MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile Server 2020 R2

管理员手册

milestone

目录

Copyright、商标和免责声明

Copyright © 2020 Milestone Systems A/S

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

XProtect Mobile (说明)

XProtect Mobile 由五个组件组成：

- XProtect Mobile 客户端

  XProtect Mobile 客户端是一个移动监控应用程序，您可以在您的 Android 或 Apple 设备上安装和使用。您可根据需要使用任意数量的 XProtect Mobile 客户端安装。

  有关详细信息，请从Milestone Systems 网站 (https://www.milestonesys.com/support/help-yourself/manuals-and-guides/)下载XProtect Mobile客户端用户指南。

- XProtect Web Client

  XProtect Web Client 可让您在 Web 浏览器中查看实时视频，并允许您下载录像。XProtect Web Client 与 XProtect Mobile 服务器的安装一起自动安装。

  有关详细信息，请从 Milestone Systems 网站 (https://www.milestonesys.com/support/help-yourself/manuals-and-guides/)下载 XProtect Web Client 客户端用户指南。

- XProtect Mobile 服务器
- XProtect Mobile 插件
- Mobile Server Manager

本手册中介绍了 XProtect Mobile 服务器、XProtect Mobile 插件和 Mobile Server Manager。

XProtect Mobile 服务器(说明)

XProtect Mobile 服务器处理从 XProtect Mobile 客户端或 XProtect Web Client 到系统的登录。

XProtect Mobile 服务器将视频流从记录服务器发布到 XProtect Mobile 客户端或 XProtect Web Client。这提供了安全的设置，其中记录服务器从不会连接至互联网。XProtect Mobile 当服务器从记录服务器接收视频流时，也会处理编码解码器和格式的复杂转换，从而允许移动设备上的视频流。

必须在您要从其访问记录服务器的任何计算机上安装XProtectMobile服务器。安装XProtectMobile服务器时，请使用具有管理员权限的帐户登录。否则，安装将无法成功完成(请参阅安装XProtectMobile服务器第 页上的12) 。

XProtect Mobile 服务器支持实时模式下的直接流和自适应流(仅适用于 XProtect Expert 和 XProtect Corporate) 。

产品比较图

XProtect 视频管理软件 包括以下产品：

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

完整功能列表可参见Milestone网站(https://www.milestonesys.com/solutions/platform/product-index/)上的产品总览页。

下表列出了各产品的主要不同之处：

名称	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
每个 SLC 的站点数量	1	1	多站点	多站点	多站点
每个 SLC 的记录服务器数量	1	1	不受限制	不受限制	不受限制
每台记录服务器的硬件设备数量	8	48	不受限制	不受限制	不受限制
Milestone Interconnect™	-	远程站点	远程站点	远程站点	中央/远程站点
Milestone Federated Architecture™	-	-	-	远程站点	中央/远程站点
记录服务器故障转移	-	-	-	冷热后备	冷热后备
远程连接服务	-	-	-	-	✓
边缘存储支持	-	-	✓	✓	✓
多级视频存储	实时数据库 + 1 存档	实时数据库 + 1 存档	实时数据库 + 1 存档	实时数据库 + 不受限制的存档	实时数据库 + 不受限制的存档

名称	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
SNMP 通知	-	-	-	✓	✓
时间控制用户访问权限	-	-	-	-	✓
降低帧速率(整理)	-	-	-	✓	✓
视频数据加密(记录服务器)	-	-	-	✓	✓
数据库签名(记录服务器)	-	-	-	✓	✓
PTZ 优先级水平	1	1	3	32000	32000
扩展 PTZ(保留 PTZ 会话并从 XProtect Smart Client 巡视)	-	-	-	✓	✓
证据锁定	-	-	-	-	✓
书签功能	-	-	仅手动	手动和基于规则	手动和基于规则
实时多流或多播/自适应流	-	-	-	✓	✓
直接流	-	-	-	✓	✓
整体安全	客户端用户权限	客户端用户权限	客户端用户权限	客户端用户权限	客户端用户权限/ 管理员用户权限
XProtect Management Client 配置文件	-	-	-	-	✓
XProtect Smart Client 配置	-	-	3	3	不受限制

名称	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
文件					
XProtect Smart Wall	-	-	-	可选	✓
系统监视器	-	-	-	✓	✓
智能地图	-	-	-	✓	✓
两步式验证	-	-	-	-	✓
DLNA 支持	-	✓	✓	✓	✓
隐私屏蔽	-	✓	✓	✓	✓
设备密码管理			✓	✓	✓

要求和注意事项

使用 XProtect Mobile 的先决条件

在开始使用 XProtect Mobile 前，您必须首先确保具备下列条件：

- 已安装且配置了至少一位用户的 VMS 正在运行。
- 在 XProtect Smart Client 中设置的摄像头和视图
- 运行 Android 或 iOS 的移动设备可从下载 XProtect Mobile 客户端应用程序的位置访问 Google Play 或 App Store℠
- 用于运行 XProtect Web Client 的 Web 浏览器

要了解有关要求的更多信息，请参阅 XProtect Mobile 系统要求第 页上的10。

XProtect Mobile 系统要求

有关不同组件最低系统要求的信息，请转到 Milestone 网站 (https://www.milestonesys.com/systemrequirements/)。

- 要查找 XProtect Mobile 客户端的要求，请选择 **XProtect Mobile** 产品图标
- XProtect Web Client**XProtect Web Client**要查找 的要求，请选择 产品图标
- 要查找 XProtect Mobile 服务器的要求，请选择已安装的 XProtect 产品图标
- XProtect Mobile 插件的要求是：
    - 正在运行的 Management Client
    - 安装 Milestone 插件与 VMS 集成

通知设置要求

- 您必须将一个或多个警报与一个或多个事件和规则进行关联。系统通知没有该要求。
- 确保您与 Milestone Systems 的 Milestone Care™ 协议是最新的
- 您的系统必须能够访问互联网

有关详细信息请参阅：

在 XProtect Mobile 服务器上设置推送通知第 页上的42上设置推送通知

通知选项卡第 页上的23

智能连接设置要求

- 您的 XProtect Mobile 服务器必须使用公共 IP 地址。该地址可以是静态地址或动态地址，但通常优先选择使用静态 IP 地址
- 您必须拥有智能连接的有效许可证

用户双重验证设置的要求

- 您已安装 SMTP 服务器
- 您已在站点导航窗格的角色节点中，将用户和组添加至 Management Client 中的 XProtect 系统。在相关角色中，选择用户和组选项卡
- 如果您从以前版本的 XProtect 升级系统，则必须重新启动移动设备服务器才能启用双重验证功能

有关详细信息请参阅：

通过电子邮件设置两步验证的用户第 页上的46

双重验证第 页上的24

手机视频推送设置要求

- 每个通道都需要硬件设备许可证
- 要启用音频和手机视频推送：
    1. 下载并安装 Milestone XProtect Device Pack 10.3a 版本或更高版本。
    2. 下载并安装 XProtect Mobile Server Installer.exe 13.2a 或更高版本。
    3. 重启 Recording Server 服务。

客户端的移动设备服务器加密要求

如果您未启用加密并使用 HTTP 连接，则 XProtect Web Client 中的按下即可发言功能将不可用。

如果为移动设备服务器的加密选择自签署证书，则 XProtect Mobile 客户端将无法与移动设备服务器进行连接。

直接流的要求

XProtect Mobile 支持实时模式下的直接流(仅适用于 XProtect Expert 和 XProtect Corporate) 。

直接流的摄像机配置要求

要在 XProtect Web Client 和 XProtect Mobile 客户端中使用直接流，您必须使用以下摄像机配置：

- 摄像机必须支持H.264编解码器(适用于所有客户端) 或H.265编解码器(仅适用于XProtectMobile客户端)
- 建议将 **GOP** 大小的值设为 **1** 秒，而 **FPS** 设置的值必须高于 **10** FPS

安装

安装 XProtect Mobile 服务器

安装 XProtect Mobile 服务器后，即可结合系统使用 XProtect Mobile 客户端和 XProtect Web Client。要减少运行管理服务器的计算机上系统资源的总体使用情况，请在单独的计算机上安装 XProtect Mobile 服务器。

管理服务器具有内置的公共安装网页。在此网页中，管理员和最终用户可以从管理服务器或系统中的任何其他计算机下载并安装所需的 XProtect 系统组件。

XProtect Mobile 安装"单个计算机"选项时，将自动安装服务器。

要安装 XProtect Mobile 服务器：

1. 在浏览器中输入以下 URL：*http://[管理服务器地址]/installation/admin* 其中，[管理服务器地址] 是管理服务器的 IP 地址或主机名。
2. 单击 XProtect Mobile 服务器安装程序的所有语言。
3. 运行下载的文件。然后，对所有警告单击是。然后，将开始执行解包。
4. 选择安装程序的语言。然后，单击继续。
5. 阅读并接受许可协议。然后，单击继续。
6. 为了安全通信，请选择用于连接到管理服务器的证书。
7. 选择安装类型：
   - 单击典型以安装 XProtect Mobile 服务器和插件
   - 单击自定义仅安装服务器或插件。例如，如果要使用 Management Client 管理 XProtect Mobile 服务器，但在该计算机上不需要 XProtect Mobile 服务器，则仅安装插件很有用

     XProtect Mobile 要在 Management Client 中管理 XProtect Mobile 服务器，必须在运行 Management Client 的计算机上安装插件。
8. 仅适用于自定义安装：选择要安装的组件。然后，单击继续。
9. 指定移动设备服务器加密。然后，单击继续。

   在指定移动设备服务器加密页面上，您可以保护移动设备服务器与客户端和服务之间的通信。

   如果未启用加密，则有些客户端中的一些功能将不可用。有关详细信息，请参阅客户端的移动设备服务器加密要求第 页上的34。

在列表中选择有效的证书。移动设备服务器数据加密(已解释) 第 页上的33*Milestone*有关在系统中建立安全通信的详细信息，请参阅移动设备服务器数据加密(已解释) 或 证书指南(只有英文版) 。

您还可以通过操作系统任务栏中的 Mobile Server Manager 托盘图标在安装完成后启用加密(请参阅在移动设备服务器上启用加密第 页上的38) 。

10. 选择移动设备服务器的服务帐户。然后，单击继续。

> 要在以后更改或编辑服务帐户凭据，您将必须重新安装移动设备服务器。

11. 在服务器 **URL** 字段中填写主要管理服务器地址。
12. 仅适用于自定义安装：指定用于与移动设备服务器通信的连接端口。然后，单击继续。

> 在典型安装中，连接端口会获取默认端口号(HTTP 端口为 8081，HTTPS 端口为 8082) 。

13. 选择文件位置和产品语言，然后单击安装。
14. 安装完成后，会显示已成功安装的组件的列表。然后，单击关闭。

您已准备配置 XProtect Mobile(参阅Mobile 服务器设置第 页上的14) 。

配置

Mobile 服务器设置

在 Management Client 中，您可以配置和编辑 XProtect Mobile 服务器设置列表，通过移动设备服务器属性部分底部工具栏上的选项卡进行访问。在那里，您可以：

- 启用或禁用服务器功能的常规配置(请参阅“常规”选项卡第 页上的14)
- 配置服务器连接设置并设置“智能连接”功能(参阅连接选项卡第 页上的16)
- 查看服务器当前状态和列出的活动用户(请参阅“服务器状态”选项卡第 页上的18)
- 设置性能参数以启用直接流和自适应流，或设置转码视频流限制(请参阅性能选项卡第 页上的19)
- 配置调查设置(请参阅调查选项卡第 页上的21)
- 配置手机视频推送设置(请参阅手机视频推送选项卡第 页上的22)
- 设置、打开和关闭系统和推送通知(请参阅通知选项卡第 页上的23)
- 为用户启用并配置其他登录步骤(请参阅双重验证第 页上的24)

“常规”选项卡

下表介绍了此选项卡上的设置。

常规

名称	说明
服务器名称	输入 XProtect Mobile 服务器的名称。
说明	输入 XProtect Mobile 服务器的可选说明。
Mobile 服务器	查看当前所选 XProtect Mobile 服务器的名称。
登录方法	选择在用户登录到服务器时要使用的身份验证方法。您可以选择： • 自动 • **Windows** 身份验证 • 基本身份验证。

功能

下表描述了如何控制 XProtect Mobile 功能的可用性。

名称	说明
启用 **XProtect Web Client**	允许访问 XProtect Web Client。默认情况下，该功能为启用。
启用所有摄像机视图	包括所有摄像机视图。此视图显示允许用户在记录服务器上查看的所有摄像机。默认情况下，该功能为启用。
启用操作**(**输出和事件**)**	允许访问 XProtect Mobile 客户端和 XProtect Web Client 中的操作。默认情况下，该功能为启用。 如果禁用此功能，则客户端用户无法查看输出和事件，即使这些配置正确也是如此。
启用流入音频	在 XProtect Web Client 和 XProtect Mobile 客户端中启用流入音频功能。默认情况下，该功能为启用。
启用一键通	在 XProtect Web Client 和 XProtect Mobile 客户端中启用一键通 (PTT) 功能。默认情况下，该功能为启用。
拒绝内置管理员角色访问 **XProtect Mobile** 服务器	启用此选项可防止分配给内置管理员角色的用户访问 XProtect Mobile 客户端或 XProtect Web Client 中的视频。

日志设置

您可以看到日志设置信息。

名称	说明
日志文件位置	查看系统保存日志文件的位置。
保留日志	查看保留日志的天数。默认为三天。

配置备份

如果您的系统有多个 XProtect Mobile 服务器，则可以使用备份功能导出当前设置并将其导入其他 XProtect Mobile 服务器。

名称	说明
导入	导入附带全新 XProtect Mobile 服务器配置的 XML 文件。
导出	导出您的 XProtect Mobile 服务器配置。本系统会在 XML 文件中存储配置。

连接选项卡

连接选项卡中的设置用于以下任务：

- 配置连接设置第 页上的40
- 向用户发送电子邮件消息第 页上的41
- 在复杂网络中启用连接第 页上的40
- 在路由器上启用通用即插即用发现功能第 页上的40

有关更多信息，请参阅智能连接(已解释) 第 页上的39。

常规

名称	说明
连接类型	选择 XProtect Mobile 客户端和 XProtect Web Client 用户连接至 XProtect Mobile 服务器的方式。可以在以下选项中进行选择：仅 **HTTP**、**HTTP** 和 **HTTPS** 或仅 **HTTPS**。有关详细信息，请参阅客户端的移动设备服务器加密要求第 页上的34。
客户端超时 **(HTTP)**	设置 XProtect Mobile 客户端和 XProtect Web Client 必须向 XProtect Mobile 服务器指示它们已启动并运行的频率的时间范围。默认值为 30 秒。 Milestone 建议不要增大时间范围。
启用 **UPnP** 发现功能	该功能可以让您通过 UPnP 协议在网络上发现 XProtect Mobile 服务器。 XProtect Mobile 客户端具有基于 UPnP 查找 XProtect Mobile 服务器的扫描功能。
启用自动端口映射	当 XProtect Mobile 服务器安装在防火墙后方时，路由器中需要端口映射，因此客户端仍然可以从 Internet 访问服务器。 启用自动端口映射选项可以让 XProtect Mobile 服务器自身进行端口映射，只要路由器

名称	说明
	是为其配置。
启用**"**智能连接**"**	通过智能连接，您可以验证是否已正确配置 XProtect Mobile 服务器，而无需使用移动设备或平板电脑进行验证。它还能简化客户端用户的连接流程。

互联网访问

名称	说明
配置自定义互联网访问	如果您使用 UPnP 端口映射将连接转至特定连接，请选中配置自定义互联网访问复选框。 然后提供 **IP** 地址或主机名以及用于连接的端口。例如，如果您的路由器不支持 UPnP 或者您拥有路由器链，则可以执行此操作。
禁用默认地址	禁用默认 IP 地址以仅使用自定义 IP 地址或主机名连接到移动设备服务器。
选择后可动态地检索 **IP** 地址	如果您的 IP 地址经常更改，请选中选择后可动态检索 **IP** 地址复选框。
HTTP 端口	输入 HTTP 连接的端口号。
HTTPS 端口	输入 HTTPS 连接的端口号。
服务器地址	列出连接到移动设备服务器的所有 IP 地址。

"智能连接**"**通知

名称	说明
电子邮件邀请	输入"智能连接"通知接收人的邮件地址。

名称	说明
电子邮件语言	指定电子邮件中所用的语言。
“智能连接”令牌	移动设备用户可用于连接 XProtect Mobile 服务器的唯一标识符。
指向“智能连接”的链接	移动设备用户可用于连接 XProtect Mobile 服务器的链接。

“服务器状态”选项卡

查看 XProtect Mobile 服务器的状态详细信息。详细信息为只读：

名称	说明
服务器活动起始时间	显示 XProtect Mobile 服务器最后启动的时间和日期。
CPU 使用率	显示移动设备服务器上的当前 CPU 使用量。
外部带宽	显示 XProtect Mobile 客户端或 XProtect Web Client 与移动设备服务器之间使用的当前带宽。

活动用户

查看当前与 XProtect Mobile 服务器连接的 XProtect Mobile 客户端或 XProtect Web Client 的状态详细信息。

名称	说明
用户名	显示连接到移动设备服务器的每个 XProtect Mobile 客户端或 XProtect Web Client 用户的用户名。
状态	显示 XProtect Mobile 服务器和相应 XProtect Mobile 客户端或 XProtect Web Client 用户之间当前的关系。可能的状态有：

名称	说明
	• 已连接：客户端和服务器交换密钥和加密凭据时的初始状态 • 已登录：XProtect Mobile 客户端或 XProtect Web Client 用户登录到 XProtect 系统。
视频带宽使用 **(kB/s)**	显示当前向每个 XProtect Mobile 客户端或 XProtect Web Client 用户开放的总视频流带宽。
音频带宽使用 **(kB/s)**	显示当前为每个 XProtect Web Client 用户打开的音频流的总带宽。
转码视频流	显示当前为每个 XProtect Mobile 客户端或 XProtect Web Client 用户打开的总转码视频流。
直接视频流	显示当前为每个 XProtect Mobile 客户端或 XProtect Web Client 用户打开的直接视频流总数（仅适用于 XProtect Expert 和 XProtect Corporate）。
转码音频流	显示当前为每个 XProtect Web Client 用户打开的总转码音频流。

性能选项卡

在性能选项卡上，可以对 XProtect Mobile 服务器的性能进行以下设置和限制：

视频流设置**（**仅适用于 **XProtect Expert** 和 **XProtect Corporate)**

名称	说明
启用直接流	在 XProtect Web Client 和 XProtect Mobile 客户端中启用直接流。默认情况下，该功能为启用。
启用自适应流	在 XProtect Web Client 和 XProtect Mobile 客户端中启用自适应流。默认情况下，该功能为启用。
流模式	启用自适应流功能后，可以从列表中选择流模式的类型： • 优化视频质量**（**默认**)** - 选择具有等于或高于所请求的分辨率的最低可用分辨率的流

名称	说明
	• 优化服务器性能 - 降低分辨率请求，然后选择等于或高于此请求的最低可用分辨率的流 • 为低带宽优化分辨率 - 选择可用分辨率最低的流(如果使用 3G 或不稳定的网络，建议使用此项)

转码视频流限制

级别 **1**

级别**1**是XProtectMobile服务器上的默认限制。在此处设置的任何限制都会应用于XProtectMobile的转码视频流。

名称	说明
级别 **1**	选中该复选框以对 XProtect Mobile 服务器性能启用第一级别的限制。
最大 **FPS**	设置从 XProtect Mobile 服务器发送到客户端的最大每秒帧数(FPS) 的限制。
最大图像分辨率	设置从 XProtect Mobile 服务器发送到客户端的映像分辨率限制。

级别 **2**

如果要强制执行与级别**1**中的默认限制不同的限制级别，请选中级别**2**复选框。不能设定比第一级别中的设置更高的任何设置。例如，如果在级别**1**上将“最大FPS”设置为45，则在级别**2**上只能将“最大FPS”设置为44或更低的值。

名称	说明
级别 **2**	选中该复选框可对 XProtect Mobile 服务器性能启用第二级别限制。
CPU 阈值	在系统强制执行视频流限制之前，在 XProtect Mobile 服务器上设置 CPU 负载的阈值。

名称	说明
带宽阈值	在系统强制实施视频流限制之前，在 XProtect Mobile 服务器上设置带宽负载阈值。
最大 **FPS**	设置从 XProtect Mobile 服务器发送到客户端的最大每秒帧数(FPS) 的限制。
最大图像分辨率	设置从 XProtect Mobile 服务器发送到客户端的映像分辨率限制。

级别 **3**

还可选中级别 **3** 复选框创建第三限制级别。不能设定比级别 1 和级别 2 中的设置更高的任何设置。例如，如果在级别 **1** 上将最大 **FPS** 设置为 45，并在级别 **2** 上将其设置为 32 这一级别，则在级别 **3** 上只能将最大 **FPS** 设置为 31 或更低的值。

名称	说明
级别 **3**	选中该复选框可对 XProtect Mobile 服务器性能启用第三级别限制。
CPU 阈值	在系统强制执行视频流限制之前，在 XProtect Mobile 服务器上设置 CPU 负载的阈值。
带宽阈值	在系统强制实施视频流限制之前，在 XProtect Mobile 服务器上设置带宽负载阈值。
最大 **FPS**	设置从 XProtect Mobile 服务器发送到客户端的每秒帧数(FPS) 的限制。
最大图像分辨率	设置从 XProtect Mobile 服务器发送到客户端的映像分辨率限制。

系统不会立即从一个级别切换至另一个级别。如果 CPU 或带宽阈值高出或低于所指示级别的程度不足 5%，则会继续使用当前级别。

调查选项卡

调查设置

您可以启用调查，以便人们可以使用 XProtect Mobile 客户端或 XProtect Web Client 访问录制的视频并调查事件，以及准备和下载视频证据。

名称	说明
调查文件夹	显示视频导出保存在硬盘驱动器上的位置。
将调查文件夹的大小限制为	输入调查文件夹可以包含的兆字节的最大数。默认大小为 2000 MB。
查看由其他用户进行的调查	选中此复选框可以让用户访问并非他们所创建的调查。
在 **AVI** 导出中包括时间标记	选中此复选框可包括下载 AVI 文件的日期和时间。
为 **AVI** 导出使用的编解码器	选择在准备 AVI 包供下载时要使用的压缩格式。 您可以选择的编解码器可能因操作系统而异。如果您没有看到所需的编解码器，您可以通过在运行 XProtect Mobile 服务器的计算机上安装它以将其添加到列表。
AVI 导出使用的音频比特率	当视频导出中包含音频时，从列表中选择适当的音频比特率。默认值为 160000 Hz。
在导出失败时保留或删除数据**(MKV** 和 **AVI)**	选择是否保存在调查中没有成功准备好以供下载的数据，或者将其删除。

调查

名称	说明
调查	列出目前系统已设置的调查。如果您不再想保存调查，请使用删除或删除所有按钮。例如，如果要在服务器上释放更多可用磁盘空间，该操作将非常有用。
详细信息	要删除为调查导出的单个视频文件，但要保留调查本身，请在列表中选择调查。在调查详细信息组中，选择数据库、**AVI** 或 **MKV** 字段右边的删除图标以导出。

手机视频推送选项卡

如果启用了手机视频推送，则可以指定以下设置：

名称	说明
手机视频推送	在移动设备服务器上启用手机视频推送。
通道数	显示 XProtect 系统中已启用的手机视频推送通道的数量。
通道	显示相关通道的通道数。不可编辑。
端口	相关视频推送通道的端口号。
MAC 地址	相关视频推送通道的 MAC 地址。
用户名	输入与相关手机视频推送通道关联的用户名。
摄像机名称	如果识别出摄像机，则显示摄像机的名称。

一旦完成所有必要步骤(请参阅设置视频推送以推送视频流第 页上的43)，则选择查找摄像机搜索相关摄像机。

通知选项卡

使用通知选项卡可打开或关闭系统通知和推送通知。

如果您打开通知，并已配置一个或多个警报和事件，则 XProtect Mobile 会在事件发生时通知用户。当应用程序打开时，通知将在移动设备上的 XProtect Mobile 中传递。推送通知会通知未打开 XProtect Mobile 的用户。会将这些通知提供给移动设备。

有关详细信息请参阅：启用向特定移动设备或所有移动设备发送推送通知第 页上的42

下表介绍了此选项卡上的设置。

名称	说明
通知	选中此复选框可打开通知。
维护设备注册	选中此复选框可存储有关连接到此服务器的设备和用户的信息。系统会将通知发送到这些设备。 如果清除此复选框，则还清除设备列表。要让用户重新开始接收通知，您必须选中此复选框，并且用户必须将其设备再次连接到服务器。

已注册的设备

名称	说明
已启用	选中此复选框可开始向设备发送通知。
设备名称	已连接到此服务器的移动设备的列表。 您可以通过选中或清除启用复选框来启动或停止向特定设备发送通知。
用户	将接收通知的用户的名称。

双重验证

可用的功能取决于正在使用的系统。有关详细信息，请参阅 https://www.milestonesys.com/solutions/platform/product-index/。

使用双重验证选项卡为以下用户启用并指定其他登录步骤：

- XProtect Mobile iOS 或 Android 移动设备上的应用程序
- XProtect Web Client

第一种验证是密码。第二种验证类型是验证码，您可以将其配置为通过电子邮件发送给用户。

有关详细信息，请参阅通过电子邮件设置两步验证的用户第 页上的46。

下表描述了此选项卡上的设置。

提供者设置 > 电子邮件

名称	说明
SMTP 服务器	输入两步验证电子邮件的简单邮件传输协议 (SMTP) 服务器的 IP 地址或主机名。
SMTP 服务器端口	指定用于发送电子邮件的 SMTP 服务器的端口。 默认端口号为 25(无 SSL) 和 465(有 SSL) 。

名称	说明
使用 **SSL**	如果您的 SMTP 服务器支持 SSL 加密，请选中此复选框。
用户名	指定登录 SMTP 服务器的用户名。
密码	指定登录 SMTP 服务器的密码。
使用安全密码身份验证 **(SPA)**	如果您的 SMTP 服务器支持 SPA，请选中此复选框。
发件人电子邮件地址	指定发送验证码的电子邮件地址。
电子邮件主题	指定电子邮件的主题。示例：您的两步验证码。
电子邮件文本	输入您想要发送的消息。示例：您的验证码是 {0}。 如果您忘了包括 {0} 变量，系统默认会将验证码添加到文本末尾。

验证码设置

名称	说明
重新连接超时 **(0-30** 分钟 **)**	指定 XProtect Mobile 客户端用户在发生网络断开等情况时无需重新验证登录信息的时间段。默认时间为三分钟。 该设置不适用于 XProtect Web Client。
验证码将在 **(1-10** 分钟 **)** 后过期	指定用户可以使用接收到的验证码的时间段。在此时间段后，验证码将失效，用户需要请求新的验证码。默认时间为五分钟。
验证码尝试输入次数 **(1-10** 次 **)**	指定在提供的验证码无效之前的最大代码输入尝试次数。默认数量为三。
验证码长度 **(4-6** 个字符 **)**	指定验证码的字符数。默认长度为六。

名称	说明
验证码组成	指定您希望系统生产的验证码的复杂度。您可以在以下项中选择： • 大写拉丁字母 **(A-Z)** • 小写拉丁字母 **(a-z)** • 数字 **(0-9)** • 特殊字符 **(!@#...)**

用户设置

名称	说明
用户和组	列出添加到 XProtect 系统的用户和组。 如果已在 Active Directory 中配置组，移动设备服务器将使用 Active Directory 中的详细信息，如电子邮件地址。 Windows 组不支持双重验证。
验证方法	为每个用户或组选择一个验证设置。您可以在以下项中选择： • 无登录：用户无法登录 • 无双重验证：用户必须输入用户名和密码 • 电子邮件：除了用户名和密码，用户还必须输入验证码
用户详细信息	输入每位用户将接收验证码的电子邮件地址。

直接流(已解释)

XProtect Mobile 支持实时模式下的直接流(仅适用于 XProtect Expert 和 XProtect Corporate) 。

直接流是一种视频流传输技术，可将视频从 XProtect 系统直接通过 H.264 编码解码器传输到客户端，大多数现代 IP 摄像机均支持这种传输。直接流不需要进行任何转码，因此消除了 XProtect 系统上的一些压力。

直接流技术与 XProtect 中的转码设置相反，在默认转码设置中，XProtect 系统将摄像机上使用的编码解码器中的视频解码为 JPEG 文件。启用此功能可减少相同配置的摄像机和视频流的 CPU 使用率。对于同样的硬件，直接流还可以提高流传输性能 - 并发视频流的数量最多可以达到转码的 5 倍。

还可以使用直接流功能将视频从支持 H.265 编解码器的摄像机直接传输到 XProtect Mobile 客户端。

在 Management Client 中，您可以为客户端启用或禁用直接流(请参阅Mobile 服务器设置第 页上的14) 。

在以下情况下，视频流将从直接流退回到转码：

- 直接流功能已在 Management Client 中禁用或未满足要求(请参阅直接流的要求第 页上的11)
- 流式摄像机的编解码器不同于 H.264(适用于所有客户端) 或 H.265(仅适用于 XProtect Mobile 客户端)
- 视频开始播放时间不能超过十秒钟
- 流式摄像机的帧速率设置为每秒一帧 (1 FPS)
- 丢失与服务器或摄像机的连接
- 您在直播视频期间使用隐私屏蔽功能

自适应流媒体传输(已解释)

XProtect Mobile 支持实时模式下的自适应流(仅适用于 XProtect Expert 和 XProtect Corporate) 。

在同一摄像机视图中查看多个实时视频流时，自适应流非常有用。该功能优化了 XProtect Mobile 服务器的性能，并提高了运行 XProtect Web Client 的设备的解码能力和性能。

为了利用自适应流，您的摄像机必须具有以不同分辨率定义的多个流。在此情况下，该功能可实现：

- 优化视频质量 - 选择具有等于或高于所请求的分辨率的最低可用分辨率的流
- 优化服务器性能 - 降低分辨率请求，然后选择等于或高于此请求的最低可用分辨率的流
- 为低带宽优化分辨率 - 选择可用分辨率最低的流(如果使用 3G 或不稳定的网络，建议使用此项)

缩放时，所请求的实时视频流始终是可用的最高分辨率的视频流。

当所请求的流的分辨率降低时，带宽使用通常会降低。带宽使用还取决已定义流的配置中的其他设置。

可以启用或禁用自适应流，并在 Management Client 中的移动设备服务器设置的性能选项卡上设置功能的首选流模式(请参阅Mobile 服务器设置第 页上的14) 。

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。

XProtect 视频管理软件在 中，通过使用具有非对称加密 (RSA) 的 SSL/TLS 获得安全通信。

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

证书颁发机构 (CA) 可以使用 CA 证书向服务器上的 Web 服务颁发证书。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 SSL/TLS 连接。

有关 TLS 的详细信息：https://en.wikipedia.org/wiki/Transport_Layer_Security

证书具有到期日。XProtect 视频管理软件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。

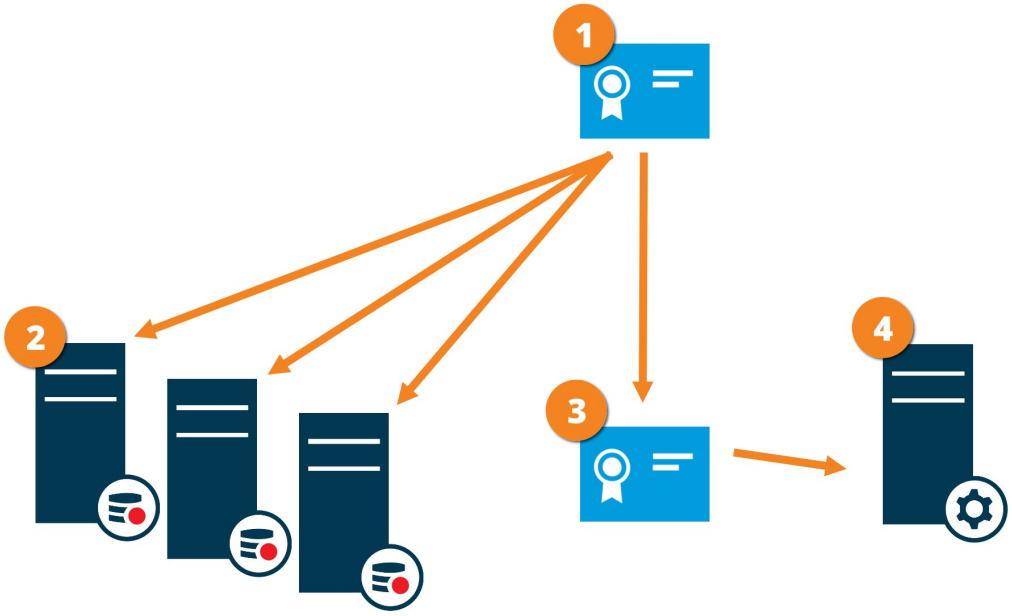
更新具有相同主体名称的证书并将其添加到 Windows 证书存储时，服务器将自动获取新证书。这样可以更轻松地为许多服务器更新证书，而无需为每个服务器重新选择证书，也无需重新启动服务。

管理服务器加密（已解释）

您可以加密管理服务器和记录服务器之间的双向连接。在管理服务器上启用加密时，它适用于连接到管理服务器的所有记录服务器的连接。如果在管理服务器上启用加密，则还必须在所有记录服务器上启用加密。在启用加密之前，必须在管理服务器和所有记录服务器上安装安全证书。

管理服务器的证书分发

该图说明了如何在 XProtect 视频管理软件 中签署、信任和分发证书以保护与管理服务器的通信的基本概念。



❶ CA 证书充当受信任的第三方，受主体/所有者(管理服务器) 和证书验证方(记录服务器) 的信任

❷ 必须在所有记录服务器上信任 CA 证书。通过这种方式，记录服务器可以验证 CA 颁发的证书的有效性。

❸ CA 证书用来在管理服务器与记录服务器之间建立安全连接

❹ 必须在运行管理服务器的计算机上安装 CA 证书

私人管理服务器证书要求：

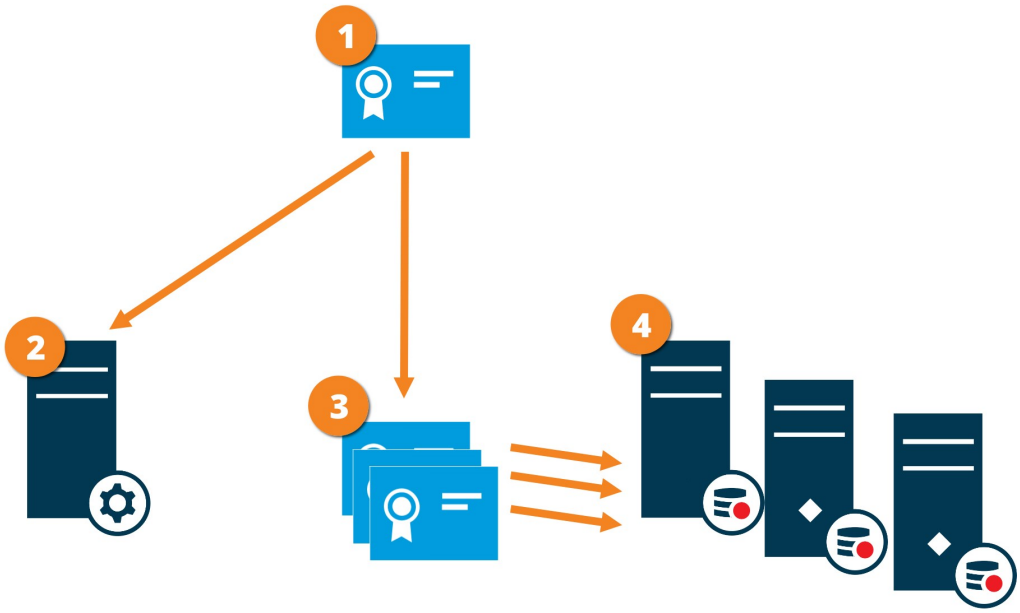
- 向管理服务器颁发，以便管理服务器的主机名包含在证书中，作为主体(所有者) 或位于作为证书颁发对象的 DNS 名称列表中
- 通过信任用于颁发管理服务器证书的 CA 证书，在管理服务器本身上受信任
- 通过信任用于颁发管理服务器证书的 CA 证书，在连接到管理服务器的所有记录服务器上都受信任

从管理服务器到记录服务器的加密(已解释)

您可以加密管理服务器和记录服务器之间的双向连接。在管理服务器上启用加密时，它适用于连接到管理服务器的所有记录服务器的连接。这一通信的加密必须遵循管理服务器上的加密设置。因此，如果启用了管理服务器加密，则还必须在记录服务器上启用加密，反之亦然。在启用加密之前，必须在管理服务器和所有记录服务器(包括故障转移记录服务器) 上安装安全证书。

证书分发

该图说明了如何在 XProtect 视频管理软件 中签署、信任和分发证书以保护来自管理服务器的通信的基本概念。



❶ CA 证书充当受信任的第三方，受主体/所有者(记录服务器) 和证书验证方(管理服务器) 的信任

❷ 必须在管理服务器上信任公共 CA 证书。通过这种方式，管理服务器可以验证 CA 颁发的证书的有效性

❸ CA 证书用来在记录服务器与管理服务器之间建立安全连接

❹ 必须在运行记录服务器的计算机上安装 CA 证书

私人记录服务器证书要求：

- 向记录服务器颁发，以便记录服务器的主机名包含在证书中，作为主体(所有者) 或位于作为证书颁发对象的 DNS 名称列表中
- 通过信任用于颁发记录服务器证书的 CA 证书，在管理服务器上受信任

管理服务器和 Data Collector Server 之间的加密(已解释)

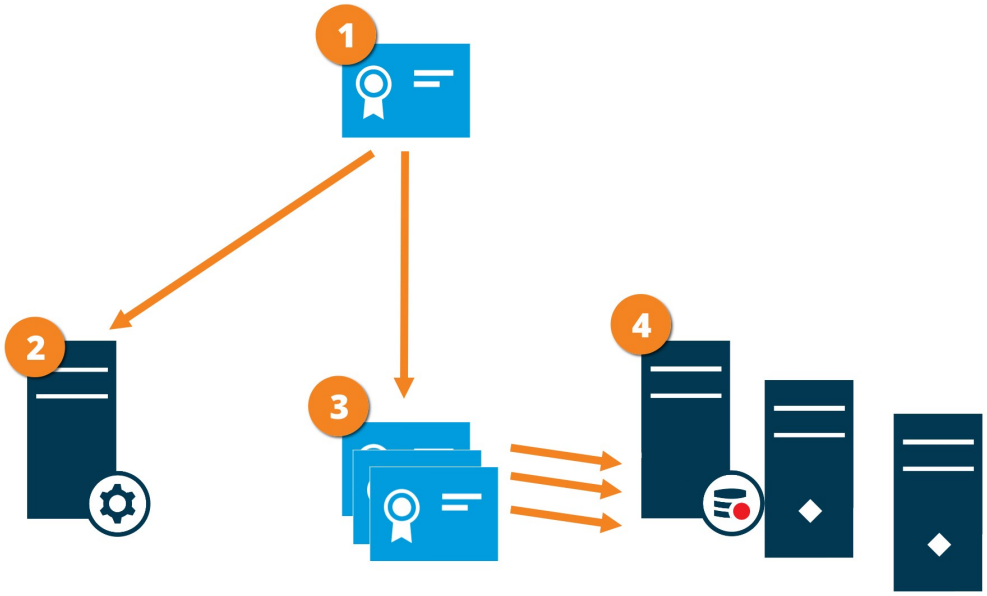
当您具有以下类型的外部服务器时，您可以加密管理服务器与关联的 Data Collector 之间的双向连接：

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

在管理服务器上启用加密时，它适用于连接到管理服务器的所有 Data Collector 服务器的连接。这一通信的加密必须遵循管理服务器上的加密设置。因此，如果启用了管理服务器加密，则还必须在与每个外部服务器关联的 Data Collector 服务器上启用加密，反之亦然。在启用加密之前，必须在管理服务器和所有与外部服务器关联的 Data Collector 服务器上安装安全证书。

证书分发

该图说明了如何在 XProtect 视频管理软件 中签署、信任和分发证书以保护来自管理服务器的通信的基本概念。



❶ CA 证书充当受信任的第三方，受主体/所有者(数据收集器服务器) 和证书验证方(管理服务器) 的信任

❷ 必须在管理服务器上信任公共 CA 证书。通过这种方式，管理服务器可以验证 CA 颁发的证书的有效性

❸ CA 证书用来在数据收集器服务器与管理服务器之间建立安全连接

❹ 必须在运行数据收集器服务器的计算机上安装 CA 证书

私人数据收集器服务器证书要求：

- 向数据收集器服务器颁发，以便数据收集器服务器的主机名包含在证书中，作为主体(所有者) 或位于作为证书颁发对象的 DNS 名称列表中
- 通过信任用于颁发数据收集器服务器证书的 CA 证书，在管理服务器上受信任

对从记录服务器检索数据的客户端和服务器进行加密(已解释)

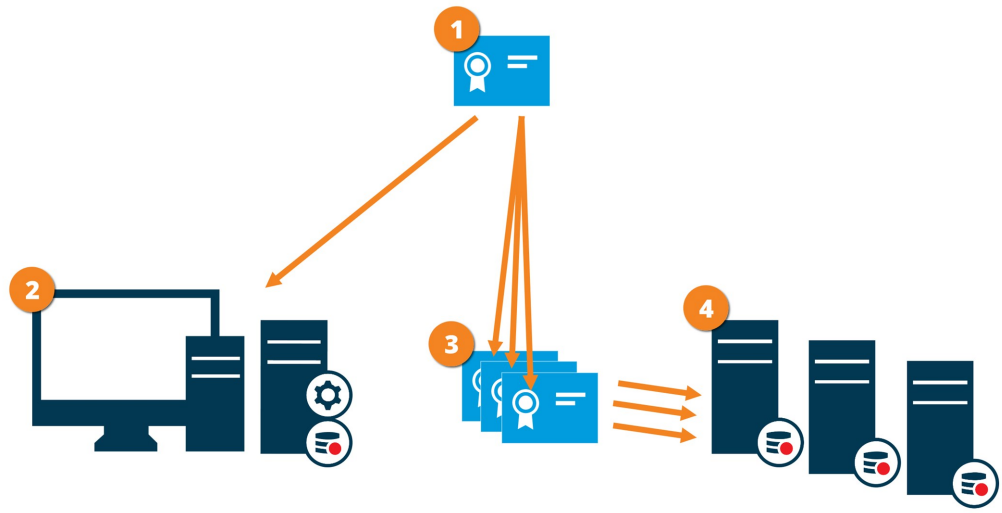
如果在记录服务器上启用加密，则与从记录服务器检索数据流的所有客户端、服务器和集成的通信都经过加密。在本文档中称为“客户端”：

- XProtect Smart Client
- Management Client
- Management Server(适用于系统监视器以及电子邮件通知中的图像和 AVI 视频剪辑)
- XProtect Mobile 服务器
- XProtect Event Server
- XProtect LPR
- ONVIF Bridge
- XProtect DLNA Server
- 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

> 对于使用 MIP SDK 2018 R3 或更早版本构建的用于访问记录服务器的解决方案：如果使用 MIP SDK 库进行集成，则需要使用 MIP SDK 2019 R1 重新构建它们；如果集成直接与记录服务器 API 进行通信而不使用 MIP SDK 库，则集成商必须自己添加 HTTPS 支持。

证书分发

该图说明了如何在 XProtect 视频管理软件 中签署、信任和分发证书以保护与记录服务器的通信的基本概念。



❶ CA 证书充当受信任的第三方，受主体/所有者(记录服务器) 和证书验证方(所有客户端) 的信任

❷ 必须在所有客户端上信任 CA 证书。通过这种方式，客户端可以验证 CA 颁发的证书的有效性

❸ CA 证书用来在记录服务器与所有客户端和服务之间建立安全连接

❹必须在运行记录服务器的计算机上安装 CA 证书

私人记录服务器证书要求：

- 向记录服务器颁发，以便记录服务器的主机名包含在证书中，作为主体(所有者)或位于作为证书颁发对象的 DNS 名称列表中
- 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受信任，通过信任用于颁发记录服务器证书的 CA 证书
- 运行记录服务器的服务帐户必须能够访问记录服务器上证书的私钥。

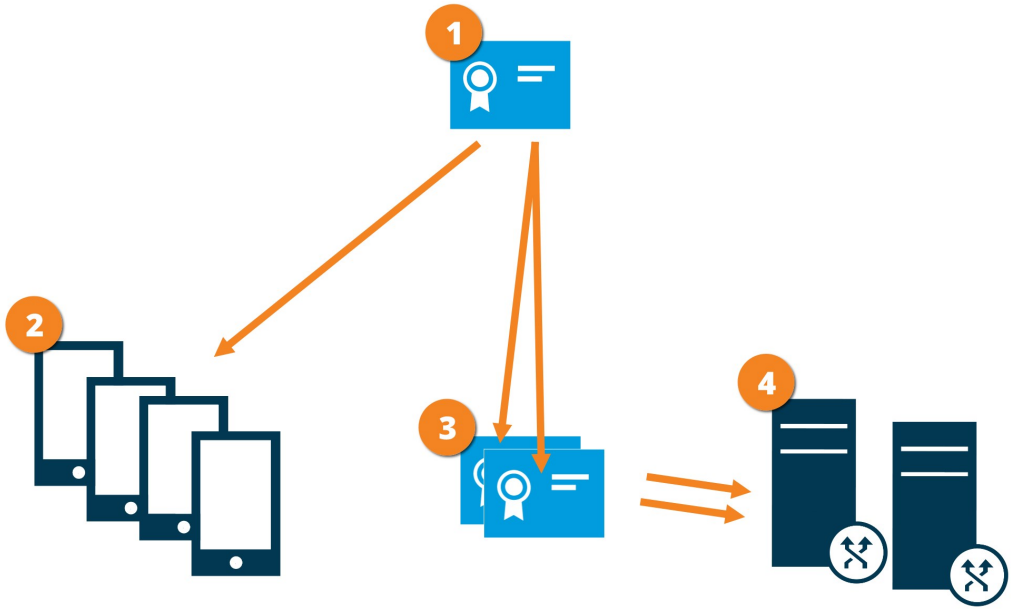
如果在记录服务器上启用加密，并且您的系统应用故障转移记录服务器，则 Milestone 建议您还准备故障转移记录服务器以进行加密。

移动设备服务器数据加密(已解释)

在 XProtect 视频管理软件 中，每个移动设备服务器都启用或禁用加密。如果在移动设备服务器上启用加密，那么对于与检索数据流的所有客户端、服务和集成之间的通信，您可以选择使用加密通信。

移动设备服务器的证书分发

该图说明了如何在XProtect视频管理软件中签署、信任和分发证书以保护与移动设备服务器的通信的基本概念。



❶CA 证书充当受信任的第三方，受主体/所有者(移动设备服务器)和证书验证方(所有客户端)的信任

❷必须在所有客户端上信任 CA 证书。通过这种方式，客户端可以验证 CA 颁发的证书的有效性

❸ CA 证书用来在移动设备服务器与客户端和服务之间建立安全连接

❹ 必须在运行移动设备服务器的计算机上安装 CA 证书

CA 证书要求：

- 移动设备服务器的主机名必须包含在证书的名称中，作为主体(所有者) 或位于作为证书颁发对象的 DNS 名称列表中
- 必须在运行从移动设备服务器检索数据流的服务的所有设备上都信任证书
- 运行移动设备服务器的服务帐户必须能够访问 CA 证书的私钥

客户端的移动设备服务器加密要求

如果您未启用加密并使用 HTTP 连接，则 XProtect Web Client 中的按下即可发言功能将不可用。

如果为移动设备服务器的加密选择自签署证书，则 XProtect Mobile 客户端将无法与移动设备服务器进行连接。

启用加密 (in English)

Enable encryption to and from the management server

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see 管理服务器加密(已解释) 第 页上的28.

Prerequisites:

- A server authentication certificate is trusted on the computer that hosts the management server

First, enable encryption on the management server.

Steps:

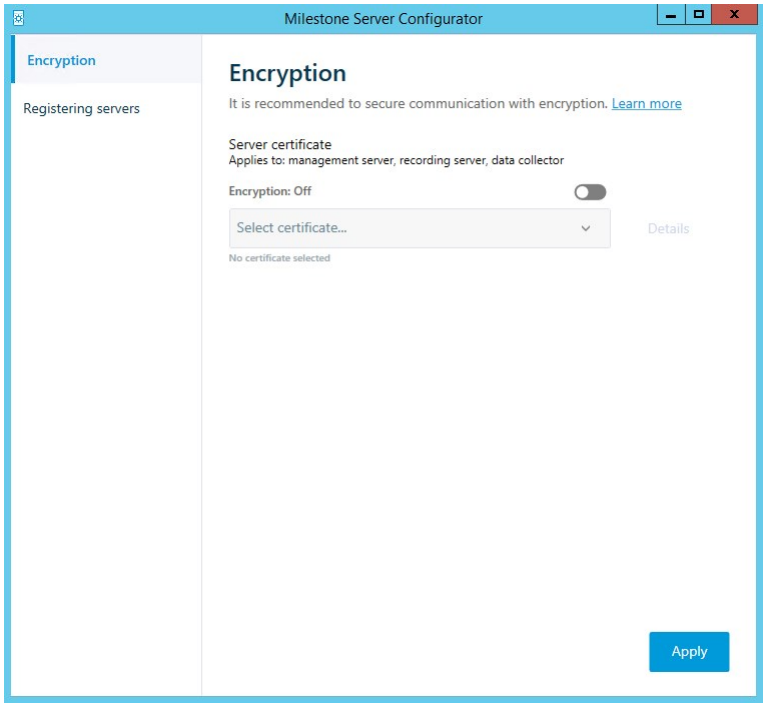
1. On the computer that runs the management server, right-click the Management Server Manager icon in the notification area and select **Server Configurator**.

   The **Server Configurator** window appears. The options in this window depend on what servers are installed on the computer.

2. Under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

   When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.

To complete the enabling of encryption, the next step is to update the encryption settings on each recording server and each server with a data collector (Event Server, Log Server, LPR Server, and Mobile Server). For more information, see Enable server encryption for recording servers or remote servers第 页上的35.

Enable server encryption for recording servers or remote servers

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see 从管理服务器到记录服务器的加密(已解释) 第 页上的29 and 管理服务器和 Data Collector Server 之间的加密(已解释) 第 页上的30.

Prerequisites:

- You have enabled encryption on the management server, see 启用加密 (in English)第 页上的34

Steps:

1. On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator**from the Windows startup menu.

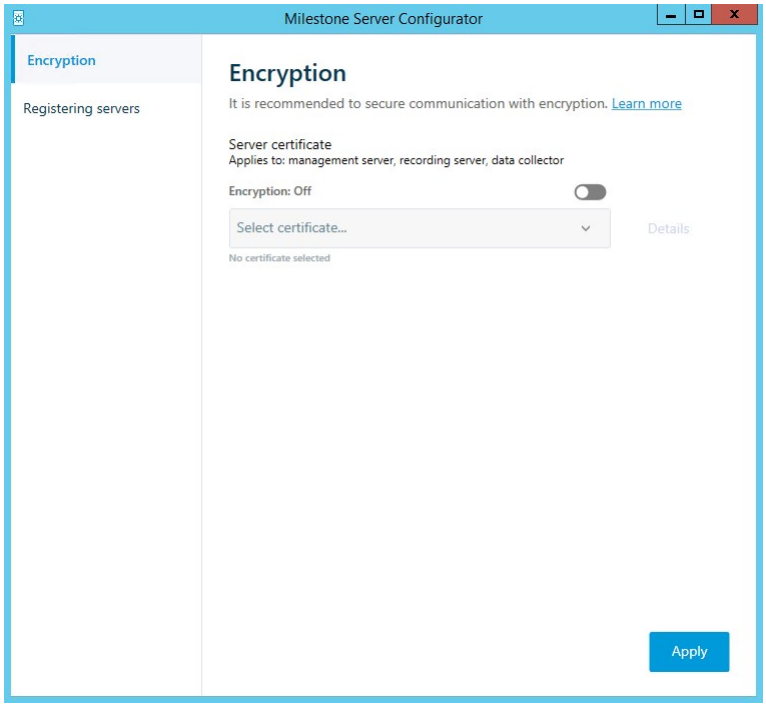
   The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

   When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

   The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

   Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.

> When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

Enable encryption to clients and servers

You can encrypt connections from the recording server to clients and servers that stream data from the recording server. For more information, see 对从记录服务器检索数据的客户端和服务器进行加密(已解释) 第 页上的31.

Prerequisites:

- The server authentication certificate to be used is trusted on all computers running services that retrieve data streams from the recording server

- XProtect Smart Client and all services that retrieve data streams from the recording server must be version 2019 R1 or later
- Some third-party solutions created using MIP SDK versions earlier than 2019 R1 may need to be updated

Steps:

1. On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator** from the Windows startup menu.

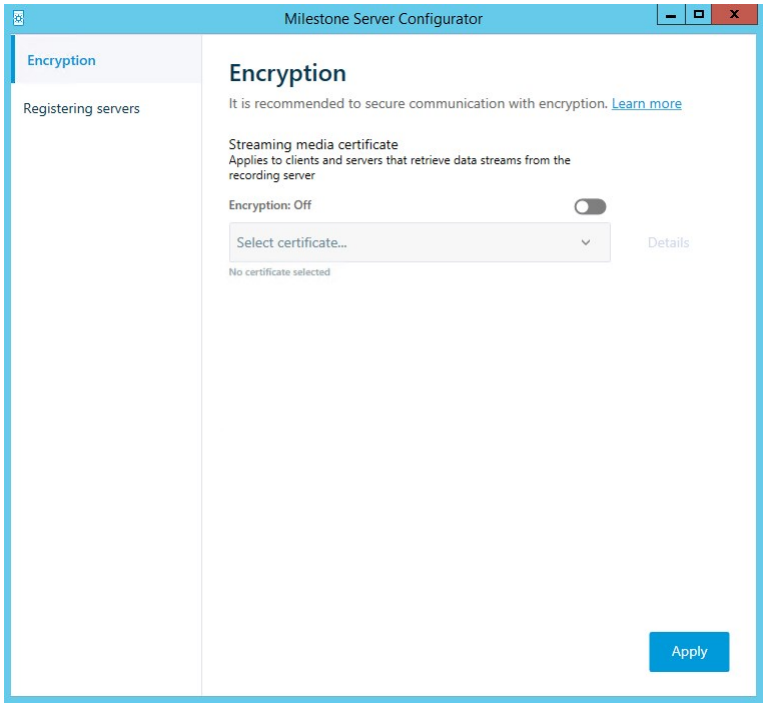
   The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Streaming media certificate**, turn on encryption and select the certificate to encrypt communication between the clients and servers that retrieve data streams from the recording server.

   When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

   The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

   Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.

When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

To verify if the recording server uses encryption, see View encryption status to clients.

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安全连接的授权。有关详细信息，请参阅移动设备服务器数据加密(已解释) 第 页上的33和客户端的移动设备服务器加密要求第 页上的34。

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。

要在安装了移动设备服务器后启用加密：

1. 在安装移动设备服务器的计算机上，右键单击操作系统任务栏中的 Mobile Server Manager 托盘图标，然后选择编辑证书。
2. 选中将从移动设备服务器检索数据流的客户端和服务的连接加密复选框。
3. 要选择有效的证书，请单击 ••• 。此时会打开“Windows 安全性”对话框。
4. 选择要应用的证书。
5. 单击确定。

编辑证书

如果用于安全连接的证书已过期，则可以选择运行移动设备服务器的计算机上安装的另一个证书。

要更改证书：

1. 在安装移动设备服务器的计算机上，右键单击操作系统任务栏中的 Mobile Server Manager 托盘图标，然后选择编辑证书。
2. 要选择有效的证书，请单击 ••• 。此时会打开“Windows 安全性”对话框。

3. 选择要应用的证书。
4. 单击确定。

   此时会显示一条消息，告知您证书已安装，而且已重新启动 Mobile Server 服务以应用更改。

Milestone Federated Architecture 和主/从属服务器(已解释)

如果您的系统支持主/从属设置中的 Milestone Federated Architecture 或服务器，则您可以使用 XProtect Mobile 客户端或 XProtect Web Client 访问这些服务器。使用此功能可以通过登录到主服务器来访问所有从属服务器上的所有摄像机。

如果处于 Milestone Federated Architecture 设置中，您可以通过中央站点访问子站点。仅在中央站点上安装 XProtect Mobile 服务器。

这意味着当 XProtect Mobile 客户端或 XProtect Web Client 的用户登录到服务器以查看系统中所有服务器的摄像机时，他们必须连接到主服务器的 IP 地址。用户必须拥有系统中所有服务器的管理员权限，才能使摄像机显示在 XProtect Mobile 客户端或 XProtect Web Client 中。

智能连接(已解释)

通过智能连接，您可以验证是否已正确配置 XProtect Mobile，而无需使用移动设备或平板电脑进行验证。它还能简化 XProtect Mobile 客户端和 XProtect Web Client 用户的连接流程。

此功能需要您的 XProtect Mobile 服务器使用公共 IP 地址，且您的系统具有 Milestone Care Plus 订阅包的许可。

若远程连接设置成功建立，系统会在 Management Client 中提供实时反馈，并确认可以从互联网访问 XProtect Mobile 服务器。

通过智能连接，XProtect Mobile 服务器可以在内部与外部 IP 地址之间无缝切换，并从任何位置连接至 XProtect Mobile。

若要降低计算机移动设备客户端的设置难度，您可以直接从ManagementClient内向最终用户发送电子邮件。该电子邮件包括将服务器直接添加到XProtectMobile所用的链接。此操作将完成设置，而无需输入网络地址或端口。

设置 Smart Connect

要设置智能连接功能，请执行以下操作：

1. 在 Management Client 的导航窗格中，展开服务器，然后选择移动设备服务器。
2. 选择移动设备服务器，并单击连接选项卡。
3. 在路由器上启用通用即插即用发现功能。
4. 配置连接设置。
5. 向用户发送电子邮件消息。
6. 在复杂网络中启用连接。

在路由器上启用通用即插即用发现功能

要轻松将移动设备连接到XProtectMobile服务器，您可以在路由器上启用通用即插即用(UPnP)。UPnP可以让XProtectMobile服务器自动配置端口转发。但是，您也可以通过使用其Web界面在路由器上手动设置端口转发。根据路由器，设置端口映射的过程可能各不相同。如果您不确定如何在路由器上设置端口转发，请参阅设备的文档。

每隔五分钟，XProtect Mobile 服务器 服务便会验证服务器对于互联网上的用户是否可用。状态会显示在属性窗格的左上角： 

.

在复杂网络中启用连接

如果您拥有包含自定义设置的复杂网络，则您可以为用户提供进行连接所需的信息。

在连接选项卡的互联网访问组中，指定以下内容：

- 如果您使用UPnP端口映射将连接转至特定连接，请选中配置自定义互联网访问复选框。然后提供**IP**地址或主机名以及用于连接的端口。例如，如果您的路由器不支持UPnP或者您拥有路由器链，则可以执行此操作
- 如果您的 IP 地址经常更改，请选中选择后可动态地检索 **IP** 地址复选框

配置连接设置

1. 在 Management Client 的导航窗格中，展开服务器，然后选择移动设备服务器。
2. 选择服务器，并单击连接选项卡。
3. 使用常规组中的选项指定以下内容：
   - 为了让 XProtect Mobile 客户端和 XProtect Web Client 用户轻松将移动设备连接到 XProtect Mobile 服务器，请选中启用智能连接复选框。
   - 在连接类型字段中指定要使用的协议
   - 在打开安全连接之前，请确保您熟悉数字证书。要了解如何在 XProtect Mobile 服务器上添加证书，请参阅编辑证书第 页上的38
   - 设置 XProtect Mobile 客户端和 XProtect Web Client 必须向移动设备服务器指示它们已启动并运行的频率的时间范围
   - 要使XProtectMobile服务器可通过UPNp协议在网络上被发现，请选择启用**UPNp**发现功能复选框
   - 如果已为 XProtect Mobile 服务器配置了路由器，要使其自身执行端口映射，请选中启用自动端口映射复选框

向用户发送电子邮件消息

若要降低 XProtect Mobile 客户端和 XProtect Web Client 的设置难度，您可以直接从 Management Client 内向最终用户发送电子邮件。该电子邮件包括将服务器直接添加到 XProtect Mobile 所用的链接。此操作将完成设置，而无需输入网络地址或端口。

1. 在对此人员的电子邮件邀请字段中，输入智能连接通知收件人的电子邮件地址，然后指定语言。
2. 接下来，进行以下操作之一：
   - 要发送消息，请单击发送。
   - 将信息复制到您使用的消息程序

有关详细信息请参阅：

智能连接设置要求第 页上的11

连接选项卡第 页上的16

发送通知(已解释)

您可以启用XProtect Mobile以在发生事件时通知用户，例如当警报触发或设备或服务器出现问题时。无论应用程序是否正在运行，始终发送通知。当在移动设备上打开XProtect Mobile时，应用程序会发出通知。即使应用程序未运行，也会发送系统通知。用户可以指定其希望接收的通知类型。例如，用户可以选择接收以下内容的通知：

- 所有警报
- 仅分配给它们的警报
- 仅与系统相关的警报

  它们可能在服务器脱机或重新联机时发生。

您还可以使用推送通知以告知没有打开 XProtect Mobile 的用户。这些就是所谓的推送通知。推送通知会传送给移动设备，这是让用户在外出时了解动态的好方法。

使用推送通知

要使用推送通知，您的系统必须能够访问互联网。

推送通知使用 Apple、Microsoft 和 Google 的云服务：

- Apple 推送通知服务 (APN)
- Microsoft Azure 通知中心
- Google 云消息推送通知服务

允许您的系统在一个时间段内发送的通知数量存在一定限制。如果系统超过此限制，则在下一个时间段内每隔 15 分钟只发送一个通知。通知包含在 15 分钟内发生的事件的摘要。在下一个时间段后，将会删除限制。

另请参阅通知设置要求第 页上的10和通知选项卡第 页上的23。

在 XProtect Mobile 服务器上设置推送通知

要设置推送通知，请执行下列步骤：

1. 在 Management Client 中，选择移动服务器，然后单击通知选项卡。
2. 要向连接到服务器的所有移动设备发送通知，请选中通知复选框。
3. 要存储有关连接到服务器的用户和移动设备的信息，请选中维护设备注册复选框。

服务器仅向此列表中的移动设备发送通知。如果清除维护设备注册复选框并保存更改，则系统会清除列表。要再次接收推送通知，用户必须重新连接设备。

启用向特定移动设备或所有移动设备发送推送通知

要让 XProtect Mobile 在发生事件时通过向特定移动设备或所有移动设备发送推送通知的方式通知用户：

1. 在 Management Client 中，选择移动服务器，然后单击通知选项卡。
2. 进行以下操作之一：
   - 对于单个设备，为已注册的设备表中列出的每个移动设备选中已启用复选框
   - 对于所有移动设备，选择通知复选框

停止向特定移动设备或所有移动设备发送推送通知

可以通过多种方法停止向特定移动设备或所有移动设备发送推送通知。

1. 在 Management Client 中，选择移动服务器，然后单击通知选项卡。
2. 进行以下操作之一：
   - 对于各个设备，清除每个移动设备的已启用复选框。用户可以使用其他设备连接到 XProtect Mobile 服务器
   - 对于所有设备，清除通知复选框

要暂时对所有设备停止，请清除维护设备注册复选框，然后保存更改。系统会在用户重新连接后再次发送通知。

设置调查

设置调查以使得用户可以使用 XProtect Web Client 或 XProtect Mobile 访问记录的视频并调查事件，以及准备和下载视频证据。

要设置调查，请执行下列步骤：

1. 在 Management Client 中，单击移动服务器，然后单击调查选项卡。
2. 选中已启用复选框。默认情况下，已选中此复选框。
3. 在调查文件夹字段中，指定存储用于进行调查的视频的位置。
4. 在将调查文件夹的大小限制为字段中，输入调查文件夹可以包含的兆字节的最大数。

5. 可选：要允许用户访问其他用户创建的调查，请选中查看由其他用户进行的调查复选框。如果不选中此复选框，则用户只能查看自己的调查。
6. 可选：要包括下载视频的日期和时间，请选中在 **AVI** 导出中包括时间标记复选框。
7. 在为 **AVI** 导出使用的编解码器字段中，选择在准备 AVI 包供下载时要使用的压缩格式。

> 列表中的编解码器可能会有所不同，具体取决于您的操作系统。如果您没有看到要使用的编解码器，可以在运行 Management Client 的计算机上安装它，然后它将显示在此列表中。

> 此外，编解码器可以使用不同的压缩率，这可能会影响视频质量。更高的压缩率会降低存储要求，但也会降低视频质量。更低的压缩率需要更多的存储和网络容量，但会提高质量。一个好的做法是在进行选择之前研究编解码器。

8. 从**AVI**导出的已用音频比特率列表中，选择视频导出中包含音频时的相应音频比特率。默认值为160000 Hz。
9. 在导出失败**(** 对于 **MKV** 和 **AVI)** 时保留或删除数据字段中，指定是否保存已成功下载的数据，尽管该数据可能不完整，或者将其删除。

> 若要让用户能够保存调查，您必须向分配给用户的安全角色授予导出权限。

清理调查

如果您拥有不再需要保存的调查或视频导出，可以将其删除。例如，如果您要在服务器上腾出更多的可用磁盘空间，则该操作很有用。

- 要删除调查以及为其创建的所有视频导出，请在列表中选择调查，然后单击删除。
- 要删除为调查导出的单个视频文件，但要保留调查本身，请在列表中选择调查。在调查详细信息组中，单击数据库、**AVI** 或 **MKV** 字段右边的删除图标以导出。

使用手机视频推送以推送视频流(已解释)

您可以设置手机视频推送，使得用户可以让其他人了解情况，或者通过将视频流从他们的移动设备摄像机推送到您的 XProtect 监控系统来记录视频供之后进行调查。视频流也可以有音频。

另请参阅手机视频推送选项卡第 页上的22和手机视频推送设置要求第 页上的11。

设置视频推送以推送视频流

要让用户将视频流从他们的移动设备推送到 XProtect 系统，请在 XProtect Mobile 服务器上设置手机视频推送。

在 Management Client 中，按照以下顺序执行这些步骤：

1. 在手机视频推送选项卡上，选中手机视频推送复选框以启用该功能。
2. 为视频流添加手机视频推送通道。
3. 在Recording Server上将手机视频推送驱动程序添加为硬件设备。驱动程序会模拟摄像机设备，这样您就可以将视频流推送到 Recording Server。
4. 将手机视频推送驱动程序设备添加到手机视频推送的通道。

为视频流添加手机视频推送通道

要添加通道，请按照下列步骤操作：

1. 在导航窗格中，选择移动设备服务器，然后选择移动设备服务器。
2. 在手机视频推送选项卡上，选中手机视频推送复选框。
3. 在右下角单击添加，以在通道映射下添加手机视频推送通道。
4. 输入将使用通道的用户帐户(已在角色下添加) 的用户名。XProtect Mobile必须允许此用户帐户访问 服务器和记录服务器(在整体安全选项卡上) 。

   > XProtect Mobile要使用手机视频推送，用户必须使用此帐户的用户名和密码登录到其移动设备上的 。

5. 记下端口号。在记录服务器上将视频推送驱动程序添加为硬件设备时，需要使用它。
6. 单击确定以关闭"手机视频推送通道"对话框并保存通道。

删除手机视频推送通道

您可以删除不再使用的通道：

- 选择要删除的通道，然后单击右下角的删除

在 上将手机视频推送驱动程序添加为硬件设备Recording Server

1. 在导航窗格中，单击记录服务器。
2. 右键单击您要将视频流推送到的服务器，然后单击添加硬件以打开添加硬件向导。
3. 选择手动作为硬件侦测方法，然后单击下一步。

4. 输入摄像机的登录凭据：
   - 用户名请输入出厂默认值或摄像机上指定的用户名
   - 密码请 输入 **Milestone**，然后单击下一步

   它们是硬件的凭据，而不是用户的凭据。这些凭据与通道的用户名不相关。

5. 在驱动程序列表中，展开 **Milestone**，选中手机视频推送驱动程序复选框，然后单击下一步。

   系统会生成手机视频推送驱动程序设备的 MAC 地址。我们建议您使用此地址。只有当您在使用手机视频推送驱动程序设备遇到问题时才更改它，或者诸如需要添加新地址和端口号时才更改它。

6. 在地址字段中，输入安装 XProtect Mobile 服务器的计算机的 IP 地址。
7. 在端口字段中，输入您为推送视频流所创建的通道的端口号。端口号在您创建通道时分配。
8. 在硬件型号列中，选择手机视频推送驱动程序，然后单击下一步。
9. 当系统检测到新硬件后，单击下一步。
10. 在硬件名称模板字段中，指定是同时显示硬件型号和 IP 地址，还是只显示型号。
11. 通过选中已启用复选框指定是否启用相关设备。您可以将相关设备添加到手机视频推送驱动程序的列表，即使未启用它们。您可以稍后启用它们。

    如果您要在推送视频流时使用位置信息，则必须启用元数据端口。

    如果要在传输视频流时播放音频，则必须启用与用于视频流传输的摄像机相关的麦克风。

12. 在左侧选择相关设备的默认组，或者选择添加至组字段中的特定组。通过将设备添加到组，可以更简便地同时将设置应用到所有设备或者更换设备。

将手机视频推送驱动程序设备添加到手机视频推送的通道

将手机视频推送驱动程序设备添加到手机视频推送的通道，请按照以下步骤操作：

1. 在站点导航窗格中，单击 **Mobile** 服务器，然后单击手机视频推送选项卡。
2. 单击查找摄像机。如果成功，则手机视频推送驱动程序摄像机的名称会显示在摄像机名称字段中。
3. 保存配置。

为现有的手机视频推送通道启用音频

在满足音频在手机视频推送中的启用要求后(参阅手机视频推送设置要求第 页上的11) ，在ManagementClient中：

1. 在站点导航窗格中展开服务器节点，然后单击记录服务器。
2. 在总览窗格中，选择相关的记录服务器文件夹，然后展开手机视频推送驱动程序文件夹，并用右键单击与手机视频推送相关的麦克风。
3. 选择启用以启用麦克风。
4. 在同一文件夹中，选择与手机视频推送相关的摄像机。
5. 在属性窗格中，单击客户端选项卡(参阅"客户端"选项卡属性) 。
6. 在相关麦克风字段的右侧，单击 ••• 。此时会打开选定设备对话框。
7. 在记录服务器选项卡上，展开记录服务器文件夹并选择与手机视频推送相关的麦克风。
8. 单击确定。

通过电子邮件设置两步验证的用户

可用的功能取决于正在使用的系统。有关详细信息，请参阅 https://www.milestonesys.com/solutions/platform/product-index/。

要对 XProtect Mobile 客户端或 XProtect Web Client 的用户执行其他登录步骤，请在 XProtect Mobile 服务器上设置双重验证。除了标准用户名和密码，用户还必须输入通过电子邮件接收的验证码。

两步验证可提高监控系统的防护级别。

在 Management Client 中，执行以下步骤：

1. 输入关于 SMTP 服务器的信息第 页上的46。
2. 指定将发送给用户的验证码第 页上的47。
3. 将登录方法分配给用户和 Active Directory 组第 页上的47。

另请参阅用户双重验证设置的要求第 页上的11和双重验证第 页上的24。

输入关于 SMTP 服务器的信息

提供商会使用关于 SMTP 服务器的信息：

1. 在导航窗格中，选择移动设备服务器，然后选择相关的移动设备服务器。
2. 在两步验证选项卡中，选择启用两步验证复选框。
3. 在提供商设置下方的电子邮件选项卡上，输入有关 SMTP 服务器的信息，然后指定系统将在客户端用户登录并为第二次登录进行设置时向其发送的电子邮件。有关每个参数的详细信息，请参阅双重验证第 页上的24。

有关详细信息，请参阅双重验证第 页上的24。

指定将发送给用户的验证码

要指定验证码的复杂度，请执行以下操作：

1. 在双重验证选项卡的验证码设置部分，指定 XProtect Mobile 客户端用户在发生网络断开等情况时无需重新验证登录信息的时间段。默认时间为三分钟。
2. 指定用户可以使用接收到的验证码的时间段。在此期间之后，验证码将无效，用户必须请求新的验证码。默认时间为五分钟。
3. 指定在提供的验证码无效之前的最大代码输入尝试次数。默认数量为三。
4. 指定验证码的字符数。默认长度为六。
5. 指定您希望系统生产的验证码的复杂度。

有关详细信息，请参阅双重验证第 页上的24。

将登录方法分配给用户和 Active Directory 组

XProtect在两步验证选项卡的用户设置部分，会显示添加至 系统的用户和组列表。

1. 在登录方法列，选择每个用户或组的验证方法。
2. 在详细信息字段，添加交付详细信息，如单个用户的电子邮件地址。XProtect Web ClientXProtect Mobile用户下次登录 或 应用程序时，需要进行二次登录。
3. 如果已在 Active Directory 中配置组，XProtect Mobile 设备服务器将使用 Active Directory 中的详细信息，如电子邮件地址。

   Windows 组不支持双重验证。

4. 保存配置。

您需要完整通过电子邮件设置两步验证用户的步骤。

有关详细信息，请参阅双重验证第 页上的24。

操作(说明)

您可以通过在常规选项卡上启用或禁用操作来管理 XProtect Mobile 客户端中的操作选项卡或 XProtect Web Client 的可用性。默认情况下启用操作，此处显示所连接设备的所有可用操作。

有关详细信息，请参阅“常规”选项卡第 页上的14。

为输出命名，以用于 XProtect Mobile 客户端和 XProtect Web Client (已解释)

要使用当前摄像机正确显示操作，必须创建一个与摄像机同名的输出组。

示例：

当您创建一个输出组，其输出连接到名为“AXIS P3301, P3304 - 10.100.50.110 - 摄像机 1”的摄像机时，必须在名称字段中输入相同的名称(在设备组信息下)。

在说明字段中，您可以添加更多说明，例如“AXIS P3301, P3304 - 10.100.50.110 - 摄像机 1 - 灯开关”。

如果不遵循这些命名约定，则动作在相关设备的视图的动作列表中不可用。相反，动作显示在动作选项卡上的其他动作的列表中。

有关详细信息，请参阅输出设备(已解释)。

维护

Mobile Server Manager (说明)

Mobile Server Manager 是连接到移动设备服务器的托盘控制功能。右键单击通知区域中的 Mobile Server Manager 托盘图标将打开一个菜单，您可以从中访问移动设备服务器功能。

您可以：

- 访问 XProtect Web Client第 页上的49
- 启动、停止和重新启动 Mobile Server 服务第 页上的50
- 填写/编辑管理服务器地址第 页上的50
- 显示/编辑端口号第 页上的50
- 编辑证书第 页上的38
- 打开今天的日志文件(请参阅访问日志和调查(说明) 第 页上的51)
- 打开日志文件夹(请参阅访问日志和调查(说明) 第 页上的51)
- 打开调查文件夹(请参阅访问日志和调查(说明) 第 页上的51)
- 更改调查文件夹第 页上的51
- 请参阅 XProtect Mobile 服务器 状态(请参阅显示状态(已解释) 第 页上的52)

访问 XProtect Web Client

如果计算机上安装了XProtectMobile服务器，则可以使用XProtectWebClient访问摄像机和视图。由于无需安装XProtectWebClient，因此可以从已安装XProtectMobile服务器的计算机或要用于该目的的其他任何计算机访问它。

1. 在 XProtect Mobile 中设置 Management Client 服务器。
2. 如果使用安装 XProtect Mobile 服务器的计算机，可以右键单击通知区域中的 Mobile Server Manager 托盘图标，然后选择打开 **XProtect Web Client**。
3. 如果不使用安装XProtectMobile服务器的计算机，您可以从浏览器进行访问。继续执行此过程中的步骤4。
4. 打开互联网浏览器(Internet Explorer、Mozilla Firefox、Google Chrome 或 Safari) 。
5. 输入外部 IP 地址，即运行 XProtect Mobile 服务器的服务器的外部地址和端口。

   示例：XProtect Mobile 服务器安装在 IP 地址为 127.2.3.4 的服务器上，并被配置为在端口 8081 上接受 HTTP 连接，并在端口 8082 上接受 HTTPS 连接(安装程序的默认设置) 。

   在浏览器的地址栏中，如果要使用标准 HTTP 连接，请输入：**http://127.2.3.4:8081**。如果要使用安全的 HTTPS 连接，请输入：**https://127.2.3.4:8082**。现在可以开始使用 XProtect Web Client。

6. 在浏览器中将地址添加为书签以便将来便捷访问 XProtect Web Client。如果在已安装 XProtect Mobile 服务器的本地计算机上使用 XProtect Web Client，则还可以使用安装程序创建的桌面快捷方式。单击该快捷方式可启动默认浏览器并打开 XProtect Web Client。

必须首先清除运行 XProtect Web Client 的互联网浏览器的缓存，然后才能使用新版本 XProtect Web Client。系统管理员必须要求 XProtect Web Client 用户在升级后清除浏览器缓存或以远程方式强制执行该操作(只能在域中于 Internet Explorer 内进行)。

启动、停止和重新启动 Mobile Server 服务

如果需要，可以从 Mobile Server Manager 启动、停止和重新启动 Mobile Server 服务。

- 要执行这些任务中的任何一个，请右键单击 Mobile Server Manager 图标，然后分别选择启动 **Mobile Server** 服务、停止 **Mobile Server** 服务或重新启动 **Mobile Server** 服务

填写/编辑管理服务器地址

1. 右键单击 Mobile Server Manager 图标，然后选择管理服务器地址。
2. 在服务器 **URL** 字段中填写服务器的 URL 地址。
3. 单击确定。

显示/编辑端口号

1. 右键单击 Mobile Server Manager 图标，然后选择显示/编辑端口号。
2. 要编辑端口号，请输入相关端口号。您可以指定 HTTP 连接的标准端口号或 HTTPS 连接的安全端口号，或同时指定两者。
3. 单击确定。

编辑证书

如果用于安全连接的证书已过期，则可以选择运行移动设备服务器的计算机上安装的另一个证书。

要更改证书：

1. 在安装移动设备服务器的计算机上，右键单击操作系统任务栏中的 Mobile Server Manager 托盘图标，然后选择编辑证书。
2. 要选择有效的证书，请单击 ••• 。此时会打开“Windows 安全性”对话框。

3. 选择要应用的证书。
4. 单击确定。

   此时会显示一条消息，告知您证书已安装，而且已重新启动 Mobile Server 服务以应用更改。

访问日志和调查(说明)

通过 Mobile Server Manager，您可以快速访问当天的日志文件，打开保存日志文件的文件夹，然后打开保存调查的文件夹。

要打开其中任何一个文件，请右键单击 Mobile Server Manager 图标，然后选择：

- 打开今天的日志文件
- 打开日志文件夹
- 打开调查文件夹

> 如果从系统中卸载 XProtect Mobile 服务器，则不会删除其日志文件。具有相应用户权限的管理员可以在以后访问这些日志文件，如果不再需要它们，也可以决定将其删除。日志文件的默认位置为 **ProgramData** 文件夹。如果更改日志文件的默认位置，现有日志不会被复制到新位置，也不会被删除。

更改调查文件夹

调查的默认位置在 **ProgramData** 文件夹中。如果更改调查文件夹的默认位置，则现有调查不会自动复制到新位置，也不会被删除。要更改在硬盘上保存调查导出的位置，请执行以下操作：

1. 右键单击 Mobile Server Manager 图标，然后选择更改调查文件夹。

   Investigations location 窗口将打开。
2. 在显示当前位置的 **Folder** 字段旁边，单击文件夹图标以浏览现有文件夹或创建新文件夹> 单击 **OK**。
3. 从 **Old investigations** 列表中，选择要应用于存储在当前位置的现有调查的操作。选项包括：
   - **Move**：将现有调查移至新文件夹

     > 如果您不将现有调查移动到新文件夹，您将无法再看到它们。

   - **Delete**：删除现有调查
   - **Donothing**：现有调查保留在当前文件夹位置。更改调查文件夹的默认位置后，您将无法再看到它们
4. 单击 **Apply** > 单击 **OK**。

显示状态(已解释)

右键单击 Mobile Server Manager 图标并选择显示状态，或者双击 Mobile Server Manager 图标打开窗口，其中显示 XProtect Mobile 服务器的状态。可以看到以下信息：

名称	说明
服务器运行起始时间	上次启动 XProtect Mobile 服务器的时间和日期。
连接的用户	当前连接到 XProtect Mobile 服务器的用户数量。
硬件解码	指示是否正在 XProtect Mobile 服务器上进行硬件加速的解码。
CPU 使用率	XProtect Mobile 服务器当前使用的 CPU 百分比。
CPU 使用历史记录	详细列出 XProtect Mobile 服务器的 CPU 使用历史记录的图表。

故障排除

故障排除 XProtect Mobile

连接

1. 为什么我不能从我的 **XProtect Mobile** 客户端连接到我的记录/**XProtect Mobile** 服务器？

   为了连接到您的记录，必须将 XProtect Mobile 服务器安装在运行 XProtect 系统的服务器上，或者安装在专用服务器上。您的 XProtect 视频管理设置中也需要相关的 XProtect Mobile 设置。这些可以作为插件安装，也可以作为产品安装或升级的一部分安装。有关如何获取 XProtect Mobile 服务器以及如何在 XProtect 系统中集成与 XProtect Mobile 客户端相关的设置的详细信息，请参阅配置部分(参阅Mobile 服务器设置第 页上的14) 。

2. 我刚刚打开我的防火墙，现在无法将移动设备连接到我的服务器。为什么无法连接呢？

   如果在安装 XProtect Mobile 服务器时关闭了防火墙，则必须手动启用 TCP 和 UDP 通信。

3. 通过 **HTTPS** 连接运行 **XProtect Web Client** 时如何避免安全警告？

   出现警告是因为证书中的服务器地址信息不正确。连接仍将被加密。
   XProtect Mobile 服务器中的自签名证书需要替换为您自己的证书，该证书与用于连接到 XProtect Mobile 服务器的服务器地址相匹配。这些证书通过 Verisign 等官方证书签发机构获得。有关更多详细信息，请咨询所选的签发机构。
   XProtect Mobile 服务器不使用 Microsoft IIS。这意味着，由签发机构使用 IIS 提供的生成证书签发请求 (CSR) 文件的指令不适用于 XProtect Mobile 服务器。您必须使用命令行证书工具或其他类似的第三方应用程序手动创建 CSR 文件。此过程应仅由系统管理员和高级用户执行。

图像质量

1. 在 **XProtect Mobile** 客户端中查看视频时，为什么有时图像质量较差？

   XProtect Mobile 服务器会根据服务器与客户端之间的可用带宽自动调整图像质量。如果您遇到的图像质量低于 XProtect® Smart Client 中的图像质量，则可能是带宽太小而无法通过 XProtect Mobile 客户端获取全分辨率图像。造成这种情况的原因可能是服务器的上游带宽太小，或者客户端上的下游带宽太小。请参阅 **XProtect Smart Client** 用户手册，您可从我们的网站 (https://www.milestonesys.com/support/help-yourself/manuals-and-guides/) 下载该用户手册。

   如果您在无线带宽混合的区域中，则可能会发现当您进入带宽更好的区域时，图像质量会提高。

2. 当我通过办公室的 **Wi-Fi** 连接到我家里的 **XProtect** 视频管理系统时，为什么图像质量较差？

   检查您的家庭互联网带宽。许多私人互联网连接都具有不同的下载和上传带宽，例如，通常描述为 20 Mbit/2 Mbit。这是因为家庭用户很少需要将大量数据上传到互联网，而是需要使用大量数据。XProtect 视频管理系统需要将视频发送到 XProtect Mobile 客户端，并且受您的连接的上传速度限制。如果在 XProtect Mobile 客户端网络的下载速度良好的多个位置上图像质量始终较差，则可以通过升级家庭互联网连接的上传速度来解决该问题。

硬件加速解码

1. 我的处理器是否支持硬件加速解码？

   只有 Intel 的较新版本处理器才支持硬件加速解码。请访问 Intel 网站 (https://ark.intel.com/Search/FeatureFilter?productType=processors/)，检查是否支持您的处理器。

   在菜单中，确保将技术 > **Intel Quick Sync Video**设置为是。

   如果支持您的处理器，则默认情况下会启用硬件加速解码。您可以在 Mobile Server Manager 中的显示状态中查看当前状态(参阅显示状态(已解释) 第 页上的52) 。

2. 我的操作系统是否支持硬件加速解码？

   XProtect 支持的所有操作系统也都支持硬件加速。

   确保从系统上的 Intel 网站安装最新的图形驱动程序。Windows Update 无法提供这些驱动程序。

   如果移动设备服务器安装在虚拟环境中，则不支持硬件加速解码。

3. 如何在移动设备服务器上禁用硬件加速解码？ **(** 高级**)**

   如果移动设备服务器上的处理器支持硬件加速解码，则默认情况下会启用硬件加速解码。要关闭硬件加速解码，请执行以下操作：

   1. 找到文件 VideoOS.MobileServer.Service.exe.config。路径通常为：C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config。
   2. 在记事本或类似的文本编辑器中打开该文件。如有必要，请将文件类型 .config 与记事本关联。
   3. 找到字段 <add key="HardwareDecodingMode" value="Auto" />。
   4. 将值“Auto”替换为“Off”。
   5. 保存并关闭该文件。

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/。