

MAKE THE
WORLD SEE

Milestone Systems

XProtect® on AWS

Getting started guide - Bring Your Own License (BYOL)

XProtect Corporate

XProtect Expert

XProtect Professional+

XProtect Express+



Contents

- Copyright, trademarks, and disclaimer** 4
- Overview** 5
 - About this guide 5
 - XProtect on AWS 5
 - What's new? 6
- Licensing** 7
 - XProtect on AWS licensing 7
- Requirements and considerations** 8
 - Getting started checklist 8
 - Cost considerations 9
 - Before you start deployment 10
- Deployment** 13
 - The XProtect BYOL CloudFormation template 13
 - Subscribe to XProtect in AWS Marketplace 13
 - Create the XProtect BYOL CloudFormation stack 14
 - Stack details 15
- Configuration** 20
 - Connect to your deployment with Remote Desktop Protocol (RDP) 20
 - Get the EC2 Instance ID 20
 - Add your XProtect license 20
 - Connecting the deployed VPC to your on-premises network 21
 - Securing your deployment 22
 - Download the XProtect® Device Pack 23
- Optimization** 24
 - Update NVIDIA drivers for hardware acceleration 24
 - Reducing costs for AWS services 24
- Expanding the deployment** 26
 - System scaling 26

Archiving recordings	26
Archiving using Amazon S3	27
Surveillance Bridge	27
Archiving using Amazon FSx	27
FSx for Windows File Server storage	27
Create FSx shares	28
File system details for FSx	28
Attach your FSx shares to XProtect	31
Removing XProtect	33
Delete the XProtect CloudFormation stack	33
Unsubscribe	33

Copyright, trademarks, and disclaimer

Copyright © 2023 Milestone Systems A/S

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file `3rd_party_software_terms_and_conditions.txt` located in your Milestone system installation folder.

Overview

About this guide

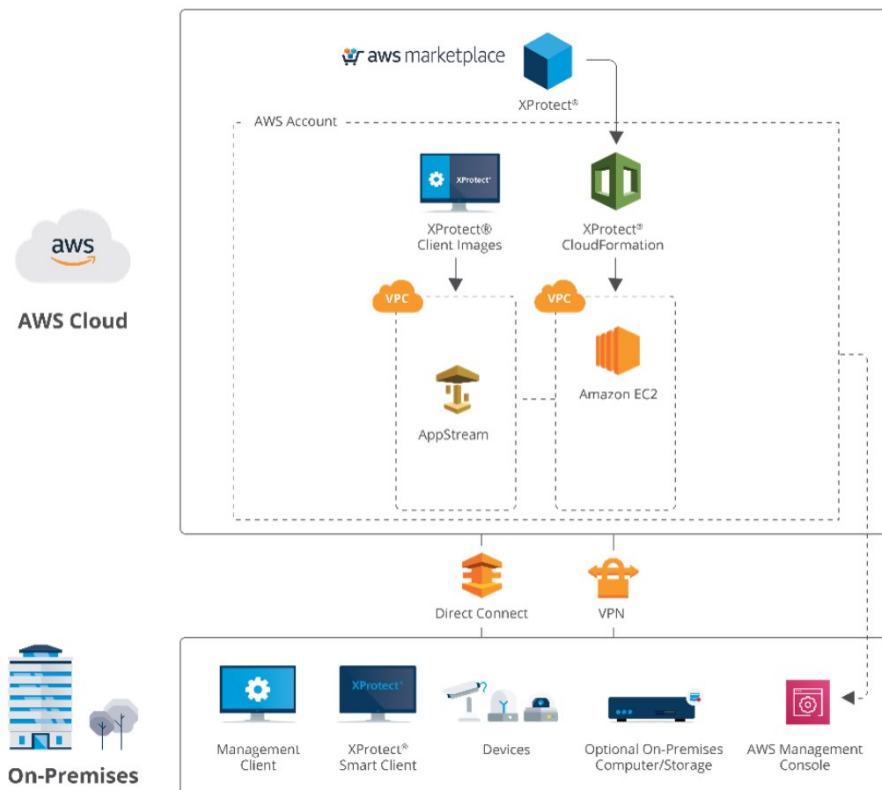
This single computer installation guide for XProtect® on AWS provides information for getting started with your XProtect VMS deployment in your AWS infrastructure. The guide includes checklists and tasks that help you deploy and configure your system and verify connections between your server and clients.

XProtect on AWS

Designing and deploying hardware infrastructure for your VMS can be time-consuming and costly. With the power of AWS, you can create an infrastructure that supports your XProtect VMS in minutes. You can seamlessly scale your system up or down, add unlimited storage, and provide disaster recovery for you VMS seamlessly.

The XProtect BYOL CloudFormation template deploys all the XProtect VMS core components, including XProtect Smart Client and XProtect Management Client, inside a Virtual Private Cloud (VPC). See [The XProtect BYOL CloudFormation template on page 13](#).

On-premise cameras, sensors, and other IoT devices are connected to the VPC through a secure connection. The on-premise devices transmit video, audio, metadata, and other streams to the VMS on AWS without the need for any additional on-premises hardware or gateway equipment for aggregation or buffering.



XProtect on AWS supports different deployment scenarios to fit your needs. You can have single or multisite deployments where the infrastructure is hosted on the cloud or is divided between cloud and on-premises.

For more information, see the [XProtect on AWS White Paper](#).

What's new?

In XProtect BYOL latest version:

Store archived recordings in Amazon S3 buckets:

- Automatically transfer archived recordings to a selected S3 class bucket with the Surveillance Bridge plug-in by Tiger Technology. See [Surveillance Bridge on page 27](#).

Operating system:

- XProtect VMS now runs on Windows Server 2022.

Licensing

XProtect on AWS licensing

The licensing of XProtect BYOL follows the same license terms and uses the same Software License Code (SLC) as traditional on-premises deployments.



If you have not yet purchased a license for your XProtect product, you can get a license from a Milestone distributor or reseller using the [Milestone partner network](#).

You might need to upgrade the license to match the XProtect release versions that are available on AWS Marketplace.

See the complete feature list, which is available on the product overview page on the Milestone website (<https://www.milestonesys.com/products/software/product-index/>).

Requirements and considerations

Getting started checklist

Use this checklist to go through the deployment and configuration steps of your XProtect BYOL in the correct order:

Step	Description
<input type="checkbox"/>	Make sure that you meet the deployment prerequisites. See Before you start deployment on page 10 .
<input type="checkbox"/>	Configure and deploy the CloudFormation stack. See Subscribe to XProtect in AWS Marketplace on page 13 and Create the XProtect BYOL CloudFormation stack on page 14 .
<input type="checkbox"/>	Connect to your deployment. See Connect to your deployment with Remote Desktop Protocol (RDP) on page 20 .
<input type="checkbox"/>	Connect to your on-premises network using Amazon services. See Connecting the deployed VPC to your on-premises network on page 21 .
<input type="checkbox"/>	Add and activate your XProtect license. See Add your XProtect license on page 20 .
<input type="checkbox"/>	Configure and maintain XProtect on AWS securely. See Securing your deployment on page 22
<input type="checkbox"/>	Download and install the necessary device drivers. See Download the XProtect® Device Pack on page 23
<input type="checkbox"/>	Scale your system. See System scaling on page 26 .
<input type="checkbox"/>	Move archived recordings to another location.

Step	Description
	See Archiving recordings on page 26
<input type="checkbox"/>	Reduce costs for AWS services by optimizing the user access. See Reducing costs for AWS services on page 24

Cost considerations

AWS and third-party services are priced independently of your Milestone XProtect license. These costs should be part of your considerations when you design your VMS and network.

After you deploy, you can modify the architecture with additional AWS and third-party services.



Costs associated with AWS services also vary, depending on the region you have selected. For more information about how AWS charges for usage and services used by XProtect on AWS, see the [XProtect on AWS Pricing Calculator](#).

Required AWS services

Service	Cost considerations
Amazon EC2	Hosts the operating system and the VMS. The cost is based on the data transfer out from the Amazon Virtual Private Cloud (VPC), often referred to as data egress. The cost depends on the number of cameras in the system, their resolution and frame rate, and the degree of server-side motion detection.
Amazon EBS	Used for storing the operating system, the VMS components, and the media database. The cost is based on the volume sizes.
Amazon VPC	Hosts the VMS infrastructure. There is no additional charge for creating and using an Amazon VPC itself, you can pay for Amazon Web Services solutions, such as Amazon EC2, and optional VPC capabilities.

Optional Amazon and third-party services

Service	Cost considerations
Amazon FSx	Used for video archiving. The cost is based on the type of storage, throughput capacity, and backup storage. See FSx for Windows File Server storage on page 27 .
Surveillance Bridge by Tiger Surveillance	Moves video recordings from an EBS block storage to an S3 bucket and provides disaster recovery for the media database. Requires a separate license. See Surveillance Bridge on page 27
Amazon S3 (used by Surveillance Bridge)	Surveillance Bridge stores video archives in S3 buckets. The cost is based on storage size, period, and class.
AWS Site-to-Site VPN	Used for connecting the deployed VPC to your network topology. The cost is calculated per VPN connection.
AWS Direct Connect	Used for connecting the deployed VPC to your network topology. The cost is based on port hours and capacity.
Amazon AppStream 2.0	Used for connecting the deployed VPC to your network topology. The cost is based on the type of operation and usage patterns, most significantly on the number of users and the duration of usage. No charge for data egress.

After you deploy, you can add additional AWS and third-party services to extend your cloud architecture.




Before you start deployment

Before you deploy the XProtect BYOL CloudFormation template, you must meet the prerequisites below.




Consult the [Milestone Cloud Solutions training track](#) for interactive courses that cover Milestone cloud fundamentals, and XProtect on AWS design and deployment.

AWS deployment prerequisites


Prerequisite	Description
AWS account	<p>You must create or use an existing AWS account. Milestone recommends that you use the AWS managed policy for the developer power user job function that you can assign to an AWS user account. This policy allows the user to deploy the AWS CloudFormation stack, view and manage the EC2 instance, create and access S3 buckets, and more. See Developer power user job function.</p> <div style="background-color: #f9e79f; padding: 10px; border-left: 3px solid #c07040;">  Amazon strongly recommends that you don't use the root user for your everyday tasks. To keep your infrastructure secure, create users, and only give them the permissions required to run the relevant tasks. </div>
AWS Elastic Block Store (EBS)	<p>The XProtect BYOL CloudFormation deploys two EBS gp2 volumes.</p> <p>You select the storage size during deployment. Milestone recommends that the media volume size be configured to hold a minimum of 24 hours of video recordings.</p> <div style="background-color: #d9e1f2; padding: 10px; border-left: 3px solid #0070c0; margin-bottom: 10px;">  If you have a large number of connected cameras or users, you must increase the size of disk that holds Microsoft SQL Server Express above the default size. </div> <div style="background-color: #d9e1f2; padding: 10px; border-left: 3px solid #0070c0;">  You can increase the volume size but you cannot reduce it. </div>
AWS region and availability zone	<p>Each AWS region is a separate geographic area. Each AWS region has multiple, isolated locations known as availability zones.</p> <p>XProtect on AWS is available in almost all regions. Milestone recommends that you select the region that is closest to you.</p> <p>You can use any availability zone within a region to deploy XProtect on AWS in.</p>

XProtect VMS prerequisites

 For general XProtect VMS prerequisites, refer to the [XProtect VMS administrator manual](#).

Prerequisite	Description
XProtect product license	XProtect BYOL requires a software license (.lic) file and associated Software License Code (SLC), see XProtect on AWS licensing on page 7 .
Sensitive data	When you configure your XProtect VMS, secure your installation and the collected surveillance data. For more information about data protection and the usage data collection, see the GDPR privacy guide .

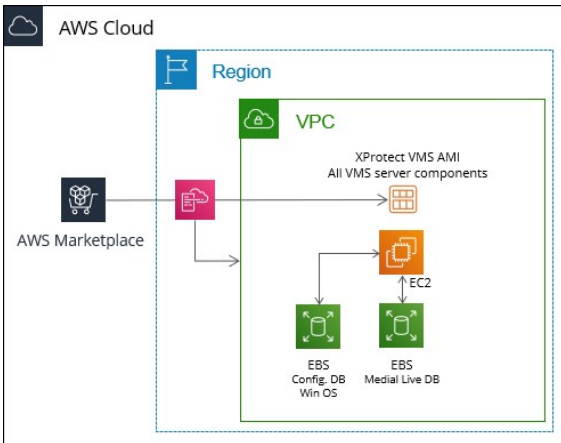
Network prerequisites

Prerequisite	Description
EC2 host name	<p>Prepare a name for your EC2 instance that will also act as a Windows Active Directory (AD) host name and domain name in your network.</p> <div style="background-color: #f9cb9c; padding: 10px; border-left: 3px solid #c00000;">  <p>You cannot change the host name of the EC2 instance after you have deployed the XProtect BYOL CloudFormation stack.</p> </div> <p>For more information about AD naming conventions and character limits, see Naming conventions in Active Directory.</p>
Network bandwidth consumption	<p>When you design the network topology that connects to the customer site, consider the required bandwidth, network load, and need for redundancy.</p> <p>The main load on your network consists of three elements:</p> <ul style="list-style-type: none"> • Camera video streams • Clients displaying video • Archiving of recorded video

Deployment

The XProtect BYOL CloudFormation template

The XProtect BYOL CloudFormation template deploys all components that are necessary to run the XProtect VMS.



The CloudFormation template:

- Creates a new Virtual Private Cloud (VPC) and subnet.
- Deploys a single-server XProtect VMS installation on an Amazon Elastic Compute Cloud (EC2) instance using a custom Amazon Machine Image (AMI).
- Attaches two Amazon Elastic Block Storage (EBS) volumes to the EC2 instance:

Volume	Description
Operating system volume (disk 0)	The volume contains the Windows Server 2022 operating system, XProtect VMS software, and Microsoft SQL Server Express for the VMS databases.
Media database volume (disk 1)	The volume contains database optimized for recording and storing audio and video data from your connected cameras and devices.

Subscribe to XProtect in AWS Marketplace

To deploy the XProtect CloudFormation stack, you must first subscribe to the product in AWS Marketplace.

1. Go to <https://aws.amazon.com/marketplace>
2. Enter Milestone in the search bar. Select the XProtect product to subscribe to:
 - **Milestone XProtect (Essential+)** (used for demo purposes)
 - **Milestone XProtect (BYOL)**

Then, select **Continue to Subscribe**.



The charges for using the AWS services are listed when you subscribe to your XProtect product in AWS Marketplace.

After you have subscribed, you are ready to deploy XProtect on AWS.

Create the XProtect BYOL CloudFormation stack

To create a stack, you must subscribe to XProtect BYOL. See [Subscribe to XProtect in AWS Marketplace on page 13](#).

After you have subscribed to XProtect BYOL in AWS Marketplace, you can create the XProtect BYOL CloudFormation stack.

Use the CloudFormation service role that you created with the necessary permissions for creating and deploying your XProtect stack. See [Give users the permissions to deploy and manage XProtect VMS](#).



In the AWS Management Console, you find roles on the **Identity and Access Management (IAM)** page -> **Roles** tab.

To launch the CloudFormation console:

1. Go to <https://console.aws.amazon.com/marketplace/> and select your XProtect subscription. Then, select **Launch CloudFormation stack**.
2. On the **Configure this software** page, select your region. Then, select **Continue to Launch**.
3. On the **Launch this software** page, under **Choose Action**, select **Launch CloudFormation**. Then, select **Launch** to open the AWS CloudFormation console.

You are now ready to create the stack. The process consists of four steps:

1. In the **Create Stack** step, select **Next** to continue.
2. In the **Specify Stack Details** step, you configure the XProtect VMS and network settings. See [Stack details on page 15](#). Select **Next** to continue.

3. In the **Configure Stack Options** step, you configure any additional options and permissions.

If you have selected to install Surveillance Bridge, you must allow AWS CloudFormation to connect and manage the S3 bucket. In **Capabilities**, select **I acknowledge that AWS CloudFormation might create IAM resources with custom names**.

Select **Next** to continue.

4. In the **Review** step, you verify your configuration. Select **Submit** to create the stack.



Deploying the XProtect BYOL CloudFormation stack takes about 30 minutes.

Stack details

In the second step of the deployment process, you configure the VMS and network settings.




For details about how to set up and configure the XProtect VMS, see the [XProtect VMS Administrator manual](#).

Stack name

Parameter	Description
Stack name	Specify a name to identify the XProtect BYOL CloudFormation stack with.

XProtect Configuration

Parameter	Description
XProtect language	<p>Select the display language of the installed XProtect products.</p> <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin-top: 10px;">  For more information about XProtect supported languages, see Milestone products supported languages. </div>



Parameter	Description
Retention time	<p>Select the number of days video recordings are saved for in the media database.</p> <p>The default retention time is seven days.</p> <p>If you increase the Retention time from the default value, you should also increase the size of the Media database volume accordingly.</p>



Plugin

Parameter	Description
Storage Bridge	<p>Select if you want to install Surveillance Bridge for archiving recordings. See Surveillance Bridge on page 27.</p>


EC2 Configuration

Parameter	Description
User name for the administrator account	<p>Specify a user name for the administrator account. You use this account to access your EC2 instance using Remote Desktop Protocol (RDP).</p>
Password for the administrator account	<p>Specify a password for the administrator account.</p> <p>The password must be between 8 and 32 characters long and contain at least:</p> <ul style="list-style-type: none"> • One number • One special character • Capital letter
Instance type	<p>Select the type of the EC2 instance.</p> <p>The default instance type is c5.large.</p>

Parameter	Description
	<div style="background-color: #f9e79f; padding: 10px; border: 1px solid #ccc; margin-bottom: 10px;">  <p>If the template fails to deploy due to the selected Instance type, restart the deployment and select a different availability zone.</p> </div> <p>Recommended maximum number of cameras per instance type</p> <p>The camera numbers are estimated for 10% video recordings with 1080p resolution at 30 FPS:</p> <ul style="list-style-type: none"> • c5.large can support up to 18 cameras • c5.xlarge can support up to 40 cameras • c5.2xlarge can support up to 96 cameras • g4dn.xlarge* can support up to 113 cameras • g4dn.2xlarge* can support up to 275 cameras • g4dn.4xlarge* can support up to 480 cameras <p>*Requires enabling hardware acceleration.</p> <p>To learn more about the different instance types, go to Instance types.</p>
<p>Operating System Volume Size</p>	<p>Select the size in GB of the Elastic Block Storage (EBS) volume that contains all VMS components except the media database.</p> <p>The default volume size is 150 GB.</p>
<p>Delete Operating System Volume</p>	<p>Select if the operating system volume (disk 0) should be deleted when you terminate the EC2 instance.</p> <div style="background-color: #f9e79f; padding: 10px; border: 1px solid #ccc; margin-top: 10px;">  <p>Terminating the EC2 instance or deleting the EBS operating system volume does not unsubscribe you from XProtect BYOL.</p> </div>
<p>Media Volume Size</p>	<p>Select the size in GB of the EBS volume that contains the media database used to store video recordings.</p>

Parameter	Description
	<p>The default volume size is 100 GB.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #ccc;">  <p>Milestone recommends that you configure the media volume size to hold a minimum of 24 hours of video recordings. You can use another storage option to archive your recordings if you need to keep them for a longer time period.</p> </div>
Delete Media Volume	Select if the media database volume (disc 1) should be deleted when you terminate the EC2 instance.
Instance Hostname (optional)	<p>Create a custom name for the EC2 instance to find it in your network environment.</p> <p>If you leave this field blank, a random instance name is assigned to the EC2 instance.</p> <div style="background-color: #ffe0b2; padding: 10px; border: 1px solid #ccc;">  <p>You cannot change the Instance Hostname after deployment.</p> </div>

Network configuration

Parameter	Description
Availability zone	<p>Select an AWS availability zone within your selected region that the EC2 instance deploys in.</p> <div style="background-color: #ffe0b2; padding: 10px; border: 1px solid #ccc;">  <p>If the script fails to deploy due to the selected Instance type, restart deployment and select a different Availability Zone.</p> </div>
RDP ingress CIDR block	Specify the range of inbound IP addresses that will access the VPC using RDP.

Parameter	Description
VPC CIDR block	<p>Specify the range of IP addresses that creates the virtual network of the VPC.</p> <p>The default Classless Inter-Domain Routing (CIDR) IP block is 10.0.0.0/16.</p>
Subnet CIDR block	<p>Specify the range of IP addresses that creates the subnet of the VPC.</p> <p>The default CIDR IP block is 10.0.0.0/24.</p>

Configuration

Connect to your deployment with Remote Desktop Protocol (RDP)

You can manage your XProtect VMS installation from an RDP client.

1. Go to <https://console.aws.amazon.com/ec2/> and select **Instances**.
2. Select the **Instance ID** of your EC2 instance.



If you do not know your **Instance ID**, see [Get the EC2 Instance ID on page 20](#).

Then, select **Connect**.

3. In **Connect to instance**, select **RDP client**, then select **Download Remote Desktop File**.
4. Open the downloaded .rdp file and select **Connect** on any identification warnings that might appear.
5. Log in with the user name and password you specified during deployment and select **Connect**.

You are now connected to the VPC and the EC2 instance, which is running XProtect.



Make sure you have added your IP address on the inbound rules list of the security group that is associated with the instance.

Get the EC2 Instance ID

You need the address of the EC2 instance to connect to your XProtect VMS installation.

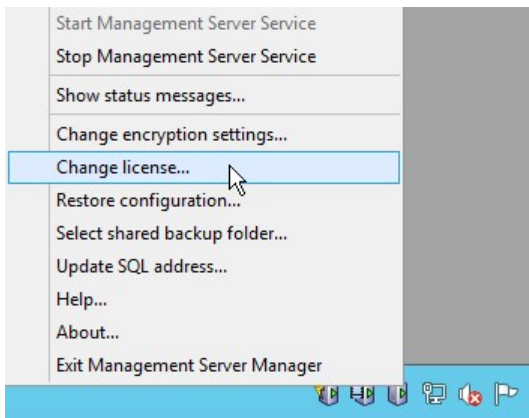
1. To open the AWS CloudFormation console, go to <https://console.aws.amazon.com/cloudformation/>
2. Select the XProtect CloudFormation stack that you created. It is identified by the **Stack name** that you specified during configuration.
3. In the **Resources** tab, you will see all the stack elements that were created by the XProtect CloudFormation template. Select the **Physical ID** link that corresponds to the EC2 instance.

Add your XProtect license

After you deploy, you are ready to add the software license (.lic) file to your deployment and activate your license to start using your XProtect product.


To add your XProtect license, connect to your deployment and follow the steps below:

1. Copy your software license (.lic) file to the Windows desktop of your deployment.
2. In the Windows notification area, right-click the management server and select **Change license...**



3. In the **Change XProtect License** window, select **Import License**. Locate the license that you copied in step 1 and select **Open**.
4. Select **OK**.

Your license is now imported into your installation.


 You must activate your license to enable the correct XProtect version in your XProtect VMS installation.

After you add your XProtect license to your installation, you must activate the license using XProtect Management Client. To activate your license:

- Use [online license activation](#) to activate your license if your deployment is connected to the internet.
- Use [offline license activation](#) to activate your license if you have restricted internet connectivity.

Connecting the deployed VPC to your on-premises network

There are many AWS and third-party network services that connect the deployed VPC to your network.

 Deployment scenarios depend on the specifics of your organization's network infrastructure. Milestone recommends that you consult your organization's IT department or network consultant.

AWS has services that securely connect your on-premises network or branch office site to your VPC. These services allow full connectivity to on-premises cameras, devices, recording servers, and Active Directory.

AWS Site-to-Site VPN

If you have a simple deployment, you can use AWS Site-to-Site VPN to connect your on-premise network to a single VPC. This connection type requires that you do a special configuration of the router. See [Site-to-Site VPN](#).



AWS provides a list of tested devices but other devices might be compatible. For more information about compatible gateway devices, see [Your customer gateway device on AWS](#).

AWS Transit Gateway

AWS Transit Gateway acts as a centralized, managed connectivity hub between VPCs and VPN connections. If you have an advanced XProtect deployment with multiple distributed sites, use AWS Transit Gateway to connect multiple VPCs using multiple VPN connections. See [AWS Transit Gateway](#).



If you are an existing AWS customer, you likely already have an AWS Transit Gateway infrastructure in place.



Gateway devices that use both the VPN Gateway and the Transit Gateway must support the Internet Key Exchange (IKE) protocol. AWS also requires special configuration of your gateway devices. For more information and a list of tested gateway devices, see the [AWS Site-to-Site VPN user guide](#).

AWS Direct Connect

AWS Direct Connect allows you to establish a dedicated connection from an on-premises network to one or more VPC. It provides an alternative to using the internet to utilize AWS cloud services. With AWS Direct Connect, you can have secure and private connections to AWS for workloads which require higher speed or lower latency than the internet. It is best suited for large enterprises using AWS infrastructure and services. See [AWS Direct Connect features](#).

Securing your deployment

Because your XProtect VMS deployment is connected to the internet, you should ensure the security and stability of your installation.

Installing Windows updates

To ensure the continued stability and security of the installation, keep your installation up to date with the latest updates to your Windows Server version, as well as upgrades to your license and Milestone Care™ coverage. Install relevant Windows updates according to the security policy of your organization.

If you restrict online connectivity to your VPC, you can connect your XProtect Essential+ deployment to a Windows update service without exposing the VPC to the internet.

Changing the password for the Windows instance

After you deploy, Milestone recommends that you change the administrator's password for the Windows instance according to the security policy of your organization.

Removing unused ports

To protect your installation, Milestone recommends that you remove all unused ports from the security group that is related to your EC2 instance. For example, if your organization is not using HTTP port 8081, you can remove that port from the **Inbound rules** table.

Download the XProtect® Device Pack

Your system uses video device drivers to control and communicate with the camera devices connected to a recording server. You must install device drivers on each recording server on your system.

From the 2018 R1 release, the device drivers are split into two device packs: the regular device pack with newer drivers and a legacy device pack with older drivers.

The regular device pack is installed automatically when you install the recording server. Later, you can update the drivers by downloading and installing a newer version of the device pack. Milestone releases new versions of device drivers regularly and makes them available on the download page (<https://www.milestonesys.com/downloads/>) on our website as device packs. When you update a device pack, you can install the latest version on top of any version you may have installed.

The legacy device pack can only be installed if the system has a regular device pack installed. The drivers from the legacy device pack are automatically installed if a previous version is already installed on your system. It is available for manual download and installation on the software download page (<https://www.milestonesys.com/downloads/>).

Stop the Recording Server service before you install, otherwise you need to restart the computer.

To ensure best performance, always use the latest version of device drivers.

To get the latest device pack after installation, go to the download section of the Milestone website and download the latest device pack installation file.



To see the device packs you need for your cameras, go to <https://www.milestonesys.com/community/business-partner-tools/device-packs/>.

Optimization

Update NVIDIA drivers for hardware acceleration

Hardware acceleration provides increased performance for video motion detection on your recording server. To enable hardware acceleration in XProtect Smart Client, see [Enabling hardware acceleration](#).



Hardware-accelerated video motion detection is available only for XProtect Corporate and XProtect Expert . For more information about the different XProtect VMS versions, see the [Milestone product index page](#).

To get the latest stability and performance enhancements for your GPU-enabled EC2 instance, you must update your NVIDIA GPU drivers. You can check the latest driver version and download the drivers for your NVIDIA GPU from <https://www.nvidia.com/Download/index.aspx/>.

Milestone recommends that you check the NVIDIA driver download page regularly.

Reducing costs for AWS services

Typically, there is no cost for data transfers in to the EC2 instance from the internet. However, there is a cost associated with transferring data out from the EC2 instance, often referred to as data egress. Working with the XProtect clients and viewing live or recorded video generates data egress. It depends on:

- The number of users.
- The type of XProtect client used.
- The frequency and duration of use.
- The amount of video streams viewed.

Adaptive streaming

Adaptive streaming is a streaming method that is used when multiple live video streams are shown in the same view. It enables the clients to automatically select the live video streams with the best match in resolution to the streams requested by the view items. Adaptive streaming reduces the network load and improves the decoding capability and performance of the client computer.

By enabling adaptive streaming, you reduce the amount of data transferred to XProtect Smart Client, XProtect Web Client, and the XProtect Mobile client.

To enable adaptive streaming, see the [XProtect VMS administrator manual](#).

Amazon AppStream 2.0

Run client applications as hosted user sessions in the cloud using Amazon AppStream 2.0. Users can access AppStream 2.0 hosted applications via HTTPS in a compatible web browser, or by using the AppStream 2.0 client application. See [Amazon AppStream 2.0](#).

Depending on your VMS installation, AppStream 2.0 might be a more cost-effective solution, because it includes the AWS costs for data egress, eliminating the costs associated with transferring multiple high-resolution video streams from the VPC to your on-premises environment.



Amazon AppStream 2.0 requires that you increase the AWS service quota of your deployment. For more information, see [How do I manage my AWS service quotas?](#).

Expanding the deployment

System scaling

By default, the XProtect BYOL CloudFormation deploys all server components on a single EC2 instance. With the AWS cloud infrastructure, you can scale individual components across multiple instances and storages to meet the expanding performance and capacity needs of your VMS installation.

Not all components are needed in all installations. You can always add components later. Such components could be additional recording servers, failover recording servers or mobile servers for hosting and providing access to XProtect Mobile and XProtect Web Client.

The XProtect CloudFormation script deploys Microsoft SQL Server Express which is a free edition of SQL Server.

For very large systems or systems with many transactions to and from the SQL Server databases, Milestone recommends that you use the Microsoft® SQL Server® Standard or Microsoft® SQL Server® Enterprise edition of SQL Server on a dedicated computer on the network and on a dedicated hard disk drive that is not used for other purposes. Installing SQL Server on its own drive improves the entire system performance.

Depending on your hardware and configuration, systems with up to 18 cameras can run on a **c5.large** instance type, while larger instances such as **g4dn.4xlarge** can support up to 480 cameras. For systems with more than 500 cameras, Milestone recommends that you use second-level scaling of dedicated EC2 instances and storage for all or some of the components.



Scaling can be done on the same VPC as on the original deployment, in a different region or availability zone, or to physical servers on your on-premises environment.

Archiving recordings

In deployments where video recordings are retained for longer than 24 hours, Milestone recommends moving the older recordings to a more cost-effective storage option. Archiving reduces the required size of the media database volume (disk 1) that holds your recordings, and helps you lower your costs because of the EBS gp2 storage's reduced capacity requirements.



To avoid filling the media database storage, you can reduce the retention time or lower the resolution and frame rate of your recordings.

Make sure that the capacity of the EBS gp2 volume (disk 1) can hold your recordings for a minimum of one day. Use another storage option for archiving. Milestone recommends the following archiving options:

- Amazon S3 with Surveillance Bridge by Tiger Surveillance. Automatically transfer archived recordings to a selected S3 class bucket. See [Surveillance Bridge on page 27](#).
- Amazon FSx for Windows File Server. The service provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. See [FSx for Windows File Server storage on page 27](#)

Archiving using Amazon S3

Surveillance Bridge

Surveillance Bridge is a plug-in by Tiger Surveillance that allows you to transition recordings from the Media database EBS volume to any S3 class while maintaining direct access to the recordings.

Surveillance Bridge allows you to select between different S3 classes and copy data from one S3 class to another (for example, from S3 Standard class to S3 Glacier Deep Archive).

It also provides disaster recovery for the Media Database volume.

You can select to install the Surveillance Bridge plug-in when you create the XProtect BYOL CloudFormation stack. The plug-in activates automatically when the stack is created. You have 30 days to test the product. To use the product afterward, you need to purchase a license from your Milestone reseller.

You can manage your storage from XProtect Management Client from the Surveillance Bridge node.

For more information about the Surveillance Bridge plug-in, see

<https://www.milestonesys.com/marketplace/tiger-surveillance/surveillance-bridge---xprotect-plug-in/>.

Archiving using Amazon FSx

FSx for Windows File Server storage

FSx for Windows File Server storage provides optimized storage performance for your XProtect archives. For high-level redundancy, you can configure FSx in a multiple availability zones where video archive is replicated synchronously within each individual availability zone and between the two availability zones.



If you have retention times shorter than one week, you may need to allocate more FSx storage capacity than needed to secure a sufficient IOPS baseline. For more information, see the [XProtect on AWS White Paper](#).

To use FSx for Windows File Server storage, take the following consideration for FSx:

- When you have defined the storage size and throughput capacity, you cannot change them.
- The share size is defined in steps of one GiB with a minimum size of two TiB and maximum size of 64 TiB.
- Integrates with Microsoft Active Directory.

- You must have an AD user service account that runs the recording server.
- Requires ports used in AWS for SMBv3 in your VPC Security Groups.

You can create multiple FSx shares and use them on your EC2 Windows server instance running the recording server to increase archiving storage capacity.



When scheduling XProtect archiving times, make sure the archiving job does not overlap with the AWS FSx half-hour weekly maintenance window or configure the size of disk 1 to accommodate possible postponed archiving when configured in a single availability zone.

For more information on FSx for Windows file server, see [Amazon FSx for Windows File Server](#).

Create FSx shares

Amazon FSx works with Microsoft Active Directory (AD) to integrate with your existing Microsoft Windows environment. You must create an FSx share and choose an AD for user authentication and access control.

To create an FSx share:

1. Go to <https://console.aws.amazon.com/fsx/> and select **Create file system**.
2. In the **Select file system type** step, select **Amazon FSx for Windows File Server** and then select **Next**.
3. In the **Specify file system details** step, specify the file system details. See [File system details for FSx on page 28](#).

Then, select **Next**.

4. In the **Review and create** step, verify your settings and select **Create file system** to start the creation of your FSx share.



Your FSx share status becomes **CREATING**. The expected creation time is 20-30 minutes. When the status is **AVAILABLE**, select the file system name to view the details.

You can now attach your FSx shares, see [Attach your FSx shares to XProtect on page 31](#).

File system details for FSx


When you create an FSx file share, you specify the file system details.

File system details

Parameter	Description
File system name - optional	Specify a name for use in the AWS Management console.
Deployment type	<p>Select Availability Zone (AZ). Single-AZ or Multi-AZ for redundancy.</p> <div style="border: 1px solid #0070C0; padding: 5px; background-color: #D9E1F2;">  Single-AZ has a 30-minute weekly maintenance window that you can schedule as you prefer. </div>
Storage type	Milestone recommends selecting HDD storage type for archiving.
Storage capacity	Specify the size of your FSx share.
Throughput capacity	<p>Select Specify throughput capacity to meet your throughput requirements.</p> <div style="border: 1px solid #0070C0; padding: 5px; background-color: #D9E1F2;">  When you select a higher throughput capacity, you increase the cost of running your FSx share. </div>

Network & security

Parameter	Description
Virtual Private Cloud (VPC)	Select the VPC where you have deployed your EC2 instance that is running your XProtect system.
VPC Security Groups	Specify a security group to associate with your file system's network interface.

Parameter	Description
	 To allow access to the VPC, update the inbound and outbound rules of the selected security group. See Step 1: Create your file system .
Preferred subnet	You must select the same subnet as your EC2 instance running your XProtect system.
Standby subnet	Select a relevant standby subnet.


Windows authentication

Parameter	Description
Choose an Active Directory to provide user authentication and access control for your file system	Select the Microsoft Active Directory to use. AWS Managed Microsoft Active Directory Select an Active Directory. Self-managed Microsoft Active Directory Provide the details below: <ul style="list-style-type: none"> Active Directory domain name Fully qualified domain name. DNS server IP Addresses. Service account username and password.

Encryption

Parameter	Description
Encryption key	Select your AWS Key Management Service (KMS) encryption key.

Backup and maintenance

Parameter	Description
Daily automatic backup window	Select No preference .
Automatic backup retention period	Set it to 1 days .
Weekly maintenance window	<p>Choose Select start time for 30-minute weekly maintenance window and specify the start time of the maintenance window.</p> <div style="border: 1px solid #ccc; background-color: #f9e79f; padding: 10px; margin-top: 10px;">  <p>Specify the start time so that the maintenance window does not overlap with your XProtect system archiving schedule.</p> </div>

Tags

Add tags that follows your tagging strategy.

Attach your FSx shares to XProtect

When you have created the FSx shares, you can attach them to the XProtect VMS using the DNS name and the share name as a path.

Get DNS name

You need the DNS name to add it as a share path in XProtect Management Client.

1. Go to <https://console.aws.amazon.com/fsx/> and select **File systems** from the left-hand panel.
2. On the **Network and Security** tab locate the **DNS name**. You can now connect your FSx share using the DNS name and the share name as a path in the format **\\amznfsx(xxxxxxxx).domain name\share**.

Example: \\amznfsxscrmjvvn.acme.com\share

Attach the FSx shares

To attach the FSx shares in XProtect Management Client:

1. Make sure that the AD user that runs the Recording Server service and XProtect system have the required permissions to access the share.
2. Attach the share to the EC2 instance that runs your XProtect system by adding the share path in the XProtect Management Client when you add your archive.

For more information about how to configure recording storage archiving and scheduling in XProtect Management Client, see [Storage tab \(recording server\)](#).

Removing XProtect

Delete the XProtect CloudFormation stack

To remove the XProtect CloudFormation stack and all of its contents:

1. Go to <https://console.aws.amazon.com/cloudformation/>.
2. Select the deployed CloudFormation stack - XProtect Essential+ or XProtect BYOL.
3. Select **Delete**, and in the confirmation dialog, select **Delete stack**.

Unsubscribe

To unsubscribe from the marketplace listing:

1. Go to <https://console.aws.amazon.com/marketplace/>
2. Select your XProtect marketplace listing - XProtect Essential+ or XProtect BYOL.
3. In the upper right-hand corner, select **Actions > Cancel subscription**.
4. In the **Cancel subscription** dialog box, select the **confirmation check box**, then select **Yes, cancel subscription**.

Only the services that are deployed as part of the XProtect CloudFormation stack are removed when you unsubscribe from the marketplace listing. Other services, such as EBS storage services or EC2 instances, are not removed, and you must delete or terminate these services separately. See [Delete the XProtect CloudFormation stack on page 33](#).



helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit <https://www.milestonesys.com/>.

