**窗口查看任务的进度。冗长的用户启动任务的例子包括固件更新和硬件移动。您可以查看有关任务的开始时间、估计的结束时间和进度的信息。

当前任务窗口中显示的信息不会动态更新，而是您打开窗口之时当前任务的快照。如果您已将窗口打开一段时间，请通过选择窗口右下角的**刷新**按钮来刷新信息。

系统监视器(“系统仪表板”节点)

系统监视器功能为您提供了系统服务器和摄像机当前状况的快速直观总览。

“系统监视器仪表板”窗口

拼贴图

系统监视器仪表板窗口的上部显示彩色拼贴图，这些拼贴图表示系统的服务器硬件和摄像机硬件的状态。

拼贴图将更改其状态，从而根据**系统监视器阈值**节点中设置的阈值更改颜色。有关详细信息，请参阅 第 473 页上的系统监视器阈值(“系统仪表板”节点)。定义阈值，以便拼贴图颜色表示以下含义：

拼贴图颜色	说明
绿色	**正常**状态。所有方面运行正常。
黄色	**警告**状态。一个或多个监视参数高于**正常**状态所对应的阈值。
红色	**临界**状态。一个或多个监视参数高于**正常**和**警告**状态所对应的阈值。

带监视参数的硬件列表

如果单击拼贴图，则可以在**系统监视器仪表板**窗口底部查看由拼贴图表示的每种硬件的每个所选监视参数的状态。

示例：摄像机的实时 FPS 监视参数已达到“警告”状态。

“自定义仪表板”窗口

选择窗口右上角的**自定义**可打开**自定义仪表板**窗口。

在**自定义仪表板**窗口中，可以选择要创建、编辑或删除的拼贴图。创建或编辑拼贴图时，可以选择要在拼贴图上监视的硬件和监视参数。

“详细信息”窗口

如果选择一个拼贴图，然后从带有监视参数的硬件列表中，选择摄像机或服务器右侧的**详细信息**按钮，则可以根据所选硬件查看系统信息并创建有关以下内容的报告：

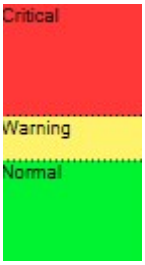
硬件	信息
管理服务器	显示以下相关数据： • CPU 使用率 • 可用内存 选择**历史记录**以查看硬件的历史记录状态，并根据上述数据创建报告。
记录服务器	显示以下相关数据： • CPU 使用率 • 可用内存 • 磁盘 • 存储 • 网络 • 摄像机 选择**历史记录**以查看硬件的历史记录状态，并根据上述数据创建报告。
故障转移记录服务器	显示以下相关数据： • CPU 使用率 • 可用内存

硬件	信息
	• 监视的记录服务器 选择**历史记录**以查看硬件的历史记录状态，并根据上述数据创建报告。
日志服务器、事件服务器等	显示以下相关数据 • CPU 使用率 • 可用内存 选择**历史记录**以查看硬件的历史记录状态，并根据上述数据创建报告。
摄像机	显示以下相关数据： • 存储 • 已用空间 • 实时 FPS(默认) • 记录 FPS • 实时视频格式 • 记录视频格式 • 接收到的媒体数据 (Kbit/s) • 可用内存 选择摄像机名称以查看其历史状态并创建有关以下内容的报告： • 从摄像机接收到的数据 • 摄像机磁盘使用量

如果您从服务器操作系统访问系统监视器的详细信息，可能会出现有关**InternetExplorer增强安全配置**的消息。按照说明，将**系统监视器**页面添加至**受信任的站点区域**，然后继续操作。

系统监视器阈值(“系统仪表板”节点)

通过系统监视器阈值，您可以定义和调整阈值，**系统监视器仪表板**上的拼贴图应直观地指示您的系统硬件更改状态。例如，当服务器的 CPU 使用率从正常状态(绿色)变为警告状态(黄色)或从警告状态(黄色)变为严重状态(红色)时。



三种状态之间的阈值示例

您可以更改服务器、摄像机、磁盘和存储的阈值，并且所有阈值都有一些常用的按钮和设置。

通用用户界面元素

按钮与设置	说明	单位
计算间隔	通常，与您的不同硬件的连接会出现短暂的中断。如果将计算间隔指定为 0 秒，则所有短暂的中断都将触发有关硬件状态变化的警报。因此，请定义一定长度的计算间隔。 如果您在内部定义一 (1) 分钟的计算，则意味着仅当整分钟的平均值超过阈值时，您才会收到警报。使用正确的计算间隔设置，您将不会收到假阳性警报，而只会收到有关持续问题的警报，例如 CPU 使用率或内存消耗。 要更改计算间隔的值，请参阅 第 256 页上的编辑何时应更改硬件状态的阈值。	秒
高级	如果选择**高级**按钮，则可以为单个服务器、摄像机、磁盘和存储定义阈值和计算间隔。有关详细信息，请参阅下文。	-
创建规则	您可以将**系统监视器**中的事件与规则结合起来以触发操作，例如，当服务器的 CPU 使用率非常重要或磁盘可用空间不足时。 有关详细信息，请参阅 第 68 页上的规则和事件(已作说明) 和 第 236 页上的添加规则。	-

服务器阈值

阈值	说明	单位
CPU 使用率	您监视的服务器上 CPU 使用率的阈值。	%
可用内存	您监视的服务器上使用的 RAM 的阈值。	MB
NVIDIA 解码	您监视的服务器上 NVIDIA 解码使用率的阈值。	%
NVIDIA 内存	您监视的服务器上使用的 NVIDIA RAM 的阈值。	%
NVIDIA 渲染	您监视的服务器上 NVIDIA 渲染使用率的阈值。	%

摄像机阈值

阈值	说明	单位
实时 FPS	您监视的摄像机上显示实时视频时使用的摄像机 FPS 的阈值。	%
记录 FPS	您监视的摄像机上，系统在记录视频时使用的摄像机 FPS 的阈值。	%
已用空间	您监视的摄像机使用的空间的阈值。	GB

磁盘阈值

阈值	说明	单位
可用空间	您监视的磁盘上可用空间的阈值。	GB

存储阈值

阈值	说明	单位
保留时间	该阈值显示关于存储空间何时不足的预测。显示的状态基于您的系统设置，并且每天更新两次。	天

证据锁定(“系统仪表板”节点)

系统仪表板节点下的**证据锁定**会显示当前监控系统上所有受保护数据的总览。

以下元数据可用于所有证据锁定:

- 受保护数据的开始日期和结束日期
- 锁定证据的用户
- 不再锁定证据的时间
- 数据存储位置
- 每个证据锁定的大小

证据锁定窗口中显示的所有信息均为快照。按 F5 刷新。

配置报告(“系统仪表板”节点)

在安装和配置视频管理软件系统时,您会做出许多选择,并且可能需要记录这些内容。随着时间的推移,您也很难记住自安装和初始配置以来或刚过去的几个月中更改过的所有设置。这就是为什么可以打印包含您的所有配置选项的报告。

创建和打印配置报告时,可以使用以下设置:

名称	说明
报告	可能包含在配置报告中的元素列表。
全部选择	将**报告**列表中的所有元素添加到配置报告中。
全部清除	从配置报告中删除**报告**列表中的所有元素。
封面	自定义报告的封面。
格式化	设置报告的格式。
排除敏感数据	从配置报告中删除个人数据,例如用户名、电子邮件地址和其他类型的敏感数据,并使其符合 GDPR。 报告中始终不包括有关许可证所有者的信息。
导出	选择报告的保存位置并创建为 PDF。

“服务器日志”节点

“服务器日志”节点

系统日志(选项卡)

日志中的每一行均代表一个日志条目。日志条目包含多个信息字段:

名称	说明
日志级别	信息、警告或错误。
本地时间	系统服务器的本地时间的时间戳。
邮件文本	记录事件的标识码。
类别	记录事件的类型。
来源类型	发生记录事件的设备的类型,如服务器或设备。
来源名称	记录事件发生的设备的名称。
事件类型	由记录事件表示的事件的类型。

审核日志(选项卡)

日志中的每一行均代表一个日志条目。日志条目包含多个信息字段:

名称	说明
本地时间	系统服务器的本地时间的时间戳。
邮件文本	显示记录事件的说明。
权限	有关是否允许(准许)远程用户动作的信息。
类别	记录事件的类型。
来源类型	发生记录事件的设备的类型,如服务器或设备。

名称	说明
来源名称	记录事件发生的设备的名称。
用户	导致记录事件的远程用户的用户名。
用户位置	远程用户引起记录事件的计算机的 IP 地址或主机名。

规则触发日志(选项卡)

日志中的每一行均代表一个日志条目。日志条目包含多个信息字段:

名称	说明
本地时间	系统服务器的本地时间的时间戳。
邮件文本	显示记录事件的说明。
类别	记录事件的类型。
来源类型	发生记录事件的设备的类型,如服务器或设备。
来源名称	记录事件发生的设备的名称。
事件类型	由记录事件表示的事件的类型。
规则名称	触发日志条目的规则的名称。
服务名称	发生记录事件的服务的名称。

元数据使用节点

元数据和元数据搜索

要管理和配置元数据设备,请参阅第258页上的显示或隐藏元数据搜索类别和搜索筛选器。

什么是元数据?

元数据是关于数据的数据,例如,描述视频图像的数据、图像中的内容或对象,或记录图像位置的数据。

元数据可以由以下对象生成:

- 提供数据的设备自身，如提供视频的摄像机
- 第三方系统或通过常规元数据驱动程序进行的集成

元数据搜索

元数据搜索是使用与元数据相关的搜索类别和搜索筛选器在 XProtect Smart Client 中进行的任何视频记录搜索。

默认的 Milestone 元数据搜索类别为：

- 位置：用户可以定义地理坐标，并根据这些坐标来定义搜索半径。
- 人员：用户可以搜索性别、大致身高和年龄，也可以选择显示人脸结果。
- 车辆：用户可以搜索车辆的颜色、速度和类型，也可以搜索特定的牌照。

元数据搜索要求

要获得搜索结果，需要满足以下条件之一：

- 您的视频监控系统中至少有一台设备可以执行视频分析并且配置正确
- 您的视频监控系统中的视频处理服务可生成元数据

无论哪种情况，元数据都必须采用所需的元数据格式。

有关详细信息，请参阅有关元数据搜索集成的文档。

访问控制节点

访问控制属性

“常规设置”选项卡（访问控制）

名称	说明
启用	默认情况下，系统已启用，表示它们在 XProtect Smart Client 中对于具有足够权限的用户可见，并且 XProtect 系统会收到访问控制事件。 您可以禁用系统（例如，在维护期间）以避免创建不需要的警报。
名称	显示在管理应用程序以及客户端中的访问控制集成的名称。可使用新名称覆盖现有名称。
说明	提供对访问控制集成的说明。这是可选的。
集成插件	显示在初始集成期间选择的访问控制系统的类型。

名称	说明
上次配置刷新	显示上一次从访问控制系统导入配置的日期和时间。
刷新配置	当您需要在 XProtect 中反映对访问控制系统所作的更改时，例如假设您添加或删除了门，请单击此按钮。 会显示访问控制系统的配置更改摘要。在应用新配置之前，检查该列表以确认正确反映了您的访问控制系统。
需要操作员登录	如果访问控制系统支持不同的用户权限，则为客户端用户启用其他登录。如果启用此选项，则访问控制系统将无法在 XProtect Mobile 客户端使用。 仅在集成插件支持有差别的用户权限时，才会看到该选项。

以下字段的命名和内容导入自集成插件。下面是一些典型字段的示例：

名称	说明
地址	输入安装有集成访问控制系统的服务器的地址。
端口	指定服务器上连接访问控制系统的端口号。
用户名	按照在访问控制系统中的定义输入用户的名称，该用户应为 XProtect 中集成系统的管理员。
密码	指定用户的密码。

“门和关联的摄像机”选项卡（访问控制）

此选项卡提供门访问点与摄像机、麦克风或扬声器之间的映射。您在集成向导中关联摄像机，但可以随时更改设置。到麦克风和扬声器的映射通过摄像机上的相关麦克风或扬声器内隐。

名称	说明
门	列出访问控制系统中定义的可用门访问点，按照门进行分组。 为更方便地导航到相关的门，可在访问控制系统中使用顶部下拉列表框对门进行筛选。 **已启用**：默认启用已获得许可的门。可以禁用门以释放许可证。 **许可证**：显示门是否已获得许可或许可证是否已过期。门被禁用时，该字段为空字段。

名称	说明
	删除:单击**删除**将从访问点删除摄像机。如果删除所有摄像机,会自动清除关联摄像机的复选框。
摄像机	列出 XProtect 系统中配置的摄像机。 从列表中选择摄像机,将其拖放到相应的访问点以将该访问点与该摄像机关联。

"访问控制事件"选项卡(访问控制)

事件类别用于将事件分组。事件类别的配置会影响 XProtect 系统中访问控制的行为,并且允许您(例如)定义警报以对多个事件类型触发单个警报。

名称	说明
访问控制事件	列出从访问控制系统导入的访问控制事件。集成插件控制事件的默认启用和禁用。您可以在集成之后随时禁用或启用事件。 启用事件后,事件存储在 XProtect 事件数据库中,并且(例如)可用于在 XProtect Smart Client 中筛选。
来源类型	显示可以触发访问控制事件的访问控制单元。
事件类别	为访问控制事件指定一个或多个事件类别,或无事件类别。在集成期间,系统自动将相关事件类别映射到事件。这会在 XProtect 系统中启用默认设置。您可以随时更改映射。 内置事件类别是: • 拒绝访问 • 已授予访问权限 • 访问请求 • 警报 • 错误 • 警告 还会显示集成插件定义的事件和事件类别,但您也可定义自己的事件类别,请参阅**用户定义类别**。 ⚠ 如果更改 XProtect Corporate 系统中的事件类别,请确保现有访问控制规则仍然有效。

名称	说明
用户定义类别	用于创建、修改或删除用户定义的事件类别。 如果内置类别不满足您的需要，您可以(例如)配合为访问控制操作定义触发事件来创建事件类别。 添加到 XProtect 系统的所有集成系统共用这些类别。它们允许设置跨系统处理，如跨系统处理警报定义。 如果您删除用户定义的事件类别，在该类别被任何集成使用时，您会收到警告。如果无论如何也要删除它，那么该类别的所有配置(如访问控制操作)将不再工作。

"访问请求通知"选项卡(访问控制)

您可以指定在发生给定事件时，XProtect Smart Client 屏幕上显示的访问请求通知。

名称	说明
名称	输入访问请求通知的名称。
添加访问请求通知	单击以添加和定义访问请求通知。 要删除通知，请单击右侧的 **X**。 如果 XProtect Smart Client 的用户登录到 Milestone Federated Architecture 层次结构中的父站点，则来自子站点的访问请求通知也会出现在 XProtect Smart Client 中。
访问请求通知详细信息	指定在给定事件发生时，哪些摄像机、麦克风或扬声器出现在访问请求通知中。还指定当通知弹出时用于警示用户的声音。
添加命令	选择哪些命令应在 XProtect Smart Client 的访问请求通知对话框中作为按钮提供。 相关访问请求命令： • 启用在来源单元上可用的、与访问请求操作相关的所有命令。例如**开门** 所有相关命令： • 启用来源单元上的所有命令 访问控制命令： • 启用选定的访问控制命令

名称	说明
	系统命令： • 启用 XProtect 系统中预定义的命令 要删除命令，请单击右侧的 **X**。

“持卡人”选项卡(访问控制)

使用**持卡人**选项卡检查访问控制系统中的持卡人相关信息。

名称	说明
搜索持卡人	输入持卡人姓名的字符，如果存在该姓名，则会显示在列表中。
名称	列出从访问控制系统检索的持卡人的姓名。
类型	列出持卡人的类型，例如： • 员工 • 保安 • 宾客

如果访问控制系统支持在 XProtect 系统中添加/删除图片，则可以为持卡人添加图片。如果访问控制系统不包含持卡人的图片，该操作将很有用。

名称	说明
选择图片	指定到含有持卡人图片的文件的路径。如果访问控制系统管理图片，则该按钮不可见。 允许的文件格式是 .bmp、.png、和 .jpg。 图片尺寸会调整，以使视图最大化。 Milestone 建议使用二次图片。
删除图片	单击可以删除图片。如果访问控制系统有图片，则删除之后会显示该图片。

事件节点

事件属性(事件节点)

以下信息描述了与 XProtect Incident Manager 相关的设置。

您在这些选项卡上为您的 XProtect Smart Client 操作员定义所有事件属性:

- 类型
- 状态
- 类别
- 类别 1-5

所有事件属性均有以下设置:

名称	说明
名称	事件属性名称不必唯一,但使用唯一和描述性的事件属性名称在许多情况下都有好处。
说明	定义的事件属性的进一步解释。例如,如果您已经创建了名为*位置*的类别,其说明可能是*事件在哪里发生?*

Transact 节点

交易数据来源(“交易”节点)

下表描述了交易数据来源的属性。

有关交易数据来源的详细信息,请参阅添加交易数据来源(向导)。

交易来源(属性)

名称	说明
启用	如果您要禁用交易来源,请清除该复选框。交易数据流将停止,但已经导入的数据仍会保留在事件服务器上。您仍可在 XProtect Smart Client 中查看已禁用的交易数据来源中的交易(如果在其保留期限内)。

名称	说明
	即使是已禁用的交易来源，仍需要交易来源许可证。
名称	如果要更改名称，请在此处输入新的名称。
连接器	无法更改在创建交易来源时所选的连接器。要选择不同的连接器，您需要创建新的交易来源，并在向导中选择所需连接器。
交易定义	可以选择不同的交易定义，用于定义如何将接收到的交易数据转换为交易和交易行。这包括定义以下项的内容： • 交易的开始和结束时间 • 交易在 XProtect Smart Client 中的显示方式
保留期限	指定交易数据在事件服务器上的保存时间，以天为单位。默认保留期限为 30 天。达到保留期限时，将自动删除数据。这是为了防止超出数据库存储容量的情形。 最小值为 1 天，最大值为 1000 天。
TCP 客户端连接器	如果选择了 **TCP 客户端连接器**，请指定以下设置： • **主机名**：输入与交易数据来源关联的 TCP 服务器的主机名 • **端口**：输入与交易数据来源关联的 TCP 服务器上的端口名
串行端口连接器	如果选择了**串行端口连接器**，则指定这些设置并确保它们与交易来源上的设置匹配： • **串行端口**：选择 COM 端口 • **波特率**：指定每秒传输的比特数 • **奇偶校验**：指定用于检测传输错误的方法。默认情况下，已选中**无** • **数据位**：指定用于表示一个数据字符的比特数 • **停止位**：指定用于表示字节传输时间的比特数。大多数设备需要 1 比特 • **握手**：指定用于确定交易数据来源和事件服务器之间的通信协议的握手方法

交易数据定义(“交易”节点)

下表描述了用于交易数据来源的定义的属性。

有关创建和添加交易数据定义的详细信息，请参阅创建和添加交易数据定义。

交易定义(属性)

名称	说明
名称	输入名称。
编码	选择交易来源(如收银机)所使用的字符集。这可帮助 XProtect Transact 将交易数据转换为可以理解的文本,以供您在配置定义时使用。 如果选择了错误的编码,数据可能会显示为无意义的文本。
开始收集数据	从连接的交易来源收集交易数据。您可以使用此数据来配置交易定义。 等待至少一个(建议更多)交易完成。
停止收集数据	在收集了用于配置定义的足够数据后,单击此按钮。
从文件加载	如果您要从已存在的文件导入数据,请单击此按钮。通常,这是您以前创建的文件格式为 .capture 的文件。它可以是其他文件格式。此处要注意的是,导入文件的编码必须与为当前定义选择的编码相匹配。
保存到文件	如果要将收集的原始数据保存到文件,请单击此按钮。您可在以后重新使用它。
匹配类型	选择匹配类型,用于在收集的原始数据中搜索启动模式和停止模式: • 使用完全匹配:搜索操作将识别包含您在**启动模式**和**停止模式**字段中所输入的确切内容的字符串 • 使用通配符:搜索操作将识别包含您在**启动模式**和**停止模式**字段中所输入的字符串与通配符符号(*、#、?)相组合的内容 * 会匹配任何数量的字符。例如,如果您输入“Start tra*tion”,则搜索操作将识别包含“Start transaction”的字符串。 # 会精确匹配 1 位。例如,如果您输入“# watermelon”,则搜索操作将识别包含(例如)“1 watermelon”的字符串。? 会精确匹配 1 个字符。例如,您可以使用搜索表达式“Start trans?ction”来识别包含“Start transaction”的字符串 • 使用正则表达式:可使用此匹配类型识别包含特定表示法或约定(如日期格式或信用卡号码)的字符串。有关详细信息,请参阅 Microsoft 网站 (https://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/)
原始数据	来自所连接交易来源的交易数据字符串显示在此部分中。
启动模式	指定用于指示交易开始位置的启动模式。在**预览**字段中插入了水平线以通过视觉方式表示

名称	说明
	交易的开始和结束位置，并有助于单独区分各个交易。
停止模式	指定用于指示交易停止位置的停止模式。停止模式不是强制的，但如果接收到的数据在实际交易之间包含不相关的信息(如关于营业时间或特别优惠的信息)，则它很有用。 如果不指定停止模式，将以下一收据的开始位置来定义收据的结束。收据的开始由您在**启动模式**字段中输入的内容确定。
添加过滤器	使用**添加筛选器**按钮来指示您要在 XProtect Smart Client 中省略的字符，或要由其他字符或断线替换的字符。 当交易来源字符串包含用于非打印用途的控制字符时，更换字符很有用。必须添加断线，才能使 XProtect Smart Client 中的收据类似于原始收据。
过滤器文本	显示当前在**原始数据**部分中选择的字符。如果您知道要省略或替换的字符，但它们未出现在所收集的原始数据字符串中，则可以在**字符**字段中手动输入字符。 如果字符是控制字符，则您需要输入其十六进制字节值。为字节值使用此格式：{XX} 和 {XX,XX,...}(如果字符由多个字节组成)。
动作	对于添加的每个过滤器，您应指定针对所选字符的处理方式： • 省略：您选中的字符将被筛选掉 • 替换：您选中的字符将被您指定的字符替换 • 添加断线：您选中的字符将被断线替换
替换	输入要替换选定字符的文本。仅在选中**替换**动作时才会涉及。
删除未定义为筛选器文本的控制字符	删除添加筛选器后尚未删除的非打印字符。 在**原始数据**窗格和**预览**部分中，查看启用或禁用此设置时交易数据字符串的变化方式。
预览	可使用**预览**部分验证您是否已识别并过滤掉不需要的字符。此处显示的输出类似于现实中的收据在 XProtect Smart Client 中的外观。

警报节点

警报定义(“警报”节点)

当您的系统在系统中注册事件时，您可以将系统配置为在 XProtect Smart Client 中生成警报。必须首先定义警报后才能进行使用;根据在系统服务器上注册的事件来定义警报。您还可以使用用户定义事件来触发警报，以及使用相同事件来触发多个不同警报。

警报定义设置:

名称	说明
启用	默认情况下已启用报警定义。要禁用它，请清除该复选框。
名称	警报名称不必唯一，但使用唯一和描述性的警报名称在许多情况下都有好处。
说明	输入关于警报以及如何解决导致警报的问题的描述性文本。 当用户处理警报时，该文本出现在 XProtect Smart Client 中。
触发事件	选择触发警报时使用的事件消息。从两个下拉菜单中进行选择: • 第一个下拉菜单:选择事件类型，例如分析事件和系统事件 • 第二个下拉菜单:选择要使用的特定事件消息。可用的消息取决于您在第一个下拉菜单中选择的事件类型
来源	指定事件的来源。除了摄像机或其他设备，来源也可以是由插件定义的来源，如 VCA 和 MIP。选项取决于所选择的事件类型。

警报触发:

名称	说明
时间配置文件	选择**时间配置文件**单选按钮可指定时间间隔，在此间隔期间警报定义处于活动状态。列表中仅会显示您已在**规则和事件**节点下定义的时间配置文件。如果未定义任何时间配置文件，则只有**始终**选项可用。
事件基于	如果需要使报警基于事件，请选择此单选按钮。在选择后，请指定开始和停止事件。您可以选择在摄像机、视频服务器和输入上定义的硬件事件。另请参阅事件总览。也可以使用全局/手动事件定义。另请参阅用户定义事件(已作说明)。

需要操作员操作：

名称	说明
时间限制	选择需要操作员动作时的时间限制。默认值为 1 分钟。在**触发的事件**下拉菜单中附加事件之前，时间限制不会处于活动状态。
触发的事件	选择在超过时间限制后触发的事件。

地图：

名称	说明
警报管理器视图	在 XProtect Smart Client > **警报管理器**中列出警报时向其分配智能地图或地图。 如果警报是由设备触发的，并且设备已添加到智能地图，则智能地图会显示警报。

其他：

名称	说明
相关摄像机	选择在警报定义中包括的摄像机（最多 15 台），即使这些摄像机本身未触发警报。例如，如果您已选择外部事件消息（例如，门被打开）作为警报的来源，这就可能相关。通过定义门附近的一台或多台摄像机，可将摄像机的事件记录与警报连接。
初始警报所有者	选择对警报负责的默认用户。
初始警报优先级	选择警报的优先级。使用 XProtect Smart Client 中的这些优先级确定警报的重要性。
警报类别	选择警报的类别，例如**假警报**或**需要调查**。
警报触发的事件	定义在 XProtect Smart Client 中警报可触发的事件。

名称	说明
自动关闭警报	如果需要由特殊事件来自动停止报警，请选中此复选框。并非所有事件都可以触发报警。清除该复选框可从一开始就禁用新警报。
可分配给管理员的警报	选中该复选框以在**分配给**列表中包含具有管理员角色的用户。 **分配给**列表位于 XProtect Smart Client 中**警报管理器**选项卡上的警报详细信息中。 清除该复选框以从**分配给**列表中筛选出具有管理员角色的用户以缩短列表。

警报数据设置(“警报”节点)

配置警报数据设置时，请指定以下各项：

“警报数据级别”选项卡

优先级

名称	说明
级别	使用您选择的等级数字来添加新优先级或使用/编辑默认优先级等级(数字 1、2 或 3)。这些优先级用于配置**初始警报优先级**设置。
名称	输入实体的名称。可以创建任意数量。
声音	选择要与警报关联的声音。使用其中一种默认声音，或在**声音设置**中添加更多。
重复声音	确定声音是应该只播放一次还是重复播放，直到在 XProtect Smart Client 中，操作员单击警报列表中的警报。
启用桌面通知	对于每个警报优先级，您都可以启用或禁用桌面通知。如果在使用支持 XProtect 配置文件的 Smart Client 视频管理软件，则还必须在所需的 Smart Client 配置文件上启用通知。请参阅 第 403 页上的“警报管理器”选项卡(Smart Client 配置文件)。

状态

名称	说明
级别	除了默认状态等级(数字 **1**、**4**、**9** 和 **11**,它们无法编辑或重复使用),使用您选择的等级数字来添加新状态。这些等级状态只有在 XProtect Smart Client 的*警报列表*中可见。

类别

名称	说明
级别	使用您选择的等级数字添加新类别。这些类别级别用于配置**初始警报类别**设置。  级别 99 保留为供 XProtect Mobile 客户端的“紧急警报”使用。
名称	输入实体的名称。可以创建任意数量。

“警报列表配置”选项卡

名称	说明
可用列	使用 > 选择在 XProtect Smart Client 的*警报*列表中可用的列。使用 < 清除选择。**完成后**,已选列应包含要包括在内的项。

“关闭的原因”选项卡

名称	说明
启用	选择启用该条件:对于所有警报,都必须先指定关闭原因然后才能将其关闭。
原因	添加关闭原因以供在关闭警报时用户可以从中选择。示例为*已解决的侵入者*或*假警报*。可以创建任意数量。

声音设置(“警报”节点)

配置声音设置时，请指定以下各项：

名称	说明
声音	选择要与警报关联的声音。声音列表包含大量默认 Windows 声音。您还可以添加新声音(.wav 或 .mp3)。
添加	添加声音。浏览声音文件并上传一个或多个 .wav 或 .mp3 文件。
删除	从手动添加的声音的列表中删除所选声音。无法删除默认声音。
测试	测试声音。在该列表中，选择声音。声音会播放一次。

联合站点层级

联合站点属性

本节将介绍**常规**选项卡和**父站点**选项卡。

“常规”选项卡

可以更改与当前登录的站点相关的一些信息。

名称	说明
名称	输入站点的名称。
说明	输入站点说明。
URL	使用该列表添加和删除此站点的 URL，并指出站点是否是外部站点。外部地址可从本地网络外部访问。
版本	站点管理服务器的版本号。
服务帐户	运行管理服务器的服务帐户。
上次同步的时间	层次结构上次同步的时间和日期。
上次同步的状态	层次结构上次同步的状态。可能为**成功**或**失败**。

“父站点”选项卡

该选项卡显示关于当前登录站点的父站点的信息。如果站点没有父站点，则该选项卡不可见。

名称	说明
名称	显示父站点的名称。
说明	显示父站点的说明(可选)。
URL	列出此父站点的 URL，并指出它们是否为外部父站点。外部地址可从本地网络外部访问。
版本	站点管理服务器的版本号。
服务帐户	运行管理服务器的服务帐户。
上次同步的时间	层次结构上次同步的时间和日期。
上次同步的状态	层次结构上次同步的状态。可能为**成功**或**失败**。

helpfeedback@milestone.dk

关于 Milestone

Milestone Systems 是领先的开放式平台视频管理软件提供商；其技术可帮助全球企业了解如何确保安全、保护资产并提高业务效率。Milestone Systems支持开放式平台社区，积极推动网络视频技术开发和使用领域的协作与创新，其可靠且可扩展的解决方案在全球超过 15 万个站点中得到了验证。Milestone Systems 成立于 1998 年，是 Canon Group 旗下的一家独立公司。有关详细信息，请访问 https://www.milestonesys.com/。