MAKE THE
WORLD SEE

Milestone Systems

XProtect® on AWS

Getting started guide - Bring Your Own License (BYOL) 2020 R3

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

Contents

Copyright, trademarks, and disclaimer

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 VMS helps you get started with your XProtect VMS deployment in your AWS infrastructure. The guide has checklists and tasks that help you deploy and configure your system and verify connections between server and clients.

It is recommended that you have a good understanding of application deployment in AWS VPC environments and know how to manage EC2 instances and storage as well as security and network services in the AWS Management Console. For more information about the competencies recommended by AWS, consult the AWS Learning Path Tool.

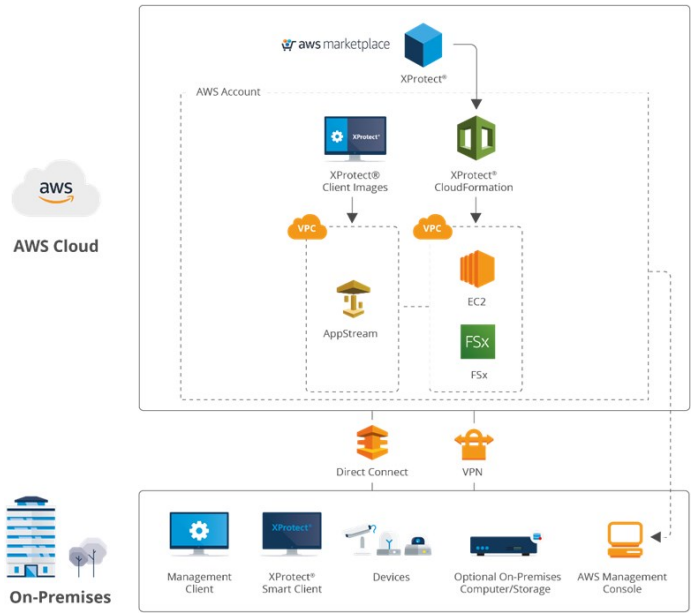
Introduction

Milestone Bring Your Own License (BYOL) 2020 R3 provides the XProtect software in an AWS CloudFormation template that you deploy as a stack in your AWS infrastructure. The CloudFormation stack contains an Amazon Elastic Compute Cloud (EC2) instance and an Amazon Virtual Private Cloud (VPC), which runs Windows Server 2019.

The BYOL model allows you to insert your XProtect license into the deployed XProtect VMS product as you would in a traditional on-premises environment.

If you have not yet purchased a license, get a license for your desired XProtect version from a Milestone distributor or reseller using the Milestone partner network.

The XProtect BYOL CloudFormation deploys all the XProtect VMS core components (including XProtect Smart Client and XProtect Management Client) on the operating system volume, alongside a local Microsoft SQL Server Express database that stores and maintains all the configuration, event data and system logs needed to run XProtect. Video recordings are stored on a separate Amazon Elastic Block Store (EBS) volume, which you can expand according to your usage.



AWS and third party services are priced independently of your Milestone XProtect license and should be considered when designing your VMS and network topology. Cost considerations for services used by the XProtect BYOL deployment include:

AWS service	Cost considerations
Computation	
EC2	Cost of the instance will vary based on the number of cameras in the system and their resolution and frame rate, as well as the degree of server-side motion detection.
Storage	
EBS	Cost is based on the size of the operating system volume and the media database volume.
Amazon FSx (optional)	Recommended for video archiving. Cost is based on storage type, throughput capacity, and backup storage.
Networking	
Site-to-Site VPN (optional)	Cost is calculated per VPN connection.

AWS service	Cost considerations
Direct Connect (optional)	Cost is based on port hours and capacity.
Client Access	
VPC	Cost is based on the type of operation and data egress.
Amazon AppStream 2.0 (optional)	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 extend the deployment architecture according to your usage through added AWS and third-party services.

Costs associated with AWS services also vary according to your region. For more information about how AWS charges for usage and services used by XProtect on AWS, see the XProtect on AWS Pricing Calculator.

This guide explains how to deploy and use the XProtect BYOL CloudFormation and is divided as follows:

- Overview – Information about this guide and an introduction to XProtect BYOL
- Requirements and considerations – Prerequisites for deploying the XProtect BYOL CloudFormation template and a deployment checklist
- Deployment – An explanation of the XProtect BYOL CloudFormation template configuration parameters and how to connect to your deployment
- After you deploy – Important steps to take after you have connected, including adding your license and securing your deployment
- Expanding your deployment – How to scale your deployment and optimize access to your VMS
- Unsubscribe – How to unsubscribe from XProtect BYOL

It is recommended that you have a good understanding of application deployment in AWS VPC environments and know how to manage EC2 instances and storage as well as security and network services in the AWS Management Console. For more information about the competencies recommended by AWS, consult the AWS Learning Path Tool.

Requirements and considerations

Getting started checklist

Follow the checklist to make sure that you carry out the steps of your XProtect BYOL deployment and configuration in the correct order. Each step is detailed in the later sections of this guide.

☐	AWS deployment prerequisites	• Have an AWS account • Have a key pair
☐	XProtect VMS prerequisites	• Obtain your software license (.lic) file and register your XProtect Software License Code (SLC) • Optional: Prepare a name for the EC2 instance • Make sure your camera models and firmware are supported by the XProtect system • Assign static IP addresses or make DHCP reservations to all cameras and devices • Network bandwidth consumption • Virus scanning (explained)
☐	Configuration and deployment	• Subscribe to XProtect BYOL in AWS Marketplace • Configure and deploy the XProtect BYOL CloudFormation template
☐	Connecting to your deployment via RDP	• Connect via Remote Desktop Protocol • Change the Windows administrator account password of your EC2 instance
☐	Connecting your on-premises network	• Configure AWS VPN end points • Configure site-to-site VPN end points • Configure on-premises VPN end points • Configure and join the on-premises domain
☐	Adding your XProtect license	• Add your XProtect product license

		• Activate your XProtect license
☐	Securing your deployment	• Install Windows updates • Download the latest XProtect Device Pack • Optional: Install Nvidia drivers for hardware acceleration
☐	Scaling your system	• System scaling considerations • Define storage for archiving • Use Amazon FSx to create storage drives
☐	Optimizing client access	• Adaptive Streaming in XProtect • Running XProtect Smart Client in Amazon AppStream 2.0

Before you start deployment

Before you deploy the XProtect BYOL CloudFormation, you must meet the following AWS deployment prerequisites and XProtect VMS prerequisites.

It is highly recommended that you consult the Milestone Cloud Solutions training track for interactive courses that cover Milestone cloud fundamentals, as well as XProtect on AWS design and deployment.

AWS deployment prerequisites

Have an AWS account

You must create or use an existing AWS account with the necessary permissions.

It is not recommended to use root user credentials to manage or deploy your AWS infrastructure.

If you are an AWS Identity and Access Management (IAM) user, then you have the necessary permissions by default. However, you might need to contact your IT department for account access settings depending on the network infrastructure of your organization.

Have a key pair

To connect to the EC2 instance, you must create or use an existing key pair.

For information about how to create a key pair in the EC2 console or to import your own public key, see Create a key pair using Amazon EC2.

XProtect VMS prerequisites

Obtain a software license (.lic) file and register your XProtect Software License Code (SLC)

XProtect BYOL requires a software license (.lic) file and associated Software License Code (SLC), which must be registered in Milestone Customer Dashboard.

If you have not yet purchased a license, get a license for your desired XProtect version from a Milestone distributor or reseller using the Milestone partner network.

Register your SLC in Milestone Customer Dashboard:

1. Log in to Milestone Customer Dashboard.
2. Register software license codes (SLCs) in Milestone Customer Dashboard.

For more information about how to get your software license (.lic) if you have previously registered your SLC, see Get a software license (.lic) file in Milestone Customer Dashboard.

Prepare an EC2 instance hostname

To connect your XProtect BYOL deployment to your on-premises infrastructure, prepare a name for your EC2 instance that will also act as a Windows Active Directory (AD) hostname and domain name in your network topology. The name of the EC2 instance is entered into the **Instance Hostname** field when you deploy the XProtect BYOL CloudFormation.

If you do not plan to include your deployment to an existing network topology, it is still important to consider a valid EC2 **Instance Hostname** as XProtect VMS does not support changing the hostname after deployment.

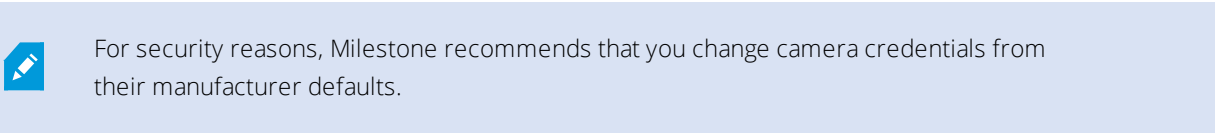
For more information about AD naming conventions and character limits, see Naming conventions in Active Directory.

Prepare cameras and devices

Make sure camera models and firmware are supported by the XProtect system.

On the Milestone website, you can find a detailed list of supported devices and firmware versions (https://www.milestonesys.com/supported-devices/). Milestone develops unique drivers for devices or device families, and generic drivers for devices based on standards like ONVIF, or devices that use the RTSP/RTP protocols.

Some devices that use a generic driver and that are not specifically listed as supported may work, but Milestone does not provide support for such devices.



For security reasons, Milestone recommends that you change camera credentials from their manufacturer defaults.

Assign static IP addresses or make DHCP reservations to all cameras and devices.

See the camera's documentation for information about network configuration. If your system is configured with default port settings, you must connect the camera to HTTP port 80. You can also choose to change the default port settings.

Network bandwidth consumption

To make sure that sufficient bandwidth is available on your network, you must understand how and when the system consumes bandwidth. The main load on your network consists of three elements:

- Camera video streams
- Clients displaying video
- Archiving of recorded video

The recording server retrieves video streams from the cameras, which results in a constant load on the network. Clients that display video consume network bandwidth. If there are no changes in the content of the client views, the load is constant. Changes in view content, video search, or playback, make the load dynamic.

Archiving of recorded video is an optional feature that lets the system move recordings to a network storage if there is not enough space in the internal storage system of the computer. This is a scheduled job that you have to define. Typically, you archive to a network drive which makes it a scheduled dynamic load on the network.

Your network must have bandwidth headroom to cope with these peaks in the traffic. This enhances the system responsiveness and general user experience.

Virus scanning (explained)

The XProtect software contains a database and as with any other database you need to exclude certain files and folders from virus scanning. Without implementing these exceptions, virus scanning uses a considerable amount of system resources. On top of that, the scanning process can temporarily lock files, which could result in a

disruption in the recording process or even corruption of databases.

When you need to perform virus scanning, do not scan recording server folders that contain recording databases (by default C:\mediadatabase\, as well as all subfolders). Also, avoid performing virus scanning on archive storage directories.

Create the following additional exclusions:

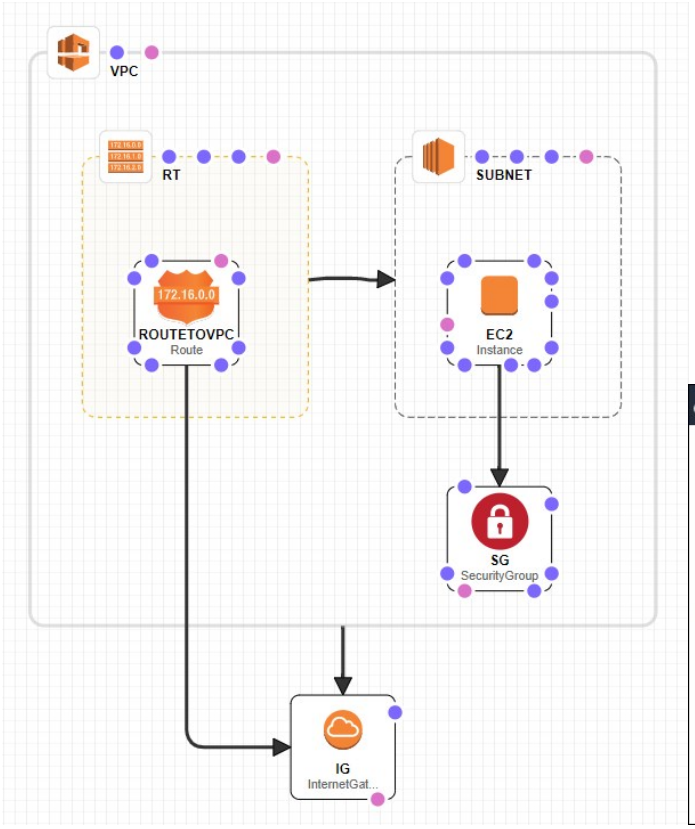
- File types: .blk, .idx, .pic
- Folders and subfolders:
    - C:\Program Files\Milestone
    - C:\Program Files (x86)\Milestone
    - C:\ProgramData\Milestone

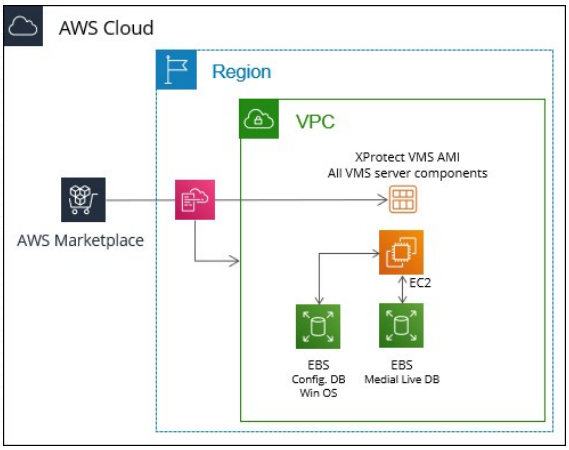
Your organization may have strict guidelines regarding virus scanning, but it is important that you exclude the above folders and files from virus scanning.

Deployment

Configuration and deployment

The XProtect BYOL CloudFormation stack includes a Virtual Private Cloud (VPC) and the required AWS services to create a cloud-based VMS deployment. The XProtect BYOL CloudFormation template uses a custom Amazon Machine Image (AMI) to configure and deploy the XProtect VMS software on a Elastic Compute Cloud (EC2) instance.





The XProtect BYOL CloudFormation template deploys two Elastic Block Storage (EBS) volumes. The first volume contains the Windows Server 2019 operating system, the XProtect VMS software, and Microsoft SQL Server Express database that contains VMS logs and configuration entries. The second volume contains a live media database for your video recordings. Both volumes use the gp2 EBS volume type to meet the storage performance and redundancy level that your XProtect system requires.

Operating System volume (Disk 0)	Media Database volume (Disk 1)
Windows operating system	XProtect Media database
XProtect software	Database optimized for recording and storing audio and video data from your connected cameras and devices (recordings) The default video recording retention time (1 week) can be increased in Management Client after deployment
Microsoft SQL Server Express database Holds the XProtect configuration, logs and events	For optimal performance, Milestone recommends that you set video retention to one day and use FSx for archive storage. For more information, see system scaling.

Elastic Block Store (EBS) considerations:

- The XProtect BYOL CloudFormation deploys the EBS gp2 storages with the volume sizes configured before deployment
- Volume sizes can be increased but not reduced
- Milestone recommends that the media volume size be configured to hold a minimum of 24 hours of video recordings
- The size of disk 0 holding the Microsoft SQL Server Express should be increased above the default size if you have a large number of connected cameras or users
- Volume performance tuning is possible
- Redundancy is available at disk level within your availability zone (AZ)

You can change volume types, tune performance, or increase volume size as needed by your XProtect system. For more information about EBS, see Amazon Elastic Block Store (EBS).

If you meet the prerequisites then you are ready to configure and deploy the XProtect BYOL CloudFormation template.

Subscribe

To deploy the XProtect BYOL CloudFormation, you must first subscribe to XProtect BYOL in AWS Marketplace:

1. Go to the **XProtect Bring Your Own License (BYOL) 2020 R3** marketplace listing.
2. In the upper right-hand corner, select **Continue to Subscribe**.
3. Read the Terms and Conditions and in the upper right-hand corner, select **Continue to Configuration**.
4. In the **Region** dropdown list, select your region. In the upper right-hand corner, select **Continue to Launch**.
5. In the lower right-hand corner, select **Launch** to open the AWS CloudFormation console.

Configure and deploy

After you have subscribed, configure and deploy the XProtect BYOL CloudFormation template using the following steps:

Parameter	Description
XProtect configuration	
XProtect language	The display language of the installed XProtect products. For more information about XProtect supported languages, see Milestone products supported languages.
Retention time	The number of days video recordings are saved for in the media database. If you increase the **Retention time** from the default value of 7 days, then you should also increase the EBS **Media volume size** accordingly.
Elastic Compute Cloud (EC2) configuration	
Instance type	The size and type of the EC2 instance. Milestone recommends the following instance types depending on the number of cameras in your installation:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>EC2 instance type</th><th>Recommended maximum number of cameras

(10% video recordings with 1080p resolution at 30FPS)</th></tr>
<tr><td>c5.large</td><td>18</td></tr>
<tr><td>c5.xlarge</td><td>40</td></tr>
<tr><td>c5.2xlarge</td><td>96</td></tr>
<tr><td>g4dn.xlarge*</td><td>113</td></tr>
<tr><td>g4dn.2xlarge*</td><td>275</td></tr>
<tr><td>g4dn.4xlarge*</td><td>480</td></tr>
<tr><td colspan="2">*Requires the manual installation of Nvidia drivers for hardware acceleration after deployment</td></tr>
</table>


If the template fails to deploy due to the selected Instance type, restart deployment and select a different Availability zone below.


For more information about choosing the proper EC2 instance type, see the XProtect on AWS White Paper.
</td></tr>
<tr><td>Operating system volume size</td><td>The size in GB of the Elastic Block Storage (EBS) volume that contains all VMS components except for the media database used to store video recordings. After deployment, you can expand the EBS volume size as needed.</td></tr>
</table>

Parameter	Description
	 You cannot reduce the size of EBS volumes from the initially set value.
Delete operating system volume	Whether the operating system volume should be deleted if you terminate the EC2 instance.  Terminating the EC2 instance or deleting the EBS operating system volume does not unsubscribe you from XProtect BYOL. For more information, see Unsubscribe.
Media volume size	The size in GB of the EBS volume that contains the media database used to store video recordings. After deployment, you can expand the EBS volume size as needed.  You cannot reduce the size of EBS volumes from the initially set value.  Milestone recommends that the media volume size is configured to hold a minimum of 24 hours of video recordings using archive storage after deployment.
Delete media volume	Whether the media database volume should be deleted if you terminate the EC2 instance.  Terminating the EC2 instance or deleting the EBS media volume does not unsubscribe you from XProtect BYOL. For more information, see Unsubscribe.
Key pair name	The key pair used to decrypt the Remote Desktop Protocol (RDP) Windows login password and access your Virtual Private Cloud (VPC). For more information about key pairs, see Create a key pair using Amazon EC2.

Parameter	Description
Instance hostname	An optional custom name that you specify for the EC2 instance to find it in your network environment. The hostname cannot be longer than 15 characters and cannot contain symbols or spaces. Leave this field blank for a randomly assigned instance name. ⚠ You cannot change the **Instance hostname** after deployment.
Network configuration	
Availability zone	The AWS availability zone within your selected region that the EC2 instance deploys in. ⚠ If the script fails to deploy due to the selected **Instance type**, restart deployment and select a different **Availability zone**.
RDP ingress CIDR block	The range of inbound IP addresses that will access the VPC using RDP.
VPC CIDR block	The range of IP addresses that create the virtual network of the VPC.
Subnet CIDR block	The range of IP addresses that create the subnet of the VPC.

✎ Deploying the XProtect BYOL CloudFormation stack takes about 20 minutes.

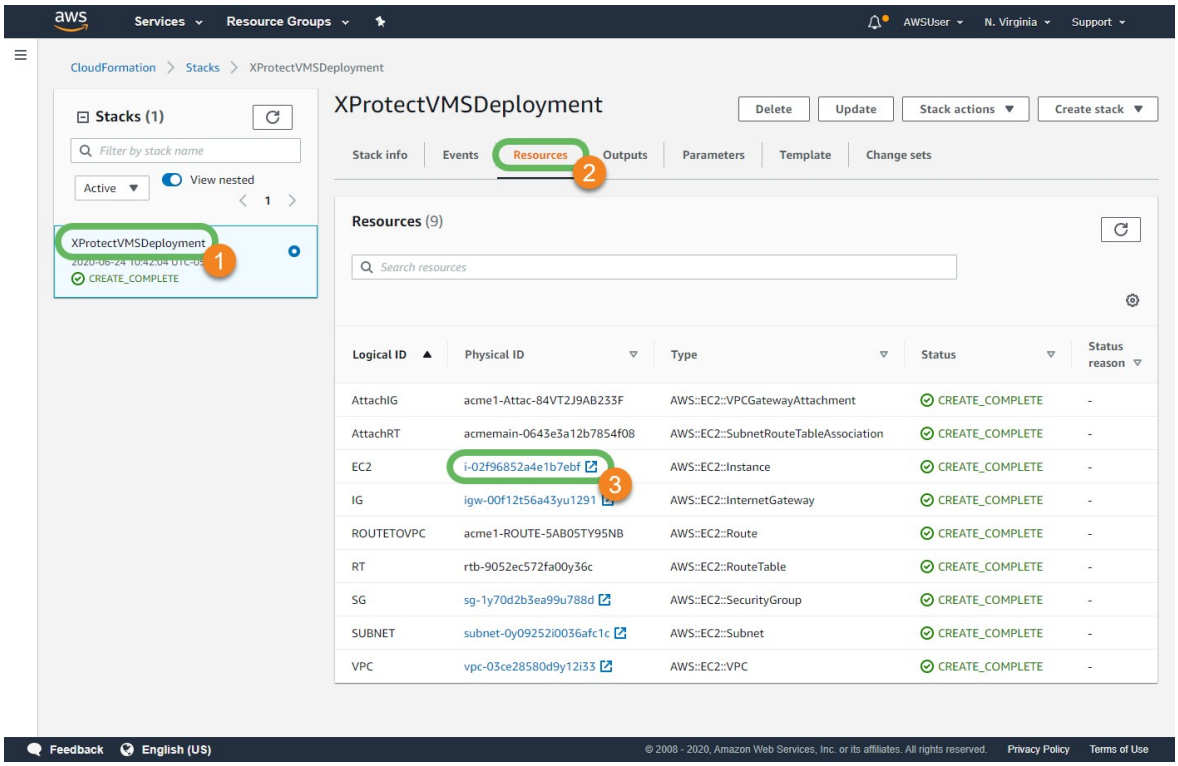
Connect to your deployment

After you deploy the XProtect BYOL CloudFormation stack, you can connect to the EC2 instance using the Remote Desktop Protocol (RDP) key pair that you specified during configuration.

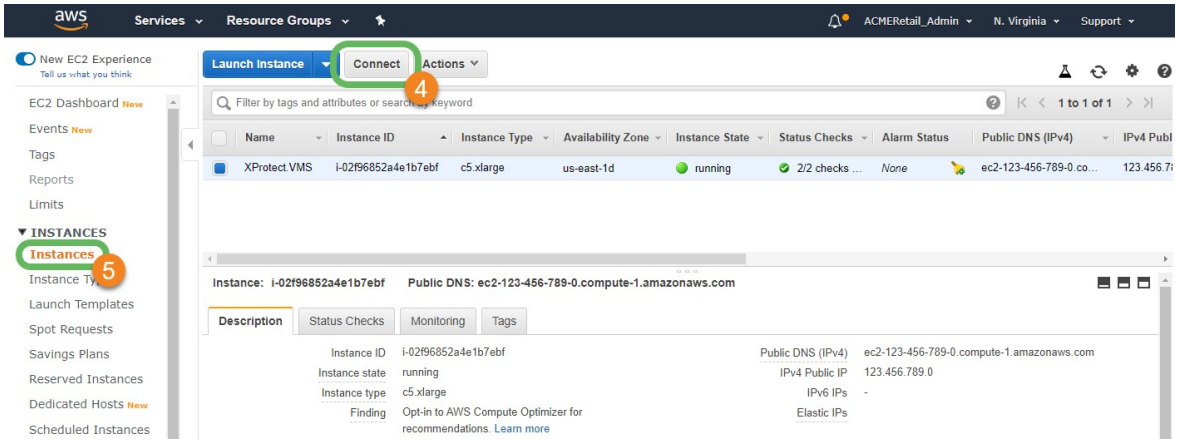
Access the EC2 instance that you created via RDP:

1. In the AWS Management Console, open the **CloudFormation** page.
2. Select the XProtect BYOL CloudFormation stack that you created. It is identified by the **Stack name**❶ that you specified during configuration.

3. In the **Resources** ❷ tab, you will see all the stack elements that were created by the XProtect BYOL CloudFormation template. Select the **Physical ID** ❸ link that corresponds to the EC2 instance.



4. At the top of the EC2 **Instances** ❺ page, select **Connect** ❹.



5. Select **Get Password**.
6. The **Key Name** shows the name of the key pair that you specified during configuration. To associate the key pair with the Key Pair name, select **Choose File** and locate the key pair file on your local machine.
7. Select **Decrypt Password** to view the password for the RDP connection.
8. Select **Back** to return to the previous screen, then select **Download Remote Desktop File**.

9. Open the downloaded .rdp file and select **Connect** on any identification warnings that may appear.
10. Enter the password that you decrypted in step 7 and select **Connect**.

You are now connected to the EC2 instance, which is running XProtect. It is recommended that you change the password of your EC2 instance for added security.

> If you have problems connecting, make sure that the IP address that you are accessing the EC2 instance from is part of the **RDP Ingress CIDR Block** that you specified during configuration.

Connect your on-premises network

If you meet the XProtect VMS prerequisites, you are ready to connect to your on-premises network. There are many AWS and 3rd party network services that connect the deployed VPC to your network topology.

> Possible deployment scenarios are discussed in the XProtect on AWS White Paper. Deployment scenarios depend on the specifics of your organization's network infrastructure. It is highly recommended that you consult your organization's IT department or network topology consultant.

AWS has services that securely connect your on-premises network or branch office site to your VPC. The most common services are:

- Site-to-Site VPN
- Transit Gateway
- Direct Connect

These services allow full connectivity to on-premises cameras, devices, recording servers, and Active Directory.

Site-to-Site VPN considerations:

- Connectivity to one VPC
- Best suited for simpler deployments
- Requires special configuration of your router

> AWS provides a list of tested devices but other devices may be compatible. For more information about compatible gateway devices, see Your customer gateway device on AWS.

Transit Gateway Considerations:

- Acts as a centralized managed connectivity hub between VPCs and VPN connections for advanced routing
- Connectivity to multiple VPCs
- Connectivity to multiple VPNs
- Best suited for advanced XProtect deployments with multiple distributed sites

> If you are an existing AWS customer, you likely have a Transit Gateway infrastructure in place. For more information about the AWS Transit Gateway service, see AWS Transit Gateway.

> 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.

Direct Connect considerations:

- A dedicated network connection between your network and one of the AWS Direct Connect locations
- Private virtual interface from your on-premises network directly to your VPC
- Does not rely on Internet Service Provider (ISP) availability
- Scalable high bandwidth connections for heavy network loads and low latency
- Best suited for large enterprises using AWS infrastructure and services
- Limited availability

> For more information on the AWS Direct Connect service, see AWS Direct Connect features.

After you deploy

Adding your XProtect license

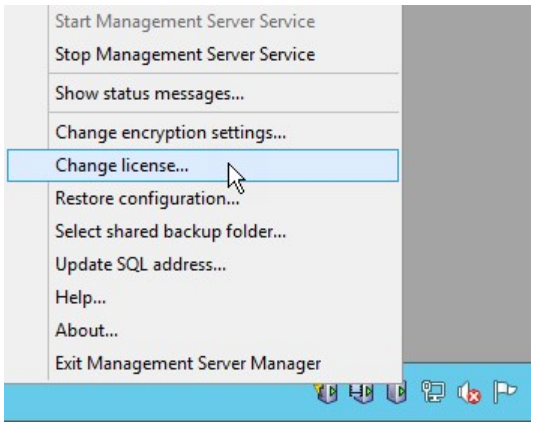
After you deploy, you are ready to add the software license (.lic) file to your deployment and activate your license. Before you continue, make sure to obtain a software license (.lic) file and register your XProtect Software License Code (SLC) as described in the prerequisites.

> ⚠ If you have not yet purchased a license, get a license for your desired XProtect version from a Milestone distributor or reseller using the Milestone partner network.

Add your XProtect license

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 notification area of the Windows task bar (also known as the system tray), right-click on the **Management Server tray icon**.
3. Select **Change license** in the pop-up menu.



4. In the Milestone XProtect Management Server **Change License** window, select **Import License**.
5. Locate the license that you copied in step 1 and select **Open**.
6. 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.

Activate your XProtect license

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

- By default your deployment is connected to the internet. Use online license activation to activate your license
- Alternatively, if you have restricted internet connectivity, use offline license activation to activate your license

For more information about activating your license in Milestone Customer Dashboard, see Activating licenses.

Securing your deployment

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

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.

Technical support for XProtect BYOL is provided by the Milestone channel partner through whom the XProtect VMS software license is obtained. In addition, Milestone Support provides a wide set of self-service and support resources to end-users.

Install Windows updates

Install relevant Windows updates according to the security policy of your organization. If you restrict online connectivity to your deployment, you can connect your deployment to a Windows update service without exposing the VPC to the internet.

Update your XProtect license and Milestone Care™ coverage

Using Milestone Customer Dashboard (online.milestonesys.com), you can update your XProtect license and monitor the status of your Milestone Care™ coverage, and set up automated email notifications for when an update is available or when your Milestone Care™ coverage is about to expire.

Milestone Customer Dashboard is a web service that is independent of your XProtect VMS installation's internet connectivity. Depending on your configuration, Milestone Customer Dashboard can also monitor the status of your installation and report any errors that occur. For more information, see the user manual for Milestone Customer Dashboard.

Change the password of your EC2 instance

After deployment, change the Windows administrator password of your EC2 instance according to the security policy of your organization.

Download the XProtect® Device Pack

A device pack is a set of drivers that is installed with your XProtect system to interact with your devices. Device packs are installed on the recording server. Milestone adds support for new devices and firmware versions on an ongoing basis, and releases device packs every two months on average. A device pack is automatically included when you install the XProtect system.

To get the latest device pack after installation, go to the download section of the Milestone website (https://www.milestonesys.com/downloads/) and download the relevant installation file.

If your system uses very old cameras, you may need to download the device pack for legacy devices. For more information, see XProtect Device Packs.

Install Nvidia drivers for hardware acceleration

If you deploy or upgrade to a GPU-enabled EC2 instance, install the compatible Nvidia Tesla T4 driver to take advantage of hardware acceleration in your deployment.

To get the latest Nvidia Tesla T4 driver, see Installing NVIDIA drivers on Windows instances. Make sure to regularly check for driver updates on the Nvidia driver download page to get the latest stability and performance enhancements for your GPU-enabled EC2 instance.

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.

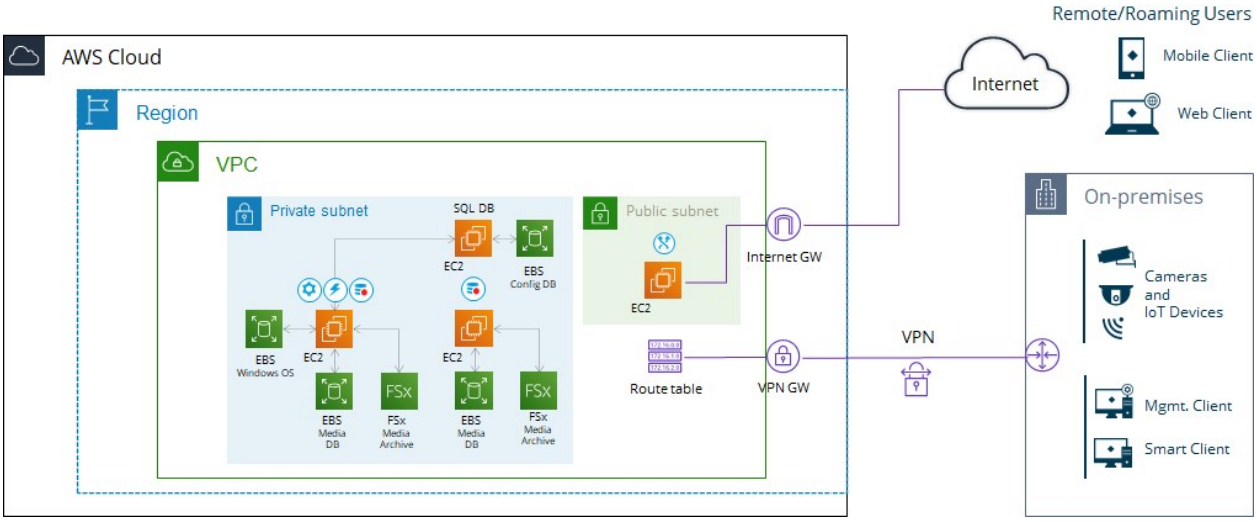
Hardware-accelerated video motion detection is available only for XProtect Expert and XProtect Corporate. For more information about the different XProtect VMS versions, see the Milestone product index page.

Expanding your deployment

System scaling (explained)

By default, the XProtect BYOL CloudFormation deploys all server components on a single EC2 instance. The AWS cloud infrastructure allows you to 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.



Depending on your hardware and configuration, systems with up to 10-20 cameras can run on a smaller EC2 instance type, while larger recommended instances can support up to 480 cameras. For systems with more than 480 cameras, Milestone recommends that you use second-level scaling of dedicated instances and storages 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. For more information about how to expand and connect to your on-premises environment, see Connect your on-premises network on page 20.

XProtect archiving

In deployments where video recordings are retained for longer than a few days, Milestone recommends using the XProtect archiving feature that moves recordings that are older than a specified threshold to a more cost-effective storage option. Archiving reduces the required size of the media database volume (disk 1) that hold your recordings, and it facilitates a cost reduction due to the reduced capacity requirement of the EBS gp2 storage.

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

Retention times and media storage dimensioning

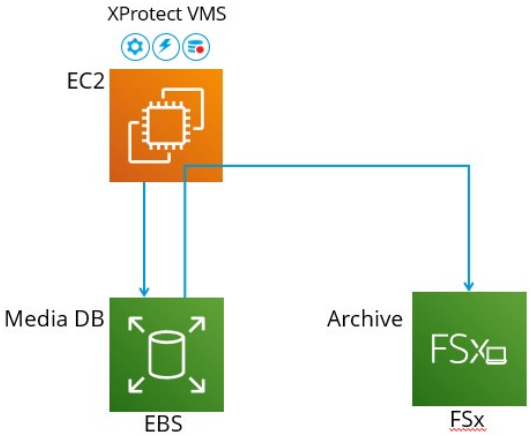
In these recommendations the retention time definition of a week can vary due to your specific system requirements. For more information about media storage dimensioning, see the XProtect on AWS White Paper.

For retention times shorter than 1 week

- Make sure that the capacity of the EBS gp2 storage (disk 1) can hold your recordings for a minimum of 1 day
- Consider defining a third EBS st1 type volume for archiving

For retention times longer than 1 week

- Make sure that the capacity of the EBS gp2 storage (disk 1) can hold your recordings for a minimum of 1 day
- Use FSx for Windows File Server storage for archiving



Besides the recommended EBS storage option, there are alternatives to XProtect archiving in an AWS deployment that is not connected to a domain. The alternative storage options are not described in this guide.

Archiving to FSx for Windows File Server storage

Milestone recommends archiving to FSx for Windows File Server storage. This type of share will deliver the archiving storage performance and redundancy level that your XProtect system requires.

If you have retention times shorter than 1 week, you may need to allocate more FSx storage capacity than needed to secure a sufficient IOPS baseline. For more information about IOPS and media storage dimensioning, see the XProtect on AWS White Paper.

FSx for Windows File Server considerations:

- Share size is defined in steps of 1 GiB with a minimum size of 2 TiB and maximum size of 64 TiB
- Redundancy by replication to multiple availability zones (AZ)
- Integrates with Microsoft Active Directory
- Requires AD user service account running the recording server to be used
- 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.

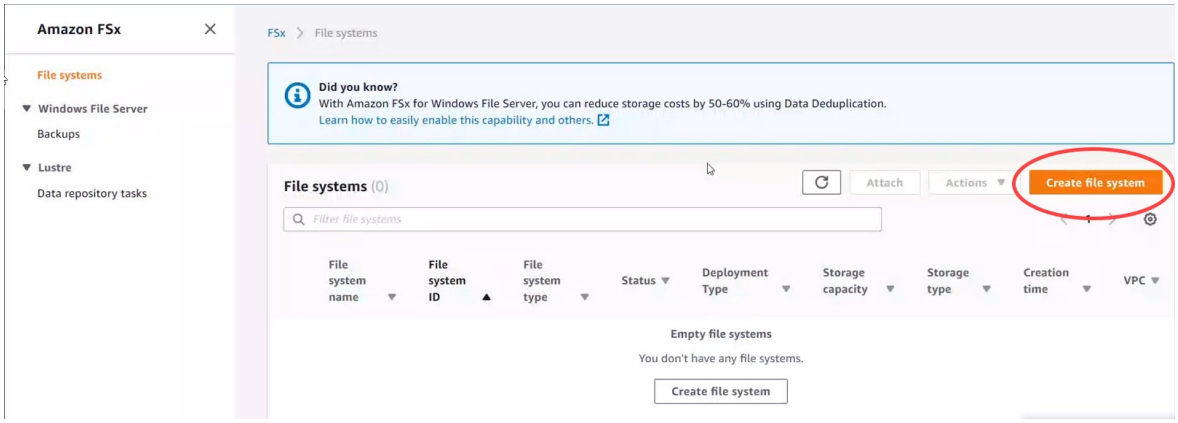
When scheduling XProtect archiving times, make sure the archiving job does not overlap with the AWS FSx half-hour weekly service window or configure the size of disk 1 to accommodate possible postponed archiving when configured in a single availability zone.

For more information on FSx for Windows file server, see Amazon FSx for Windows File Server.

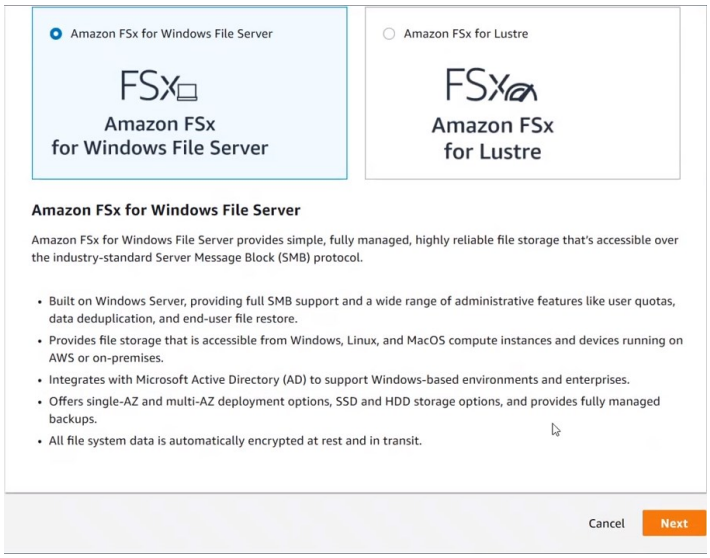
How to create FSx shares

Log in and start creation

1. Log in to the AWS Management Console and locate the Amazon FSx file system. Select **Create file system**.

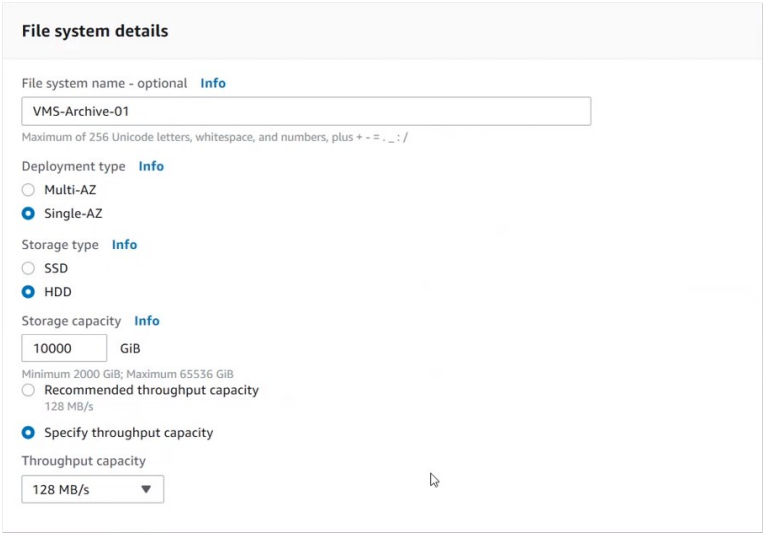


2. Select **Amazon FSx for Windows File Server** and select **Next**.



Specify file system details

1. File system name: Specify a name for use in the AWS Management console.



2. Deployment type: Select Availability Zone (AZ). **Single-AZ** or **Multi-AZ** for redundancy.

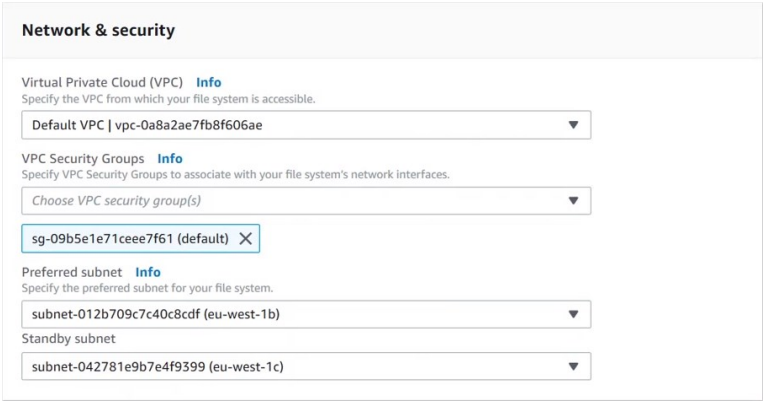
> **Single-AZ** has a 30-minute weekly maintenance window that you can schedule as you prefer.

3. Storage type: Milestone recommends selecting **HDD** storage type for archiving.
4. Storage capacity: Specify the size of your FSx share.
5. Throughput capacity: Select **Specify** to meet your throughput requirements.

> When selecting a higher throughput capacity you increase the cost of running your FSx share.

Specify Network and Security

1. Virtual Private Cloud (VPC): Select the VPC where your EC2 instance running your XProtect system is deployed.



2. VPC Security Groups: Specify VPC Security Groups to associate with your file system's network interface.

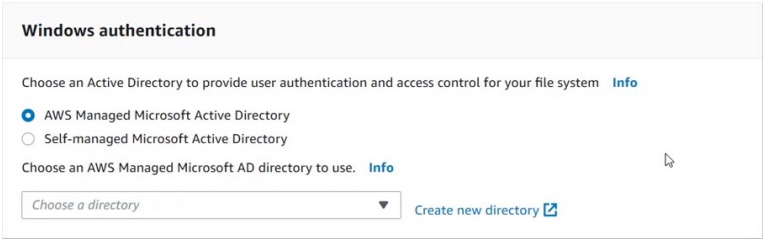
> Make sure to add the relevant ports used in AWS for SMBv3 to your VPC Security Groups.

3. Preferred subnet: Select the same subnet as your EC2 instance running your XProtect system.
4. Standby subnet: Select a relevant standby subnet.

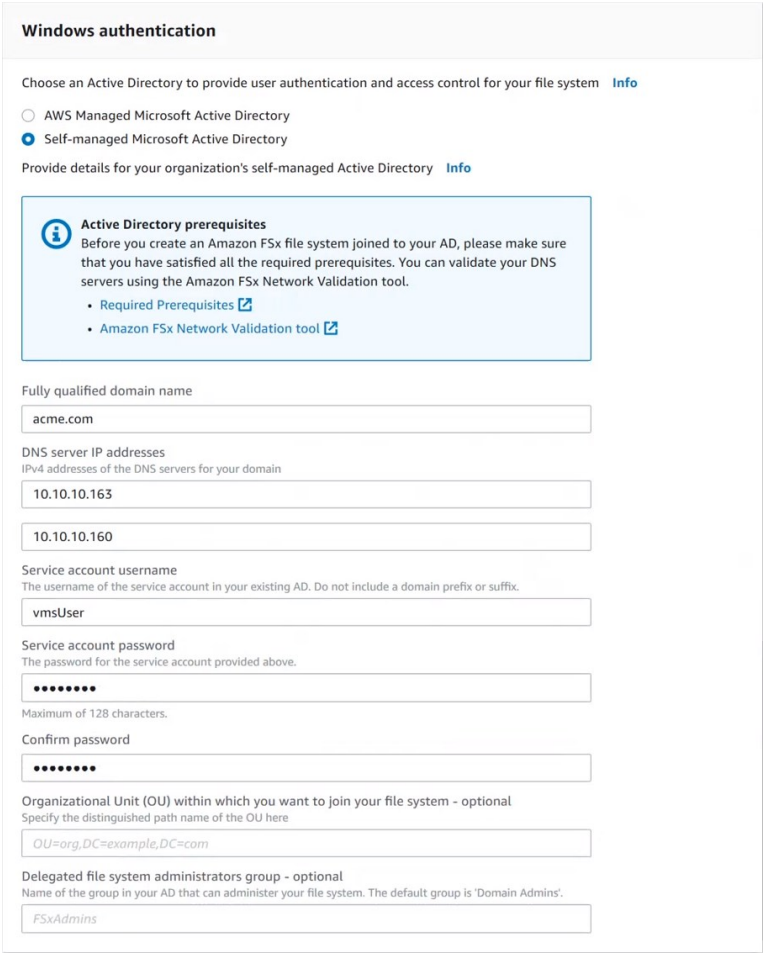
Windows authentication

Active Directory: Choose an **AWS Managed** or **Self-managed** Microsoft Active Directory to provide user authentication and access control for your file system.

A. For an **AWS Managed** Microsoft AD select a directory to use.



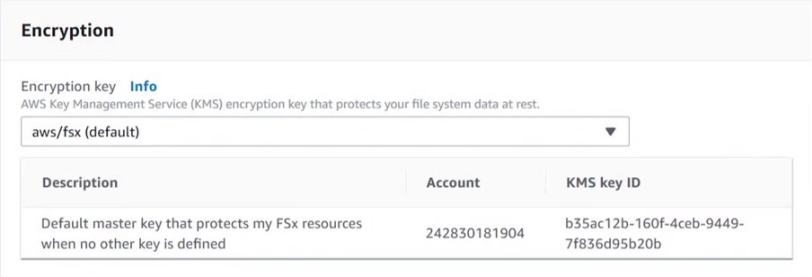
B. For a **Self-managed** Microsoft AD provide the details below:



1. Fully qualified domain name.
2. DNS server IP Addresses.
3. Service account username and password.

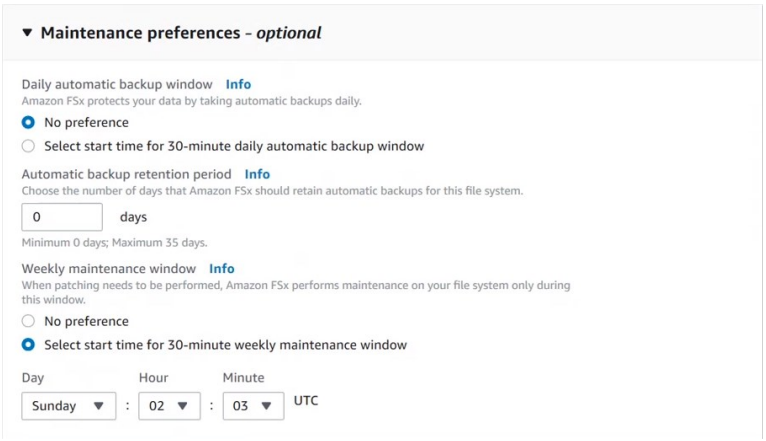
Encryption

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



Maintenance preferences

1. Daily automatic backup window: Select **No preference**.

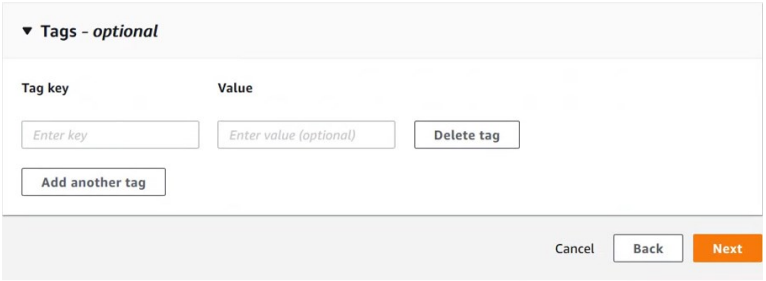


2. Automatic backup retention period: Set it to **0 days**.
3. Single-AZ weekly maintenance window: Choose **Select start time for 30-minute weekly maintenance window** and specify the start time of the maintenance window.

> Specify the start time so that the maintenance window does not overlap with your XProtect system archiving schedule.

Tags

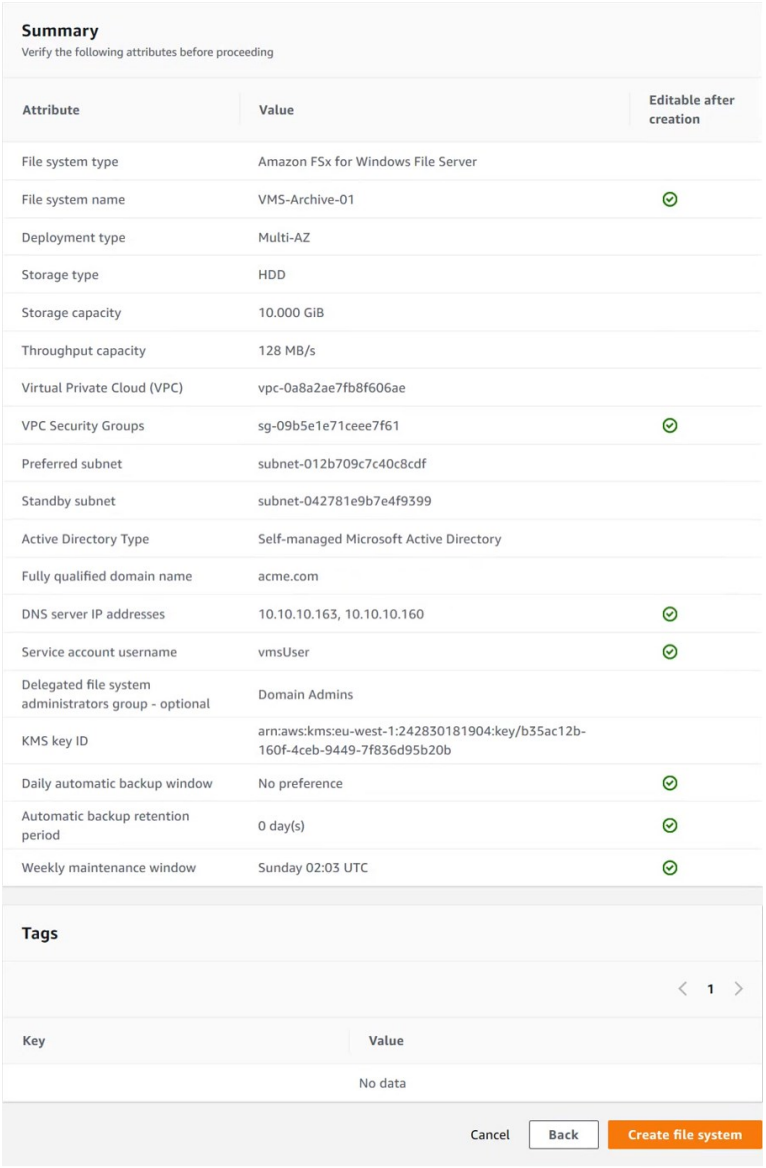
1. Add tags that follows your tagging strategy.



2. Select **Next**.

Summary

1. Verify your settings.



Summary

Verify the following attributes before proceeding

Attribute	Value	Editable after creation
File system type	Amazon FSx for Windows File Server	
File system name	VMS-Archive-01	✓
Deployment type	Multi-AZ	
Storage type	HDD	
Storage capacity	10.000 GiB	
Throughput capacity	128 MB/s	
Virtual Private Cloud (VPC)	vpc-0a8a2ae7fb8f606ae	
VPC Security Groups	sg-09b5e1e71ceee7f61	✓
Preferred subnet	subnet-012b709c7c40c8cdf	
Standby subnet	subnet-042781e9b7e4f9399	
Active Directory Type	Self-managed Microsoft Active Directory	
Fully qualified domain name	acme.com	
DNS server IP addresses	10.10.10.163, 10.10.10.160	✓
Service account username	vmsUser	✓
Delegated file system administrators group - optional	Domain Admins	
KMS key ID	arn:aws:kms:eu-west-1:242830181904:key/b35ac12b-160f-4ceb-9449-7f836d95b20b	
Daily automatic backup window	No preference	✓
Automatic backup retention period	0 day(s)	✓
Weekly maintenance window	Sunday 02:03 UTC	✓

Tags

< 1 >

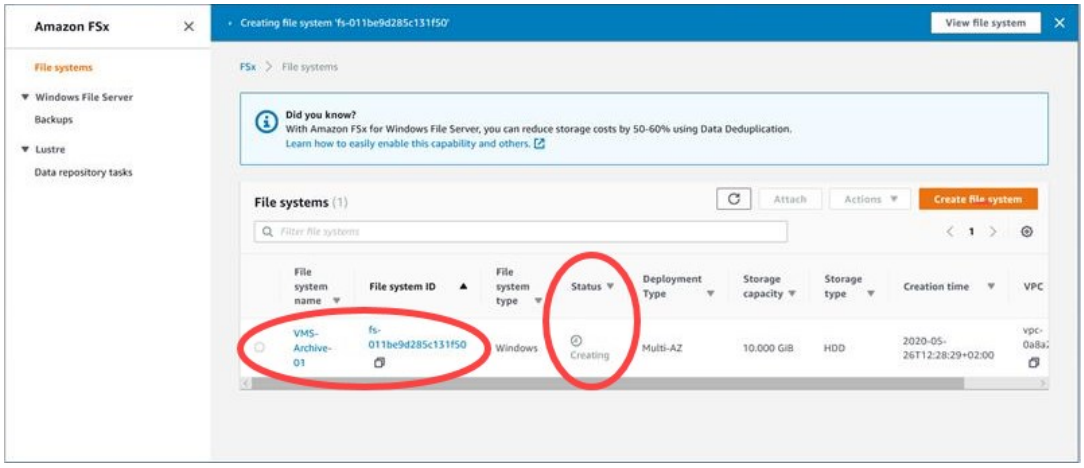
Key	Value
No data	

Cancel | Back | Create file system

2. Select **Create file system** to start the creation of your FSx share.

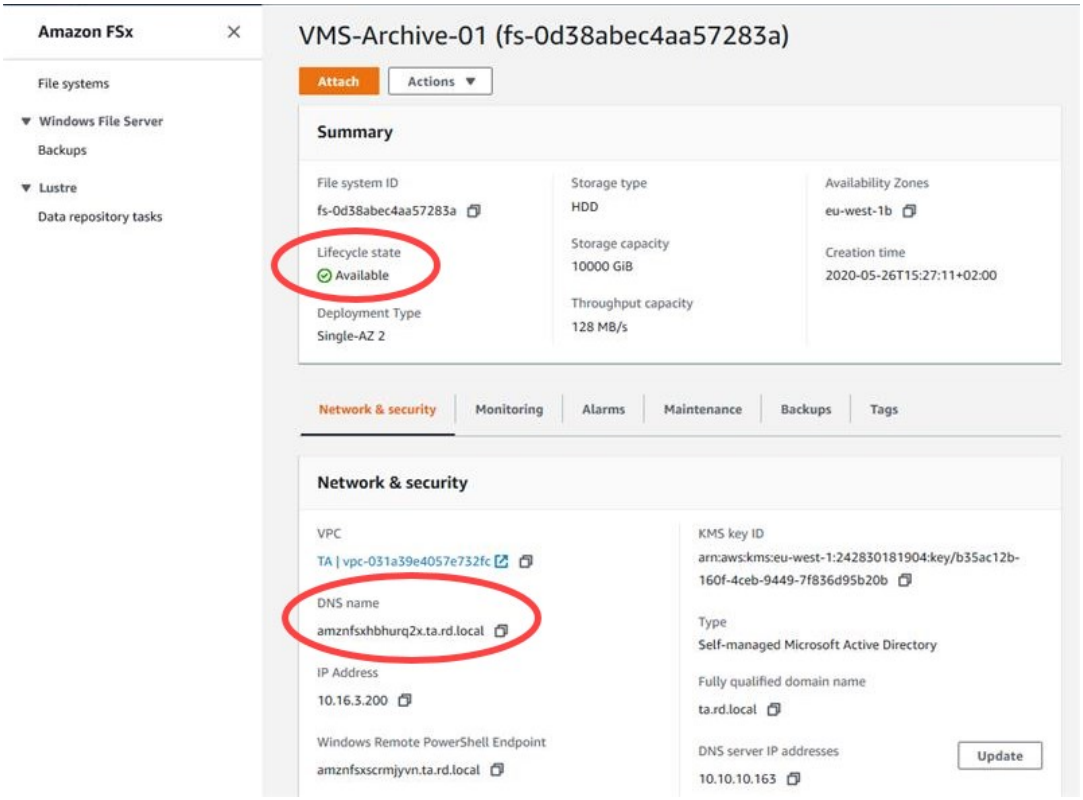
File systems

1. Your FSx share is created and you can follow the status. The expected creation time is 20-30 minutes.



2. When the status is **Available**, select the file system name to view the details.

3. 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 following format:

\\amznfsx(xxxxxxxx).domain name\share

Example: **\\amznfsxscrmjyvn.acme.com\share**

How to connect your FSx shares

In your Active Directory

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 adding your archive.

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

Adaptive Streaming

To optimize the Smart Client performance and reduce the AWS data egress costs, Milestone recommends the Adaptive Streaming feature available in XProtect Corporate and XProtect Expert. Adaptive Streaming enables Smart Client to automatically select the live video stream with the most optimal resolution. This reduces the amount of data transferred to and handled by Smart Client.

Consult the XProtect on AWS White Paper for performance test results of Smart Client using Adaptive Streaming. For more information, see Enabling adaptive streaming.

Amazon AppStream 2.0

As an alternative to running the XProtect client applications on your local workstation, AWS offers the possibility to run client applications as hosted user sessions in the AWS cloud using the Amazon AppStream 2.0 service. Users can access AppStream 2.0 hosted applications via HTTPS and a compatible web browser, or by using the AppStream 2.0 client application.

Depending on your VMS installation, AppStream 2.0 may be a more cost-effective solution as it includes AWS cloud egress data, 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?.

Consult the XProtect on AWS White Paper for performance test results of Smart Client execution on AppStream 2.0 as well as recommendations for suitable EC2 AppStream 2.0 Fleet instance types. For more information about AppStream 2.0, see Amazon AppStream 2.0.

Unsubscribe

Unsubscribe from XProtect BYOL

1. Delete the CloudFormation stack:
    1. In the AWS Management Console, open the CloudFormation service page.
    2. Select the deployed XProtect BYOL CloudFormation stack.
    3. Select **Delete**, and in the confirmation dialog, select **Delete stack**.
2. Unsubscribe from the marketplace listing:
    1. In the AWS Management Console, open the AWS Marketplace Subscriptions service page.
    2. Select the XProtect BYOLmarketplace listing.
    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**.

You are now unsubscribed from XProtect BYOL.

Any services that you deploy other than those deployed by the XProtect BYOL CloudFormation, such as EBS storage services or EC2 instances, will not be removed when you unsubscribe from the marketplace listing. You must delete or terminate these services separately.

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/.