Administration of Symantec™ Data Loss Prevention 11.5
Study Guide

The following tables list the Symantec SCS Certification exam objectives for the Administration of Symantec Data Loss Prevention 11.5 exam and how these objectives align to the Symantec Data Loss Prevention 11.5: Administration course.

Recommended courses to prepare for this exam:
- Symantec Data Loss Prevention 11.5: Administration (ILT/VA or WBT)

The product documentation for this exam is:
- Symantec Data Loss Prevention Administration Guide
- Symantec Data Loss Prevention Custom File Type Detection Guide
- Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)
- Symantec Data Loss Prevention Installation Guides
- 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 Integration Guide for Squid Web Proxy
- 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 Guides
- Symantec Data Loss Prevention Utilities Guide
- Symantec Data Loss Prevention VML Best Practices Guide
- Symantec Data Loss Prevention Solution Pack Descriptions
- Symantec Data Loss Prevention Third-Party License Agreements
- Symantec Data Loss Prevention Data Insight Implementation Guide
- Symantec Data Loss Prevention Detection Customization Guide
- Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server
- Symantec Data Loss Prevention Reporting API Developers Guide
- Symantec Data Loss Prevention Server FlexResponse Platform Developers 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 DLP 11.5.
- 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, Symantec Data Loss Prevention for Tablets, Network Protect, and Endpoint Prevent.
• Manage DLP Agents.
• Define tablet IP ranges to identify tablet traffic.
• Use the TrueMatch 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 Symantec Data Loss Prevention software including a Detection server.
• 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.
• Configure Mobile Device Management (MDM) virtual private network (VPN) profiles.
• Configure iOS profiles using the Symantec Management Console.
• Use Tablet Prevent to monitor email, Web, and application communications from an iPad.
• 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.
• Install Data Insight and Symantec Management Platform (SMP).

For more information on the Symantec Certification Program, visit http://go.symantec.com/certification.
## EXAM AREA 1
### Overview and Architecture

<table>
<thead>
<tr>
<th>SCS Exam Objectives</th>
<th>Course Topics from Symantec Data Loss Prevention 11.5: Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe Data Loss Prevention as it pertains to the industry.</td>
<td>Lesson: Introduction to Symantec Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>Topic: Symantec Data Loss Prevention Overview</td>
</tr>
<tr>
<td>Describe the features and functionality of Symantec Data Loss Prevention 11.5.</td>
<td>Lesson: Introduction to Symantec Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>Topic: Symantec Data Loss Prevention Overview</td>
</tr>
<tr>
<td>Describe the Symantec Data Loss Prevention 11.5 architecture including each product's architecture.</td>
<td>Lesson: Introduction to Symantec Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>Topic: Symantec Data Loss Prevention Architecture</td>
</tr>
</tbody>
</table>

## EXAM AREA 2
### Installation and Configuration

<table>
<thead>
<tr>
<th>SCS Exam Objectives</th>
<th>Course Topics from Symantec Data Loss Prevention 11.5: Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe how to install Symantec Data Loss Prevention 11.5.</td>
<td>Not covered in this course; requires on-the-job experience.</td>
</tr>
<tr>
<td></td>
<td>Information in product documentation.</td>
</tr>
<tr>
<td>Describe how to configure policies to effectively capture incidents including all TrueMatch detection methods.</td>
<td>Lesson: Policy Management</td>
</tr>
<tr>
<td></td>
<td>Topic: Policy overview</td>
</tr>
<tr>
<td></td>
<td>Topic: Creating policy groups</td>
</tr>
<tr>
<td></td>
<td>Topic: Using policy templates</td>
</tr>
<tr>
<td></td>
<td>Topic: Building policies</td>
</tr>
<tr>
<td></td>
<td>Topic: Policy development best practices</td>
</tr>
<tr>
<td></td>
<td>Lesson: Described Content Matching</td>
</tr>
<tr>
<td></td>
<td>Topic: DCM detection methods</td>
</tr>
<tr>
<td></td>
<td>Topic: Using DCM in policies</td>
</tr>
<tr>
<td></td>
<td>Lesson: Exact Data Matching and Directory Group Matching</td>
</tr>
<tr>
<td></td>
<td>Topic: Exact data matching (EDM)</td>
</tr>
<tr>
<td></td>
<td>Topic: Directory group matching (DGM)</td>
</tr>
<tr>
<td></td>
<td>Topic: Advanced EDM</td>
</tr>
<tr>
<td></td>
<td>Lesson: Indexed Document Matching</td>
</tr>
<tr>
<td></td>
<td>Topic: IDM detection methods</td>
</tr>
<tr>
<td></td>
<td>Topic: Using IDM in policies</td>
</tr>
<tr>
<td></td>
<td>Lesson: Vector Machine Learning</td>
</tr>
<tr>
<td></td>
<td>Topic: Vector Machine Learning (VML)</td>
</tr>
<tr>
<td></td>
<td>Topic: Creating a VML profile</td>
</tr>
<tr>
<td>Describe how to configure and manage automated and smart response rules to remediate incidents appropriately.</td>
<td>Lesson: Response Rule Management</td>
</tr>
<tr>
<td></td>
<td>Topic: Response rule overview</td>
</tr>
<tr>
<td></td>
<td>Topic: Creating Automated Response rules</td>
</tr>
<tr>
<td></td>
<td>Topic: Creating Smart Response rules</td>
</tr>
<tr>
<td></td>
<td>Topic: Response rule best practices</td>
</tr>
<tr>
<td>SCS Exam Objectives</td>
<td>Course Topics from Symantec Data Loss Prevention 11.5: Administration</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Describe how to configure Network Monitor to capture network incidents. | Lesson: Network Monitor Review  
Topic: Review of Network Monitor  
Topic: Protocols  
Topic: Traffic filtering  
Topic: Network Monitor best practices |
| Describe how to configure Network Prevent with appropriate MTAs or web proxies to capture incidents and block network communications. | Lesson: Introduction to Network Prevent  
Topic: Network Prevent overview  
Topic: Introduction to Network Prevent (Email)  
Topic: Introduction to Network Prevent (Web) |
| Describe how to configure Network Discover targets to capture incidents and configure Network Protect to quarantine or copy files. | Lesson: Introduction to Network Discover and Network Protect  
Topic: Network Discover and Network Protect overview  
Topic: Configuring Discover targets  
Topic: Protecting data  
Topic: FlexResponse platform  
Topic: Running and managing scans  
Topic: Reports and remediation  
Topic: Network Discover and Network Protect best practices |
| Describe how to configure Endpoint Prevent agents to block endpoint actions and configure Endpoint Discover targets to capture endpoint incidents. | Lesson: Introduction to Endpoint Prevent  
Topic: Endpoint Prevent overview  
Topic: Configuring Endpoint Prevent  
Topic: Detection capabilities at the Endpoint  
Topic: Managing agents  
Topic: Creating Endpoint response rules  
Topic: Capturing Endpoint Prevent incidents and viewing them in reports  
Topic: Endpoint Prevent best practices  
Lesson: Introduction to Endpoint Discover  
Topic: Endpoint Discover overview  
Topic: Creating and running Endpoint Discover targets  
Topic: Using Endpoint Discover reports and reporting features |
| Describe how to configure filters to focus the amount of traffic or amount of files that are scanned. | Lesson: Network Monitor Review  
Topic: Traffic filtering  
Topic: Network Monitor best practices |
| Describe how to configure DLP for Tablets with appropriate iOS profiles, VPN settings, and MDM/SMM settings to capture incidents and block tablet communications. | Lesson: Introduction to Symantec Data Loss Prevention for Tablets  
Topic: Overview  
Topic: Installation and configuration  
Topic: MDM configuration and integration  
Topic: VPN configuration  
Topic: Policy and response rule configuration  
Topic: Reporting and remediation  
Topic: Logging and troubleshooting |
### EXAM AREA 3
Management and Reporting

<table>
<thead>
<tr>
<th>SCS Exam Objectives</th>
<th>Course Topics from Symantec Data Loss Prevention 11.5: Administration</th>
</tr>
</thead>
</table>
| Describe and apply the various tasks and tools associated with server and system administration. | Lesson: System Administration  
Topic: Server administration  
Topic: Troubleshooting |
| Describe how to manage DLP Agents.                                                   | Lesson: Introduction to Endpoint Prevent  
Topic: Endpoint Prevent best practices  
Lesson: Managing Endpoint DLP Agents  
Topic: Managing agents |
| Describe how to create, use, and distribute reports.                                 | Lesson: Navigation and Reporting  
Topic: Reporting and analysis  
Topic: Report navigation, preferences, and features  
Topic: Report filters  
Topic: Report commands |
| Describe how to remediate incidents effectively including use of role-based access control. | Lesson: Incident Remediation and Workflow  
Topic: Incident remediation and workflow  
Topic: Managing users and attributes  
Topic: Custom attribute lookup |
| Describe how to manage and maintain policy components.                               | Lesson: Policy Management  
Topic: Policy overview  
Topic: Creating policy groups  
Topic: Using policy templates  
Topic: Building policies  
Topic: Policy development best practices  
Lesson: Response Rule Management  
Topic: Response rule overview  
Topic: Creating Automated Response rules  
Topic: Creating Smart Response rules  
Topic: Response rule best practices |
| Describe how to reduce risk over time.                                               | Lesson: Enterprise Enablement  
Topic: Preparing for risk reduction  
Topic: Risk reduction  
Topic: DLP Maturity model |

### EXAM AREA 4
Basic Troubleshooting

<table>
<thead>
<tr>
<th>SCS Exam Objectives</th>
<th>Course Topics from Symantec Data Loss Prevention 11.5: Administration</th>
</tr>
</thead>
</table>
| Identify basic database issues in Symantec Data Loss Prevention 11.5.               | Not covered in this course; requires on-the-job experience.  
Information in product documentation. |
<table>
<thead>
<tr>
<th>SCS Exam Objectives</th>
<th>Course Topics from Symantec Data Loss Prevention 11.5: Administration</th>
</tr>
</thead>
</table>
| Identify and describe how to troubleshoot Enforce issues in Symantec Data Loss Prevention 11.5. | Lesson: System Administration  
Topic: Server administration  
Topic: Troubleshooting  
Lesson: Introduction to Symantec Data Loss Prevention  
Topic: Symantec Data Loss Prevention Architecture |
| Identify and describe how to troubleshoot endpoint agent issues in Symantec Data Loss Prevention 11.5. | Lesson: Introduction to Endpoint Prevent  
Topic: Detection capabilities at the Endpoint  
Topic: Endpoint Prevent best practices  
Lesson: Managing Endpoint DLP Agents  
Topic: Managing agents |
| Identify and describe how to troubleshoot detection issues in Symantec Data Loss Prevention 11.5. | Lesson: Described Content Matching  
Topic: DCM detection methods  
Topic: Using DCM in policies  
Lesson: Exact Data Matching and Directory Group Matching  
Topic: Exact data matching (EDM)  
Topic: Directory group matching (DGM)  
Topic: Advanced EDM  
Lesson: Indexed Document Matching  
Topic: IDM detection methods  
Topic: Using IDM in policies  
Lesson: Vector Machine Learning  
Topic: Vector Machine Learning (VML)  
Topic: Creating a VML profile |
| Identify and describe how to troubleshoot detection server issues in Symantec Data Loss Prevention 11.5. | Lesson: System Administration  
Topic: Server administration  
Topic: Troubleshooting |
| Identify and describe the diagnostic tools in Symantec Data Loss Prevention 11.5. | Lesson: System Administration  
Topic: Server administration  
Topic: Troubleshooting |

If you have questions about the Symantec Certification Program, send an email to Customer_Certifications@symantec.com.
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