Welcome to the Management course of **Native Drive Encryption 5.2.4**, which is part of the **Native Drive Encryption On-Prem Bundle**. This course equips you with the knowledge to manage reports and queries and perform system recovery through various recovery methods.

The course is divided into modules. Each module includes an introduction, one or more lessons, demos, and a summary of the covered material. The course concludes with an overview and end-of-course exam. You must score at least 80% on the exam to receive credit for completing the course.
You should also refer to the product documentation at https://docs.trellix.com/ including the Product Guides, Installation Guide, and Release Notes.

Click the "**Start Course**" button to begin.

INTRODUCTION

About the Course

Learning Objectives

Useful Links

Disclaimer

Copyright

QUERIES AND DASHBOARDS

Module Introduction

TNE Dashboards

Viewing TNE Reports

Creating Custom TNE Queries

Creating Custom TNE Dashboard

Module Knowledge Check

Module Summary

SYSTEM RECOVERY

Module Introduction

Importing Recovery Key

Performing System Recovery using ePO (On-Prem)

Performing System Recovery using DPSSP

Rotating Recovery Keys for Security

Module Knowledge Check

Module Summary

CONCLUSION

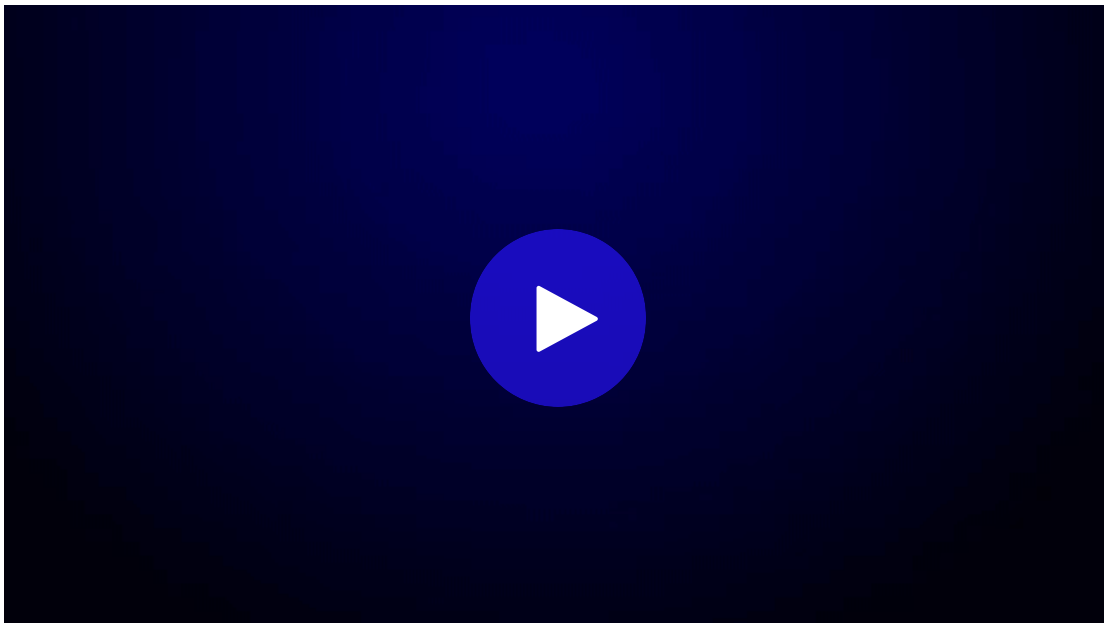
Summary

Course Exam

About the Course

Welcome to the TNE 5.2.4 On-Prem **Management** course. In this course, we'll show you how to manage reports within ePO On-prem, providing visibility into encryption statuses, policy compliance, and recovery events.

Click the play icon to watch the video.



CONTINUE

Learning Objectives

Upon completion of this training, you will be able to:

- Understand How to Manage Encryption Reports.
- Utilize Queries as Dashboard Monitors.
- View and Analyze Predefined Reports.
- Create and Customize Encryption Queries.
- Navigate the Native Drive Encryption Dashboard.
- Search and Identify Systems by Username.
- Create Custom Dashboards for Real-Time Monitoring.
- Monitor and Interpret Encryption Client Events.
- Import recovery key to ePO On-Prem.
- Perform system recovery using ePO - On-prem

- Perform system recovery using the Data Protection Self Service Portal
- Rotate recovery keys

CONTINUE

Useful Links

Product and Solutions Training
Learn the skills to successfully deploy and manage your products and solutions.

EDUCATION SERVICES

Trellix Spotlight Series
The Trellix Spotlight Series highlights upcoming Trellix product features, troubleshooting, and best practices with members from the Trellix Support team.

TRELLIX SPOTLIGHT...

Trellix on YouTube
Subscribe to the only official YouTube channel for Trellix technical support. Provides help to ensure your products successfully protect your organization, and that your experience meets your expectations.

TRELLIX ON YOUTUBE

Enterprise Product Documentation

This is a single location for all product information including:

- Release Notes

- Installation Guide
- Product Guide
- Reference Guide

DOCUMENTATION

Trellix Advanced Research Center
The Trellix Advanced Research Center provides information on current and emerging threats including:

- Threat analysis and research
- Threat predictions and trends
- Searchable threat library
- Podcast offerings, blogs, tips, and techniques
- Security updates
- Feedback, threat detection resources, and free tools

TRELLIX ARC

Trellix Thrive
Trellix Thrive provides a simple and modern experience for support, education, and professional services, so you can get started quickly and have the tools for success at your fingertips.

Key Benefits:

- **Simplify your experience.** Get started quickly, have answers at your fingertips, and connect with product support experts
- **Accelerate your journey.** Boost your knowledge, gain access to industry experts, and have the flexibility to pivot your strategy as your business changes.

- **Thrive with Living Security.** Drive a resilient security posture that can adapt to changes in the threat environment and develop a balanced approach to your security program.

TRELLIX THRIVE

Security Updates

Read about the security content of products, download .DAT files, or sign up for the .DAT Notification Service.

SECURITY UPDATES

CONTINUE

Disclaimer

This content was developed using **TNE On-prem** release 5.2.4 and may vary from the old version of the product.

All screenshots in the course were accurate at the time of course publication.

Product interface changes may occur at any time due to the flexible, cloud nature of the product.

CONTINUE

Copyright

Duplication of course materials is strictly prohibited by copyright.

CONTINUE

Module Introduction

In this module, you will learn key functionalities, including viewing reports and creating and managing custom queries and dashboards.

This module is essential for anyone responsible for managing and securing data using Native Drive Encryption.

Module Objective

Upon completion of this module, you will be able to:

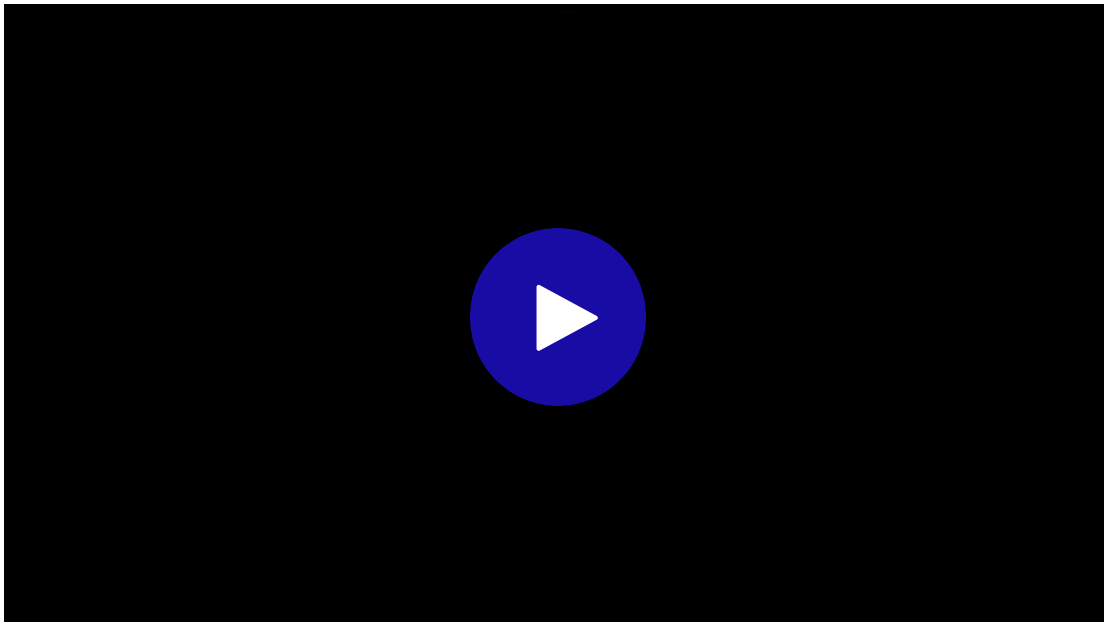
- View dashboard and reports.
- Create custom queries.
- Create custom dashboards.

CONTINUE

TNE Dashboards

This lesson explains how to navigate the Native Drive Encryption dashboard and its predefined dashboard queries and how to find systems by username.

Click the video below to watch the demonstration.

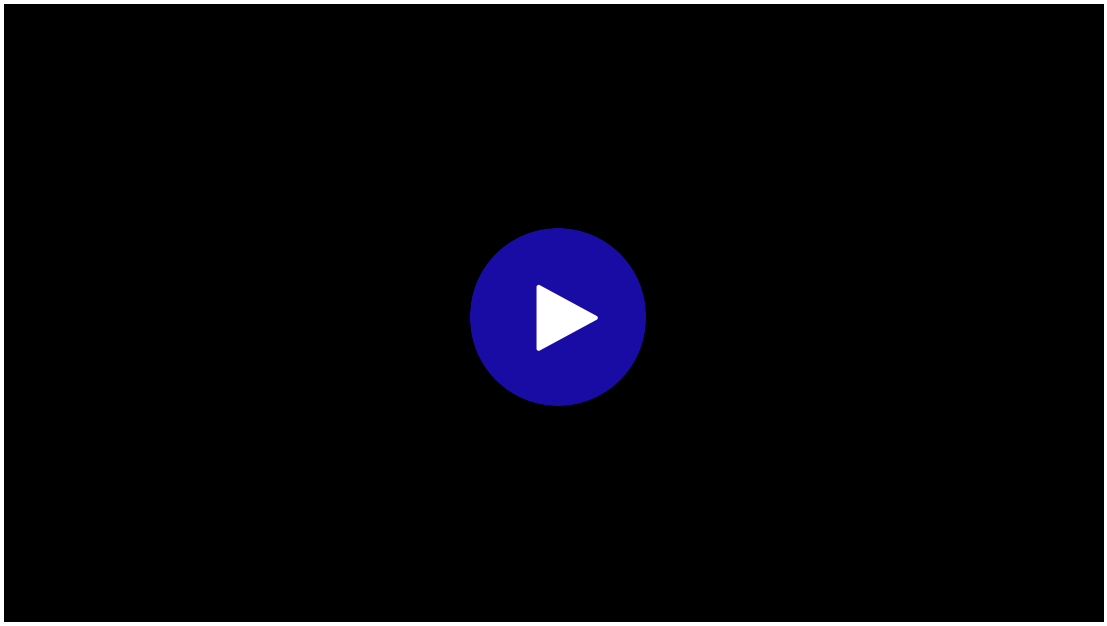


CONTINUE

Viewing TNE Reports

This lesson explains how to view and export the Native Drive Encryption reports.

Click the video below to watch the demonstration.

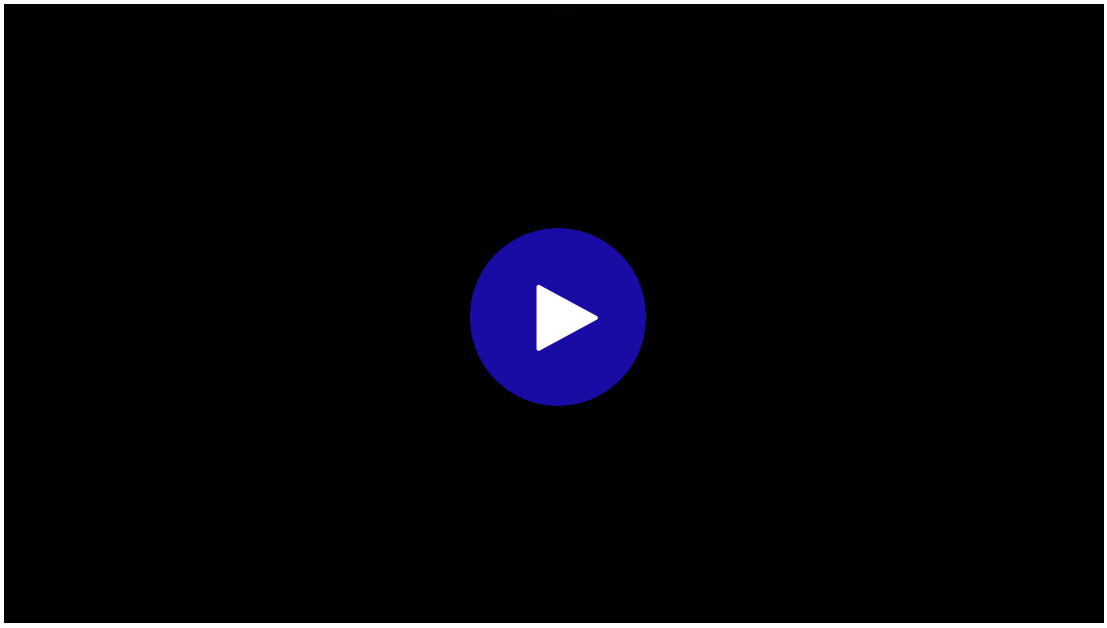


CONTINUE

Creating Custom TNE Queries

This lesson explains how to create custom Native Drive Encryption queries.

Click the video below to watch the demonstration.

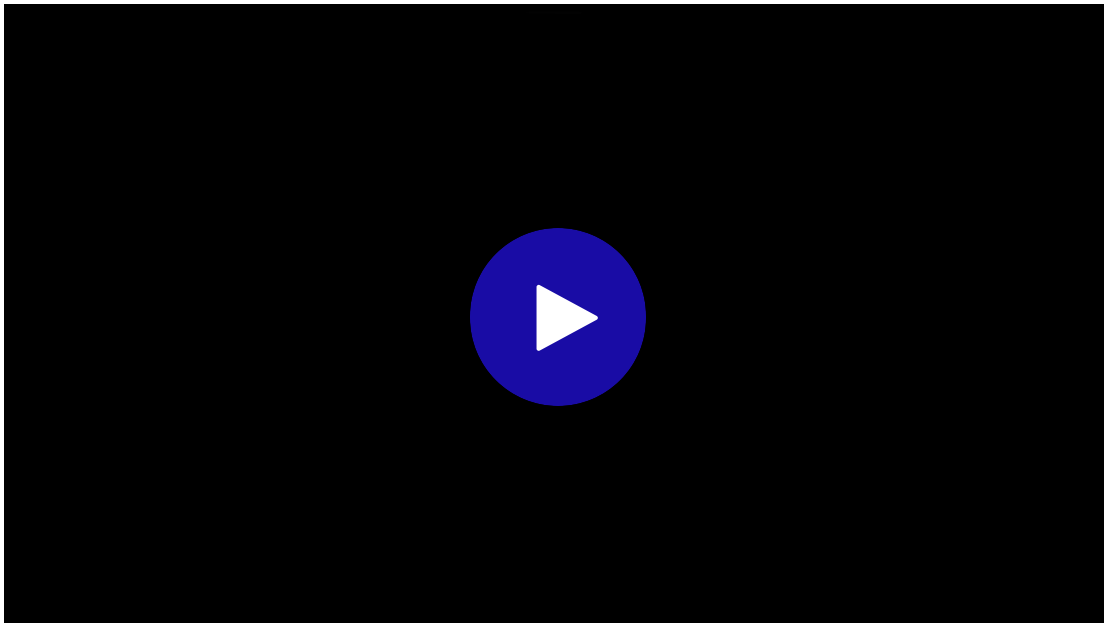


CONTINUE

Creating Custom TNE Dashboard

This lesson will guide you through the process of creating personalized dashboards. You can construct these dashboards by utilizing custom query results or by using pre-existing ePO dashboards.

Click the video below to watch the demonstration.



CONTINUE

Module Knowledge Check

Question

01/05

What is the default refresh interval for queries used as dashboard monitors in ePO?

- 1 minute
- 5 minute
- 10 minute
- 15 minute

Question

02/05

Which of the following formats cannot Native Drive Encryption query results be exported to?

- CSV
- XML
- HTML
- MP3

Question

03/05

Which report displays the list of systems that have failed activation?

- Report overall encryption status
- Activation Failures
- Report policy compliance
- Report recovery keys

Question

04/05

When a volume is locked by BitLocker, what message might be displayed for the overall encryption status?

- Encryption Complete
- Unable to determine status
- BitLocker Active
- Error: Locked Volume

Question

05/05

What does Event ID **35205** indicate?

- FileVault activation failed.
- BitLocker activation failed.
- FileVault or BitLocker activation is successful.
- Native Drive Encryption is disabled.

Module Summary

Key Points

- TNE offers dashboard monitoring.
- Users can view reports related to Native Drive Encryption.
- Custom queries and dashboards can be created.
- The dashboard can be viewed.
- Systems can be found by username.

In the next module, you will learn how to recover client systems.

CONTINUE

Module Introduction

This module focuses on Native Drive Encryption recovery. It covers importing recovery keys and performing system recovery using ePO - On-prem and the Data Protection Self-Service Portal, as well as recovery key rotation.

Module Objective

Upon completion of this module, you will be able to:

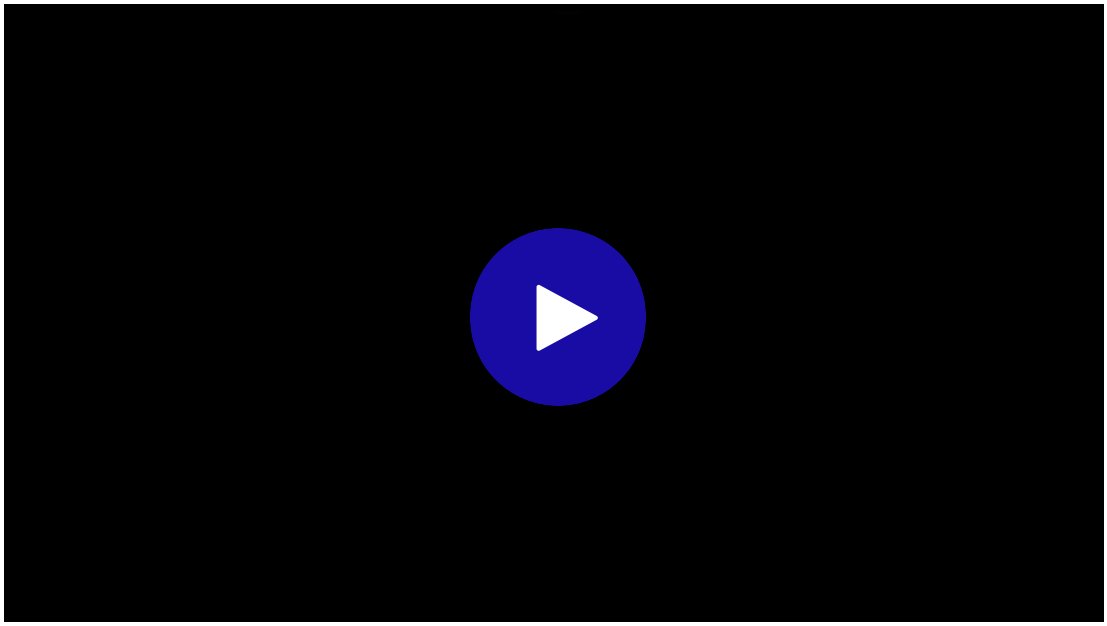
- Import a recovery key.
- Perform system recovery using ePO - On-prem.
- Perform system recovery using the Data Protection Self Service Portal (DPSSP).
- Rotate recovery keys.

CONTINUE

Importing Recovery Key

This lesson provides guidance on importing recovery keys into ePO. You will learn how to utilize the **Data Protection** menu and the **System Tree** to accomplish this. The lesson also includes a use case demonstrating how to import a FileVault recovery key using a Mac client system.

Click the video below to watch the demonstration.



CONTINUE

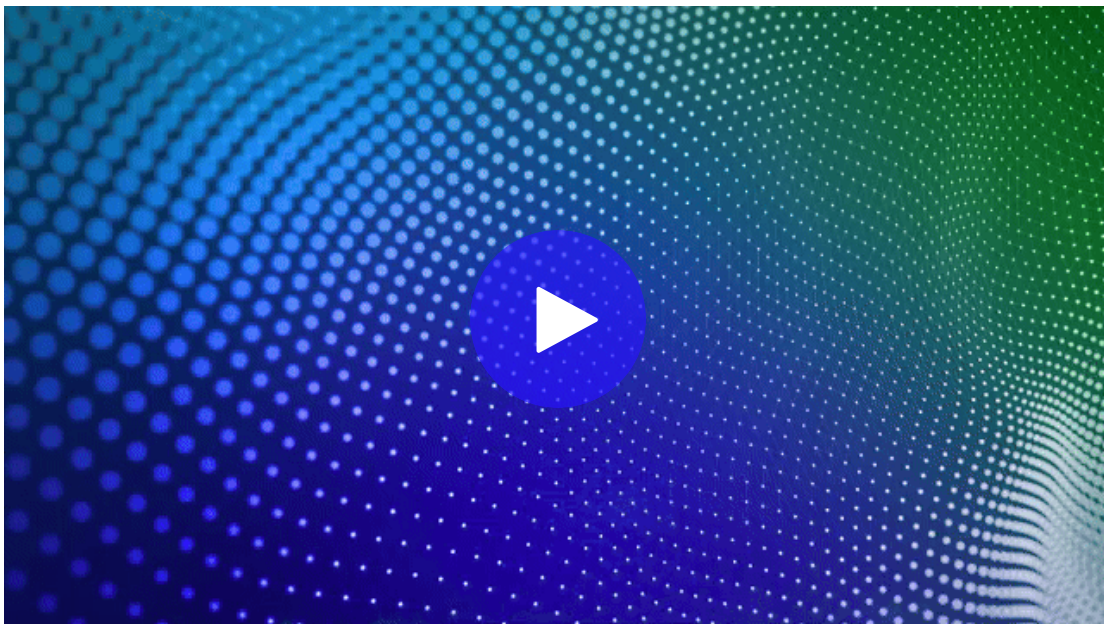
Use Case

Client users can import the recovery key directly from the client system to the ePO On-prem database.

Before you begin

- This task needs to be carried out by the client user on their Mac system.
- The FileVault policy for the client system must be enabled by the ePO administrator.
- Ensure that the Allows users to import recovery key on client policy has been enabled and enforced by the administrator on the client system.

Click the video below to watch the demonstration.

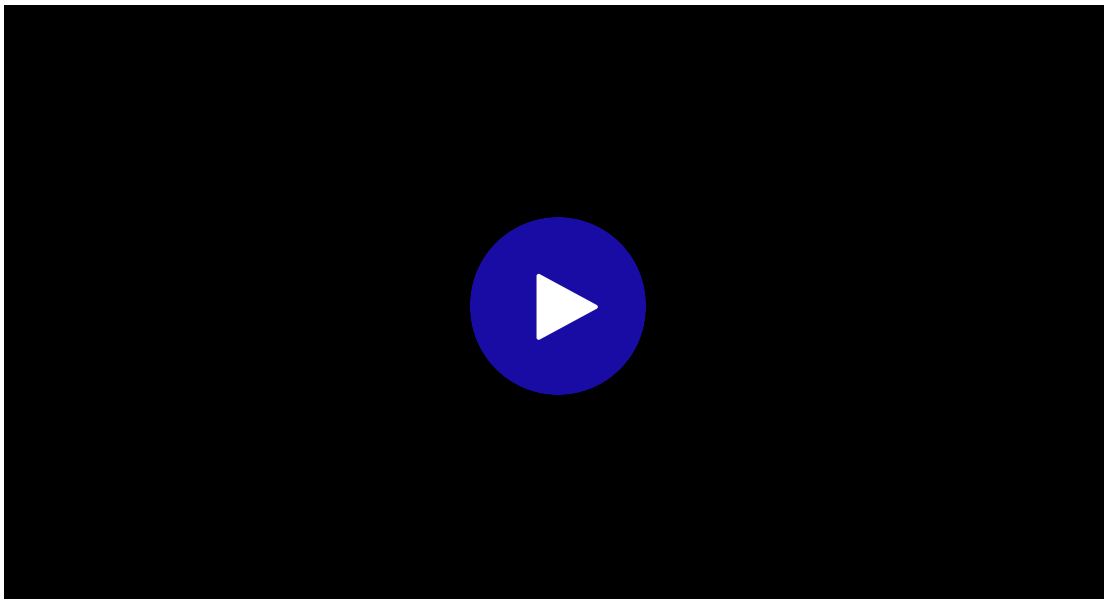


CONTINUE

Performing System Recovery using ePO (On-Prem)

This lesson will provide insights on how to recover Windows client systems using ePO On-prem.

Click the video below to watch the demonstration.

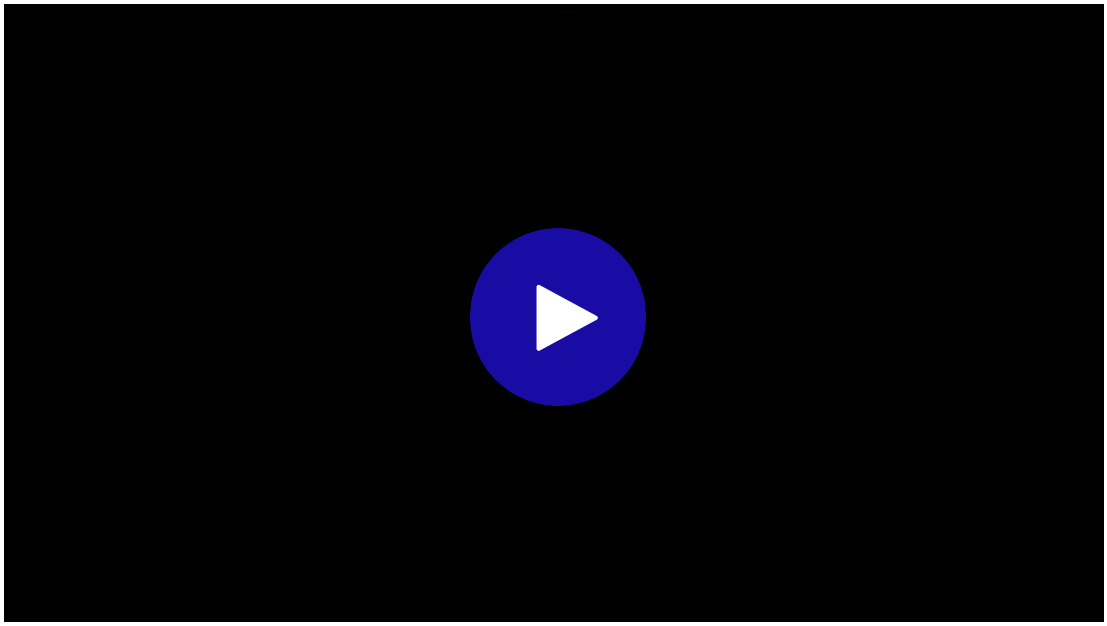


CONTINUE

Performing System Recovery using DPSSP

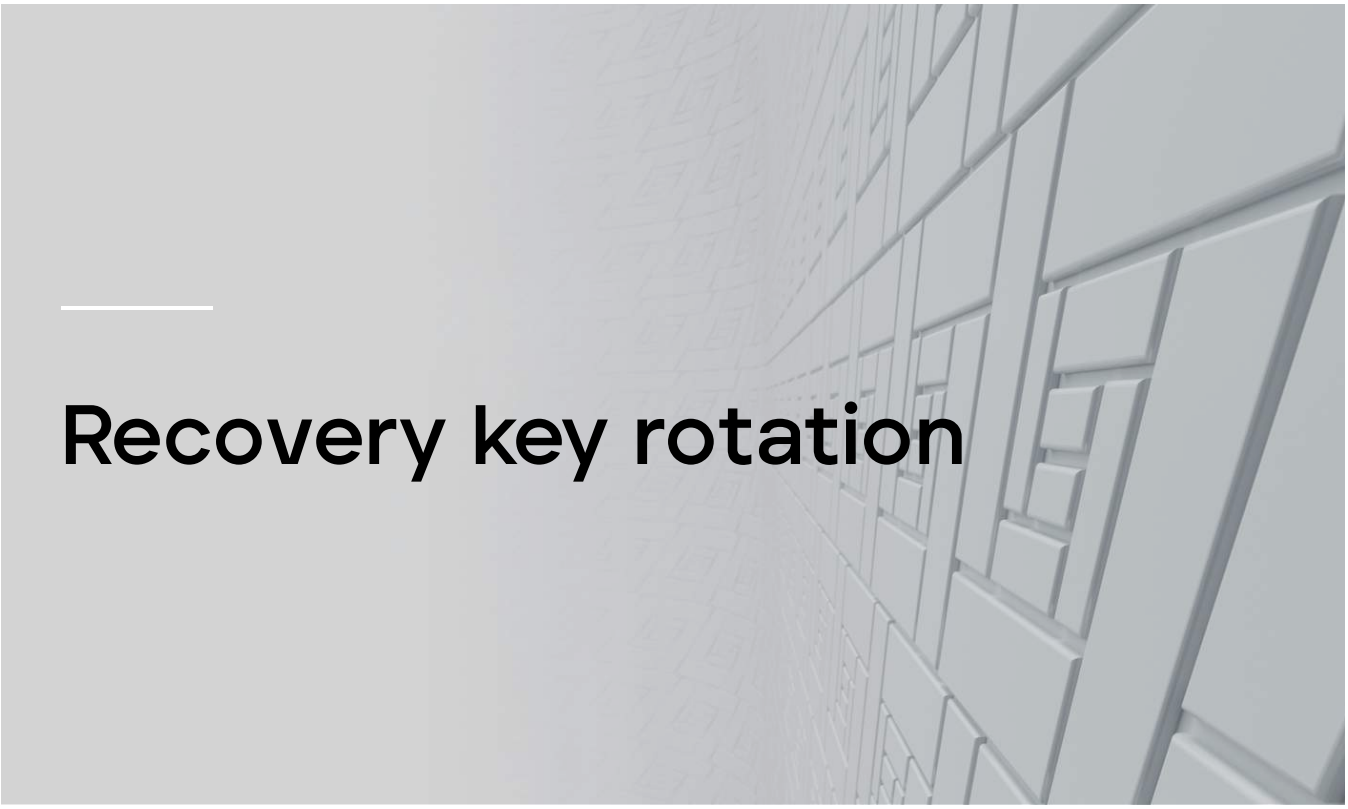
This lesson will provide you with insights on how to recover client systems using Data Protection Self-Service Portal (DPSSP).

Click the video below to watch the demonstration.



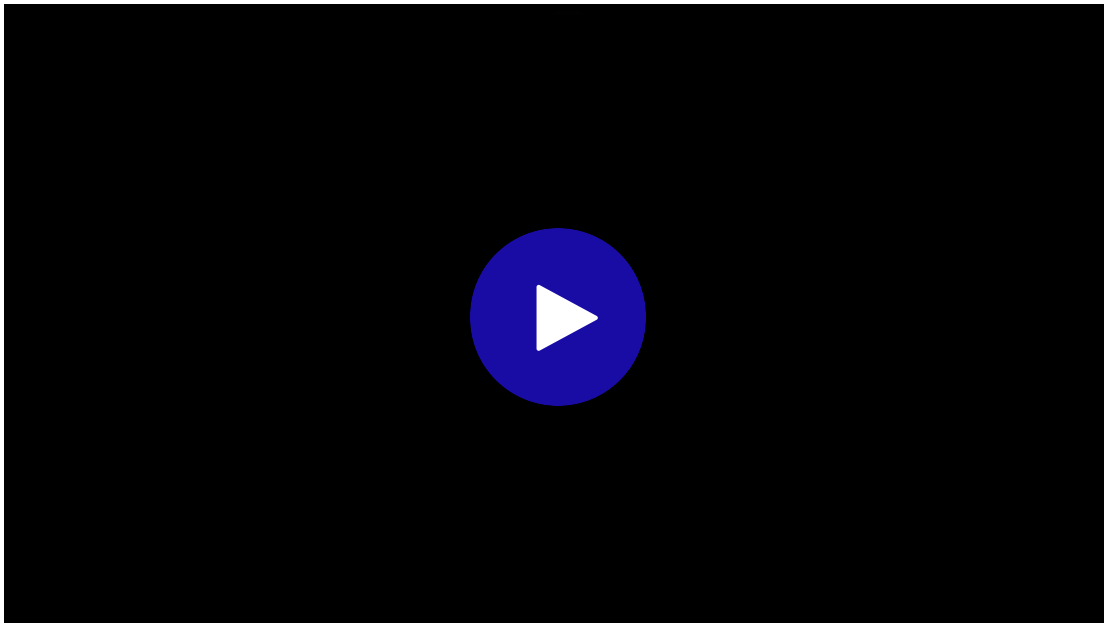
CONTINUE

Rotating Recovery Keys for Security



This lesson will guide you through the process of rotating recovery keys in Native Drive Encryption, an important security measure that provides enhanced protection for your data.

Click the video below to watch the demonstration.



CONTINUE

Module Knowledge Check

Question

01/05

What is the primary purpose of system recovery in the context of Native Drive Encryption?

- ◯ To install new software.
- ◯ To recover a system from crashes or malfunctions.
- ◯ To update system drivers.
- ◯ To back up system data.

Question

02/05

How does Native Drive Encryption *automatically* obtain a system's recovery key?

- By asking the user for it.
- By generating a new key.
- When enabling FileVault or BitLocker on a client system.
- By downloading it from the internet.

Question

03/05

Where is the serial number of a Mac system typically displayed?

- ◯ Only in the system's software settings.
- ◯ On the back, side, or bottom of the hardware.
- ◯ Only when logged in as administrator.
- ◯ On the monitor screen during startup.

Question

04/05

What is the primary purpose of the Data Protection Self-Service Portal (DPSSP)?

- ◯ To install software updates.
- ◯ To allow client users to obtain their recovery keys.
- ◯ To manage system backups.
- ◯ To monitor system performance.

Question

05/05

When configuring DPSSP server settings, which option, when enabled, will automatically block an IP address after a certain number of failed logins?

- Log authentication attempts
- Enable IP address blocking.
- Enable user blocking.
- Session timeout.

Module Summary

Key Points

- Import recovery keys using various methods.
- Perform system recovery using ePO On-prem.
- Perform system recovery using the Data Protection Self-Service Portal.
- Rotating recovery keys.

CONTINUE

Summary

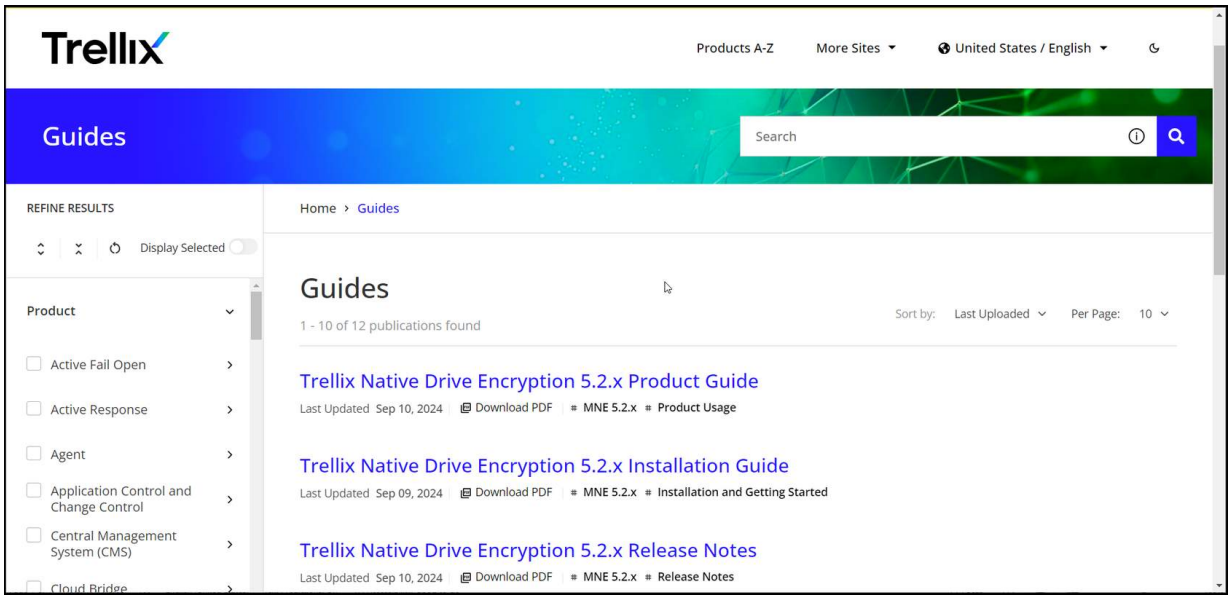
Key Takeaways

Throughout this essential training, you have learned about managing reports, recovering systems, utilizing the Data Protection Self-Service Portal (DPSSP), monitoring encryption status, handling recovery keys, and enabling users to self-recover their systems. You also learned about key rotation.

- Utilize standard reports to track activation failures, encryption status, policy compliance, and recovery keys.

- Build custom queries for detailed data analysis and visualize results in charts or tables.
- View real-time information on auto-refreshing dashboards.
- Export report data to CSV, XML, HTML, or PDF.
- Import recovery keys via the System Tree, Data Protection menu, client system, or command-line.
- Enable user self-recovery through the DPSSP.
- Users can retrieve recovery keys from the DPSSP using their system's serial number or recovery key ID.
- Review DPSSP reports for blocked users/IP addresses and recovery activity.
- Automatically rotate recovery keys after system recovery (excluding macOS).

Resources



Please refer to the Native Drive Encryption On-Prem product documentation guide for more information.

PRODUCT GUIDE

Please refer to the release notes for the latest updates and improvements.

RELEASE NOTES

Thank you for completing this course.

You must take the end of the course exam to get the credit for the course.

CONTINUE

Course Exam

To receive the credit for this course, you must pass this quiz with 80% of the score.

Question

01/10

What is the default refresh interval for dashboard monitors in Trellix Native Drive Encryption?

- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

Question

02/10

What does DPSSP stand for in the Native Drive Encryption?

- Data Protection Security System Portal
- Data Protection Self-Service Portal
- Drive Protection Security Service Protocol
- Drive Protection Self-System Protocol

Question

03/10

What are the possible visibility options when creating a custom dashboard?

SELECT ALL THAT APPLY!

- [ ] Private
- [ ] Public
- [ ] Shared with specific users
- [ ] Shared with permission sets
- [ ] Only visible to the ePO administrator

Question

04/10

What is the default authentication method selected in DPSSP Settings?

- ◯ LDAP
- ◯ AD (Active Directory)
- ◯ Local Users
- ◯ SAML

Question

05/10

Which of the following are valid export formats for Native Drive Encryption query results? SELECT ALL THAT APPLY!

- [ ] CSV
- [ ] DOCX
- [ ] XML
- [ ] HTML
- [ ] PDF

Question

06/10

Which query displays the list of users who are blocked in DPSSP?

- Blocked IP addresses
- Number of recoveries per user
- Blocked users
- User activity logs

Question

07/10

What actions can be performed on a TNE query in ePO? SELECT ALL THAT APPLY!

- [ ] Run
- [ ] Delete the whole system
- [ ] Edit
- [ ] Delete
- [ ] Export

Question

08/10

Where can you find the full DPSSP URL?

- Menu > Reporting > Queries & Reports
- Menu > Configuration > Server Settings > DPSSP Settings
- Menu > Systems > System Tree
- Menu > Data Protection > Native Drive Encryption recovery

Question

09/10

Which of these is NOT a Native Drive Encryption standard report?

- Activation Failures
- Report recovery keys
- System diagnostic report
- Report policy compliance

Question

10/10

What are the primary methods for recovering encryption keys for Native Drive Encryption? SELECT ALL THAT APPLY!

- [ ] Using System Tree
- [ ] Using Data Protection menu
- [ ] Using a USB drive
- [ ] From a client system
- [ ] Using the command-line