

# Trend Micro Apex One for Certified Professionals

**Bitte beachten Sie:** Der Kurs ersetzt das Training "Trend Micro OfficeScan XG SP1 for Certified Professionals".

In diesem Training lernen Sie, wie Sie Trend Micro Apex One™ verwenden. Dieser Kurs behandelt die grundlegende Architektur, die Sicherheitsfunktionen, die Einsatzszenarien und das Troubleshooting. In praktischen Übungen lernen die Teilnehmer die Konfiguration der Apex One-Schutzfunktionen sowie die für eine erfolgreiche Implementierung und langfristige Wartung erforderlichen Administrationsoptionen. Dieser Kurs, der von Trend Micro zertifizierten Trainern unterrichtet wird, beinhaltet eine Vielzahl von praktischen Laborübungen, die es den Teilnehmern ermöglichen, die Unterrichtsinhalte in die Praxis umzusetzen.

#### Kursinhalt

- Apex One Overview
- Apex One Server
- Apex One Web Management Console
- Security Agents
- Managing Off-Premise Agents
- Keeping Apex One Updated
- Trend Micro Smart Protection
- Protecting Endpoint Computers from Malware
- Protecting Endpoint Computers Through Behavior Monitoring
- Protecting Endpoint Computers from Unknown Threats
- Detecting Emerging Malware Through Trend Micro™ Connected Threat Defense
- Blocking Web Threats
- Protecting Endpoint Computers Through Traffic Filtering
- Preventing Data Leaks on Endpoint Computers
- Deploying Policies Through Apex Central
- Blocking Unapproved Applications on Endpoint Computers
- Protecting Endpoint Computers from Vulnerabilities
- Detecting and Investigating Security Incidents on Endpoint Computers
- Troubleshooting Apex One

**E-Book** Sie erhalten ausführliche Kursunterlagen von Trend Micro in englischer Sprache. Wahlweise stellen wir die Printversion oder ein Trend Micro e-Kit zur Verfügung.

#### Zielgruppe

Dieser Kurs richtet sich an IT-Experten, die für den Schutz von Endgeräten vor Datenmissbrauch und gezielten Angriffen verantwortlich sind. Dazu gehören auch diejenigen, die sich mit folgenden Themen auseinandersetzen:

- Operations
- Deployment
- Security Response
- Compliance

#### Voraussetzungen

Es gibt keine Voraussetzungen für die Teilnahme an diesem Kurs, jedoch sind Grundkenntnisse der Produkte und Dienstleistungen von Trend Micro sowie ein Verständnis der grundlegenden Netzwerkkonzepte und -prinzipien hilfreich.

Grundkenntnisse in den folgenden Themen sind ebenfalls von Vorteil:

- Windows®-Server und -Clients
- Microsoft® Internet Information Server (IIS)
- Allgemeines Verständnis von Malware

#### Kursziel

Nach Abschluss des Kurses können die Teilnehmer die Zertifizierungsprüfung zum Trend Micro Certified Professional Apex One ablegen. Die Prüfung ist im Kurspreis inkludiert. Für die Registrierung zum Examen wird ein Account im Trend Micro Education Portal benötigt.

#### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/TMAP](http://www.experteach.at/go/TMAP)

#### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

#### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

#### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.	
<b>Termine in Österreich</b>	<b>3 Tage</b>	<b>€ 1.995,-</b>
<b>Online Training</b>	<b>3 Tage</b>	<b>€ 1.995,-</b>
Termine auf Anfrage		

Stand 24.01.2025



# Inhaltsverzeichnis

## Trend Micro Apex One for Certified Professionals

### Apex One Overview

- Trend Micro solutions
- Key features of Apex One
- Apex One components
- Deployment methods
- Threat detection

### Apex One Server

- Apex One Server tasks
- Apex One Server services and components
- Configuration repositories
- Installing/upgrading Apex One Server
- Apex One plug-ins and utilities

### Apex One Web Management Console

- Logging into the console
- Integrating with Active Directory
- Creating new administrative accounts

### Security Agents

- Security Agent tasks
- Security Agent services and components
- Security Agent tree
- Installing Agents
- Migrating from other endpoint security software
- Agent-to-Server/Server-to-Agent communication
- Endpoint location
- Moving Security Agents
- Uninstalling Security Agents
- Agent settings and grouping
- Agent self-protection
- Agent privileges

### Managing Off-Premise Agents

- Protection features
- Installing the Apex One Edge Relay Server
- Registering the Apex One Edge Relay Server
- Edge Relay Server and external Agent communication
- Edge Relay Server digital certificates

### Keeping Apex One Updated

- ActiveUpdate
- Updating the Apex One Server
- Updating Security Agents
- Update Agents

- Security compliance

### Trend Micro Smart Protection

- Smart Protection services and sources
- Configuring the Smart Protection source

### Protecting Endpoint Computers from Malware

- Scanning for malware
- Scan settings
- Quarantining malware
- Smart Scan
- Spyware/grayware protection
- Preventing outbreaks

### Protecting Endpoint Computers Through Behavior Monitoring

- Malware behavior blocking
- Ransomware protection
- Anti-exploit protection
- Fileless malware protection
- Newly encountered program detection
- Event monitoring
- Behavior monitoring exceptions

### Protecting Endpoint Computers from Unknown Threats

- Common Vulnerabilities and Exposures exploits
- Predictive machine learning
- Offline predictive machine learning

### Detecting Emerging Malware Through Trend Micro™ Connected Threat Defense

- Connected Threat Defense requirements
- Deep Discovery Analyzer
- Suspicious Objects

### Blocking Web Threats

- Web reputation
- Detecting suspicious connections
- Protecting against browser exploits

### Protecting Endpoint Computers Through Traffic Filtering

- Firewall filtering
- Application filtering
- Certified Safe Software list

- Stateful inspection
- Intrusion Detection System
- Firewall policies and profiles

### Preventing Data Leaks on Endpoint Computers

- Data Loss protection
- Installing Data Loss protection
- Configuring data identifiers, data loss prevention templates and policies
- Device control

### Deploying Policies Through Apex Central

- Apex Central
- Apex Central management modes
- Managing Apex One policies in Apex Central
- Data Discovery policies

### Blocking Unapproved Applications on Endpoint Computers

- Integrated Application Control
- Application Control criteria
- Implementing Application Control
- User-based Application Control
- Lockdown Mode
- Best practices

### Protecting Endpoint Computers from Vulnerabilities

- Integrated Vulnerability Protection
- Vulnerability Protection Pattern
- Implementing Vulnerability Protection
- Network Engine settings

### Detecting and Investigating Security Incidents on Endpoint Computers

- Integrated Endpoint Sensor
- Endpoint Detection and Response
- Apex One Incident Response Model
- Managed Detection and Response

### Troubleshooting Apex One

- Debugging the Apex One Server and Agents
- Troubleshooting communication issues
- Troubleshooting virus infection
- Troubleshooting Apex One services
- Troubleshooting sample submission

