

ArcSight Management Center (ArcMc) Administration (ARCMCA)

ID ARCMCA Price 4,000.— €(excl. tax) Duration 5 days

Important notes for the booking of Open Text trainings

Please note that prepayment is required for participation in an Open Text training course. Participation in a training course is possible for 12 months after booking the course. Cancellations are excluded. For further information, please refer to **our** [General Terms and Conditions](#).

Course Overview

This course is designed to provide ArcSight System Administrators with the foundational and hands-on skills needed to effectively centralize the administration and monitoring of various ArcSight components, such as Transformation Hub, Logger, SmartConnectors, FlexConnectors, and other standalone ArcSight Management Center (ArcMC) devices in the ArcSight ecosystem.

It covers ArcMC version 24.1: Core ArcMC (formerly known as Fusion) and Software ArcMC (standalone).

Highlights:

- Installing and Configuring Software ArcMC
- Configuring Core ArcMC in an ArcSight Platform instance
- Centrally Configuring, Monitoring and Deploying Connectors
- Using Configuration Templates to facilitate the administration of ArcSight Components
- Tools to manage user and groups in standalone ArcMCs and Loggers
- Implement monitoring of various metrics for ArcSight components and devices

Who should attend

System Administrators interested in managing ArcSight components centrally.

Prerequisites

To be successful in this course, you should have the following prerequisites or knowledge:

- Familiar with the installation and configuration of ArcSight Connectors
- Basic understanding of ArcSight Logger functionality such as event searches, Receivers and User Management
- Basic understanding of the ArcSight Platform Solution and Transformation Hub component

Course Objectives

On completion of this course, participants should be able to:

- Describe ArcMC product features
- Perform the installation and administration of standalone ArcMC devices
- Perform the configuration of Core ArcMC in an ArcSight Platform instance
- Implement Role-based access to manage users and groups for Loggers and ArcMCs
- Identify the scenarios for using ArcMC Node Management and Configuration Management features
- Perform rapid installation of connectors using ArcMC Instant Connector Deployment feature
- Centrally enable monitoring and alerts for managed ArcSight components
- Create Configuration Templates to rapid configure subscribers and identify non-compliant managed components.
- Understand the upgrade process for Connectors, Loggers and standalone ArcMCs

Course Content

- Introduction to Product Features and Architecture
- Installing Software ArcMC (Non-Containerized)
- System Administration for ArcMC (Non-Containerized)
- Node Management with Fusion ArcMC (Containerized) – ArcMC and Logger Nodes
- Node Management – Importing Hosts with Connectors using Core and Software ArcMC Consoles
- Node Management – Managing Connector Parameters using ArcMC Console

- Configuration Management
- Managing Users on Managed Products
- Documenting Capabilities in ArcSight Platform Instance
- Managing Transformation Hub - Importing Host in Core ArcMC
- Managing Transformation Hub – Routing Events Between Topics
- Managing Breach Rules and Monitoring Dashboards in ArcMC
- Generator ID Management in ArcMC
- ArcMC Product Administration – Application Tools
- ArcMC Product Administration – Repositories and Node Upgrades

Detailed Course Outline

Chapter 1: Introduction to Product Features and Architecture

- Describe problems ArcSight Management Center solves
- Recognize the ArcSight Platform architecture
- Describe where ArcMC fits in the ArcSight Platform
- Understand the deployment options for ArcMC functionality: containerized or standalone (also known as non-containerized)

Chapter 2: Installing Software ArcMC (Non-Containerized)

- Recognize the requirements for installing Software ArcMC
- Describe the installation steps for Software ArcMC
- Recognize uploading ArcMC licenses and start/stop of ArcMC processes
- Describe how the ArcMC product's UI is organized
- Log into the ArcMC UI to verify a healthy operational status

Chapter 3: System Administration for ArcMC (Non-Containerized)

- Describe the System Admin Sub-Menu options in the UI interface
- Differentiate ArcMC Appliance and Software ArcMC System Admin capabilities
- Locate and configure software ArcMC device settings
- Define a Password Policy and Login Banner for ArcMC users
- Review and configure Sys Admin settings, including defining a password policy and login banner

Chapter 4: Node Management with Fusion ArcMC (Containerized) – ArcMC and Logger Nodes

- Recognize how ArcMC uses Node Management to manage ArcMC (non-containerized) instance and Logger node types

- Describe the Node Management Tasks available in the ArcMC Console
- Understand how to add nodes from a host
- Learn how to import hosts from a CSV file
- Identify, add, and organize ArcSight hosts and nodes using locations
- Describe ArcMC Agent functionality and installation and upgrade steps
- Understand how the initial configuration feature serves as a rapid and uniform setup for multiple ArcSight Loggers
- Create location management entities
- Import software ArcMC and Logger nodes using manual and bulk operations
- Address credential issues, and upgrading, ArcMC agent version

Chapter 5: Node Management – Importing Hosts with Connectors using Core and Software ArcMC Consoles

- Recognize how ArcMC uses Node Management to manage Hosts with Connectors node type.
- Gain experience installing and configuring Connectors
- Learn how to import a host with connectors
- Identify the steps to re-scan a host to bring new Connectors as managed nodes
- Explore how a single host can comprise multiple nodes (connectors) for management purposes
- Describe the Node Management tools to manage connectors, containers, and destinations through the ArcMC interface
- Recognize the Health indicators in the ArcMC Monitor Summary dashboard
- Install a connector via SmartConnector wizard
- Describe the steps to import Windows, and Linux hosts with connectors as ArcMC managed nodes

Chapter 6: Node Management – Managing Connector Parameters using ArcMC Console

- Recognize how ArcMC uses Node Management to centrally manage Connectors' Configuration settings
- Describe the main connector managed components: container, connector configuration and destination configuration
- Manage Connector parameters using Core ArcMC Console
- Pull and review audit logs generated connectors via Core ArcMC console
- Describe how Node Management deals with day-to-day operations and fine tuning of Hosts with Connector nodes

Chapter 7: Configuration Management

- Describe how ArcMC Configuration Management works
- Identify the differences between Initial configurations and

- subscriber configurations
- Create various subscriber configurations
- Discuss Best Practices for use of configuration management
- Create configuration templates for managing settings in managed software ArcMC, Logger and Connectors
- Create policies to manage several types of receivers in Logger nodes
- Consolidate Filter resources in Logger nodes
- Create mapping file configuration for managed connectors
- Create configuration baselines for managed nodes
- Manage ArcSight Network Model resources such as Networks and Zones settings for managed connectors

Chapter 8: Managing Users on Managed Products

- Describe how user management and role-based access control are applied to managing users in an ArcSight Deployment
- Describe the different components that make up User Management
- Run and investigate non-compliant user configurations
- Implement role-based access control RBAC for standalone ArcMCs and Logger devices
- Describe the steps to generate compliance reports to list and validate users/groups/roles implemented in managed nodes

Chapter 9: Documenting Capabilities in ArcSight Platform Instance

- Identify the ArcSight Platform capabilities using ITOM and Core Interfaces
- Describe the configuration of ArcSight Platform to enable ArcMC functionality known as Core ArcMC
- Articulate how the Core UI is organized
- Describe how to validate the state of ArcSight Platform components (pods) using CLI and ITOM Interface
- Document the capabilities deployed in your ArcSight Platform instance
- Identify the versions of Core (Fusion) and Transformation Hub capabilities
- Recognize the dependencies between Fusion, Transformation Hub and ArcMC

Chapter 10: Managing Transformation Hub - Importing Host in Core ArcMC

- Describe the steps to integrate Transformation Hub (TH) and ArcMC
- Describe and configure Producers and Consumers in TH
- Identify the state of TH in the Summary Dashboard
- Import Transformation Hub as a managed node using the Core ArcMC interface

- Manage Connectors with Transformation Hub Destinations
- Identify the steps to configure ESM and Logger as Transformation Hub Consumers

Chapter 11: Managing Transformation Hub – Routing Events Between Topics

- Recognize the configuration properties for topic and routing rules resources
- Describe the steps to create Kafka topics in Transformation Hub via Core ArcMC interface
- Configure Route and Filter of Events Between Topics from Core ArcMC interface
- Describe the steps to set a Logger consumer to pull events from a newly created topic
- Recognize the ArcMC Monitoring Dashboards to validate event routing configuration and operation

Chapter 12: Managing Breach Rules and Monitoring Dashboards in ArcMC

- Describe the steps to create breach rules for managed nodes and devices
- Identify the built-in monitoring rules and dashboards
- Recognize ArcMC Monitoring Dashboards to determine node and device health
- Describe the steps to Inspect Audit logs in ArcMC generated by breach rules

Chapter 13: Generator ID Management in ArcMC

- Recognize Global Event ID Design and Features
- Describe the steps to configure ArcMC as a Generator ID Manager
- Recognize how ArcMC assigns Generator IDs to Manage Nodes
- Describe the steps to assign Generator IDs to software ArcMC (non-containerized) and Logger processes via ArcMC Generator ID Manager
- Identify the assigned Generator IDs using the Generator ID Manager panel

Chapter 14: ArcMC Product Administration – Application Tools

- Describe the ArcMC tools under the Administration > Application menu: Backup, Restore Snapshot Logger Data Consumption Report
- Describe the steps to perform rapid installation of connectors using ArcMC's Instant Deployment feature
- Recognize how Audit Events are forwarded by a standalone ArcMC Software instance
- Describe the steps to install and configure a Syslog Connector via Configuration Management Templates

- Identify ArcMC Audit Events in standalone ArcMC Software and Logger Interfaces

Chapter 15: ArcMC Product Administration – Repositories and Node Upgrades

- Recognize how ArcMC repositories are used to upload upgrade or content update files
- Identify the steps to upgrade Logger and standalone ArcMC Software managed nodes
- Perform upgrade of Connectors Framework and parser using ArcSight Update Files
- Describe the steps to perform the remote upgrade of Loggers, Software ArcMC and Connectors via Core (Fusion) ArcMC interface.
- Describe the steps to install, configure and upgrade Syslog Connectors using ArcMC interface

About Fast Lane



Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

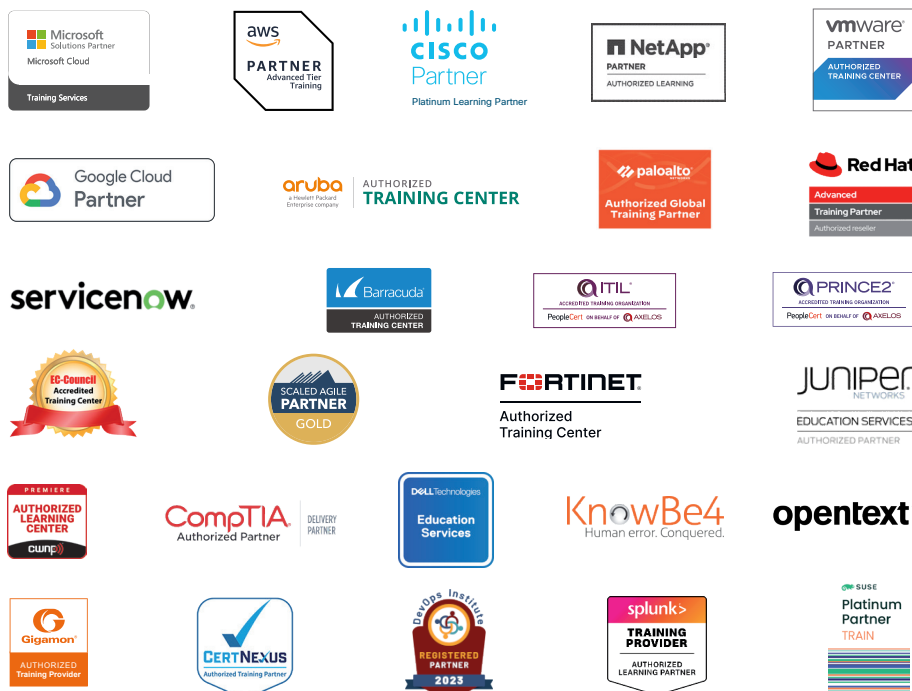
- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center



Worldwide Presence
with high-end training centers
around the globe



Multiple Awards
from vendors such as AWS,
Microsoft, Cisco, Google, NetApp,
VMware



Experienced SMEs
with over 19.000 combined
certifications

Germany

**Fast Lane Institute for Knowledge
Transfer GmbH**

Tel. +49 40 25334610

info@flane.de / www.flane.de

Austria

ITLS GmbH

(Partner of Fast Lane)

Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Switzerland

**Fast Lane Institute for Knowledge
Transfer (Switzerland) AG**

Tel. +41 44 8325080

info@flane.ch / www.flane.ch