ManageEngine Password Manager Pro
Product Training

Course Objective

The primary objective of this course is to enable you to securely store, access and administer shared administrative passwords.

At the end of the training, you should be able to:

1. Set up Password Manager Pro
2. Maintain a central repository of passwords
3. Define and enforce standard IT practices and policies
4. Define roles and access scope for users
5. Control unauthorized access to shared passwords
6. Set up disaster recovery

Who Should Attend?

IT Managers, IT administrators and Network Administrators who are looking to

- Eliminate password fatigue and security lapses by deploying a secure, centralized vault for password storage and access
- Improve IT productivity many times by automating frequent password changes required in critical systems
- Provide preventive & detective security controls through approval workflows & real-time alerts on password access
- Control access to sensitive IT resources and enforce standard password policies
- Meet security audits and regulatory compliance such as SOX, HIPAA and PCI

Detailed Agenda

Introduction

1. Password Management Challenges
2. Password Manager Pro (PMP) – The Pragmatic Solution
3. What you can do with PMP?
4. Key Features
5. Benefits

Installation & Basic Settings

1. Supported OS
2. Minimum Hardware Requirements
3. Supported Browsers
4. Components of PMP
5. Installation Procedure
6. Installation as server startup service
7. Ports used by PMP
8. Mandatory Settings
9. Managing Encryption Key

Getting Started

1. Connecting Web-Interface
2. Arrangement of Web-Interface
3. Important Terminologies

Setting Up Users

1. Various Ways of Adding Users
2. Adding Users Manually
3. Importing Users in Bulk
4. Integrating Active Directory / LDAP
5. Defining Roles
    - Administrator
    - Password Administrator
    - Password Auditor
    - Password User
6. Grouping Users
7. Managing Users

Resource Management

1. Resource Types
2. Adding Resources Manually
3. Adding Resource Details
4. Adding Accounts
5. Storing Documents, Digital Images, Keys
6. Storing Website Credentials
7. Settings for Remote Password Reset
8. Password Reset by Deploying Agents
9. Importing Resources
10. Editing Resources

11. Resource Groups
12. Nested Resource Groups – Hierarchical arrangement of resource groups (feature coming up in the next release)
13. Managing Resource Types
14. Viewing Resources
15. Retrieving Passwords
16. Copying Password to Clipboard
17. Changing Passwords
18. Verifying Password Integrity
19. Customizing Resource/Password Fields
20. Password Policies
21. Windows Service Account Reset
22. Exporting Resources for offline access

Password Ownership & Sharing

1. Sharing Resources with other Users/User Groups
2. Sharing Resource Groups with other Users/User Groups
3. Sharing Accounts With other Users/User Groups
4. Sharing Accounts Groups with other Users /User Groups
5. Defining Access Scope
    - View Only Privilege
    - Modify Privilege
    - Manage Privilege
6. Transferring Resource Ownership

Password Access Control Workflow

1. Significance of Access Control Workflow
2. Implementing Request-Release Flow
3. Approval Process
4. Password Retrieval Use-Cases (when access control is enabled)

Password Management Operations

1. Configuring Bulk Password Reset
2. Bulk Operations based on Resource Groups
3. Scheduled Password Rotation
4. Password Action Notifications
    - When Passwords are Retrieved
    - When Passwords are Changed
    - When Password Share is Changed
    - When Passwords Expire
    - When Password Policy is Violated
    - When Passwords in PMP go out of Sync with the Actual Resource

Smartcard Authentication

- Smartcard Authentication for logging into PMP

Two-Factor Authentication

1. Introduction to Two-Factor Authentication (TFA)
2. TFA using PhoneFactor Authentication

3. TFA using Unique Password through Email
4. RSA Integration

Automatic Login to Target Systems

1. Auto Logon Helper – Introduction
2. Defining Auto-logon Helper
3. Automatically Logging in to Target Systems/Websites

Password Reset Listener

1. Introduction
2. Defining Scripts
3. Defining Reset Listener
4. Approval for Listener

Application-to-Application Password Management

1. Introduction to Password Management APIs
2. Flavors of PMP APIs
3. Configuring PMP API
4. Commands to be used

Backup & Disaster Recovery

1. Database Backup – Options
    - Live Backup
        a. Setting up Live Backup
    - Scheduled Backup

    a. Setting up Scheduled Backup

2. Disaster Recovery

High Availability

1. Significance
2. Setting up High Availability
3. Verifying High Availability Setup

Audit & Notifications

1. Audit Types
2. Resource Audit
    - Details Captured
    - Audit Filters
    - Exporting Audit Trails
    - Setting Up Notifications
3. User Audit
    - Details Captured
    - Audit Filters
    - Exporting Audit Trails
    - Setting Up Notifications
4. Task Audit
    - Details Captured
    - Audit Filters
    - Exporting Audit Trails

- Setting Up Notifications on the Occurrence of Audit Trails

Reports

1. Types – Canned Reports & Custom Reports
2. Usage
3. Password Reports
4. User Reports
5. General Reports
6. Compliance Reports
7. Exporting Reports in Different Formats
8. Custom Reports - Tips

Optional General Settings

1. Significance
2. Swithching on/off features on need basis

Miscellaneous Operations & Tools

1. Dashboard View
2. Rebranding PMP
3. Displaying Common Message to Users
4. Changing Application Login Password
5. Customizing Email Notification Content
6. Personal Password Management
7. Troubleshooting Tips

8. Best Practices
9. Maintenance Process
10. Discussion