Administration of Symantec™ Data Loss Prevention 12
Exam Details

Contents

General Information

You are about to take the Administration of Symantec Data Loss Prevention 12 exam.

This exam is based primarily on training content taught in the *Symantec Data Loss Prevention 12: Administration* course. The recommended course to prepare for this exam includes: *Symantec Data Loss Prevention 12: Administration (ILT/VA/WBT)* and *Symantec Data Loss Prevention 12: Install and Deploy* courses.

Recommended Preparation

Recommended Training:
Symantec Data Loss Prevention 12: Administration (ILT/VA or WBT)
Symantec Data Loss Prevention 12: Install and Deploy (WBT)

- Symantec Data Loss Prevention 12: Differences (WBT – available to SYMC Internals Only)

Note regarding recommended training course: If you do not have prior experience with this product, it is recommended that you complete an in-person, classroom training or Virtual Academy virtual classroom training class in preparation for the SCS exam. If you have experience with this product, you may find an online course equivalent to be sufficient. Be cautioned that attendance in a training course does not guarantee passage of a certification exam.

Familiarity with product documentation:

- Symantec Data Loss Prevention Third Party License Agreements
- Symantec Data Loss Prevention 64-bit Server Migration and Tuning Guide
- Symantec Data Loss Prevention Administration Guide
- Symantec Data Loss Prevention Data Insight Implementation Guide

- Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)
- Symantec Data Loss Prevention Email Quarantine Connect FlexResponse Implementation Guide
- Symantec Data Loss Prevention Encryption Insight Implementation Guide
- Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide
- Symantec Data Loss Prevention Installation Guides for Windows
- Symantec Data Loss Prevention Installation Guides for Linux
- Symantec Data Loss Prevention Lookup Plug-In Guide
- Symantec Data Loss Prevention Network Monitor and Prevent Performance Sizing Guidelines
- Symantec Data Loss Prevention Release Notes
- Symantec Data Loss Prevention Reporting API Developers Guide
- Symantec Data Loss Prevention Integration Guide for Squid Web Proxy
- Symantec Data Loss Prevention SharePoint Quarantine FlexResponse Plug-in Implementation Guide
- Symantec Data Loss Prevention Supportability Telemetry Guide
- Symantec Data Loss Prevention System Maintenance Guide
- Symantec Data Loss Prevention System Requirements and Compatibility Guide
- Symantec Data Loss Prevention TMG Integration Guide
- Symantec Data Loss Prevention Upgrade Guide for Windows
- Symantec Data Loss Prevention Upgrade Guide for Linux
- Symantec Data Loss Prevention Utilities Guide
- Symantec Data Loss Prevention VML Best Practices Guide
- Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide – Partner only
- Symantec Data Loss Prevention DLP Software
- Symantec Data Loss Prevention Upgrade Guide for Windows
- Symantec Data Loss Prevention Detection Customization Guide
- Symantec Data Loss Prevention Incident Reporting Update API Examples
- Symantec Data Loss Prevention 3rdparty attributions
- Symantec Data Loss Prevention Solution Pack Descriptions:
    - Data Classification for Enterprise Vault Solution Pack
    - Energy and Utilities Solution Pack
    - EU and UK Solution Pack
    - Federal Solution Pack
    - Financial Services Solution Pack
    - General Solution Pack
    - Health Care Solution Pack
    - High Tech Solution Pack
    - Insurance Solution Pack
    - Manufacturing Solution Pack
    - Media and Entertainment Solution Pack
    - Pharmaceutical Solution Pack

  - Retail Solution Pack
  - Standard Solution Pack
  - Telecom Solution Pack
- Symantec Data Loss Prevention Pack for Altiris IT Analytics Solution 7.1 SP2 User Guide

Examples of Hands-on Experience (Real World or Virtual):

- Experience with the product through shadowing of a successful risk assessment, technical evaluation, product deployment, or six months experience administering Symantec Data Loss Prevention 12.
- Install Symantec Data Loss Prevention software including a detection server.
- Create reports using filtering and summarization.
- Navigate to appropriate reports including dashboards, incident lists, incident snapshots, and so forth.
- Use product specific out-of-the-box reports.
- Remediate incidents using response rules, workflow, and/or roles-based access control (RBAC).
- Create new policies using the policy builder including those based on templates.
- Configure automated and smart response rules and execute appropriately.
- Use product specific response rules including those for Network Prevent, Mobile Prevent, Network Protect, Network Discover, Endpoint Prevent, and Endpoint Discover.
- Manage DLP Agents.
- Define mobile device IP ranges to identify mobile traffic.
- Use available detection methods in policies and be able to capture incidents.
- Create Network Discover file system targets and run related scans.
- Configure targets to meet bandwidth and scheduling requirements.
- Create Endpoint Discover targets and run related scans.
- Create alerts for designated events.
- Create attributes, policy groups, roles, and users.
- Configure basic system settings.
- Manage credentials.
- Use online help.
- Recognize problems with system components and begin basic troubleshooting.
- Install and upgrade Symantec Data Loss Prevention software including Oracle, Symantec Management Platform, and Endpoint agents.
- Describe and apply best practices and priorities for creating and implementing response rules.
- Select and prepare data sources for EDM indexes.
- Describe the creation of an EDM index with the Remote Indexer.
- Plan and carry out an efficient strategy for regularly updating EDM indexes.
- Use advanced EDM features.

- Select and prepare data sources for IDM indexes.
- Plan and carry out an efficient strategy for regularly updating IDM indexes.
- Select and prepare data samples for creating VML profiles.
- Implement policy best practices.
- Implement policy lifecycle stages.
- Protect data by quarantining and/or copying to a secure location.
- Understand the FlexResponse platform for custom remediation.
- Block Endpoint actions based on a user's Active Directory group membership.
- Describe server administration tasks and tools for generating event and traffic reports.
- Describe various troubleshooting techniques for the system including understanding the message chain and performing log analysis.
- Describe effective management of agents.
- Configure IP and L7 filters.
- Configure content filters to include discover and endpoint filters.
- Explain and define Mobile Device Management (MDM) virtual private network (VPN) profiles.
- Explain and define iOS profiles using the Symantec Management Console.
- Use Mobile Prevent to monitor email, Web, and application communications from an iOS device.
- Set up Active Directory/LDAP authentication, and the Certificate Authority/Simple Certification Enrollment Protocol.
- Install additional locales and language packs.
- Integrate Network Prevent for email.
- Define Data Insight and Symantec Management Platform (SMP) and explain its integration with Symantec Data Loss Prevention.

Important points you should know about this exam before you begin

- You will have up to 105 minutes to complete the exam.
- You will be presented with 70 - 80 items on the exam.
- You must score 72% correct in order to pass.
- Your final score will be calculated on the number of items you answer correctly so please be sure to answer all questions. Passing this exam counts toward a Symantec Certified Specialist (SCS) award.
- If you do not pass an exam on your first attempt, you must wait at least 3 days (72 hours) before a second attempt. If you do not pass an exam on your second attempt, then you must wait at least 2 weeks (14 days) between each additional attempt. If you need to retake an exam that you have already passed in order to fulfill a certification track requirement, you may do so after 3 months.

How to register

Exams are administered through Pearson VUE Worldwide Test Centers. Candidates are required to obtain a "CertTracker/Login and Password (ID)"in order to register for any exams.

To schedule a technical proctored exam:
1. Login to CertTracker with your username and password.

2. On the Candidate Landing Page, view the left hand navigation and click “Schedule Pearson VUE Exam” to schedule a proctored exam.

3. On the screen listing the exams, choose your exam and follow the on-screen instructions to complete your transaction.

4. See the detailed step-by-step registration instructions: Partners / Employees

IMPORTANT NOTES ABOUT REGISTRATION:
Your name must exactly match what is listed in CertTracker and your identification that is presented at a Pearson VUE test center or you will be unable to take an exam and forfeit your exam fee. Candidate name and company name changes can only be made by submitting a CertTracker Incident or emailing Global_Exams@symantec.com; please allow 24-48 hours for CertTracker updates to reflect in all systems.

You may use a voucher or major credit card (AMEX, MasterCard, Visa, or JCB) to pay for your exam.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com