Forcepoint DLP Administrator Virtual Instructor-Led Training

Datasheet

October 2021

Forcepoint

forcepoint.com

Forcepoint (DLP)Data Loss Prevention Administrator Virtual Instructor-Led Training

DTADM

The Forcepoint Data Loss Prevention (DLP) Administrator course instructs you how to test an existing deployment, administer policies and reports, handle incidents and endpoints and upgrade and manage the Forcepoint DLP system. You will develop skills in creating data policies, building custom classifiers, performing system maintenance, and using predefined policies, incident management and reports.

Audience

- System administrators, data security administrators, IT staff
- Sales engineers, consultants, implementation specialists
- Forcepoint channel partners and IT staff
- DLP incident and forensic analysts

Format:

Virtual Instructor-Led Training

Duration:

16 hours, typically delivered in 4 sessions (4 hours per session), 2 hours outside of class for the exam

Course Price:

$1,150 USD

Exam Price:

One attempt is included

Course objectives

- Identify and define core DLP terminology, resources, and architecture.
- Define and create each type of DLP classifier.
- Define and create each type of DLP resource, including URL categories, action plans, and notifications.
- Define and create each type of DLP policy, rule, and exception.
- Manage policies and rules using bulk updates and policy levels.
- Explain and test the capabilities and modes of OCR.
- Build, deploy, and manage the Forcepoint One Endpoint.
- Define the terms specific to DLP incident reporting.
- List and explain the report types in the report catalog.
- Manage and customize incident reports.
- Analyze and perform each type of workflow on a DLP incident.
- Explain the features of the Incident Risk Ranking dashboard.
- Create and configure an administrator with role-based permissions.
- Define and perform discovery activities.
- Define and perform fingerprinting and machine learning activities.
- Explain the functionality of file tagging and how DLP integrates with it.
- Import and apply file tags, create classifiers, and use them in a policy and rule.
- Review the operational status of DLP components and services.
- Identify the elements included in a DLP backup and restore procedure and then perform this procedure.
- Identify and analyze the primary logs used in DLP security manager.

Prerequisites for attendance

- General understanding of system administration and internet services
- Basic knowledge of networking and computer security concepts
- A computer that meets the requirements noted at the end of this document

Certification exams

This course prepares you to take and pass the DLP Administrator certification exam. One exam attempt is included in the price of the course, but the exam is not administered during the course. A minimum score of 80% on the multiple-choice online exam is required to pass.

Course Outline

Module 1: Introduction to Forcepoint DLP

- Describe a DLP implementation and define core DLP terms.
- Identify available Forcepoint DLP product information resources and where they can be accessed.

Module 2: Configuring Forcepoint DLP Classifiers

- List and explain each Forcepoint classifier type.
- Create a functional example of each Forcepoint classifier type.
- Access the list of predefined script classifiers and identify several commonly used categories.
- Configure the parameters of a predefined script classifier.

Module 3: Configuring Forcepoint DLP resources

- List and explain each Forcepoint DLP resource.
- Configure a connection to and import a user directory.
- Create a functional example of each Forcepoint DLP resource.
- Import URL categories by enabling the linking service.
- List and explain the default action plans.
- Create a custom action plan.
- List and explain the default notifications.
- Use dynamic variables in notifications.
- Configure the default notification.

Module 4: Configuring Forcepoint DLP policies and rules

- Define what a DLP policy is, identify three broad types of them, and explain what they do.
- Explain how cumulative rules can be used in DLP.
- Configure, deploy, and test a quick policy.
- Configure and test a predefined policy.
- Configure, deploy, and test a custom policy and rule.
- Explain the purpose and function of a rule exception.
- Explain how to perform a bulk update of multiple policies and rules.
- Explain how policy levels provide scope and processing order for policies, then create a new policy level and assign policies to it.

Module 5: Analyze a transaction using OCR

- Explain the capabilities and modes of OCR.
- Configure a policy engine to work with an OCR server.
- Submit a transaction to the OCR engine and examine the results.

Module 6: The Forcepoint One Endpoint

- Identify the core features of the Forcepoint One Endpoint.
- Explain the endpoint global and profile settings.
- Deploy the Forcepoint One Endpoint.
- Identify supported endpoint encryption methods.
- Use the Forcepoint One Endpoint to encrypt files copied to removable media.
- Explain the DLP endpoint temporary bypass feature.
- Test the temporary bypass feature.
- Configure the endpoint browser extension to work in monitor-only mode.
- Test the endpoint browser extension in monitor-only mode.
- Explain the DLP endpoint employee coaching feature.
- Confirm the function of the employee coaching feature.

Module 7: Analyzing DLP incidents and reporting

- Define the core terminology of Forcepoint DLP incident reporting.
- List and explain the report types in the report catalog.

- Analyze an incident in an Incident List report.
- Perform each UI-based incident workflow action.
- Explain the function of DLP incident batch operations.
- Perform a remediation operation on a batch of incidents.
- Explain the features of the incident risk ranking dashboard.

Module 8: Managing Delegated Administrators

- Summarize attributes of delegated administrators and role-based permissions.
- Configure a delegated administrator to have role-based permissions.

Module 9: Implementing discovery

- Define terminology specific to discovery.
- Perform discovery activities, including configuration, task execution, and analysis of discovery incidents.

Module 10: Creating fingerprinting and machine learning classifiers

- Define terminology specific to fingerprinting and machine learning.
- Perform file fingerprinting activities, including configuration, task execution, and tuning of results.
- Perform machine learning activities, including configuration, task execution, and tuning of results.

Module 11: Importing file tagging labels

- Explain the functionality of classification labels and how to integrate them into the DLP data labeling framework.
- Integrate Boldon James into the DLP data labeling framework.
- Create a file labeling classifier to manage files that contain sensitive or proprietary information.
- Create and deploy a data usage policy using a file labeling classifier.
- Create and deploy a discovery policy with an action plan capable of assigning file classification labels.

Module 12: Managing system health

- Examine the DLP system health dashboard for sustained high usage.
- Review the operational status of each registered system module.
- Identify and analyze the primary logs used by the DLP security manager.
- Export information found in the primary logs.
- Explain the functionality of DLP system alerts.
- Identify the items included in a DLP backup.
- Configure and perform a DLP backup task.

To attend this virtual online course, you must have a computer with:

- A high-speed internet connection (minimum of 1 MB connection required)
- An up-to-date web browser (Google Chrome recommended)
- PDF viewer
- Zoom client
- Speakers and microphone or headset (headset recommended)

A separate tablet or e-book reader is also recommended for the course and lab book delivery.

Terms and Conditions

- Virtual Instructor-Led Trainings (VILTs) are delivered as live instructor-led training in an online classroom—no on-site delivery element.
- This course is limited to the topics described in this data sheet and may not address all of your unique requirements.
- Forcepoint trainings are standard and non-negotiable.
- Forcepoint provides the training “AS IS” and makes no warranties of any kind, express or implied.
- VILT courses must be completed within six months from purchase or the course may be forfeited.
- The training services in this course are provided pursuant to the Subscription Agreement.
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions.

For more information about this course or other Forcepoint training offerings, please visit https://www.forcepoint.com/services/training-and-technical-certification or contact Forcepoint Technical Learning Services at learn@forcepoint.com.

Forcepoint