# Lepide Protect.

## Quick start guide.

# Contents

# 1 Introduction

Managing user permissions across large networks is one of the most challenging tasks businesses face today. Excessive permissions don't just clutter the system; they pose serious security risks. Yet, identifying and revoking this permission especially for multiple users across various servers can be a complicated and time-consuming process.

Lepide Protect simplifies permissions management with an easy-to-use, powerful solution that puts you back in control. It helps businesses efficiently analyze and manage permissions, reduce risks, and ensure compliance.

With features like super admin privileges, role-based configurations, team management, and dynamic dashboards, Lepide Protect transforms a complex process into a seamless one. The platform doesn't just identify excessive permission. it provides a one-click solution to revoke unwanted access, saving time and effort.

Additionally, with real-time insights and robust safety measures like automated backups and restoration, Lepide Protect ensures your organization's data stays secure while giving you the tools to maintain control with confidence.

If you have any questions at any point in the process, you can contact our Support Team. The contact details are listed at the end of this document.

# 2 Installing Lepide Protect

## 2.1 Requirements and Prerequisites

Before you start using Lepide Protect, you need to ensure that you meet the following requirements:

a. **File Server Configuration:** Ensure the file servers are properly configured within the system. This is essential for managing permissions effectively in the domain you are setting up for permission management.

b. **Successfully Scanned Dataset under CPA:** Run a comprehensive scan using the **Current Permission Analysis (CPA)** feature to identify excessive permissions and populate the dataset with actionable insights.

c. **CPA User Privilege:** The user running policies in CPA must be a **Domain Administrator**. This user will be responsible for automating the denial of excessive permissions.

## 2.2 Super Admin Privileges

Lepide Protect requires that a single administrator with Super Admin Privileges is assigned to oversee and manage permissions for each domain.

This approach ensures:

- **Clear Accountability**: One designated admin is responsible for all permissions management
- **Streamlined Operations**: This simplifies the process by avoiding overlapping roles and duplication
- **Consistent Policy Application**: It ensures all policies are uniformly implemented across the domain

**To assign this user:**

1. From the Web Console Home screen, choose the **Settings** icon 
2. The Admin Console screen is displayed:

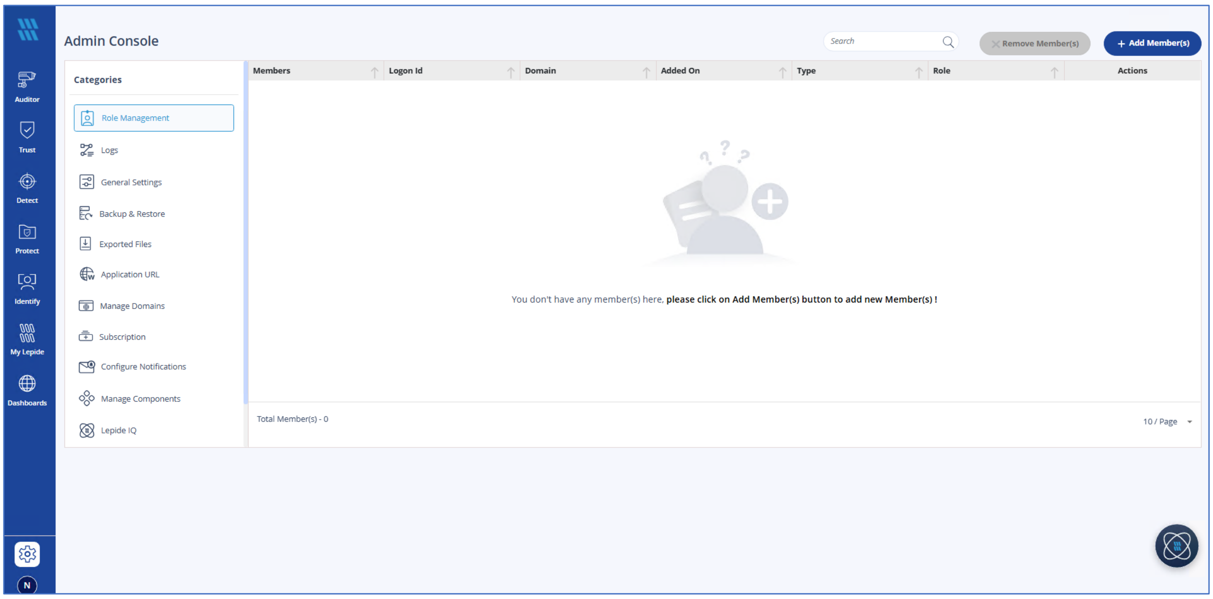



*Figure 1: Admin Console*

3. Scroll down the Categories section and click on **Lepide Protect**

The Configure Team Members screen will be displayed:

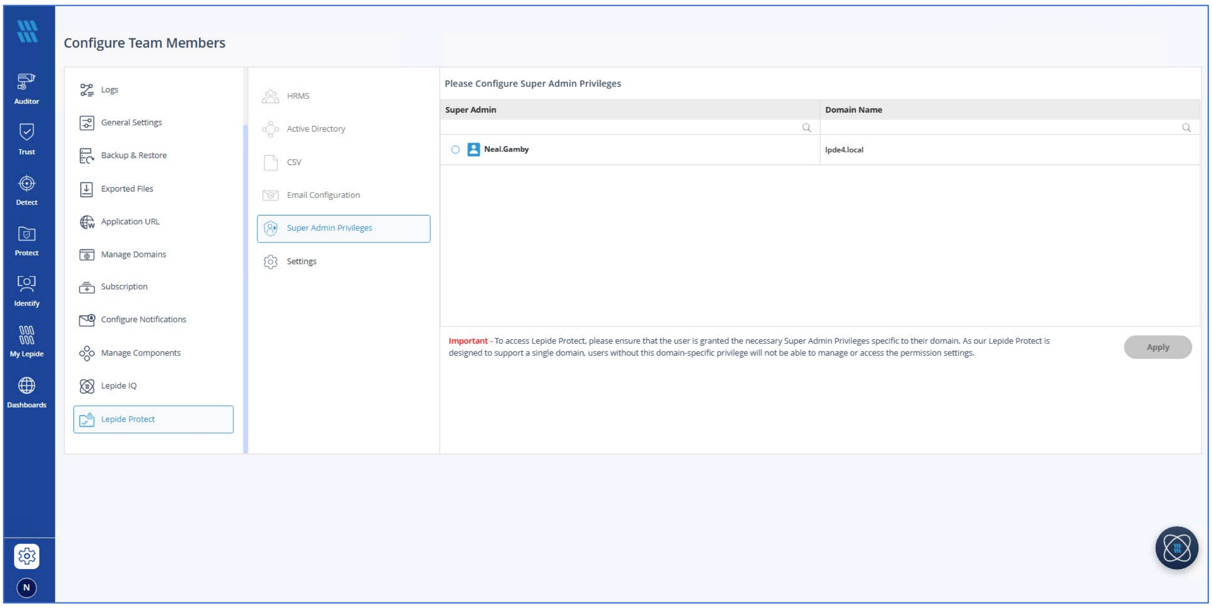



*Figure 2: Configure Team Members*

4. Select Super Admin Privileges. This will display a list of all Super Admins across different domains.
5. Select the single user who will have sole responsibility for setting permissions for a domain. This designated admin user will have the authority to oversee and control domain permissions.
6. Click **Apply**

This feature eliminates confusion, enhances operational efficiency, and ensures effective permission management.

| | |
|---|---|
| **NOTE:** | The single user with responsibility for setting permissions for a domain can delegate permissions to specified managers and this will be explained in Section 3.2 of this document |

## 2.3 Email Configuration

The Email Id needs to be configured to provide sender email details. Emails will be sent to notify users of changes to permissions.

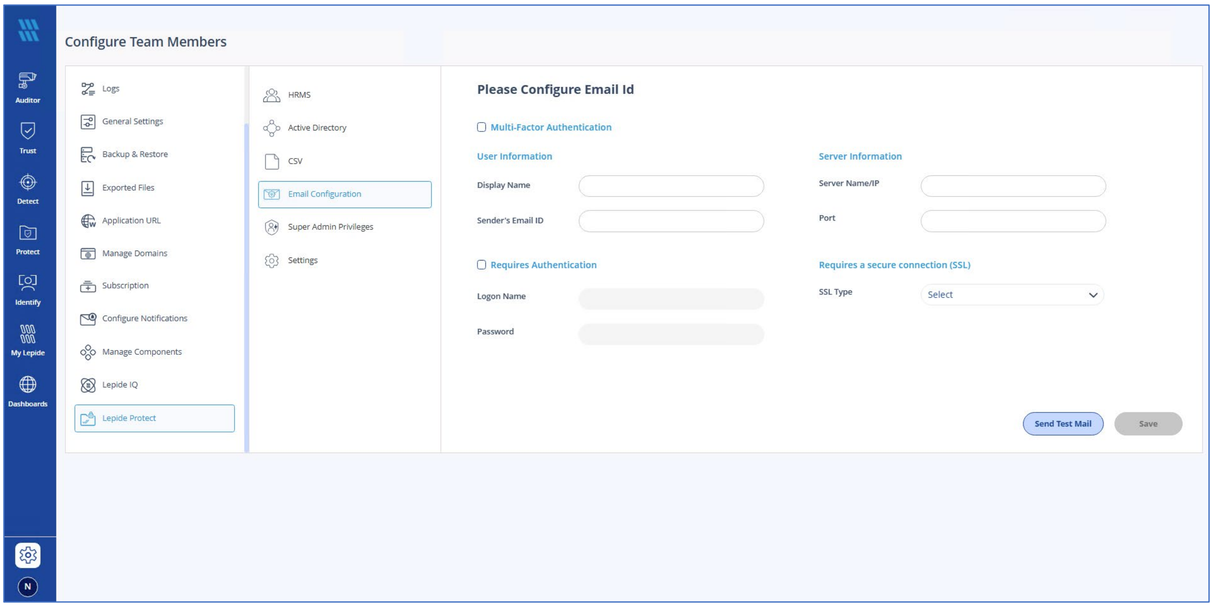



*Figure 3: Email Configuration*

- – Check the **Multi-Factor Authentication** box if required
- – Display Name
- – Sender's Email Id
- – Server Name/IP
- – Port
- – Check the **Requires authentication** box if required
- – Logon Name
- – Password
- – Server Name/IP
- – Port
- – Check the **Requires a secure connection (SSL)** if required

- Select **Send a Test Email** to check that all the settings have been added correctly
- Click **Save** when finished

## 2.4 Configuration Capabilities

Lepide Protect is designed to meet the needs of modern businesses by offering three easy-to-use configuration methods for integrating users into the system:

a. **HRMS (Human Resource Management System) Integration:** Lepide Protect supports HRMS platforms like **Zoho and Workable** which will fetch hierarchical user data directly from these systems. This data is then compared with records in Active Directory (AD) to create an accurate hierarchy, from super admins to employees. Once synchronized, the user data is uploaded into team management automatically.

   HRMS integration is fully customizable. To add an HRMS platform that isn't currently supported, please refer to the Lepide Support Team for assistance.

b. **Active Directory Integration:** By validating domain credentials, Lepide Protect accesses and syncs user hierarchies from Active Directory. This ensures that your organizational structure in AD is accurately reflected within the Lepide Protect Team Management Module.

c. **CSV-Based Customization:** For organizations that need more flexibility, Lepide Protect allows importing customized user data through CSV files. This feature enables you to define fields like managers, departments, and job titles, ensuring the system adapts to your unique team structure.

### 2.4.1 Steps to Configure Capabilities for HRMS:

1. Select **Lepide Protect**
2. Select **HRMS**
3. Select the HRMS system required and follow the steps for setup

| | |
|---|---|
| **NOTE:** | Only one configuration method can be used at a time. This ensures smooth operation and avoids any conflicts or data overlap during synchronization. |

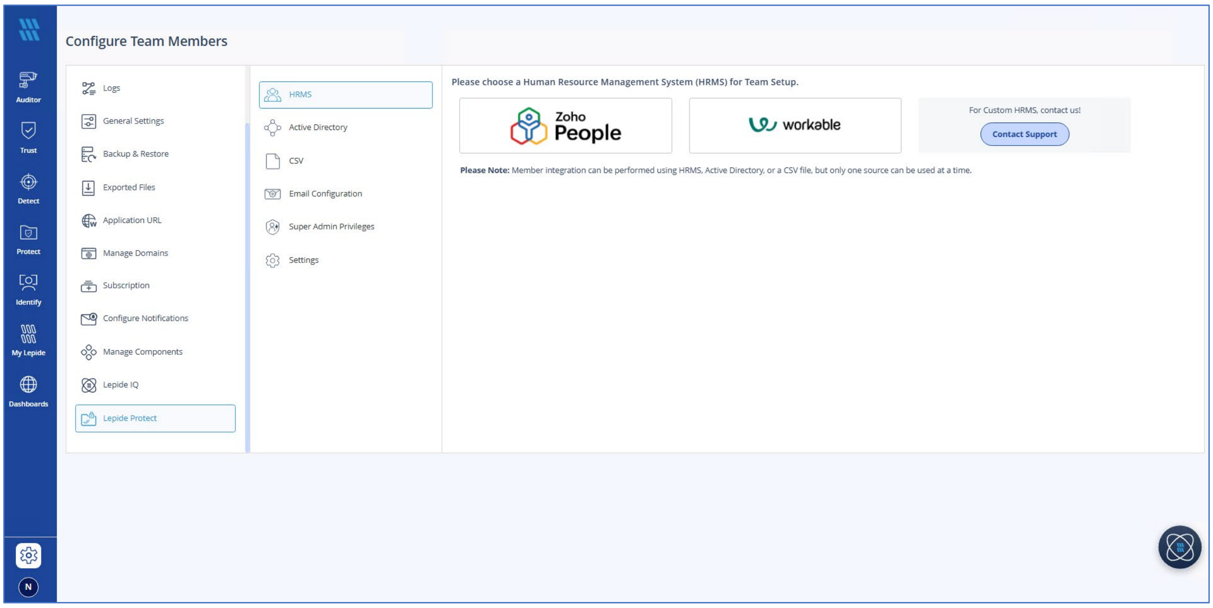



*Figure 4: Configure Team Members: HRMS*

To generate the Client ID and Secret Key for HRMS, click the ⓘ icon and the instructions are displayed:

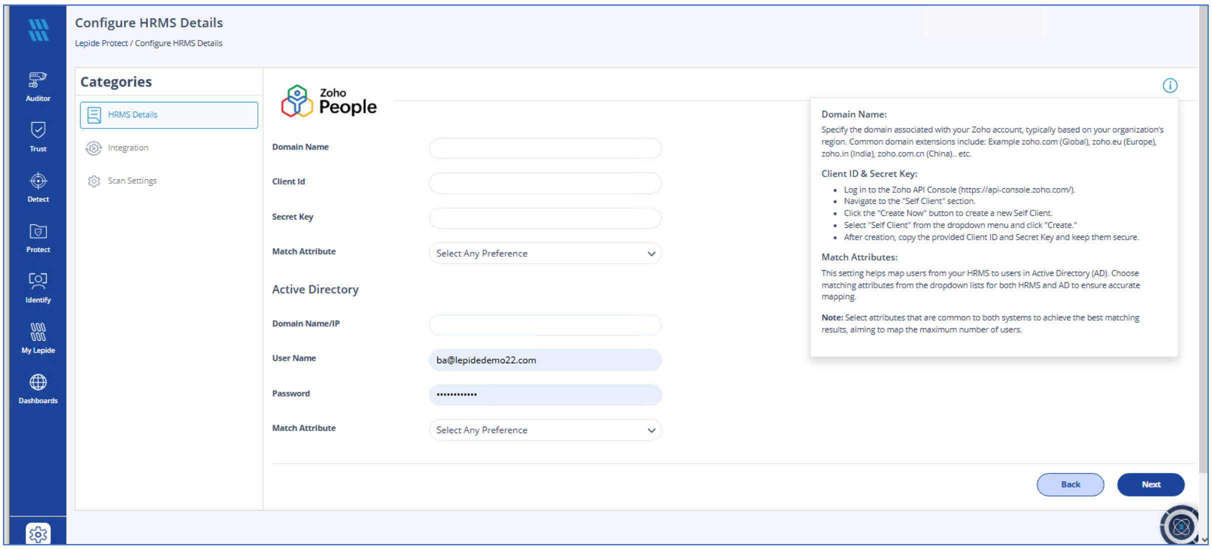



*Figure 5: HRMS with Help Instructions*

## 2.4.2 Steps to Configure Capabilities for CSV:

1. Select **Lepide Protect**
2. Select **CSV**

3. Select the CSV file and follow the steps for setup. The steps will be similar to the Active Directory setup shown in Section 2.4.3 of this guide

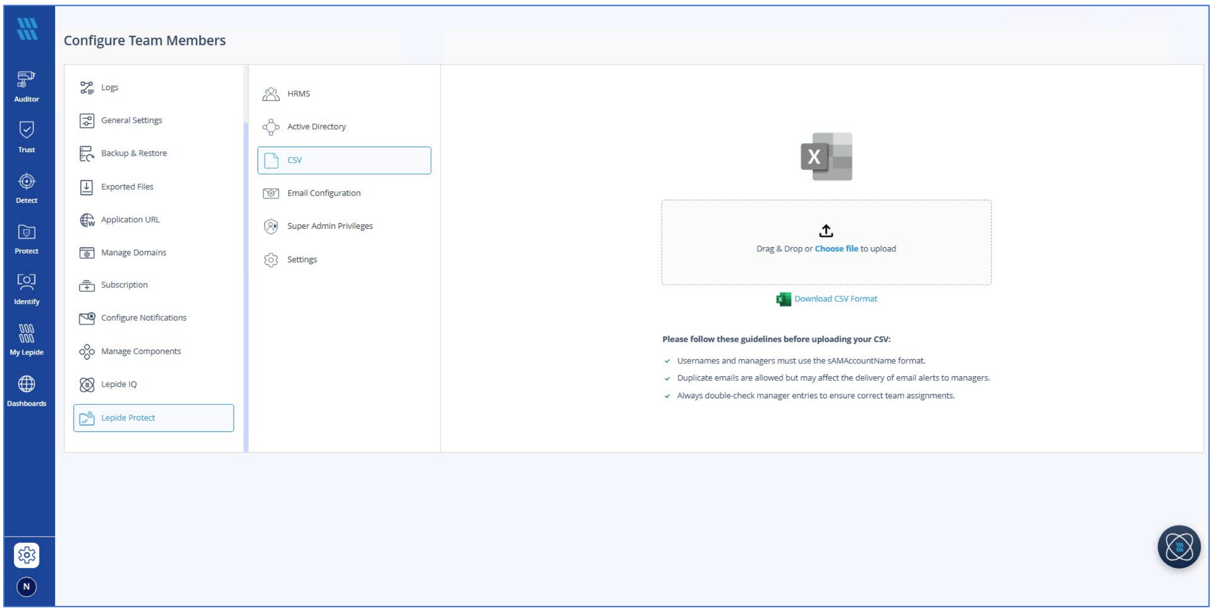



*Figure 6: Configure Team Members: CSV*

## 2.4.3 Steps to Configure Capabilities for Active Directory:

1. Select **Lepide Protect**
2. Select **Active Directory**
3. The Active Directory screen will be displayed:

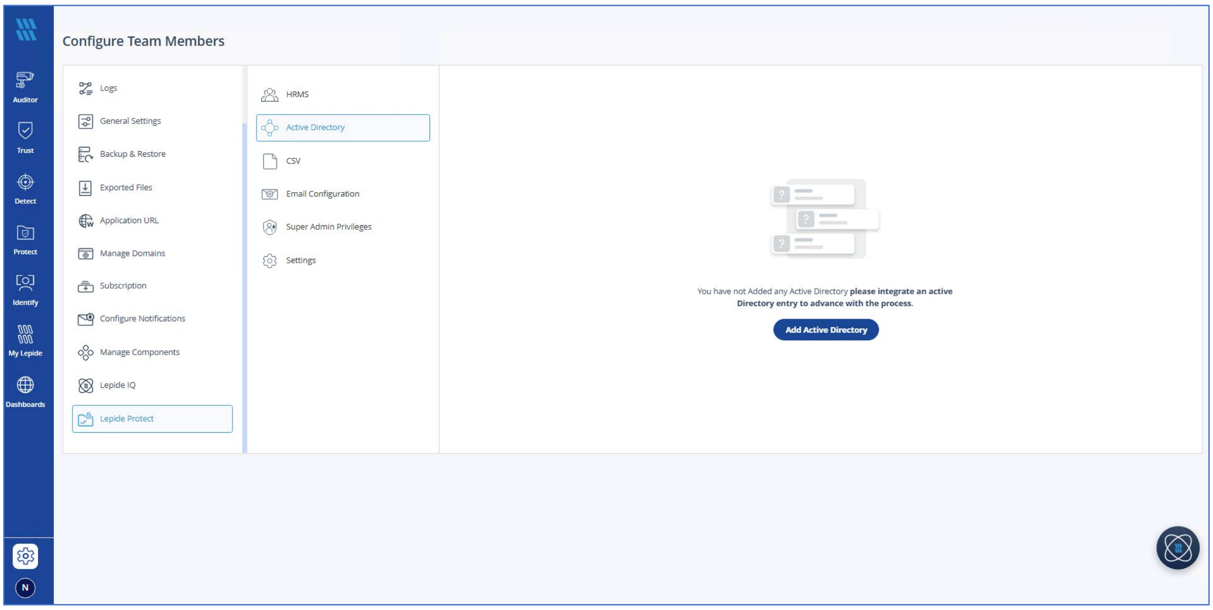



*Figure 7: Add Active Directory*

4. Click the **Add Active Directory** button

Adding Active Directory will integrate the Active Directory users with Lepide Protect to allow us to allocate the permissions for the files and folders

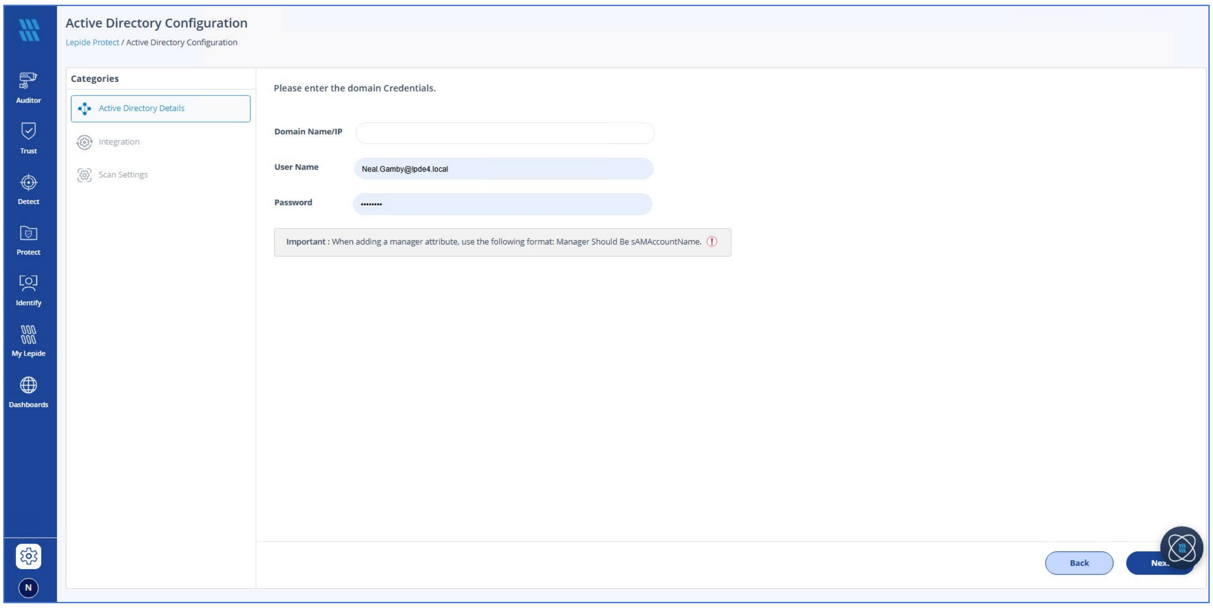



*Figure 8: Active Directory Details*

5. Enter the following details:

   – **Domain Name/IP address**
   – **User Name** – note: this should be the SAM account name
   – **Password**

6. Click **Next**

All the AD users will now be integrated into Lepide Protect and displayed in the integration page:

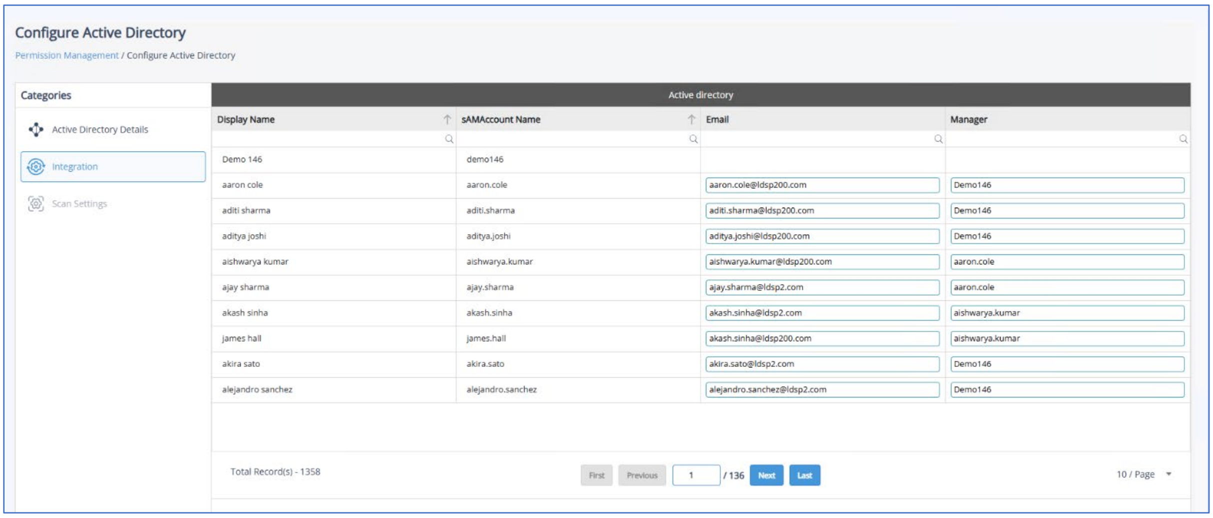


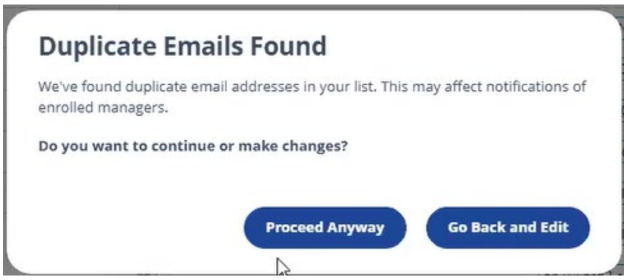

*Figure 9: Integration Page*

- The Integration Page displays the Display Name, sAMAccount Name, Email and Manager for each user.
- The **Email** address and **Manager** name can be edited on this page if required. When editing the Manager name, it is better to use their **sAMAccount Name** rather than the Display Name as this will always be unique.

| | |
|---|---|
| **NOTE:** | If either the email address or Manager name are changed within Lepide Protect, this will not be updated in Active Directory. It is only used for Lepide Protect. |

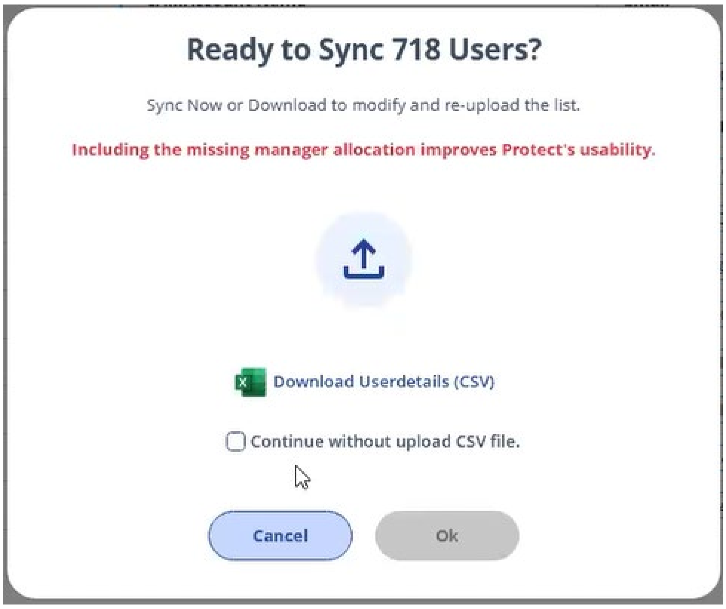
7. Click **Next**

The following dialog box will be displayed if duplicate emails are found:




8. Click either Proceed **Anyway** or **Go Back and Edit** to continue

   The following dialog box will be displayed:




- This gives you the option to download user details to a CSV file. With a large number of users, this can make it much easier to filter, sort and edit the user details.
- If this option is selected, the changes can be made in the CSV file and then this CSV file can be uploaded here with the updated details using the Upload button: 
- Clicking the Upload button will display a list of CSV files. Select the required file and click Open

9. Click **Download User details (CSV)** if required or check the **Continue without uploading CSV file**

10. Click **OK**

The Scan Settings page is displayed:

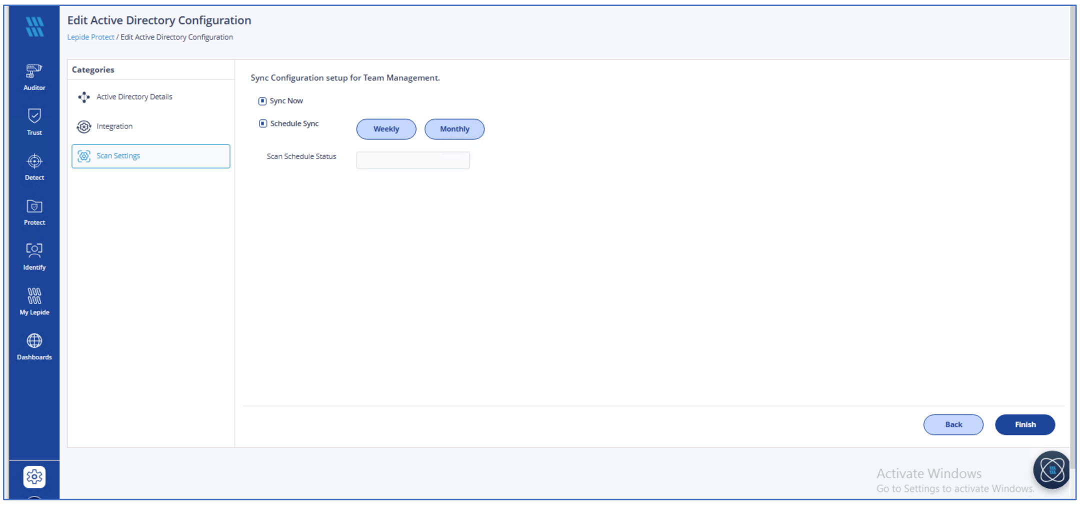



*Figure 10: Scan Settings*

11. This page allows you to sync the configuration setup for team management which means it will retrieve information from AD and display the users and managers as a hierarchical structure to make it easier to see who manages who.

Select **Sync Now** to start scanning now

Or

Select **Schedule Sync** to specify a schedule to regularly sync this information

| | |
|---|---|
| **NOTE:** | Note that any changes in Active Directory will be highlighted during the scan and you can choose whether to accept these changes or ignore them |

12. Once any changes are verified, click **Finish** to update Lepide Protect

### 2.4.4 Updating Details Manually

If a change needs to be made to Lepide Protect before the next scheduled scan, the changes can be made in the **Integration Page** and then the **Sync Now** option can be selected to update Lepide Protect.

# 3 Team Management

The Team Management Wizard simplifies the process for Super Admins to manage user hierarchies configured through the Permission Management Module. It provides a clear view of the organizational structure and supports the following key activities:

**User Enrolment:**

- User enrolment allows the Super Admin to delegate responsibility for permissions management to the specified manager of their team. This means that the manager, who will know the roles and requirements of their team, can allocate permissions accordingly.
- Enabling access in this way to managers affects **Lepide Protect features only**, without affecting console-wide privileges

**Action Management:** Allow managers to execute assigned policies and receive email notifications for updates and actions.

**User Un-enrolment:** Unassigned roles and remove users from the ability to run policies

This streamlined approach ensures managers and team members have the tools they need to maintain proper access control efficiently.

1. Hover over **Lepide Protect** and the following menu options are displayed:

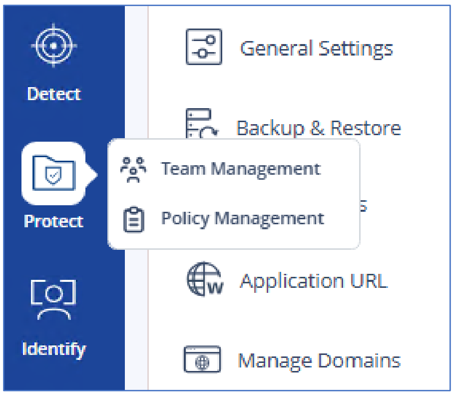



*Figure 11: Lepide Protect Menu Options*

2. Select **Team Management**

The team management screen is displayed:

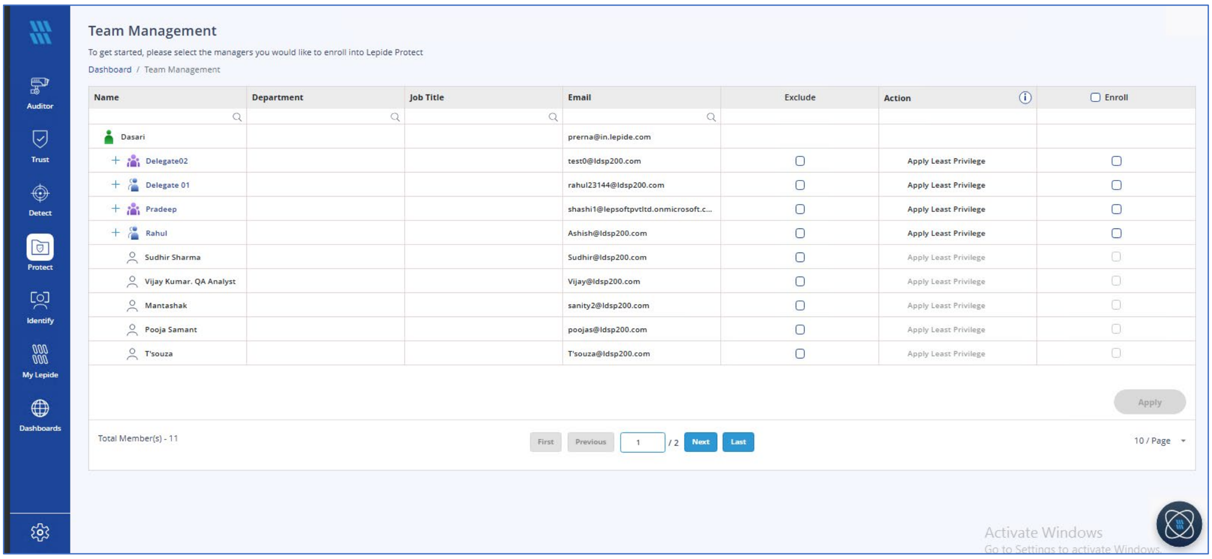



***Figure 12: Team Management***

This screen shows the single Super User responsible for all permissions management at the top of the hierarchy. Below this are the managers of the different teams and individual users. Click the '+' icon next to the manager to expand the team and view the team members. There could be further managers within these groups which can be expanded and viewed in a similar way.

**The Team Management screen has the following options:**

The icons next to the Manager name represent the following:

A manager with subordinates only

A manager with other managers and subordinates

## 3.1 Action

The **Apply Least Privilege** action will be applied when a scan is run

## 3.2 Enroll

Enrolling a Team Manager means that permissions management has been delegated to them for their particular team. Once enrolment has been selected, the relevant manager will receive an email to inform them that they now have authority to log into Lepide Protect and manage permissions for their team members.

- To enroll a Team Manager, check the **Enroll** box
- Click **Apply**

To see the managers who have been enrolled, select Role Management and the Role column will show their user role and their Lepide Protect role will be shown next to this:

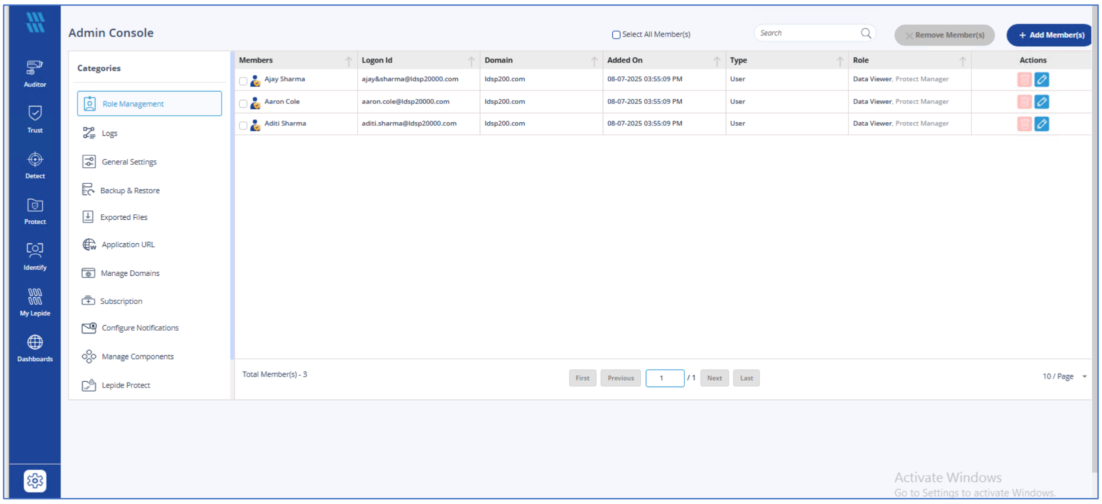



***Figure 13: Role Management***

- In the example above, Arjun has a Role of Data Viewer which can be switched to Admin if required. The other role is Protect Manager for Lepide Protect which cannot be changed here and so is disabled.

## 3.3 Exclude a Team or a User

To exclude a Team or a User from having a policy applied to them, check the **Exclude** box next to the Team or User. This provides an easy way to specify any teams or users that you want to exclude from a particular policy. Once the policy has been configured, the Exclude box can be unchecked.

**To exclude a team or user:**

- Check the box in the **Exclude** column for the relevant user or team
- Click **Apply**
- The user or team will be excluded temporarily from Policy Management

- When a user or team has been excluded there will be a green icon showing this. Clicking the icon will display a list of those Excluded:

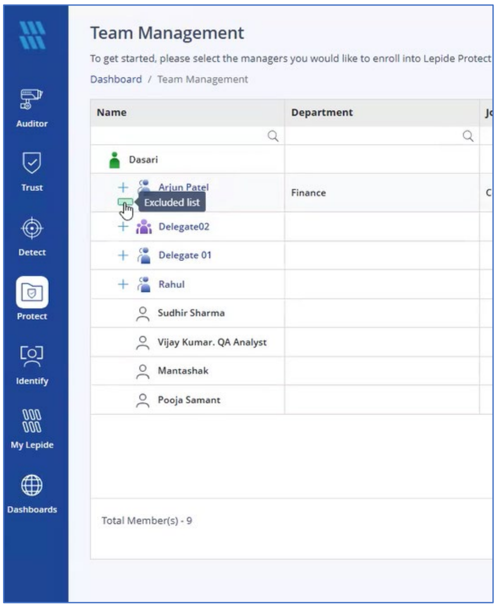



*Figure 14: Team Management Showing Excluded Icon*

- Check the box again to remove the **Exclude** option and the user or team will be included again

# 4 Policy Management

The **Policy Management** module in Lepide Protect provides a comprehensive set of tools to manage user permissions effectively. It enables you to create, execute, and manage policies across users while ensuring data integrity and compliance.

Note: Before Policy Management can be configured, the users need to have been configured as described previously in this document. Also a File Server scan needs to have been configured for auditing and a File Server scan needs to have been run.

- Hover over **Lepide Protect** and the following menu options are displayed:

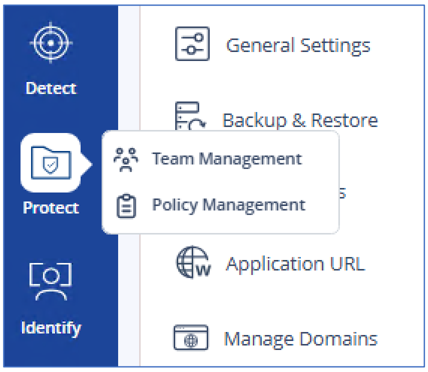



*Figure 15: Lepide Protect Menu Options*

- Select **Policy Management**

  The Policy Management screen is displayed:

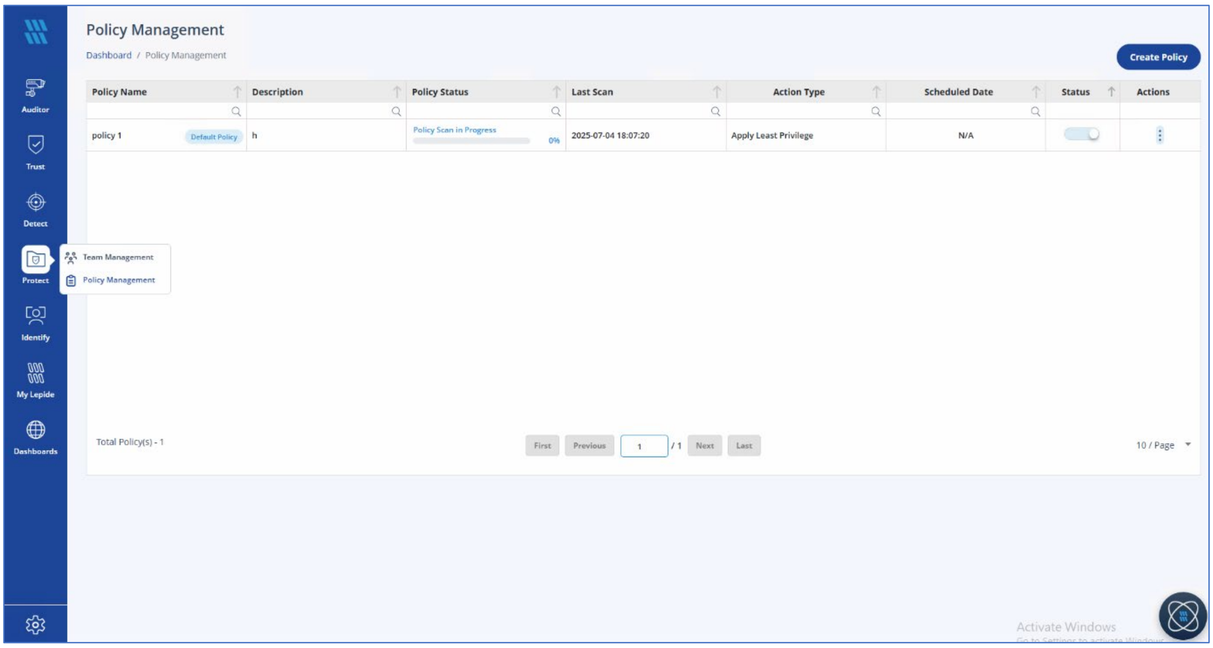



*Figure 16: Policy Management*

Lepide Protect allows you to create customized policies for specific actions. The process includes:

- Selecting the target users enrolled in team management
- Defining the policy name, action type, and timeframe for capturing excessive permissions
- Choosing the file server and folder sections fetched from the **CPA scan** from the legacy console

## 4.1 To Create a New Policy

- Click **Create Policy**

The Create Policy screen is displayed:

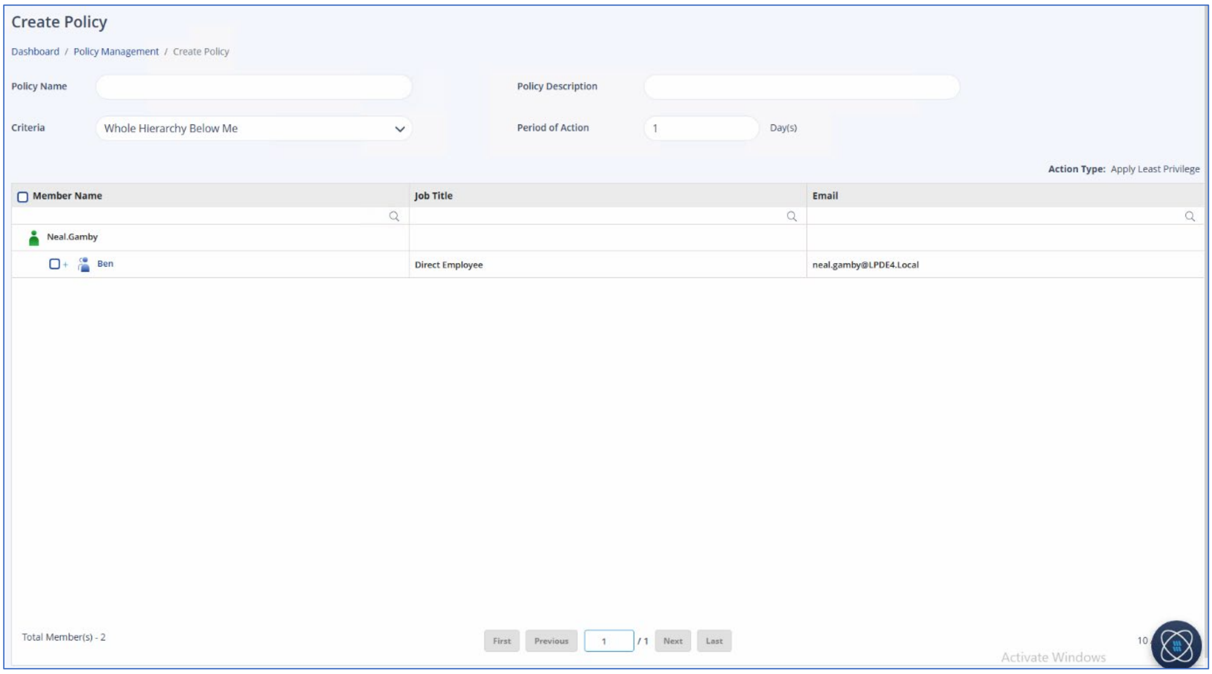



*Figure 17: Create Policy*

- Enter a **Policy Name** and optional **Description**
- Select **Criteria**

The Criteria drop down menu has the following options:

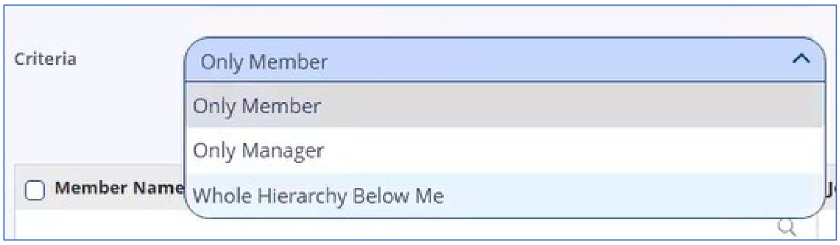



*Figure 18: Criteria*

- Members are those directly reporting to the manager
- Managers are all designated managers
- Whole Hierarchy applies to everyone below the current manager

- Select the **Period of Action** This refers to the number of days of inactivity to decide whether permissions should be removed. The default and recommended number for this is 30 days.

- Click **Next**

The list of servers and folders is displayed:

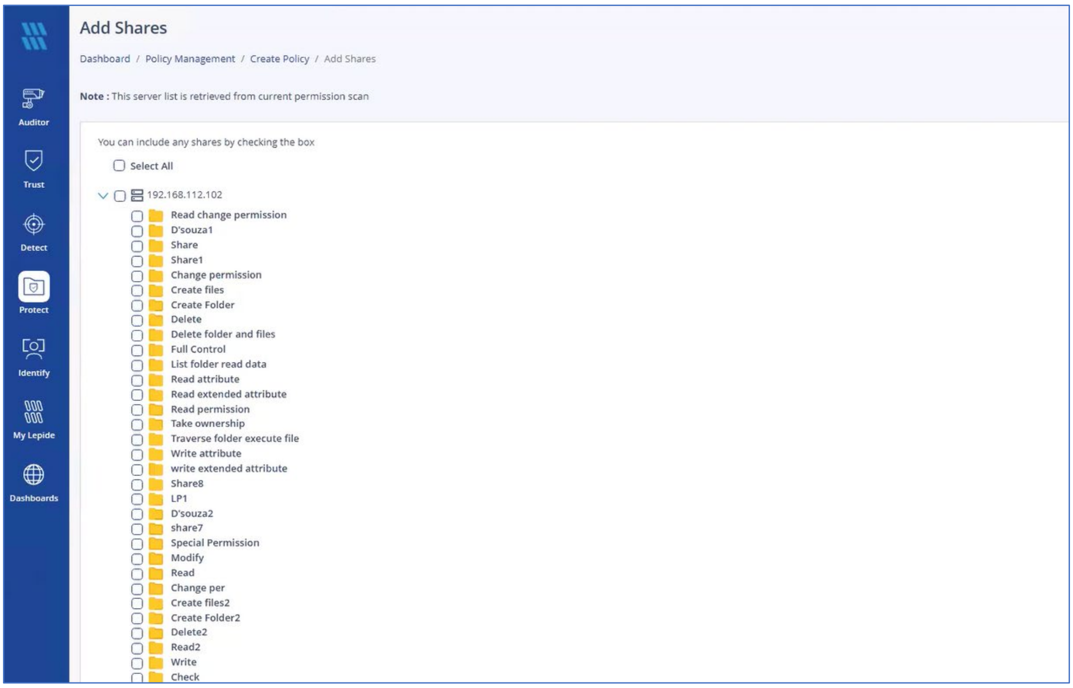



***Figure 19: Add Shares***

- Select the shares as required by checking the relevant box(es)
- Click **Next**
- Policies can be executed manually via the **Start Scan** feature or scheduled for automatic execution (weekly or monthly).

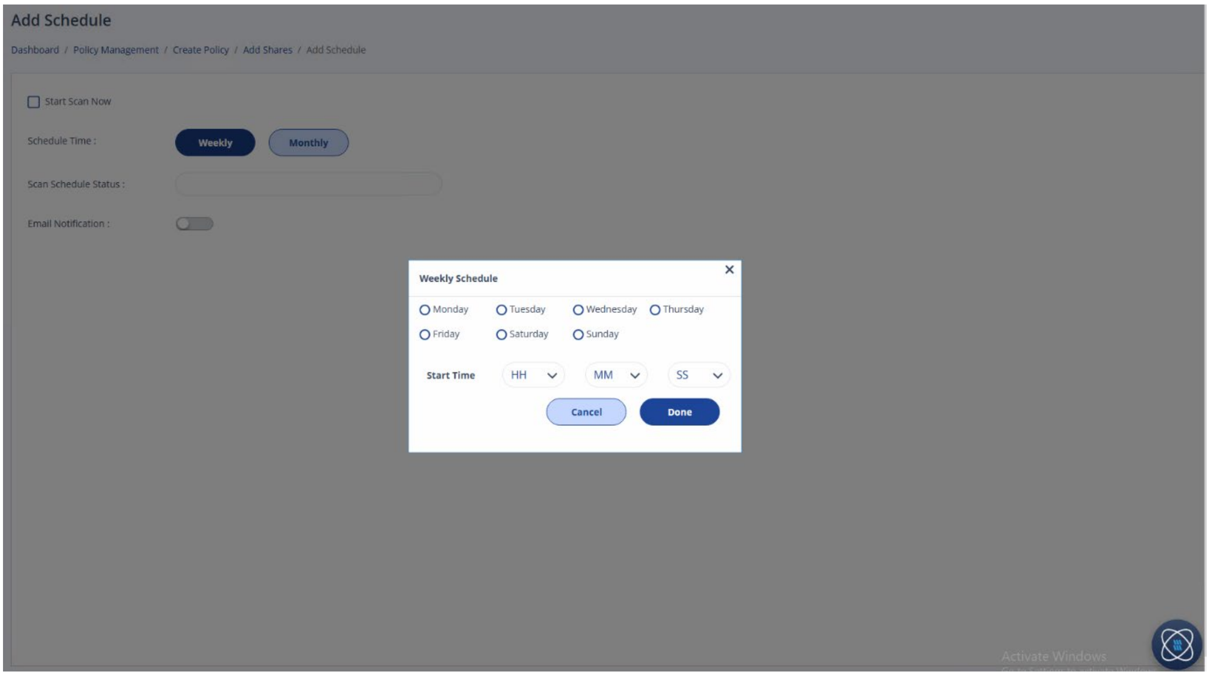



*Figure 20: Scan Options*

- Click **Finish**

The Policy will be displayed in the Policy Management page:

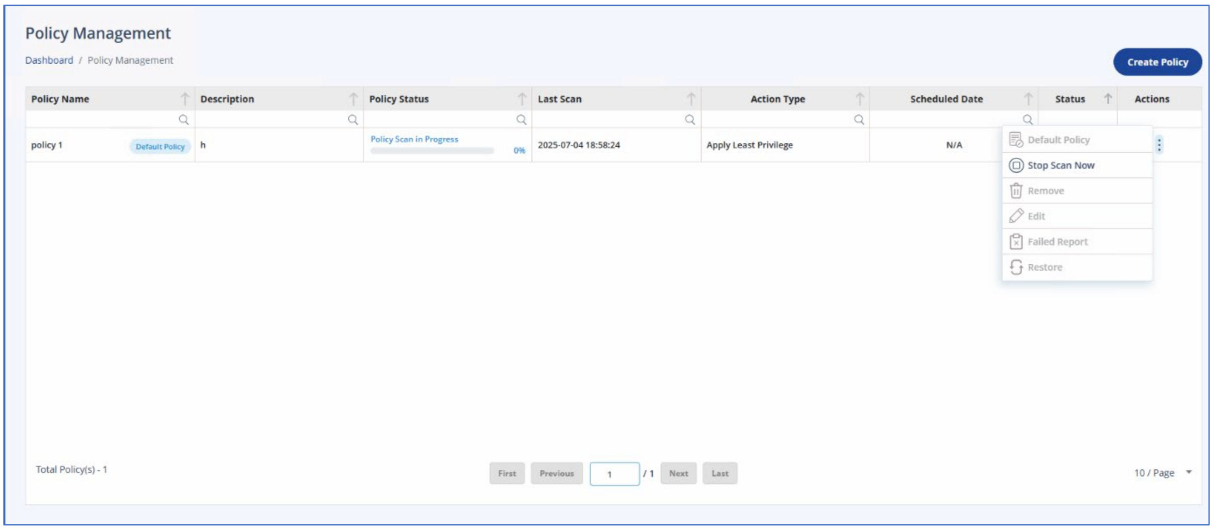



*Figure 21: Policy Scan in Progress*

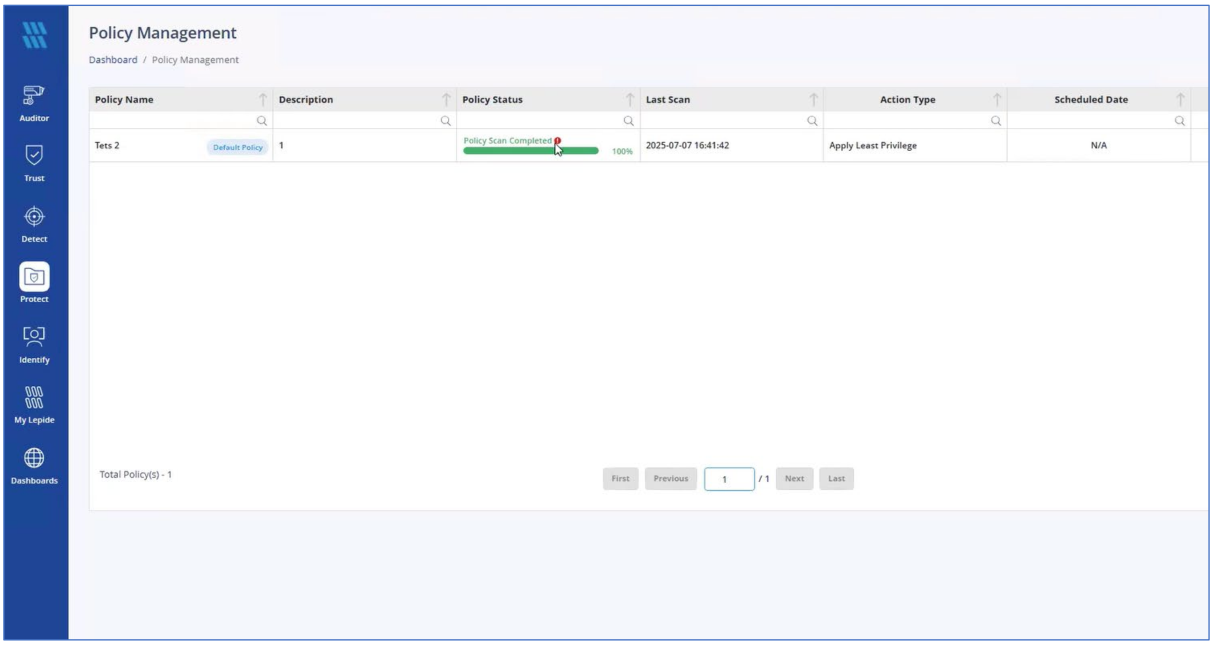



*Figure 22: Policy Scan Complete*

- Here the Policy Status shows that the scan is complete.

## 4.2 Failed Reports

- If a policy fails or partially executes for specific users, a detailed report is generated. This includes:
  - The reason for the failure.
  - The exact file path or action that caused the issue

In the example above, there is a notification 'Selected action failed to perform for one or more users – refer to failed report'.

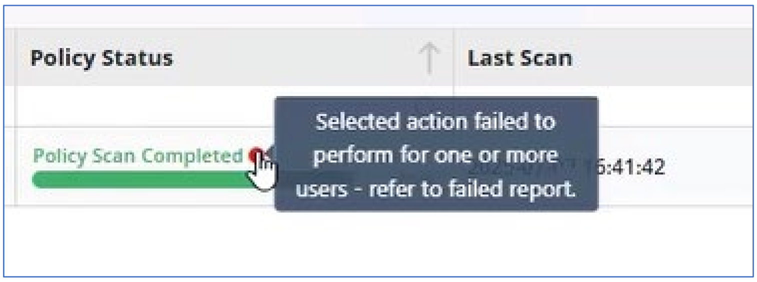



*Figure 23: Notification of Action Failed*

- The failed report is available by clicking the ⋮ icon and choosing **Failed Report** from the menu.

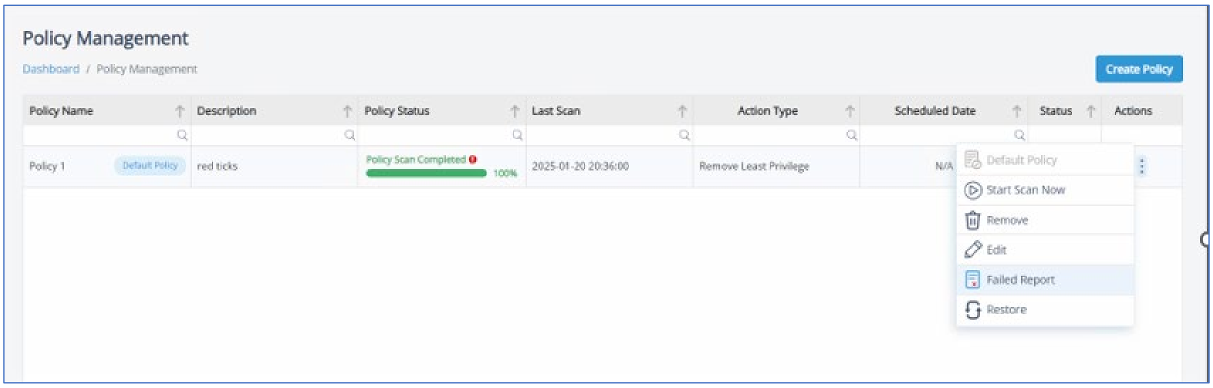



*Figure 24: Failed Report Option*

## 4.3 Edit Policy

Easily modify the options selected during the policy creation process, allowing you to update user lists, actions, or schedules as required.

- Click the ⋮ and select Edit from the menu:

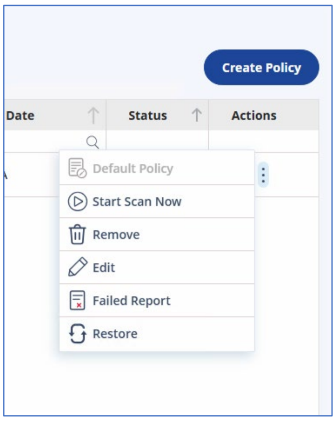
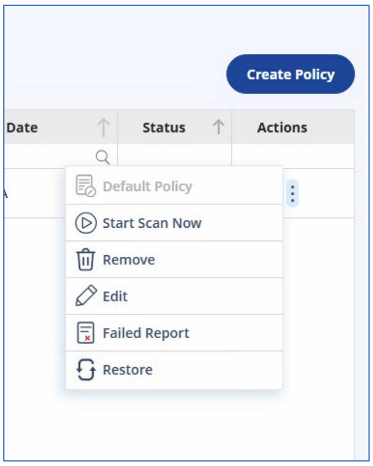



*Figure 25: Action Menu*

## 4.4 Remove Policy

- To remove a policy that is no longer needed, select **Remove** from the Action menu.




## 4.5 Restore Policy

Every successful policy execution generates a backup of the changes made by the policy automation. This ensures you can easily restore any changes using the backup.

- Backup retention is configurable under **Permission Management** settings:
  - **Minimum:** 2 backups
  - **Default: 5 backups**
  - **Maximum: 12 backups**

To restore a Policy select Restore from the Action menu:

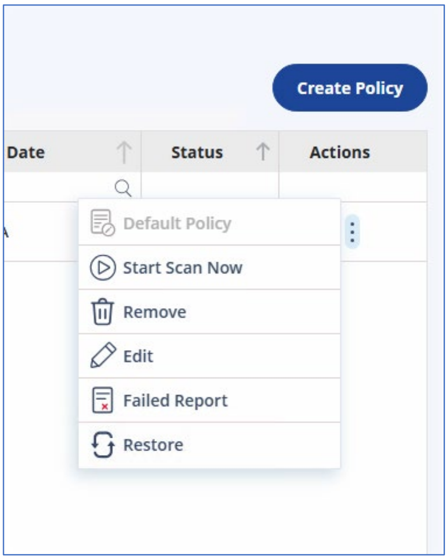



***Figure 26: Action Menu***

The following message will be displayed:

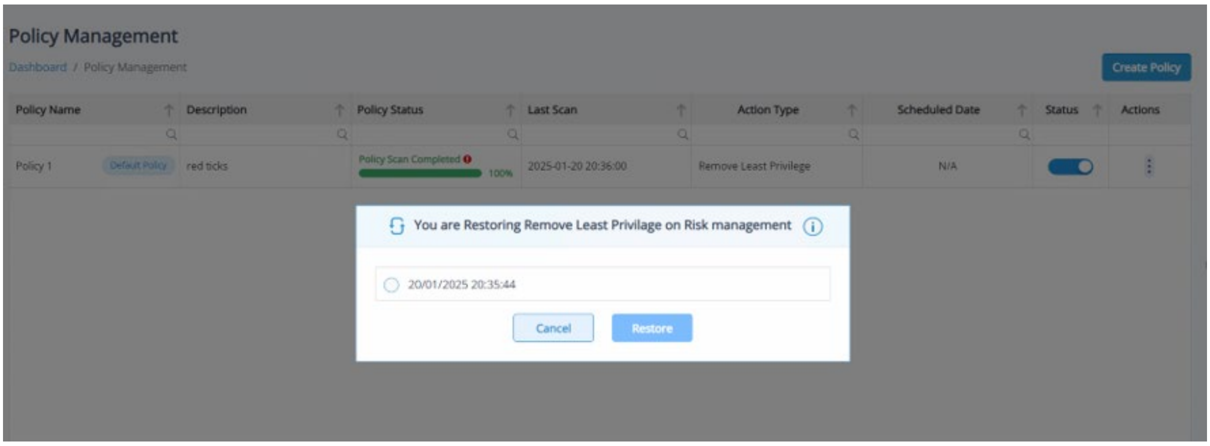



*Figure 27: Restore a Previous Policy*

- Select a backup by date and click **Restore**
- Please refer to Policy Restoration Mechanism in Section 6.2 for full details on how this works.

# 5 Protect Dashboard

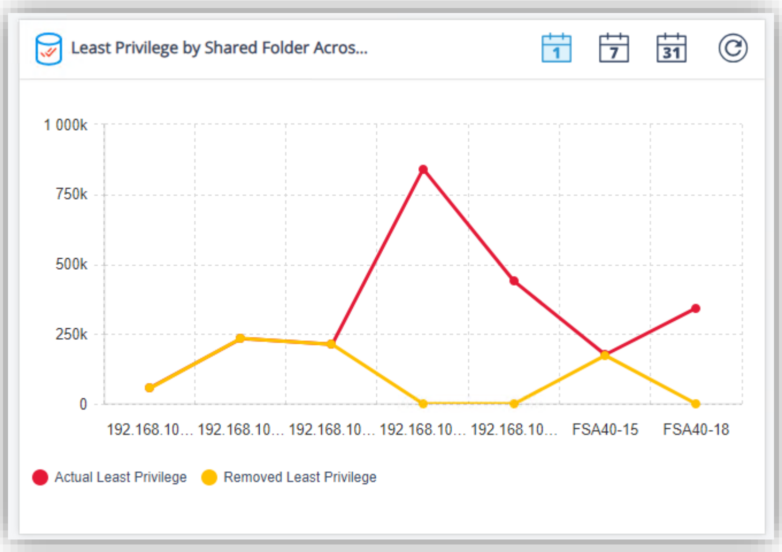
The Protect Dashboard serves as your central command center for permission management, offering real-time insights through six powerful graphs. Each visualization helps you make informed decisions about your organization's security posture.

- To view the Protect Dashboard, from the Dashboards page select **Protect**

## 5.1. Least Privileges by Shared Folder across File Server

This dynamic graph provides a comprehensive view of permission distribution:

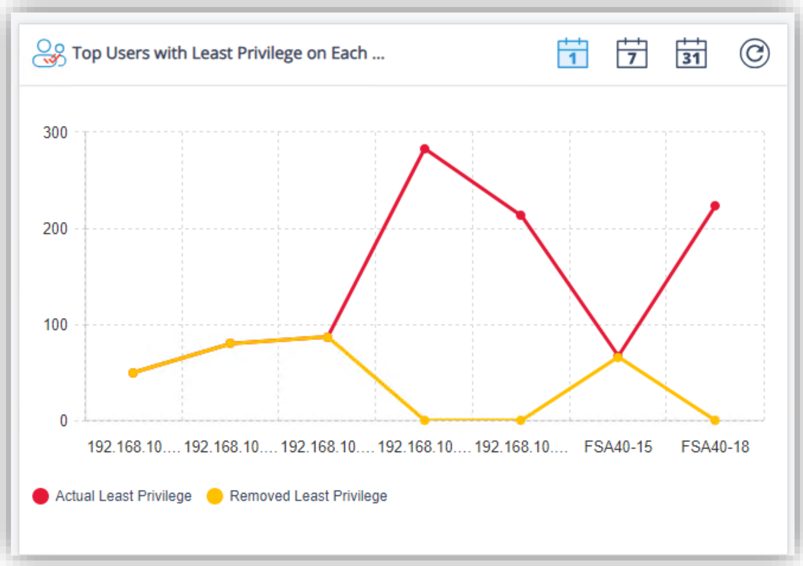
- **Upper Line:** Shows total permissions before policy implementation
- **Lower Line with Red Ticks:** Displays permissions removed through automation
- **Interactive Features:** Click any file server to drill down into specific folders
- **Use Case:** Identify high-risk folders with excessive permissions to prioritize your security efforts
- **Business Value:** Target your permission cleanup efforts where they matter most
- **Best Practice:** Review weekly to track permission reduction progress




## 5.2. Top Users with Least Privileges on Each File Server

This crucial visualization highlights permission hotspots by user:

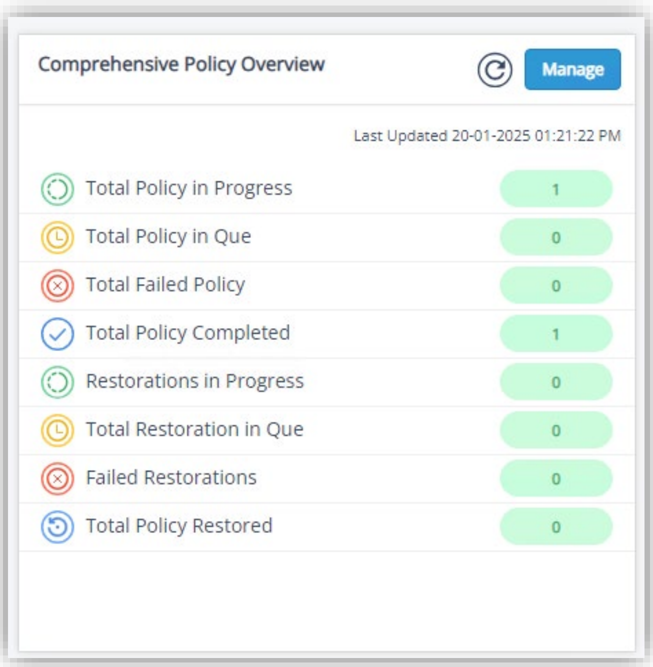
- **Red Ticks:** Indicate excessive permissions per user
- **Interactive Elements:** Click data points to see detailed user permission breakdowns
- **Sorting:** Users ranked by number of excessive permissions
- **Use Case:** Identify users who need immediate permission review
- **Action Items:** Create targeted policies for users with high red tick counts
- **Risk Mitigation:** Focus on users with the most significant security impact



## 5.3. Comprehensive Policy Overview

Track your policy implementation success with this detailed graph:

- **Policy Status:** View created, pending, and executed policies
- **Execution Tracking:** Monitor policy completion rates
- **Success Metrics:** Track policy effectiveness over time
- **Resource Planning:** Optimize policy creation and execution schedules




## 5.4. Folder Risk Reduction by Policy Action

Monitor the impact of your security measures over time:

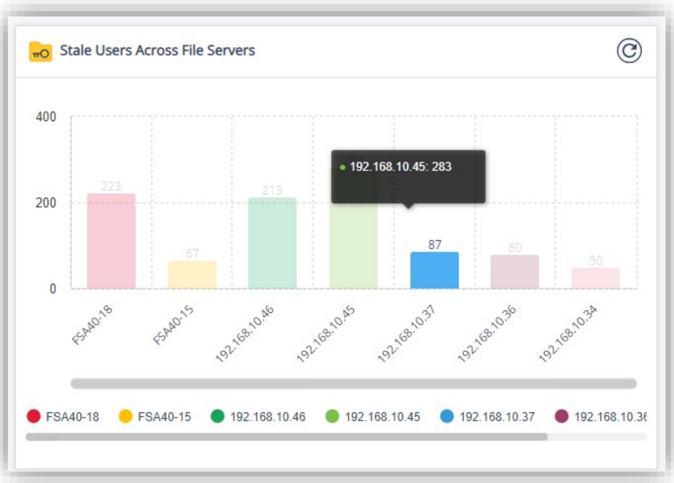
- **Three-Month Timeline:** Track risk reduction trends
- **User Impact:** See how many users are affected by each policy
- **Action Types:** Break down different types of permission changes
- **Progress Tracking:** Measure risk reduction effectiveness
- **ROI Visualization:** Demonstrate security improvement value

- **Compliance Monitoring:** Track progress toward security goals


## 5.5. Stale Users across File Server

Identify and manage inactive user accounts efficiently:

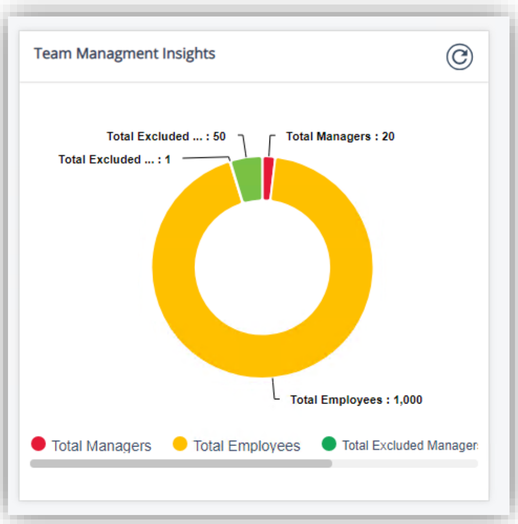
- **Active Directory Status:** Track user activity states
- **Server Distribution:** See stale user concentration by server
- **Risk Assessment:** Identify potential security vulnerabilities
- **Clean-up Opportunities:** Find quick wins for permission removal
- **Trend Analysis:** Monitor stale user accumulation over time
- **Action Planning:** Prioritize user account clean-up efforts




## 5.6. Team Management Insights

Get a clear picture of your team's permission management structure:

- **User Status:** Track configured, enrolled, and excluded users
- **Team Structure:** Visualize organizational hierarchy
- **Enrolment Trends:** Monitor team participation rates
- **Coverage Analysis:** Identify gaps in team enrolment
- **Management Efficiency:** Optimize team structure and roles



# 6 Additional Features that Enhance Permission Management

Lepide Protect offers several features to streamline and improve the efficiency of permission management:

**In-App Notifications:** Stay updated on all important actions and events directly within the app. Real-time notifications ensure you never miss critical updates or changes.

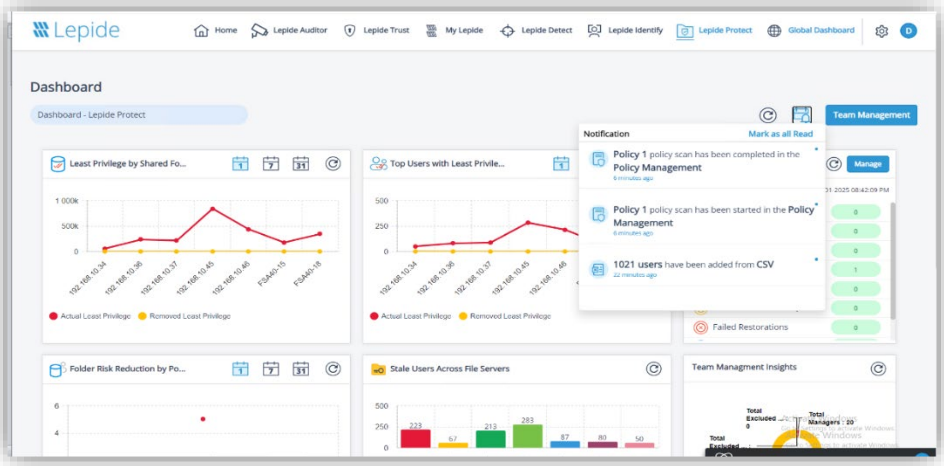



*Figure 28: Lepide Protect Dashboard*

- **Email Notification:** Receive detailed email alerts for important actions, policy executions, or failed reports. This feature keeps users informed, even when they are away from the app.
- **Default Policy:** The **Default Policy** is a pre-configured policy designed to simplify your initial setup. It provides a baseline for removing excessive permissions while still allowing customization to suit your specific needs.

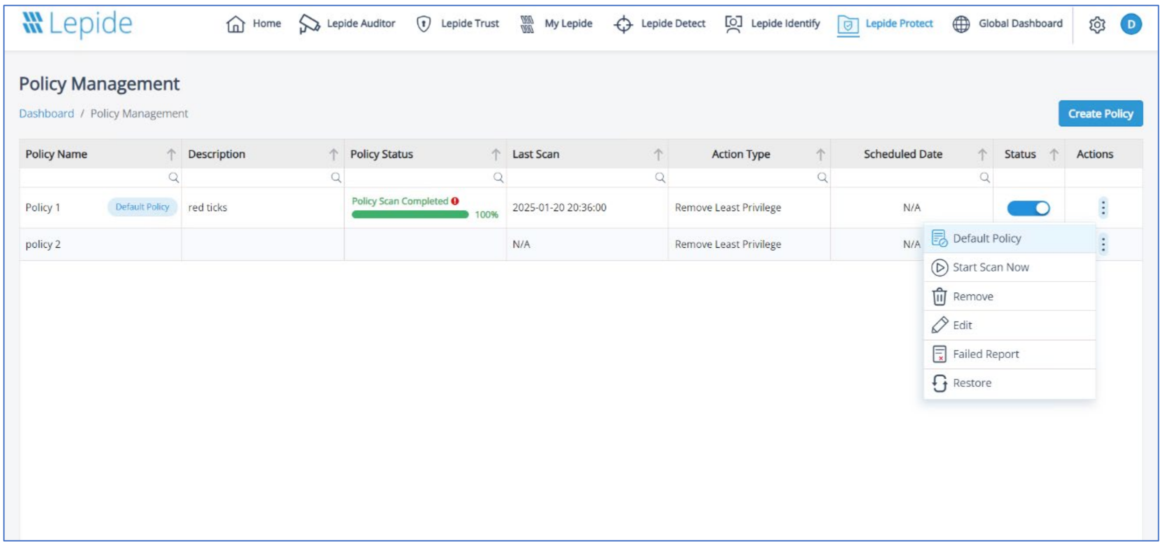



*Figure 29: Policy Management*

## 6.1 Key Features

- **Automated User Addition:**
  When a scheduled configuration is run, newly added users from Active Directory (AD) or HRMS are automatically included in the default policy.
- **One-Click Update:**
  A single click on the **Update** button from the configuration page ensures that these new users are seamlessly added to the policy, streamlining the process and saving time.

The **Default Policy** ensures efficient permission management right from the start and adapts to changes in user data with minimal effort

**Scheduling of Configurations:** Automate configuration tasks by scheduling configurations. Set specific times for scans or policy executions to minimize manual intervention and ensure consistent results.

## 6.2 Policy Restoration Functionality

### 6.2.1 Overview

Policy Restoration enables users to revert folder permission changes to a previously executed policy. Each time a policy is executed, a backup is created that records only the changes (users affected) on that specific run. Restoring to any previous backup removes all changes made on and after that backup, resetting the policy to its prior state.

### 6.2.2 Restoration Behavior

- Each backup captures the delta — i.e., only the users whose permissions were modified in that execution.
- When restoring to a selected backup (e.g., Day N), the system removes all user permission changes applied on Day N and after.
- The result is a rollback to the exact state that existed before Day N.

**Example:**

| Execution Day | Users Denied That Day |
|---|---|
| Day 1 | User1, User2 |
| Day 2 | User3 |
| Day 3 | User4 |
| Day 4 | User5 |
| Day 5 | User6 |

- Remove permissions for User3 (Day 2), User4 (Day 3), User5 (Day 4), and User6 (Day 5)
- Revert the policy state to only User1 and User2 as denied (from Day 1)

**Key Functional Rules**

- **Delta-based execution:** Each backup holds only the users affected during that specific execution
- **Subtractive restoration:** Restoration removes all users added in and after the selected backup day
- **Non-cumulative:** Backups are not merged or overlaid. Only the state prior to the selected backup is restored
- **Restoration is final:** Once restored, the current state is locked and shown as the active state until another backup is applied

**Backup Management Policy**

| Parameter | Value |
|---|---|
| Maximum Backups | 12 backups per policy execution history |
| Default Backups | 5 backups retained by default |
| Minimum Backups | 2 backups retained at all times (system-enforced) |
| Retention Strategy | On exceeding 12, the oldest non-default backup is automatically removed |
| Backup Lifecycle | All backups are time-stamped and persist until pruned by retention rules |
| Restore Behavior | Restoring a backup does not delete it; the restored state becomes inactive for further restoration |

**Functional Capabilities**

- **Jump Restoration:** Users can restore to any backup, regardless of order — including older or newer backups.
- **Flexible Rollback:** Supports both backward and forward restoration based on available backups.
- **Audit Traceability:** Each backup clearly shows which users were denied in that run for auditing and review.
- **Backup Deactivation**: Once restored, the same backup cannot be restored again unless re-executed.

**Summary**

The Policy Restoration feature offers precise rollback control for permission states, maintaining operational integrity and compliance. It is designed to be predictable, traceable, and adaptable to administrative workflows that require accurate undoing of permission changes.

# 7 Support

If you are facing any issues whilst installing, configuring, or using the solution, you can connect with our team using the contact information below.

## Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

## Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

# 8 Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.