Milestone Certified Integration Engineer (MCIE) Assessment

STUDY GUIDE
Contents
Overview.................................................................................................................................................................... 3
Resources for preparing for the MCIE............................................................................................................. 4
Tasks within the scope of the MCIE assessment.......................................................................................... 6
Overview

A Milestone Certified Integration Engineer should have the ability to install and configure a complex XProtect VMS installation with a camera count of approximately 100-10,000 cameras, including features such as multiple Management Servers, multiple Mobile Servers, edge storage, multicast, clustering, and other advanced configuration options.

For Milestone to attest that you have this knowledge and these skills, you must pass an MCIE assessment that may touch on any of the tasks listed in following section. While the assessment may include test items associated with any of these tasks, the major focus areas of the MCIE assessment surround concepts, features, and scenarios likely to be encountered in more complex VMS installations, including:

- Server virtualization
- 802.1x port security
- Camera and Server multicast
- Multiple Mobile servers with video stream limitations
- Automated software installation and startup scripting
- Milestone Interconnect with complex retrieval rules
- Camera edge recording with automated and rule-based retrieval
- Regular standby and hot standby Failover Recording Servers
- Advanced Failover Recording Server options
- Working with Domains and Domain Controllers
- Milestone Federated Architecture
- Server clustering for high availability

Before you take the MCIE assessment, ensure that you have the knowledge and skills to perform all tasks and steps listed in the following section by consulting the list of resources provided in this document. The resources below are offered in different languages, though some documents are limited to English at this time. You are allowed to access these resources during the test. However, you have only two hours to complete the test and you must already be very familiar with the entire list of content here for you to be to be successful.
Resources for preparing for the MCIE

Use the resources below to assist you in developing the skills and knowledge necessary to complete the tasks listed in the previous section.

Manuals and Guides

You can find the following resources at Milestonesys.com > Support > Manuals and guides:

- XProtect VMS Products - Administrator getting started guide
- XProtect VMS Products - Administrator manual
- XProtect Smart Client - User Manual
- XProtect Smart Client - Hardware acceleration quick guide
- XProtect VMS Products – Activate licenses quick guide
- XProtect Smart Client - Search and export video evidence quick guide
- Upgrade your XProtect VMS Product - Quick guide
- Software Manager Administrator’s Manual
- XProtect VMS Products - System Architecture Document

White Papers

You can find the following resources at Milestonesys.com > Support > White Papers:

- System Architecture Guide for IT Professionals
- Milestone Interconnect™ white paper
- Milestone Federated Architecture™ white paper
- Milestone Edge Storage white paper

eLearning

You can access Milestone eLearning courses by following the link below and logging into the Partner Learning Portal:


eLearning resources that directly support the MCIE include:

- Milestone Fundamentals of IP Surveillance Systems
- Getting Started with XProtect Smart Client
- The following XProtect modules:
  - Configuring and Using the XProtect® Smart Wall
  - Configuring and Using the Customer Dashboard
The Getting Started with XProtect Professional course does not directly support the XProtect VMS products. However, the concepts presented in these modules of the Using the Getting Started Wizards section may be useful:

- Automatically Add Devices
- Manually Add Devices
- Configure Storage and Archiving
- Adjust Motion Detection
- Add and Manage Users

Milestone Web Resources

Visit the following pages on the Milestone Systems website for more information:

https://www.milestonesys.com/support/resources/system-requirements/
https://content.milestonesys.com/?mediaid=6789BDA7-9208-497E-AF35C98423895850

Other Web Resources

Visit the following Microsoft support pages for more information:

Microsoft Virtual Academy - Networking Fundamentals

Microsoft Virtual Academy - Windows Server Administration Fundamentals
https://mva.microsoft.com/en-us/training-courses/windows-server-administration-fundamentals-8477

Windows Server Failover Clustering Overview

SQL Server database migration
https://support.microsoft.com/en-us/kb/314546

Joining a computer to a Domain

About Domain Trusts
Tasks within the scope of the MCIE assessment

The list of tasks below outlines the current scope of the MCIE assessment. Milestone Certified Integration Engineers should be able to demonstrate their knowledge of the skills required to accomplish any of these tasks.

Installing and Configuring

1. Configure a network to support an XProtect Corporate design
   - A. Check switches, verify bandwidth and PoE capabilities and budgets
   - B. Obtain and verify IP address ranges
   - C. Determine whether the cameras receive IP addresses from DHCP
   - D. Check DNS, if DHCP is used
   - E. Check RTP, time server
   - F. Check passwords and other settings on routers, firewalls, access points
   - G. Check internet access if required
   - H. Check access for Active Directory and ensure that groups are defined
   - I. Verify Microsoft SQL server access and permissions
   - J. Verify Smart Client access to remote systems if Milestone Interconnect™ is used
   - K. Establish Domain Trust if using Milestone Federated Architecture™ across multiple domains
   - L. Configure/verify multicast settings if using multicast from cameras or clients
   - M. Enable IEEE 802.1X port security if used

2. Configure cameras and other IP devices
   - A. Set the IP address or Host Name if DHCP is used
   - B. Set Admin password for devices and verify with Milestone Supported Devices list
   - C. Verify firmware version with Milestone Supported Devices list and update if needed
   - D. Hang cameras:
     - Set Field of View
     - Set Focus
     - Connect I/O
   - E. Configure Edge Storage settings
   - F. Configure onboard events and analytics
   - G. Install Milestone Screen recorder
   - H. Configure camera multicast if used
   - I. Verify protocol data with Wireshark if using unsupported non-ONVIF cameras
3. Configure a Windows server to support a given XProtect Corporate design

- A. Install Windows and verify version against Milestone product specifications
  - Set and verify host name
- B. Set and verify network settings
  - IP addresses and network masks
  - Default Gateway
  - DNS server settings
- C. Verify Internet access if required for design
- D. Check and update for appropriate Windows service packs
- E. Check .Net version and update if needed
- F. Check the Windows Installer version and update if needed
- G. Check DirectX version and update if needed
- H. Add and verify User accounts and passwords
- I. Enable remote management, including Remote Desktop if needed
- J. Add anti-virus scan exceptions
- K. Check and adjust time if needed:
  - Time and time zone
  - NTP server settings
- L. Verify and implement VM environment
- M. Enable SNMP traps and management server
- N. Verify that the hostname lookup works between servers
- O. Manually edit hosts files as necessary
- P. Establish server cluster if using redundant management servers

4. Configure storage to support a given XProtect Corporate design

- A. Enable/verify RAID if not set up with JBOD
- B. Verify NAS access, including IP, user accounts, create/edit/delete file capability
- C. Format to 64K block size

5. Prepare for a Milestone software installation

- A. Download server software
- B. Download the latest from web device pack if necessary
- C. Obtain license file
6. Install Milestone Management server
   - A. Install Management server
     - Choose between default or custom
   - B. Verify service user accounts if using NAS storage
   - C. Verify that the Windows System Tray icon status is green
   - D. Install Event Server on intended server if not installed on management server
   - E. Install Log Server on intended server if not installed on management server
   - F. Install Service Channel on intended server if not installed on management server
   - G. Create MyMilestone account and register software

7. Install Milestone Mobile server
   - A. Install Mobile Server and specify admin user account for access to management server
   - B. Verify that it is running by checking the green icon status in the Windows System Tray

8. Install Milestone Recording server(s) and Failover Recording server(s)
   - A. Download software from management server download page and install under default, unless changing service user account to access NAS storage or installing as failover server
     - Specify server access details
   - B. Verify that it is running by checking the question mark icon status in the Windows System Tray
   - C. Install device pack if a newer version is available
   - D. Add antivirus scan exceptions, if not done under Server

9. Download and install the Management Client
   - A. Download software from management server download page
   - B. Install Mobile Server plug-in
Configuring and Organizing

10. Configure Milestone server

- A. Configure application behavior and general settings in the Tools Menu
  - Configure General Settings
  - Configure server logs retention time and detail settings
  - Configure Mail server settings
  - Configure AVI generation if using AVI attachments to email notifications
  - Configure default Bookmark behavior
  - Configure Evidence Lock profiles
  - Configure Generic Event settings
  - Verify Registered Services if installing a distributed system
  - Add Enterprise servers if using
  - Configure Network settings if using IPv6 or multiple local networks
- B. Activate licenses
  - Review license information
- C. Authorize recording servers
- D. Define failover servers
- E. Configure recording server
  - Configure basic storage settings
  - Configure archiving if external storage or grooming is used
  - Configure multicast recording settings if used
  - Configure recording server network if direct Smart Client access over the Internet is required

11. Add and name devices and functions and create device groups as necessary

- A. Add and name the following devices if using:
  - Supported cameras
  - ONVIF cameras
  - I/O devices
  - Audio-only devices
  - DirectShow devices
  - Screen Recorders
  - Unsupported devices using universal driver
- B. Disable unused functions
- C. Create additional camera, microphone, speaker, input and output device groups
12. Configure devices
   - A. Name devices
   - B. Disable non-used functions
   - C. Name cameras
   - D. Name microphones
   - E. Name speakers
   - F. Name inputs
   - G. Name outputs

13. Configure Cameras
   - A. Configure camera settings and define video streams
     - Compression, brightness, contrast, etc.
     - Resolution
     - Codec
     - Rotation
     - Keyframes
     - Streaming modes
     - Target constant and variable bitrates, set priority and limits
     - Disable date/time stamp and other overlays
     - Protocol (HTTP vs HTTPS)
   - B. Streams
   - C. Recording
   - D. 360 lenses
   - E. Camera events
   - F. Privacy Masking
   - G. Motion Detection
   - H. PTZ presets
   - I. PTZ patrol
   - J. Client settings
     - Live multicast
     - Related microphone, speaker, and metadata
     - Camera keyboard shortcut number

14. Configure speakers and microphones
   - A. Settings
   - B. Recording
   - C. Audio events
15. Configure inputs and outputs
   - A. Settings
   - B. Input events
   - C. Test outputs

16. Configure client settings
   - A. View Groups
   - B. Smart Client Profiles
   - C. Management Client Profiles
   - D. Matrix recipients
   - E. Smart Wall
     - Create Smart Wall
     - Add monitors
     - Define monitor characteristics
     - Create Smart Wall presets
     - Specify Smart Wall monitor layout
     - Define Smart Wall monitor preset layouts
   - F. Define events
     - Generic Events
     - User-defined events
   - G. Install and configure Event Proxy software and Plug-In if using

Defining and Monitoring

17. Define time and notification profiles
   - A. Time profiles
   - B. Day Length time profiles
   - C. Notification profiles

18. Create rules
   - A. General rules
   - B. Administrator notification rules
   - C. Complex rules
     - Edge storage retrieval rules if used
     - Interconnect retrieval rules if used
     - Event Proxy rules if used
19. Configure security
   - A. Add Basic users
   - B. Create Roles
     - Assign profile
     - Management Client profile
     - Smart Client profile
     - Default time profile
     - Evidence Lock profile
     - Smart Client login within time profile
     - Login authorization requirement for dual or four-eye authentication
   - C. Assign users and user groups to role
   - D. Define overall security settings for role
   - E. Define detail security settings for role
     - Device access settings
     - PTZ access and priority
     - Speech (speaker) access and priority
   - F. Verify effective roles via the Tools menu

20. Define alarms
   - A. Alarm data settings
   - B. Sound settings
   - C. Alarm definitions

21. System performance and alerting
   - A. Verify system performance via System Monitor
   - B. Verify SNMP trap connectivity
   - C. Check log files:
     - Audit Log
     - Rule Log
     - Event Log
Extending and Maintaining

22. Configure Mobile server
   - A. Add Mobile Server
   - B. Set access credentials
   - C. Export settings
   - D. Enable Smart Connect and/or update firewall/router as necessary
   - E. Add Video Push
   - F. Configure Connectivity Settings
   - G. Configure Performance Settings

23. Milestone Interconnect
   - A. Add Interconnected system
   - B. Select Interconnected cameras
   - C. Configure Remote Retrieval settings

24. Milestone Federated Architecture
   - A. Configure MFA if used
   - B. Verify/adjust user permissions across sites

25. Activate License
   - A. Online or offline activation
   - B. Verify information on license overview page

26. XProtect Server service/upgrade/expansion proficiencies
   - A. Move camera
   - B. Change storage
   - C. Save/load system configuration
   - D. Download Manager:
     - Install Server-Side installers
     - Verify/change settings
   - E. Daylight Saving Time
   - F. SQL tools and maintenance:
     - Backup
     - Shrink transaction log
     - Migrate SQL from express to full
   - G. Replacing (failed) management server
   - H. Replacing (failed) recording server
   - I. Importance of SOW
J. Importance of FAT
K. Software Manager
L. Configure automatic client application deployment
M. Script custom Smart Client startup
N. Troubleshooting tools:
   - WireShark
   - Perfmon
   - Infocollector

27. Configure the Smart Client

A. Install Smart Client via the server download page
B. Verify access to slave servers
C. Create views
D. Create maps
E. Verify hardware decoding/performance
F. Verify user logins
   - Verify permissions
     - Tab access/block (live, playback, Alarms, Sequence Explorer, Setup)
     - Manage views access/block
     - Menus and functions access/block
     - Export permissions
     - Camera access
     - PTZ control and priority
     - Trigger events
     - Manage alarms
G. Configure joystick and keyboard shortcuts [Smart Client Options]
H. Configure camera performance settings [Properties menu]
I. Verify access to Interconnected cameras
J. Verify access to Smart Wall
   - Verify Smart Wall presets
K. Check audio communication
L. Manage alarms
M. Consider Smart Client time zone settings [options menu]
N. Create maps for MFA sites if used
O. Configure advanced Smart Wall settings if used

28. Configure Web Client

A. Create browser shortcut
B. Verify user logins
29. Configure Mobile client

- A. Install app from relevant online marketplace
- B. Verify user logins
- C. Verify Video Push
- D. Verify Push Notifications