

WHITE PAPER

Integração do dispositivo com o MQTT

Março 2022

Resumo

O MQTT é um protocolo padrão de mensagens que facilita a troca eficiente e confiável de dados entre dispositivos IoT e aplicativos em nuvem. Ele permite que os dispositivos (por meio de seus clientes MQTT) publiquem mensagens em um agente MQTT comum (servidor) que media a comunicação com outros dispositivos. O agente acompanha quem está publicando o quê e quem quer ver os dados, encaminhando mensagens apenas para os clientes que assinaram o tópico certo.

Em um ecossistema VMS típico, as notificações de eventos Axis dos dispositivos são transmitidas tradicionalmente para um único destino por meio da interface API VAPIX/ONVIF usando o protocolo de streaming RTSP. Mas as mesmas notificações podem ser distribuídas usando o protocolo MQTT por meio do cliente MQTT integrado do dispositivo (aplicável para dispositivos que executam o AXIS OS 9.80 ou uma versão posterior). Isso é possível tanto dentro dos ecossistemas VMS quanto fora deles, e é particularmente útil na Internet. Vários clientes MQTT inscritos na rede podem então usar e processar as notificações de eventos publicadas pelo dispositivo Axis. Existem também aplicativos de análise ACAP da Axis e de terceiros com seus próprios clientes MQTT projetados para sistemas, casos de uso e assinantes específicos.

Como exemplo de caso de uso relacionado aos produtos Axis, os dispositivos de contagem de pessoas podem enviar estatísticas por MQTT para software de visualização de dados na nuvem. Em outro exemplo, um sensor de porta de terceiros se comunica pelo MQTT com um dispositivo de sinalização e uma câmera, que emitem um alarme e iniciam uma gravação toda vez que a porta é aberta.

Sumário

1	Introdução	4
2	Protocolo MQTT	4
3	Vantagens	5
4	Limitações	6
5	Infraestrutura	6
6	Segurança	6
7	Cliente MQTT em dispositivos Axis	7
8	Cientes MQTT em aplicativos de análise ACAP	7
9	Outros clientes MQTT	7
10	Exemplos de casos de uso integrando dispositivos com o MQTT	8
	10.1 Dados de análise de contagem de pessoas para o painel da plataforma na nuvem	8
	10.2 Os dados dos sensores das portas sobre o MQTT acionam o alarme do dispositivo de sinalização e a gravação da câmera	8
11	Glossário	10
12	Atribuições de marca registrada	11

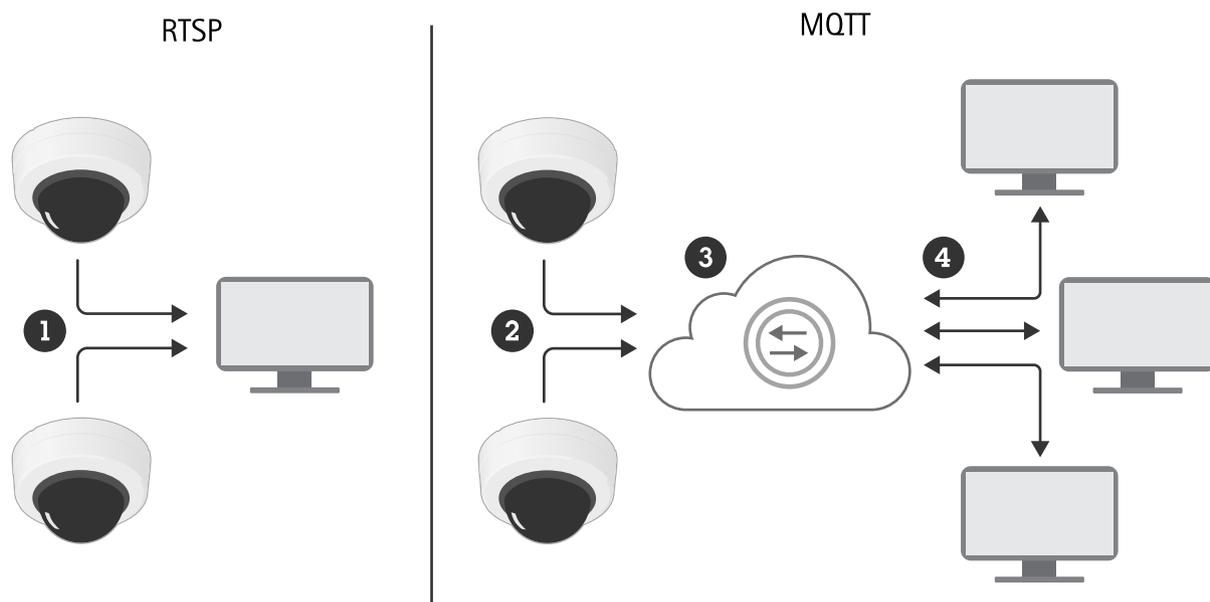
1 Introdução

O MQTT (Message Queuing Telemetry Transport) é um protocolo padrão de troca de mensagens padrão para a Internet das Coisas (IoT). Ele foi desenvolvido para integração simplificada com a IoT e é usado em uma ampla variedade de setores para conectar dispositivos remotos com o mínimo de código e largura de banda de rede. O cliente MQTT no Sistema Operacional Axis pode simplificar a integração de dados e eventos produzidos no dispositivo a sistemas que não são sistemas de gerenciamento de vídeo (VMS).

Este white paper apresenta um histórico técnico sobre MQTT, incluindo casos de uso típicos, benefícios e limitações. Ele também fornece detalhes sobre clientes MQTT em dispositivos Axis e em aplicativos de análise ACAP.

2 Protocolo MQTT

MQTT é um protocolo de publicação/assinatura. Isso significa que ele tem um padrão de mensagens diferente do RTSP ou HTTP, que são protocolos de solicitação/resposta. Com o RTSP, um lado emite uma solicitação e o outro responde. Muitos aplicativos de mensagens móveis são baseados em MQTT ou em conceitos de publicação/assinatura semelhantes. Há também protocolos de publicação/assinatura otimizados para sistemas fechados ou específicos.



Enquanto o RTSP permite apenas a comunicação um-para-um, o MQTT também permite a comunicação um-para-muitos ou muitos-para-muitos através do agente.

- 1 Stream de eventos
- 2 Publicação
- 3 Agente MQTT
- 4 Assinatura

O conceito MQTT é que todos os clientes se conectam a um agente MQTT comum (servidor), que acompanha quem está publicando o quê e quem deseja ver os dados. A conexão é geralmente uma sessão TCP na porta 1883. Um cliente também pode se conectar por TLS (normalmente na porta 8883) ou usando WebSocket (normalmente na porta 1884/8884).

Os clientes publicam mensagens com um tópico. Outro cliente pode assinar esse tópico específico ou usar curingas para obter todos os subtópicos. Uma mensagem também inclui uma carga útil que é normalmente uma estrutura de dados JSON, uma string ou até mesmo dados binários curtos. O editor não sabe se outros clientes estão assinando. O agente encaminhará mensagens apenas para clientes que tenham assinaturas de tópicos.

Com o MQTT, funciona um pouco como enviar um artigo para uma revista. As pessoas que assinam a revista poderão ler o artigo e pode ser uma comunicação de um para um ou de um para muitos (e o MQTT ainda permite a comunicação de muitos para muitos). O artigo também pode ser lido muito tempo depois de ter sido publicado originalmente.

Em comparação, usar o RTSP seria algo como fazer uma ligação telefônica. Há uma fonte e um destino para seus comandos e é sempre uma comunicação um para um. Se o seu alvo não atendeu o telefone, ele perdeu a mensagem.

Quando o MQTT é usado para distribuir notificações de eventos do Axis de dispositivos, vários clientes MQTT inscritos na rede podem usar e processar as notificações. Esta é uma grande vantagem em comparação com a forma tradicional (usando a interface de programação de aplicativos (API) VAPIX®/ONVIF® e RTSP), onde as notificações de eventos seriam transmitidas para um único destino.

3 Vantagens

Há vários benefícios em usar o MQTT. Comparado com o uso de um protocolo de solicitação/resposta como o RTSP, os principais benefícios do MQTT incluem:

- **Redução do risco de exposição de senhas de dispositivos.** Não há necessidade de um cliente acessar um dispositivo ou servidor para obter os dados. Isso significa que o cliente não precisa saber a senha nem saber como a API funciona. Isso reduz o risco de as senhas dos dispositivos serem expostas a clientes e usuários, reduzindo assim o risco de uso indevido deliberado ou acidental.
- **Ponto único de integração.** Se autorizados, todos os clientes podem obter as mensagens publicadas de todos os outros clientes com uma única conexão com um agente. No RTSP, um cliente precisa se conectar a cada cliente do qual deseja obter dados. Isso significa que o fluxo de mensagens MQTT pode ser um para um, um para muitos ou muitos para um sem qualquer carga extra para cada cliente.
- **Publique e assine com um firewall intacto** No RTSP, a API do dispositivo/servidor precisa estar acessível para o cliente. Se o dispositivo estiver atrás de um firewall e o cliente for remoto, o firewall precisa ser configurado para permitir a entrada de solicitações, expondo a API do dispositivo. Com um agente MQTT público no meio, os clientes atrás de um firewall podem publicar/assinar dados específicos sem abrir um buraco no firewall (se o firewall permitir conexões de saída).
- **Qualidade de serviço.** Ao postar uma mensagem crítica, um editor pode monitorar se essa mensagem foi recebida por outro cliente e, caso contrário, tomar uma ação alternativa.
- **Mensagens retidas.** Os editores podem marcar uma mensagem como retida, o que significa que o agente manterá uma cópia da mensagem e enviará essa mensagem para clientes recém-conectados assinando esse tópico.
- **Disponibilidade do cliente IoT.** Os pacotes do cliente MQTT estão disponíveis para todos os ambientes comuns de desenvolvimento de software, incluindo Windows®, Linux®, Android™, iOS, Node.js®, PHP e Python®. Há muito mais clientes que podem se conectar a um agente em comparação com a configuração de um fluxo de dados RTSP para um dispositivo.

- **Monitoramento e depuração simplificada de mensagens.** Há várias ferramentas MQTT que podem ser usadas para monitorar todas as mensagens publicadas e também para publicar mensagens para solucionar problemas se e como os assinantes reagem.
- **Estrutura de dados simplificado.** Como o MQTT geralmente tem como alvo clientes desconhecidos, a carga útil da mensagem geralmente leva isso em consideração para simplificar para o assinante.

4 Limitações

Existem algumas desvantagens em relação ao MQTT quando comparado com protocolos alternativos:

- **Ponto único de falha.** Se o agente estiver indisponível, todas as mensagens param de funcionar. No entanto, a infraestrutura pode ser projetada com agentes de redundância.
- **Quem publicou a mensagem?** Por desenho, o MQTT se concentra no tópico e não em quem publicou a mensagem. A menos que o editor inclua alguma ID como parte do tópico ou da carga útil, você precisará acessar o registro do agente para saber quem publicou a mensagem. É uma prática comum que os editores incluam alguma ID do cliente no tópico ou na carga útil com base no caso de uso.
- **Um cliente malicioso conectado ao agente pode publicar/assinar qualquer tópico para o qual é autorizado.** Você precisa proteger o agente (consulta a seção sobre segurança do MQTT).
- **Ele não foi desenhado para streaming contínuo de vídeo/áudio.**

Como com qualquer servidor, a taxa de transferência total da largura de banda precisa ser considerada. O dimensionamento dinâmico pode ser necessário para sistemas muito grandes que tenham muitos clientes.

5 Infraestrutura

É muito fácil configurar um agente local do Eclipse Mosquitto™ ou habilitar o Node-RED® para atuar como um agente local, como o Aedes. Também há vários provedores de serviços de Internet e outros que fornecem agentes MQTT gerenciados, como Microsoft® Azure® IoT, HiveMQ™, CloudMQTT e IBM® Cloud®.

Se um sistema não tiver clientes remotos, recomenda-se usar um agente local. Um agente local também pode atuar como um proxy para um agente público ou ser configurado para atuar como um proxy para mensagens selecionadas do agente local e mensagens do agente público.

6 Segurança

O agente precisa de proteção apropriada com base em quão críticas são as mensagens e em quais ameaças um sistema específico pode enfrentar. O MQTT oferece vários esquemas de autenticação diferentes, incluindo sem autenticação, autenticação via usuário/senha e autenticação de certificado de cliente TLS. Diferentes usuários podem ter autorizações distintas sobre qual tópico pode publicar ou assinar. O agente pode permitir que os clientes se conectem por TCP não criptografado ou por TLS criptografado (como HTTPS).

- **Sem autenticação.** Um agente local pode desabilitar a autenticação se as mensagens não forem críticas e o agente não estiver exposto para clientes da internet. Recomenda-se usar apenas para testes, desenvolvimento de sandbox e demonstrações.
- **Usuário/senha.** Esta é a configuração mais comum. Dependendo dos riscos para o sistema, o administrador do sistema pode permitir que todos os clientes MQTT compartilhem o mesmo usuário/senha ou criem usuários com acesso restrito ao tópico.

- **Certificados de cliente TLS.** Para agentes expostos à Internet em que as mensagens são classificadas como confidenciais, o agente deve ser configurado para permitir apenas clientes com um certificado TLS válido. Esse esquema requer uma PKI (infraestrutura de chave pública) e uma autoridade de certificação que possa emitir certificados de cliente nos quais o agente confia. Os provedores públicos de serviços de Internet MQTT geralmente oferecem isso.

Em algumas situações, pode ser adequado segmentar diferentes casos de uso com vários agentes, locais e/ou públicos. A segmentação de mensagens críticas e mensagens não críticas é um controle de segurança. Vários agentes também reduzirão o risco de um único ponto de falha e aprimorarão o monitoramento e a solução de problemas. O custo é a implantação e manutenção adicionais de agentes adicionais.

7 Cliente MQTT em dispositivos Axis

Em um ecossistema VMS padrão, as notificações de eventos Axis dos dispositivos são transmitidas tradicionalmente para um único destino por meio da interface API VAPIX/ONVIF usando o protocolo de streaming RTSP.

As mesmas notificações de eventos podem ser distribuídas usando o protocolo MQTT por meio do cliente MQTT integrado de um dispositivo Axis (executando o AXIS OS 9.80 ou uma versão posterior). Isso é aplicável tanto dentro dos ecossistemas VMS quanto fora deles, e é particularmente útil na Internet. Com o MQTT, vários clientes MQTT inscritos na rede podem usar e processar as notificações de eventos publicadas pelo dispositivo Axis.

8 Clientes MQTT em aplicativos de análise ACAP

Existem aplicativos ACAP da Axis e de terceiros com seus próprios clientes MQTT projetados para sistemas, casos de uso e assinantes específicos. O Axis Publisher é um exemplo que adiciona recursos, estruturas e comportamento extras necessários para alguns sistemas.

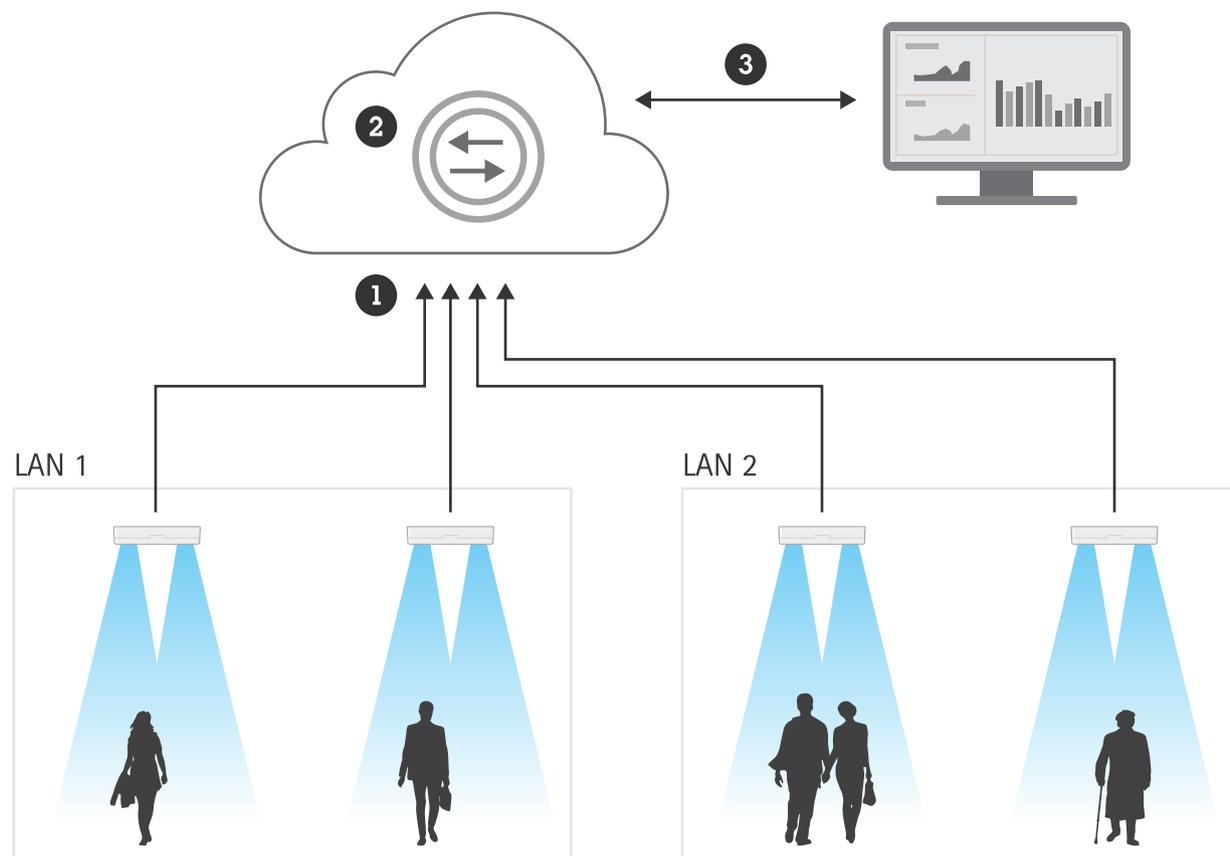
9 Outros clientes MQTT

Há uma ampla variedade de clientes MQTT que podem ser instalados no Linux, Windows, Android e iOS e que são projetados como ferramentas ou serviços para casos de uso específicos. O MQTT é muito adequado para scripts e middleware, como Node-RED/Node.js, Python e PHP. A maioria das plataformas de serviços de Internet, como Microsoft Azure IoT, AWS™ e Google Cloud Platform™, oferecem agentes MQTT para serem integrados aos serviços executados na plataforma. Há sensores, aplicativos móveis e sistemas de automação (residencial), todos com um cliente MQTT.

10 Exemplos de casos de uso integrando dispositivos com o MQTT

10.1 Dados de análise de contagem de pessoas para o painel da plataforma na nuvem

Um dispositivo com análise de contagem de pessoas gera uma notificação de evento sempre que uma pessoa é detectada entrando ou saindo de uma área definida. A notificação é repassada ao cliente MQTT que a publica em tempo real na plataforma na nuvem. Na plataforma na nuvem, uma conexão com o software de visualização de dados (por exemplo, um painel do Microsoft® Power BI®) é criada para exibir as estatísticas em tempo real dos contadores de pessoas.

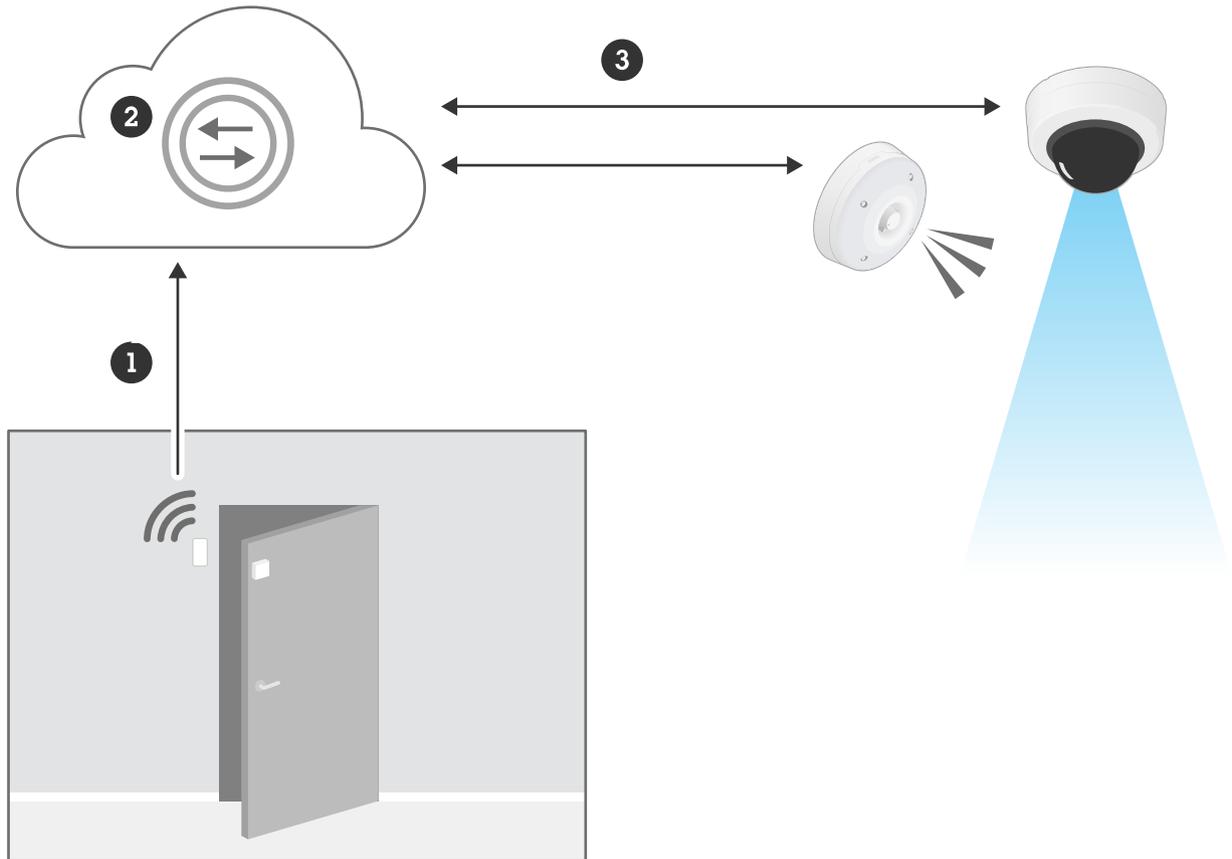


- 1 Publicação
- 2 Agente MQTT
- 3 Assinatura

10.2 Os dados dos sensores das portas sobre o MQTT acionam o alarme do dispositivo de sinalização e a gravação da câmera

Um sensor de porta MQTT de terceiros é usado para acionar uma notificação de evento se a porta for aberta. O sensor da porta publica uma mensagem MQTT para o agente MQTT na nuvem. O dispositivo de

sinalização e a câmera assinam o tópico do sensor da porta e emitem um alarme e iniciam uma gravação se a porta for aberta.



- 1 Publicação
- 2 Agente MQTT
- 3 Assinatura

11 Glossário

ACAP	<i>Plataforma de aplicativos de câmeras AXIS</i> , uma estrutura para aplicativos que adicionam funcionalidade e inteligência na borda
Aedes	Um agente MQTT
API	<i>Interface de programação de aplicativo</i> , código que permite que dois programas de software se comuniquem entre si
AWS™	Uma plataforma de serviços na nuvem
SO AXIS	O sistema operacional para dispositivos de borda da Axis
CloudMQTT	Um agente MQTT
Eclipse Mosquitto™	Um agente de mensagens de código aberto que implementa protocolos MQTT
Google Cloud Platform™	Uma plataforma de serviços na nuvem
HiveMQ™	Um agente MQTT
HTTP	<i>Protocolo de Transferência de Hipertexto</i> , um protocolo de transferência de dados usado na World Wide Web
IBM Cloud®	Uma plataforma de serviços na nuvem
IoT	<i>Internet das Coisas</i> , a interconexão, pela internet, de dispositivos de computação incorporados em dispositivos e aparelhos cotidianos
JSON	<i>JavaScript Object Notation</i> , um formato de arquivo compacto e formato de intercâmbio de dados
Microsoft® Azure® IoT	Uma plataforma de serviços na nuvem
Microsoft® Power BI®	Um programa de software de visualização de dados interativo focado em inteligência de negócios
MQTT	<i>Message Queuing Telemetry Transport</i> , um protocolo de troca de mensagens padrão para a Internet das Coisas.
Node.js®	Uma plataforma de desenvolvimento de código aberto para execução de código JavaScript no lado do servidor
Node-RED®	Uma ferramenta de programação para conectar a Internet das Coisas
ONVIF®	Um fórum aberto do setor industrial que fornece e promove interfaces padronizadas para interoperabilidade eficaz de produtos de segurança física baseados em IP.
PHP	Uma linguagem de script de uso geral voltada para o desenvolvimento web
Python®	Uma linguagem de programação de uso geral
RTSP	<i>Real Time Streaming Protocol</i> , um protocolo de rede para estabelecer e controlar sessões de mídia entre dispositivos finais
TCP	<i>Transmission Control Protocol</i> , um protocolo de transporte de dados que é um dos principais protocolos da Internet
TLS	<i>Transport Layer Security</i> , um protocolo que fornece confidencialidade e integridade das comunicações em redes de computadores
VAPIX®	A interface de programação de aplicativos (API) aberta para produtos Axis

WebSocket	Um protocolo de comunicação que fornece canais de comunicação bidirecional em uma única conexão TCP
VMS	<i>Software de gerenciamento de vídeo</i> ou <i>sistema de gerenciamento de vídeo</i>

12 Atribuições de marca registrada

Android e Google Cloud Platform são marcas registradas do Google LLC.

AWS é uma marca registrada da Amazon.com, Inc. ou de suas afiliadas nos Estados Unidos e/ou outros países.

Eclipse Mosquitto é uma marca registrada de Eclipse Foundation, Inc.

HiveMQ é uma marca registrada de HiveMQ GmbH.

IBM e IBM Cloud são marcas registradas de International Business Machines Corp, registradas em muitas jurisdições em todo o mundo.

IOS é uma marca registrada ou comercial de Cisco Systems, Inc e/ou suas afiliadas nos Estados Unidos e em alguns outros países e é usada sob licença pela Apple, Inc.

JavaScript é uma marca registrada da Oracle Corporation nos Estados Unidos.

Linux é a marca registrada de Linus Torvalds nos EUA e em outros países.

Microsoft, Windows, Microsoft Azure IoT e Microsoft Power BI são marcas registradas da Microsoft Corporation.

Node.js e Node-RED são marcas registradas da OpenJS Foundation nos Estados Unidos e/ou em outros países.

ONVIF é uma marca registrada da Onvif, Inc.

Python é uma marca registrada da Python Software Foundation.

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções de rede capazes de fornecer percepções para melhorar a segurança e novas maneiras de fazer negócios. Como líder do setor em vídeo em rede, a Axis oferece produtos e serviços de para sistemas de vigilância e análise de vídeo, controle de acesso, intercomunicação e áudio. A Axis conta com mais de 3.800 funcionários dedicados em mais de 50 países e colabora com parceiros em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e sua sede é em Lund, Suécia.

Para obter mais informações sobre a Axis, visite nosso site axis.com.