

Sicurezza negli ambienti Microsoft

Introduction

This instructor-led course addresses the MCSA and MCSE skills path for IT Pro security practitioners, specifically addressing the training needs of those preparing for the 70-299 certification exam.

The primary product focus is on Microsoft Windows Server 2003 based infrastructure solutions but will include some client focused content where appropriate. This learning product is to provide functional skills in planning and implementing infrastructure security.

This course is part of the Security Portfolio and will act as the primary entry point for IT Professionals at the implementation level. MOC 2810 will provide an entry point for students to broaden their awareness of security issues. Students will be encouraged to enhance their security design skills by attending MOC 2830.

[↩Top of page](#)

Audience

The course is for a system administrator or system engineer who has the foundation implementation skills and knowledge for the deployment of secure Microsoft Windows Server 2003 based solutions. This course is not intended to provide design skills, but will cover planning skills at a level sufficient to enable decision making for the implementation process.

[↩Top of page](#)

At Course Completion

After completing this course, students will gain the skills to:

- Plan and configure an authorization and authentication strategy.
- Install, configure, and manage certification authorities.
- Configure, deploy, and manage certificates.
- Plan, implement, and troubleshoot smart card certificates.
- Plan, implement, and troubleshoot Encrypting File System (EFS).
- Plan, configure, and deploy a secure member server baseline.
- Plan, configure, and implement secure baselines for server roles.
- Plan, configure, implement, and deploy client computer baselines.
- Plan and implement software updates.
- Plan, deploy, and troubleshoot data transmission security.
- Plan and implement security for wireless networks.
- Plan and implement perimeter security with Internet Security and Acceleration (ISA) Server 2004.
- Secure remote access.

[↩Top of page](#)

Prerequisites

Before attending this course, students must have:

- Completed MOC 2810 or equivalent knowledge.
- Experience implementing a Windows 2000 or Windows Server 2003 Active Directory environment. Experience with organizational resources such as Web, FTP and Exchange servers, (not expected to have detailed knowledge) shared resources and network services such as DHCP, DNS and WINS also helpful.

[↶Top of page](#)

Microsoft Certified Professional Exams

No Microsoft Certified Professional exams are associated with this course currently.

[↶Top of page](#)

Course Materials

The student kit includes a comprehensive workbook and other necessary materials for this class.

The following software is provided in the student kit:

- Student CD

[↶Top of page](#)

Course Outline

Module 1: Planning and Configuring an Authentication and Authorization Strategy

This module explains how to evaluate the infrastructure of your organization and create and document an authorization and authentication plan that allows the appropriate level of access to various security principals. It also describes trust relationships, domain and forest functional levels, and basic security principles.

Lessons

- Components of an Authentication Model
- Planning and Implementing an Authentication Strategy
- Groups and Basic Group Strategy in Windows Server 2003
- Creating Trusts in Windows Server 2003
- Planning, Implementing, and Maintaining an Authorization Strategy Using Groups
- Lab A: Planning and Configuring an Authentication and Authorization Strategy
- Planning and Implementing a Resource Authorization Strategy
- Planning and Implementing a Cross-Forest Authentication Strategy
- Planning and Implementing an Authentication Policy

After completing this module, students will be able to:

- Describe the components, tools, and protocols that support authentication.
- Plan and implement an authentication strategy in a multi-forest organization.
- Determine the necessary group structure for a multi-domain or multi-forest environment.
- Create trusts in a Windows Server 2003 environment.
- Plan, implement, and maintain an authorization strategy in a multi-forest organization.

Module 2: Installing, Configuring, and Managing Certification Authorities

This module describes the fundamentals of the systems that make secure communication possible. It describes methods, such as a public key infrastructure (PKI), that enable you to securely communicate on networks.

Lessons

- Overview of a PKI
- Introduction to Certification Authorities
- Installing a Certification Authority
- Managing a Certification Authority
- Backing Up and Restoring a Certification Authority
- Lab A: Installing and Configuring a Certification Authority

- Installing an Enterprise Subordinate Certification Authority
- Backing up a Certification Authority

After completing this module, students will be able to:

- Describe a PKI.
- Describe the applications and components that are used in a PKI.
- Install a certification authority.
- Create and publish Certificate Revocation Lists (CRLs) and Authority Information Access (AIA) distribution points.
- Back up and restore a certification authority.

Module 3: Configuring, Deploying, and Managing Certificates

This module explains how to ensure that the certificates are issued to the correct security principals and for the intended purpose. It describes, for example, how to make the deployment of certificates an easy and straightforward task for end users.

Lessons

- Overview of Digital Certificates
- Deploying and Revoking User and Computer Certificates
- Configuring Certificate Templates
- Managing Certificates
- Lab A: Deploying and Managing Certificates
- Configuring Multipurpose Certificate Templates
- Configuring Certificate Autoenrollment
- Updating a Certificate Template
- Implementing a Key Archiving Strategy

After completing this module, students will be able to:

- Configure certificate templates in a Microsoft Windows Server 2003 PKI environment.
- Deploy, enroll, and revoke certificates in a Windows Server 2003 PKI environment.
- Describe the applications and components that are used in a PKI.
- Export, import, and archive certificates and keys in a Windows Server 2003 PKI environment.

Module 4: Planning, Implementing, and Troubleshooting Smart Card Certificates

This module describes how to deploy, manage, and configure certificates and certificate templates in a public key infrastructure (PKI) environment.

Lessons

- Introduction to Multifactor Authentication
- Planning and Implementing a Smart Card Infrastructure
- Managing and Troubleshooting a Smart Card Infrastructure
- Lab A: Implementing Smart Cards
- Configuring a Smart Card Enrollment Station
- Simulation: Enrolling Users for Smart Cards

After completing this module, students will be able to:

- Describe the concepts of and applications for multifactor authentication.
- Plan and implement a smart card infrastructure.
- Manage and troubleshoot a smart card infrastructure.

Module 5: Planning, Implementing, and Troubleshooting Encrypting File System

This module describes how to plan, implement, and troubleshoot Encrypting File System (EFS).

Lessons

- Introduction to EFS
- Implementing EFS in a Standalone Microsoft Windows XP Environment
- Planning and Implementing EFS in a Domain Environment
- Implementing EFS File Sharing
- Troubleshooting EFS
- Lab A: Planning, Implementing, and Troubleshooting Encrypting File System
- Implementing Certificates to Support EFS
- Configuring Group Policy to Support EFS

After completing this module, students will be able to:

- Describe EFS and how it works.
- Implement EFS in a standalone Microsoft Windows XP environment.
- Plan and implement EFS in a domain environment that has a PKI.
- Implement EFS file sharing.
- Troubleshoot EFS problems.

Module 6: Planning, Configuring, and Deploying a Secure Member Server Baseline

The security of a network depends on the security configuration of the servers that make up the network. Any breach of security on a single server can jeopardize the security of all computers in the network, thereby jeopardizing the security of the network itself. In this module, students will learn how to create secure baselines for servers.

Lessons

- Overview of a Member Server Baseline
- Planning a Secure Member Server Baseline
- Configuring Additional Security Settings
- Deploying Security Templates
- Securing Servers by Using the Security Configuration Wizard
- Lab: Planning a Member Server Baseline
- Planning a Secure Member Server Baseline

After completing this module, students will be able to:

- Describe the components that make up a secure member server baseline.
- Plan a secure member server baseline.
- Configure additional security settings.
- Deploy security templates.
- Secure servers by using the Security Configuration Wizard (SCW).

Module 7: Planning, Configuring, and Implementing Secure Baselines for Server Roles

In this module, students will learn how to create secure baselines for various server roles.

Lessons

- Planning and Configuring a Secure Baseline for Domain Controllers
- Planning and Configuring a Secure Baseline for DNS Servers
- Planning and Configuring a Secure Baseline for Infrastructure Servers
- Planning a Secure Baseline for File and Print Servers
- Planning and Configuring a Secure Baseline for IIS Servers

After completing this module, students will be able to:

- Plan and configure a secure baseline for domain controllers.
- Plan and configure a secure baseline for Domain Name System (DNS) servers.

- Plan and configure a secure baseline for infrastructure servers.
- Plan a secure baseline for file and print servers.
- Plan and configure a secure baseline for Internet Information Services (IIS) servers.

Module 8: Planning, Configuring, Implementing, and Deploying a Secure Client Computer Baseline

In this module, students will learn how to create secure baselines for client computers.

Lessons

- Planning and Implementing a Secure Client Computer Baseline
- Securing Applications on Client Computers
- Planning and Implementing a Software Restriction Policy
- Implementing Security for Mobile Clients
- Lab A: Planning, Implementing, Configuring, and Deploying a Secure Client Computer Baseline
- Planning Security Templates for Client Computers
- Implementing Security Templates for Client Computers

After completing this module, students will be able to:

- Plan a secure client computer baseline.
- Secure applications on client computers.
- Plan and implement a software restriction policy on client computers.
- Implement security on mobile computers.

Module 9: Planning and Implementing Software Updates

In this module, students will learn how to plan and implement update management strategies on computers.

Lessons

- Introduction to Software Update Management
- Implementing Microsoft Baseline Security Analyzer
- Installing Windows Server Update Services
- Managing a WSUS Infrastructure
- Lab: Planning and Implementing Software Updates
- Configure MBSA Integration with WSUS Server

After completing this module, students will be able to:

- Describe the need for update management and the tools that you can use to implement update management strategies.
- Implement MBSA.
- Install WSUS.
- Manage a WSUS infrastructure.

Module 10: Planning, Deploying, and Troubleshooting Data Transmission Security

This module provides students with the information they need to plan and troubleshoot data transmission security.

Lessons

- Secure Data Transmission Methods
- Introducing IPSec
- Planning and Implementing Data Transmission Security Using IPSec
- Troubleshooting IPSec Communications
- Lab A: Implementing and Troubleshooting Data Transmission Security
- Planning IPSec Security
- Implementing IPSec Security

After completing this module, students will be able to:

- Describe various methods for securing data transmission.
- Describe the purpose and function of IPSec.
- Plan and implement data transmission security using IPSec.
- Troubleshoot IPSec communication.

Module 11: Planning and Implementing Security for Wireless Networks

A wireless network uses technology that enables two or more devices to communicate through standard network protocols and electromagnetic waves-not network cabling-to carry signals over part or all of the communication path. This module describes how to plan and implement security for wireless networks.

Lessons

- Introduction to Securing Wireless Networks
- Implementing 802.1x Authentication
- Planning a Secure WLAN Strategy
- Implementing a Secure WLAN
- Troubleshooting Wireless Networks
- Lab A: Planning and Implementing Security for Wireless Networks
- Configuring Active Directory for Wireless Networks
- Configuring Certificate Templates and Certificate Autoenrollment
- Configuring Remote Access Policies for Wireless Devices
- Configuring Group Policy for Wireless Networks

After completing this module, students will be able to:

- Describe the components and features of a secure wireless LAN (WLAN) and a wireless infrastructure.
- Plan a secure WLAN infrastructure.
- Implement a secure WLAN infrastructure.
- Troubleshoot WLAN errors and components.

Module 12: Planning and Implementing Perimeter Security with Internet Security and Acceleration Server 2004

Networks in organizations today are commonly interconnected-various networks within an organization connect to each other, and corporate networks connect to the Internet. Although this presents new business opportunities, it can also cause concerns about security, performance, and manageability.

Lessons

- Introduction to Internet Security and Acceleration Server 2004
- Installing and Managing ISA Server 2004
- Securing a Perimeter Network by Using ISA Server 2004
- Publishing Servers on a Perimeter Network
- Planning a Perimeter Network
- Implementing a Perimeter Network
- Securing an ISA Server 2000 Computer

After completing this module, students will be able to:

- Describe the ISA Server 2004 features.
- Install and manage ISA Server 2004.
- Configure a perimeter network by using ISA Server 2004.
- Publish servers on a perimeter network by using ISA Server 2004.

Module 13: Securing Remote Access

Remote access enables remote access clients to access corporate networks as if they were directly connected to the corporate network. The remote access clients connect to the network by using dial-up communication links.

The security of a network is compromised if unauthorized remote users gain access to intranet-based resources. An effective network access security design ensures confirmation of the identity of the clients attempting to access your organization's network resources and protection of specific resources from inappropriate access by users.

Lessons

- Introduction to Remote Access Technologies and Vulnerabilities
- Planning a Remote Access Strategy
- Deploying Network Access Quarantine Control Components
- Lab A: Implementing a Secure VPN Solution
- Configuring a VPN Connection
- Configuring the VPN Server for Remote Access Quarantine
- Configuring a Connection Manager Service Profile

After completing this module, students will be able to:

- Describe the various remote access technologies used for remote access and the threats associated with remote access.
- Plan a remote access strategy.
- Implement and configure a virtual private network (VPN) server.
- Deploy Network Access Quarantine Control components.