Symantec eLibrary course list - September, 2019

Product Introductions

Introduction to CAS S400
Introduction to CloudSOC
Introduction to Web Isolation
Introduction to Web Security Service
Introduction to Symantec Web Isolation
Introduction to Cloud Workload Protection
Introduction to Content Analysis
Introduction to Control Compliance Suite
Introduction to Data Loss Prevention
Introduction to Data Center Security
Introduction to Email Security.cloud
Introduction to Symantec Encryption
Introduction to Endpoint Detection and Response
Introduction to Endpoint Application Isolation and Control
Introduction to Endpoint Protection
Introduction to Endpoint Protection Cloud
Introduction to Endpoint Protection Mobile
Introduction to Ghost Solution Suite
Introduction to Information Centric Security
Introduction to Integrated Cyber Defense Exchange
Introduction to IT Management Suite
Introduction to Management Center and Reporter
Introduction to Messaging Gateway
Introduction to PacketShaper
Introduction to ProxySG Secure Web Gateway
Introduction to Secure Access Cloud
Introduction to Security Analytics
Introduction to SSLV
Introduction to Validation and ID Protection

Advanced Threat Protection

Advanced Threat Protection 3.2: Differences
ATP 3.0: Analyzing Events and Incidents to Identify Indicators of Compromise
ATP 3.0: Endpoint Data Recorder and Advanced Searches
ATP 3.0: Introducing Advanced Threat Protection
ATP 3.0: Optimizing your ATP Environment
ATP 3.0: Recovering After an Incident
ATP 3.0: Remediating and Isolating Threats
ATP 3.0: Strengthening your Cybersecurity Framework
Advanced Threat Protection: Backup and Restore
Advanced Threat Protection: Installing and Managing SSL Certificates
Advanced Threat Protection: Network Overview
Advanced Threat Protection: Preparing your SEP 14 Environment for Incident Response
Advanced Threat Protection: SEP Connection Troubleshooting

Advanced Threat Protection: ServiceNow Integration
Advanced Threat Protection: Splunk Integration
Advanced Threat Protection: Troubleshooting
Advanced Threat Protection: Updating
ATP 2.x: Analyzing Events and Incidents to Identify Indicators of Compromise
ATP 2.x: Course Introduction: Attack at Solusell
ATP 2.x: Introducing Advanced Threat Protection
ATP 2.x: Optimizing your ATP Environment
ATP 2.x: Preparing your Endpoint Environment for Incident Response
ATP 2.x: Recovering After an Incident
ATP 2.x: Remediating and Isolating Threats
ATP 2.x: Strengthening your Cybersecurity Framework

BlueTouch Online Technical Webcasts

BTO Technical Webcast Series

CloudSOC

CloudSOC Differences R2.1.3 (August 2019) **NEW!**
CloudSOC Differences R2.1.2 (May 2019)
CloudSOC R2: Understanding Reporting Options in CloudSOC and Third-Party Solutions
CloudSOC R2: Protecting Data in Cloud Applications
CloudSOC R2: Identifying and Remediating Risky Behavior in Cloud Applications
CloudSOC R2: Identifying How Data is Used and Shared in Cloud Applications
CloudSOC R2: Identifying and Addressing Potential Risks in Cloud Applications
CloudSOC R2: Configuring the Symantec CloudSOC Portal
CloudSOC R2.1.1: Differences (Sep 2018)

Cloud Web Security Services

Web Security Service Differences (July 2019) **NEW!**
WSS R1: Cloud Delivered Security **NEW!**
WSS R1: Course Overview **NEW!**
WSS R1: Create a More Effective Work Environment for Employee Web Usage **NEW!**
WSS R1: Enable Corporate Access to Securely Access the Internet **NEW!**
WSS R1: Enable Mobile Users to Securely Access the Internet **NEW!**
WSS R1: Enable Remote Users to Securely Access the Internet **NEW!**
WSS R1: Enable SSL Traffic Inspection **NEW!**
WSS R1: General Administration **NEW!**
WSS R1: Identify Web Usage and Security Statistics with Reports **NEW!**
WSS R1: Preventing Malware Caused by Web Usage **NEW!**
WSS R1: Provide Safe and Proper Web Usage Based on User Identity **NEW!**
WSS R1: Providing Threat Protection Against Malware **NEW!**
WSS R1: WSS Infrastructure, Connection Architecture and Functionality
WI R1: Enable Broad Web Access and Avoid Over-blocking while still Protecting Users from Unsafe Websites
WI R1: Prevent Users from Submitting Corporate Credentials and Other Sensitive Information on Unknown and Malicious Sites
WI R1: Reporting, Monitoring, and Troubleshooting
WI R1: Web Isolation Deployment and Configuration
WSS: SD Cloud Connector Solution Demo

WSS: Web Isolation Demo
WSS: Cloud Firewall
WSS: Traffic Redirection
WSS: SD Cloud Connector Solution
WSS: Web Isolation
Cloud WSS: Authentication
Cloud WSS: CASB CloudSOC Integration
Cloud WSS: Course Overview
Cloud WSS: DLP Integration
Cloud WSS: Explicit Proxy Access Method
Cloud WSS: Firewall/VPN Access Method Module
Cloud WSS: General Administration
Cloud WSS: Malware Analysis
Cloud WSS: Mobile Device Access Method
Cloud WSS: Policy
Cloud WSS: Proxy Forwarding Access Method
Cloud WSS: Remote Client Access Method
Cloud WSS: Reports
Cloud WSS: Selecting a Solution
Cloud WSS: SSL
Cloud WSS: Web Security Service Overview
Content Analysis 2.2 Administration

Cloud Workload Protection

CWP R1: Cloud Workload Protection for Storage **NEW!**
CWP R1: Troubleshooting
CWP R1: Managing Events
CWP R1: Monitoring Cloud Workload Protection
CWP R1: Managing Events
CWP R1: Monitoring Cloud Workload Protection
CWP R1: Managing Policies
CWP R1: Getting Started Using the Wizard
CWP R1: Introduction to Cloud Workload Protection
CWP R1: Setup and Deployment of Agents

Control Compliance Suite

CCS 12: Ad Hoc Queries
CCS 12: Controls Studio
CCS 12: External Data Integration
CCS 12: Getting Started with CCS 12.0
CCS 12: Initial Configuration
CCS 12: Installing the CCS Suite
CCS 12: Introduction to CCS 12.0
CCS 12: Reporting and Dashboards
CCS 12: Standards Manager
Control Compliance Suite 11.0 Differences
Control Compliance Suite 11.x Administration
Control Compliance Suite 11.x Assessment Manager

Control Compliance Suite 11.x Policy Manager
Control Compliance Suite 11.x Risk Manager
Control Compliance Suite Advanced Check Writing: Standards Overview
Control Compliance Suite Vendor Risk Manager 11.0.2
CCS 11.x: Asset Schema Extensions
CCS 11.x: Reports and Dashboards around KPIs

Cyber Security Services

CSS Admin R1: Achieving 24x7 Global Threat Monitoring
CSS Admin R1: Cyber Security Services Overview
CSS Admin R1: DeepSight Datafeeds and Integration
CSS Admin R1: DeepSight Portal Demo
CSS Admin R1: Impact of Security Intelligence
CSS Admin R1: Introduction to the DeepSight API
CSS Admin R1: Managed Security Services Overview
CSS Admin R1: Managed Security Services Review
CSS Admin R1: MSS Platform and Architecture Overview
CSS Admin R1: Protecting Against Advanced Threats by Leveraging Threat Intelligence in MSS
CSS Admin R1: Provide for Timely Alerts and Custom Reporting
CSS Admin R1: Providing Relevant and Efficient Intelligence Using a Sophisticated Filter
CSS Admin R1: Security Monitoring and Managed IDS
CSS Admin R1: Timely Validation of Security Incidents

Data Loss Prevention

Data Loss Prevention 15.5 Differences
DLP 15: Data Loss Prevention Landscape
DLP 15: Educating Users to Adopt Data Protection Practices
DLP 15: Enhancing Data Loss Prevention through Integrations
DLP 15: Identifying and Describing Confidential Data
DLP 15: Locating Confidential Data Stored on Premises and in the Cloud
DLP 15: Overview of Symantec Data Loss Prevention
DLP 15: Preventing Unauthorized Exposure of Confidential Data
DLP 15: Remediating Data-Loss Incidents and Tracking Risk Reduction
DLP 15: Understanding How Confidential Data Is Being Used
DLP 15: Installing Oracle and the Symantec DLP Enforce Server
DLP 15: Installing Symantec Data Loss Prevention Detection Servers
DLP 15: Installing a Symantec Data Loss Prevention OCR Server
DLP 15: Installing the Symantec Data Loss Prevention Endpoint Agent
DLP 15: Preparing to Install Symantec Data Loss Prevention
DLP 15: Symantec Data Loss Prevention Overview
DLP 15: Upgrading Symantec Data Loss Prevention
Data Loss Prevention 15.0: Differences
Data Loss Prevention 14.6: Differences
Data Loss Prevention 14.5: Differences
DLP 14.6 Install and Deploy: Differences Between 14.0 and 14.6
DLP 14.5: Data Loss Landscape
DLP 14.5: Educating Users to Adopt Data Protection Practices
DLP 14.5: Enhancing Data Loss Prevention through Third-Party Integrations

DLP 14.5: Identifying and Describing Confidential Data
DLP 14.5: Locating Confidential Data Stored on Premises and in the Cloud
DLP 14.5: Overview of Symantec Data Loss Prevention
DLP 14.5: Preventing Unauthorized Exposure of Confidential Data
DLP 14.5: Remediating Data Loss Incidents and Tracking Risk Reduction
DLP 14.5: Understanding How Confidential Data Is Being Used
Data Loss Prevention 14.0: Administration
Data Loss Prevention 14.0: Differences
Data Loss Prevention 12.5: Administration
Data Loss Prevention 12.0 Administration Training

Data Center Security

Data Center Security 6.8 Differences
Data Center Security Server Advanced 6.7 Diagnostics and Troubleshooting
DCS:SA 6.7: Advanced Prevention
DCS:SA 6.7: Agent Management and Troubleshooting
DCS:SA 6.7: Configuring Agents
DCS:SA 6.7: Detection Policies
DCS:SA 6.7: Event Management
DCS:SA 6.7: Installation and Deployment
DCS:SA 6.7: Introduction to Security Risks
DCS:SA 6.7: Policy Overview
DCS:SA 6.7: SDCS: Server Advanced Overview
DCS:SA 6.7: System Management
DCS:SA 6.7: UNIX and Legacy Prevention Policies
DCS:SA 6.7: Windows Prevention Policies
Data Center Security: Server 6.0: Administration
Data Center Security: Server 6.5: Administration
Data Center Security: Server Advanced 6.0: Administration

Deepsight

DeepSight Technical Education Modules

Deployment Solution

DS 8.1: Building an Initial Reference Image (Advanced)
DS 8.1: Building an Initial Reference Image (Basic)
DS 8.1: Execution and Maintenance of a Migration Plan (Advanced)
DS 8.1: Execution and Maintenance of a Migration Plan (Basic)
DS 8.1: Ghost Explorer (Advanced)
DS 8.1: Ghost Explorer (Basic)
DS 8.1: Imaging MacOS (Advanced)
DS 8.1: Imaging MacOS (Basic)
DS 8.1: Overview of Endpoint Lifecycle Management (Advanced)
DS 8.1: Overview of Endpoint Lifecycle Management (Basic)
DS 8.1: Planning and Preparing for a Hardware / OS Migration (Advanced)
DS 8.1: Planning and Preparing for a Hardware / OS Migration (Basic)
DS 8.1: User Data Migration (Advanced)
DS 8.1: User Data Migration (Basic)

Diagnostic and Troubleshooting Methodology

Symantec Diagnostic and Troubleshooting Methodology

Email Security

ES.cloud R1: Help Meet Compliance and Privacy Requirements
ES.cloud R1: Overview of Email Security.cloud
ES.cloud R1: Prevent Accidental and Deliberate Data Breaches
ES.cloud R1: Protect Inboxes from Malware and Spam
ES.cloud R1: Protect from Advanced Persistent Threats
Email Security Service and Web Security Service: Administration
Email Security.cloud Supporting DMARC Validation
Email Security.cloud Technical Education Courses

Encryption and Encryption Management Server

Encryption Management Server 3.4.1 Diagnostics and Troubleshooting
SEMS 3.3: Administrative Keys
SEMS 3.3: Clustering
SEMS 3.3: Configuring Client Enrollment
SEMS 3.3: Configuring General Policy Settings
SEMS 3.3: Configuring Symantec Drive Encryption
SEMS 3.3: Configuring Symantec File Share Encryption
SEMS 3.3: Consumers and Groups
SEMS 3.3: Course Introduction
SEMS 3.3: Cryptography Essentials
SEMS 3.3: Installing Symantec Encryption Desktop
SEMS 3.3: Installing Symantec Encryption Management Server
SEMS 3.3: Key Not Found
SEMS 3.3: Keys
SEMS 3.3: Mail Policy
SEMS 3.3: Monitoring and Reporting
SEMS 3.3: Other Symantec Encryption Desktop Features
SEMS 3.3: Preparing Symantec Encryption Management Server for Symantec Desktop Clients
SEMS 3.3: Server Messaging
SEMS 3.3: Symantec Drive Encryption Management Recovery
SEMS 3.3: Symantec Encryption Desktop Messaging
SEMS 3.3: Symantec Encryption Introduction
SEMS 3.3: Web Email Protection
Endpoint Encryption 11.x Technical Education Course
PGP Universal Server 3.2 and PGP Desktop 10.2: Administration

Endpoint Detection and Response

Endpoint Detection and Response 4.2 Technical Update **NEW!**
Endpoint Detection and Response 4.1 Differences
Endpoint Detection and Response 4.0 Differences

Endpoint Protection

Endpoint Protection 15 Differences (August 2019) **NEW!**
Endpoint Protection 14.2 RU1 Differences
Endpoint Protection 15.0 Differences (April 2019)
Endpoint Protection 15.0 Fundamentals
What’s New in Symantec Endpoint Cloud Connect Defense

Endpoint Protection 15.0: Differences (Nov 2018)
Endpoint Protection Cloud R2.0.1: Differences
SEP Hardening App Control: Differences
SEP Hardening App Center: Differences
What's New in Symantec Endpoint Protection 14.2
What's New in Symantec Endpoint Protection 14.1
What's New in Symantec Endpoint Protection 14
Endpoint Protection 14: Differences
Migrating to Symantec Endpoint Protection 14
SEP 14: Client Communication Issues
SEP 14: Content Distribution Issues
SEP 14: Controlling Endpoint Integrity and Compliance
SEP 14: Discovering Endpoint Client Implementation Methods and Strategies
SEP 14: Enforcing Adaptive Security Posture
SEP 14: Enforcing Content Updates on Endpoints using the Best Method
SEP 14: Extending the SEP Infrastructure
SEP 14: Installation and Migration Issues
SEP 14: Monitoring and Managing Endpoints
SEP 14: Performance Issues
SEP 14: Preparing and Delivering a Successful SEP Implementation
SEP 14: Responding to a Security Incident
SEP 14: Securing Endpoints Against File-Based Threats
SEP 14: Securing Endpoints Against Network-Based Attacks
SEP 14: Troubleshooting Techniques and Tools
SEP 14: Troubleshooting the Console
SEP Mobile Self Service Training
Endpoint Protection 12.1.5 Technical Education Course
Endpoint Protection 12.1.6 Differences
Endpoint Protection 12.x: Administration
Endpoint Protection 12.x: Maintain and Troubleshoot

Ghost Solution Suite

Ghost Solution Suite 3.0: Administration

Information Centric Analytics (ICA)

Information Centric Analytics 6.5 Skills Assessment **NEW!**
ICT 15.5: Improve Effectiveness of Data Classification by Integrating Data Loss Prevention **NEW!**
ICT 15.5: Introduction to Data Classification and Tagging
ICT 15.5: Introduction to Information Centric Tagging
ICSM 15.5: Introduction
ICT 15.5: Architecture and Implementation
ICT 15.5: Identify and Classify Documents to Prevent Unauthorized Access
Information Centric Security Module 15.5 Differences
ICE R1: Protect Sensitive Cloud Documents
ICE R1: Architecture and Implementation
ICT 15.1: Architecture and Implementation
ICA 6.5: Architecture and Implementation
ICA 6.5: Introduction

ICA 6.5: Manage and Administer
Information Centric Encryption R1.0: Introduction
Information Centric Security Module 15.1: Introduction
Information Centric Tagging 15.1: Introduction
Information Centric Analytics (ICA): Dashboards
Information Centric Analytics 6.5: Differences

Integrated Cyber Defense Exchange

Integrated Cyber Defense Exchange 1.3 Differences
Integrated Cyber Defense Exchange 1.2 Differences

IT Management Suite

ITMS 8.5: Monitoring, Alerting, and Resolving Events **NEW!**
ITMS 8.5: Server Management Suite Overview **NEW!**
ITMS 8.5: Identifying Relationships Between Assets
ITMS 8.5: Managing the Contract and Procurement Process
ITMS 8.5: Understanding Software License Compliance
IT Management Suite 8.5: Differences
IT Management Suite 8.1 Diagnostics and Troubleshooting
ITMS 8.1: Business Analytics & Reporting
ITMS 8.1: Discovering Resources within the Environment
ITMS 8.1: Effective Software Management
ITMS 8.1: Identifying Relationships Between Assets
ITMS 8.1: Improved Security Through Automated Patch Management
ITMS 8.1: Managing the Contract and Procurement Process
ITMS 8.1: Reducing Desk-side Visits with Remote Support
ITMS 8.1: Understanding Software License Compliance
ITMS 8.0 Webinar: Exploring Symantec ITMS 8.0 SCS Exam (250-423) Objectives and Use Cases
ITMS 8.0: Business Analytics and Reporting
ITMS 8.0: Discovering Resources
ITMS 8.0: Effective Software Management
ITMS 8.0: Identifying Relationships between Assets
ITMS 8.0: Improved Security Through Automated Patch Management
ITMS 8.0: Managing the Contract and Procurement Process
ITMS 8.0: Reducing Desk-side Visits Through Remote Support
ITMS 8.0: Understanding Software License Compliance
IT Management Suite 7.5: Administration
ITMS Fundamentals: Basic Architecture Overview
ITMS Fundamentals: Installing and Configuring
ITMS Fundamentals: Managing Policies, Jobs, and Tasks
ITMS Fundamentals: Managing Targets and Filters
ITMS Fundamentals: Organizational Views and Groups
ITMS Fundamentals: Securely Managing Remote Computers
ITMS Fundamentals: SMP Overview
Client Management Suite 7.6: Administration
Asset Management Suite 7.5: Administration
ServiceDesk 7.5: Administration
Managing Software Licenses with Symantec IT Management Suite 7.5

Workflow Solution 7.6: Administration
Workspace Streaming 7.5
Workspace Virtualization 7.5

Managed Security Services

Managed Security Services Portal FAQ

Management Center

MC for Proxy R1: Increase Visibility of a Secure Web Gateway Solution
MC for Proxy R1: Introduction to Management Center
MC for Proxy R1: Introduction to Symantec Reporter
MC for Proxy R1: Provide Enhanced Reporting by Integrating Reporter with Management Center
MC for Proxy R1: Simplify Administrative Overhead of a Complete Secure Web Gateway Solution
MC for Proxy R1: Increase visibility of a Secure Web Gateway Solution
MC for Proxy R1: Introduction to Management Center
MC for Proxy R1: Introduction to Symantec Reporter
MC for Proxy R1: Provide Enhanced Reporting by Integrating Reporter with Management Center
MC for Proxy R1: Simplify Administrative Overhead of a Complete Secure Web Gateway Solution
Management Center Essentials
Migration from BlueCoat Director to Symantec Management Center

Messaging Gateway

Messaging Gateway 10.7 Differences
SMG 10.6: Adaptive Reputation Management
SMG 10.6: Anti-Malware
SMG 10.6: Anti-Spam
SMG 10.6: Content Filtering
SMG 10.6: Control Center
SMG 10.6: Installation
SMG 10.6: Introduction
SMG 10.6: Introduction to Network Prevent for Email and Content Analysis
SMG 10.6: Users and Host Configuration
Messaging Gateway 10.0: Administration
Messaging Gateway Differences

Mail Threat Defense

MTD Configuring Email Security Policies

PacketShaper

PacketShaper 11.9.1: Classifying Traffic
PacketShaper 11.9.1: Fault Tolerance, Deployments and Platform Health
PacketShaper 11.9.1: Initial Configuration and Understanding Applications
PacketShaper 11.9.1: Management and Identifying Network Issues
PacketShaper 11.9.1: Prioritizing Traffic in the Network
PacketShaper 11.9.1: Responding to Network Issues
PacketShaper 11.9.1: Welcome to PacketShaper
PacketShaper Essentials 11.9.1

Protection Engine

Protection Engine 7.5 Administration and Deployment

ProxySG

ProxySG 6.6 Diagnostics and Troubleshooting
ProxySG: Access Logging on the ProxySG
ProxySG: Advanced Authentication Concepts on the ProxySG
ProxySG: Advanced Encrypted Traffic Management on the ProxySG
ProxySG: Authenticating Users on the ProxySG
ProxySG: Exceptions and Notifications on the ProxySG
ProxySG: Hypertext Transfer Protocol
ProxySG: Intro to Content Filtering
ProxySG: Intro to CPL
ProxySG: Intro to Encrypted Traffic Management
ProxySG: Intro to ProxySG S200
ProxySG: Intro to ProxySG S500
ProxySG: Introduction to Content Policy Language (CPL)
ProxySG: Introduction to Encrypted Traffic Management on the ProxySG
ProxySG: Introduction to HTTPS
ProxySG: Introduction to PSG S400
ProxySG: Introduction to the ProxySG Management Console
ProxySG: Introduction to the Symantec Blue Coat ProxySG Secure Web Gateway
ProxySG: Introduction to the Visual Policy Manager
ProxySG: Introduction to the Visual Policy Manager (Pre)
ProxySG: Managing Downloads on the ProxySG
ProxySG: Policy Tracing on the ProxySG
ProxySG: ProxyAV Essentials
ProxySG: ProxySG Integration
ProxySG: PSG Performance Monitoring
ProxySG: SG Migration 510, 810, 900, 9000
ProxySG: SGOS Architecture
ProxySG: SGOS Architecture Fundamentals
ProxySG: Symantec Blue Coat ProxySG Initial Configuration
ProxySG: Symantec Blue Coat ProxySG Proxy Services
ProxySG: Symantec Blue Coat ProxySG Security Deployment Options
ProxySG: System Diagnostics on the ProxySG
ProxySG: Troubleshooting Policies with Policy Tracing
ProxySG: Using SNMP
ProxySG: Using Stunnels and Encrypted Tap on the ProxySG
ProxySG: WebFilter, WebPulse, and the Global Intelligence Network

Reporter

Reporter Essentials

SSL Visibility Appliance

SSL Visibility 5.0 Differences
SSL Visibility 5.0 Virtual Appliance Introduction
SSL Visibility 4.5 Differences **NEW!**
SSL Visibility 4.4: Differences
SSLV 4.3: Deploying the SSLV
SSLV 4.3: Expose Encrypted Inbound Traffic
SSLV 4.3: Expose Encrypted Outbound Traffic

SSLV 4.3: Expose Encrypted Threats for Forensic Analysis While Maintaining Compliance Regulations
SSLV 4.3: Introduction to Encrypted Traffic Management
SSLV 4.3: Introduction to Encrypted Traffic Management with Symantec SSLV
SSLV 4.3: Migrate and Upgrade SSLV
SSLV 4.3: Offloading SSL Decryption for ProxySG Efficiency
SSLV 4.3: Simplify Management of Multiple SSLV Appliances with Management Center
SSLV 4.3 Administration (Basic)
SSL Visibility 4.x Deployment
SSLV 4.x Differences
SSLV Essentials 3.0.1: Course Opening
SSLV Essentials 3.0.1: Deployment Modes
SSLV Essentials 3.0.1: Integration
SSLV Essentials 3.0.1: Introduction to the SSL Visibility Appliance
SSLV Essentials 3.0.1: Monitoring and Troubleshooting
SSLV Essentials 3.0.1: PKI Management
SSLV Essentials 3.0.1: Platform Management
SSLV Essentials 3.0.1: Policies
SSLV Essentials 3.0.1: SSL Visibility Appliance Initial Configuration
SSLV Essentials 3.0.1: Working with SSL

Validation and Identity Protection

VIP Service Differences R1.2.1 (June 2019)
VIP Diagnostics and Troubleshooting R1
IAS Intro R1: Introduction to Identity and Authentication
IAS Intro R1: Introduction to Symantec Identity and Authentication Services
VIP Service R1: Improve Web Application Security with Multi-Factor Authentication
VIP Service R1: Plan and Implement the Symantec VIP Service
VIP Service R1: Review of the Symantec VIP Service
VIP Service R1: Secure VPN and Remote Access Using RADIUS and VIP Strong Authentication
VIP Service R1: Select the Appropriate VIP Strong Authentication Method
VIPAM R1: Control Access to Web Applications Based Upon Organization Requirements
VIPAM R1: Enable Multi-factor Authentication Based Upon Business Requirements
VIPAM R1: Enhance Security and Improve User Experience Through Single Sign-on
VIPAM R1: Introduction to Symantec VIP Access Manager
Validation and ID Protection Services VIP 9.X
VIP General Modules

X-Series

X-Series: Flow Processing
X-Series: High Availability
X-Series: Installation and Configuration Fundamental
X-Series: Monitoring & Troubleshooting
X-Series: Platform Hardware Overview
X-Series: System Maintenance
X-Series: System Management