Milestone Technical Configuration Level 2

Training workshop agenda

Note: This can either be an in-person or online class. For our online class, see the list of Technical Requirements on page 2 below.

Target audience

Milestone Certified Integration Technicians (MCITs) who are responsible for installing and configuring advanced features in high-complexity, video surveillance systems are encouraged to attend this workshop.

Workshop description

In the Technical Configuration Level 2 training workshop, you are introduced to real-life scenarios that use advanced features of the XProtect® Corporate VMS.

During this workshop, participants work to expand existing XProtect Corporate VMS configurations by accommodating customer business needs. New requirements and requests introduce layers of complexity into the surveillance installations and increase participants' skills in handling challenging scenarios.

Attending this workshop helps prepare you to take the Milestone Certified Integration Engineer (MCIE) online assessment.

The course duration is three full working days, 9 am to 5 pm, with a total seat time of 18 hours.

Workshop format

Along with a series of hands-on exercises that address realistic scenarios, you will receive step-by-step instructions to install, configure, and demonstrate advanced features that expand on an existing installation.

You will leave with all of the exercises used during this class as well as the full presentation used in the classroom to help transfer your knowledge to the field.

Prerequisites

To be successful in this workshop, you should first complete the Milestone Technical Configuration Level 1 workshop, and it is **REQUIRED** that you currently hold a Milestone Certified Integration Technician (MCIT) certification.

To further prepare for the prerequisite MCIT, in the Milestone Partner Learning Portal, access the Role-Specific Learning Paths and enroll in the Integration Technican learning path to take eLearning courses specific to this role.

Please note, it is not required to attend a workshop or complete a learning track before taking a certification assessment.

Workshop materials

You will receive the following downloadable materials in class:

- Milestone Technical Configuration Level 2 Lab Manual
- Milestone Technical Configuration Level 2 Presentation

Technical requirements

To maximize the learning experience, you should meet the following technical requirements:

- Internet access
- 1Mbit/s available download and upload bandwidth
- Internet latency of 900 or less (700 or less is recommended; see details below)
- Headset or speakers (microphone not required)
- 17-inch monitor or larger
- Internet browser

Browser: The Firefox browser is NOT supported. Please use another browser such as Chrome or Edge.

To check your internet latency:

- Launch this test lab: https://labondemand.com/Launch/122B02AA.
- Hover your mouse pointer over the data bars at the top of the lab window.
- A latency of 700 or less is recommended for online classes.
- A latency of 700-900 will have slow interactions with the online labs. We recommend finding an alternative internet connection for a better workshop experience.
- A latency of 900 or more does not meet the requirements. The online labs will be slow to respond and disrupt your learning. Find an alternative internet connection.

To check your connection to the Adobe Connect classroom:

- Go to https://milestonesys.adobeconnect.com/common/help/en/support/meeting_test.htm.
- Select Run Diagnostic Test.

Agenda (3 days)

Day 1:

Prepare the network and Management Servers for failover clustering
Install Management Servers and configure failover cluster
Install clients and recording servers
Add hardware via scripting and configure recording server failover

Day 2:

Perform advanced device configuration
Implement advanced role-based security
Create a Smart Client startup script
Configure advanced system behaviors

Day 3:

Unify primary and remote sites using Milestone Federated Architecture (MFA)
Perform VMS maintenance

Hands-on exercises

Scenario: You are an Integration Engineer with the responsibility of installing and configuring Milestone XProtect VMS for your customer, Larsen Warehouse.

PREPARE THE NETWORK AND MANAGEMENT SERVERS FOR FAILOVER CLUSTERING

- Verify the class materials in the fileshare
- Tour and validate the existing topology, user accounts, and network domain connections
- Configure SQL server sysadmin permissions for the XProtect Admins role
- Join MANAGEMENT SERVER 1 to the larsenwh.com domain
- Add the XProtect Admins role to the Administrators group on MANAGEMENT SERVER 1
- Adjust server preferences and settings
- Add Windows Failover Clustering to MANAGEMENT SERVER 1
- Repeat the process for MANAGEMENT SERVER 2
- Validate and create the failover cluster using Domain Administrator credentials

INSTALL MANAGEMENT SERVERS AND CONFIGURE FAILOVER CLUSTER

- Add the XProtectServiceUser user account to the local Administrators group on MANAGEMENT SERVER 1
- Install XProtect Management Server, Event Server, Log Server, and Data Collector on MANAGEMENT SERVER 1
- Repeat the process for MANAGEMENT SERVER 2
- Add XProtect services to the Windows Failover Cluster
- Edit Registered Services in the XProtect Management client on the WORKSTATION VM
- Verify that Management Server failover is working
- Verify domain policy on making exceptions for anti-virus scanning has been applied

INSTALL CLIENTS AND RECORDING SERVERS

- Locate and copy files from the Management Server for unattended software installation
- Install the Management Client on the WORKSTATION VM from the network share using a simple batch script
- Install Smart Client on workstation using Milestone Software Manager
- Add all three Recording Servers to Milestone Software Manager using a .csv import script
- Install Recording Servers on XProtect-REC1 and XProtect-REC2 using Milestone Software Manager
- Install Failover Recording Server on XProtect-REC3 using Milestone Software Manager
- Install the XProtect Mobile Server on XProtect-MOB
- Install StableFPS drivers and video files on Recording servers via batch script

ADD HARDWARE VIA SCRIPTING AND CONFIGURE RECORDING SERVER FAILOVER

- Add and configure hardware devices using a PowerShell script
- Configure and demonstrate a failover event in regular (cold) standby mode
- Configure and demonstrate a failover event in hot standby mode
- Configure advanced failover settings
- Configure a rule that triggers while failover is active or inactive

PERFORM ADVANCED DEVICE CONFIGURATION

- Install an unsupported camera using the Universal Driver
- Configure server-to-client multicast
- Add cameras from REMOTE SITE 2 with Milestone Interconnect
- Disable local recording on Interconnected cameras and enable remote playback

- Configure Interconnected cameras to send lower resolution streams by default
- Create a remote retrieval rule with an event received through Interconnect
- Configure additional streams on Interconnected cameras
- Retrieve higher-quality remote recordings to overwrite local recordings
- Create a remote retrieval rule to retrieve recordings within a time window at a certain time
- Configure remote retrieval restrictions on Interconnected cameras
- BONUS EXERCISE: Create a remote retrieval rule using device metadata and a user-defined event

IMPLEMENT ADVANCED ROLE-BASED SECURITY

- Create the Supervisors, Operators, and General Staff roles and assign domain groups
- Configure overall security for all roles via PowerShell script
- Configure advanced security for Operators
- Configure advanced security for General staff
- Configure and assign a Smart Client profile for the Supervisors role
- Configure and assign Smart Client and Evidence Lock profiles to the Operators role
- Configure and assign Smart Client and Time Profiles to the General staff role
- Configure and assign a Management Client Profile to the Supervisors role

OPTIMIZE SMART CLIENT LOGIN, STARTUP, AND NAVIGATION

- Create a basic Smart Client startup script for the General Staff role
- Create an .scs file Smart Client startup script for the General Staff role
- Add additional script functionality using the Client Scripting page within the Smart Client
- Assign Smart Client keyboard shortcuts for devices and views

CONFIGURE ADVANCED SYSTEM BEHAVIORS

- Adjust and verify Mobile Server direct streaming settings
- Adjust fallback Mobile Server streaming settings
- Install Event Proxy to enable complex event support
- Create and verify events and rules in Event Proxy
- Set up and configure SNMP traps
- Create and demonstrate a rule that sends an SNMP trap

UNIFY PRIMARY AND REMOTE SITES USING MILESTONE FEDERATED ARCHITECTURE (MFA)

- Configure MFA to join REMOTE SITE 1 to the hierarchy as a child site
- Establish a domain trust to allow connections to an external domain
- Configure MFA to join REMOTE SITE 2 to the hierarchy as a child site
- Verify access and permissions to sites in the federated hierarchy
- Work with rules in a federated environment

PERFORM VMS MAINTENANCE

- Update device passwords within the Management Client
- Update device firmware within the Management Client
- Move hardware from one Recording Server to another Recording Server
- Create a backup of the Surveillance database in SQL Server Manager
- Restore the Surveillance database using SQL Server Manager