ManageEngine
Exchange Reporter Plus

Permissions Guide

www.exchangereporterplus.com

Table of Contents

1. Overview ---- **1**

2. List of permissions required to perform specific tasks in Exchange Reporter Plus ---- **1**

3. Configuring domain permissions ---- **2**

A. Exchange Server container ---- 2

B. Domain Partitions container ---- 4

4. Configuring folder read permissions for message tracking, IIS logs, and database files ---- **6**

A. Configuring traffic log path ---- 6

B. Configuring IIS log path ---- 8

C. Configuring information store path ---- 9

5. Configuring permissions required for content reports ---- **11**

6. Permissions required for backup restoration and archiving ---- **12**

7. Configuring permissions required for auditing and monitoring ---- **12**

8. Permissions for Powershell command execution ---- **13**

A. Security Descriptor of PowerShell session ---- 14

9. Permissions required for storage reports (WMI access permissions) ---- **15**

1. Overview

This document is the one-stop solution to all your permissions-related questions and lists all the necessary privileges and permissions for reporting, monitoring, and auditing your Exchange Server, Exchange Online tenant, and Skype for Business Server.

2. List of permissions required to perform specific tasks in Exchange Reporter Plus

Tasks	Required privileges
Essential Data Gathering - This is a mandatory task for all tasks	LDAP Read privilege over all GC Objects Invoke-Command Powershell privilege WMI Query privilege Database files Read privilege
Exchange Server Distribution List Membership	LDAP Read privilege View-Only Recipents RBAC
Exchange Server Mailbox Account Properties	LDAP Read privilege View-Only Recipents RBAC
Exchange Server Public Folder Properties	LDAP Read privilege View-Only Recipents RBAC
Exchange Server Traffic Logs	LDAP Read privilege Message Tracking log folder access
Exchange Server OWA Logs Failed OWA Logs	LDAP Read privilege IIS logs folder access View-Only Recipents RBAC for Active Sync Reports
Exchange Server Mailbox Permission	LDAP Read privilege View-Only Recipents RBAC
Exchange Server Distribution Group Permission	LDAP Read privilege View-Only Recipents RBAC

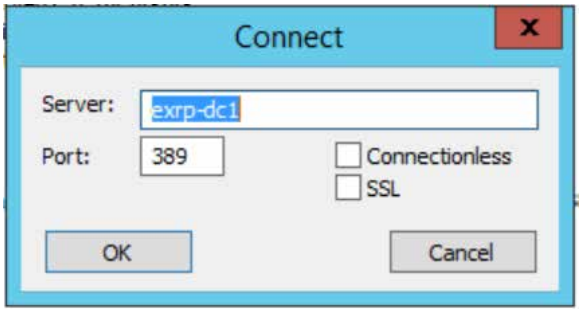
Exchange Server Content Reports Generation	LDAP Read privilege Exchange Web Services
Exchange Server Audit Reports	Exchange Server Event Logs Read privilege Domain Controller Event Logs privilege
Exchange Server Advanced Audit Reports	View-Only Audit Logs RBAC View-Only Configuration RBAC
Exchange Server Monitoring	WMI Query - CPU, Memory Utilization WMI Query, Database Folder path access, Invoke-Command Powershell Access - Storage Monitoring. Monitoring, View-Only Configuration - All Other Categories.
Exchange Server Content Search	Exchange-View-Only Administrators permissions for all mailboxes or ApplicationImpersonation role.
Exchange Online Reporting	View-OnlyRecipients, MailRecipients, AddressLists, View-OnlyConfiguration, MailboxSearch and UserOptions roles
Exchange Online Auditing	View-OnlyAuditLogs, View-OnlyConfiguration, View-OnlyRecipients and DataLossPrevention roles
Skype for Business Server Reporting	CsAdministrator or CsViewOnlyAdministrator role

3. Configuring domain permissions

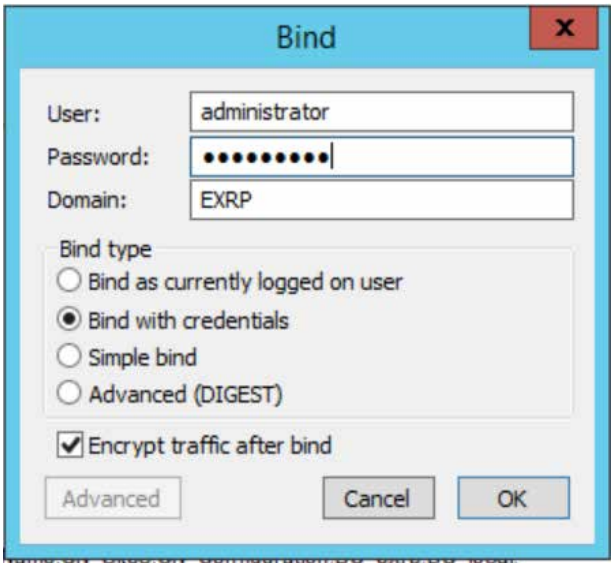
The first step in configuring domain permissions is to create a new user account called erpServiceAcc under the Domain Users group, and add this user to the Event Log Readers group. Then, provide read permissions for the Exchange Server container and Domain Partitions container as explained below:

A. Follow the steps given below to provide read permissions to the Exchange Server container:

1. Open the **ldp.exe** file that acts as a lightweight directory access protocol client and connect to the primary domain controller.

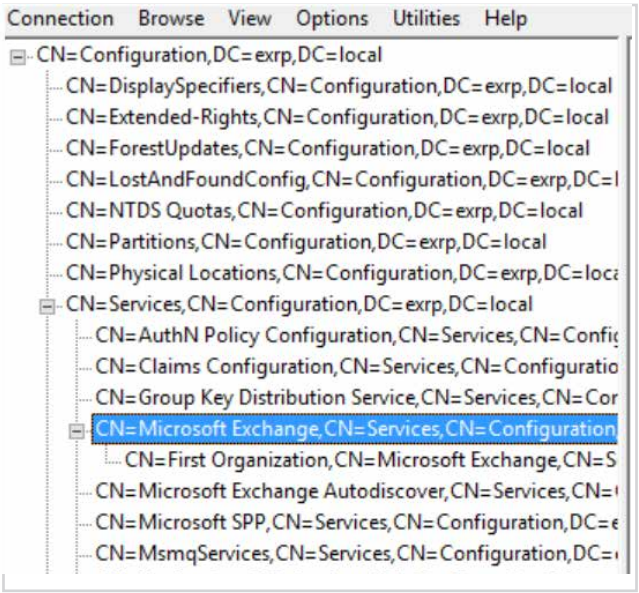


2. Apply a bind connection using administrative credentials to give permission to the **erpServiceAcc** account. (you may select a different user name as well).



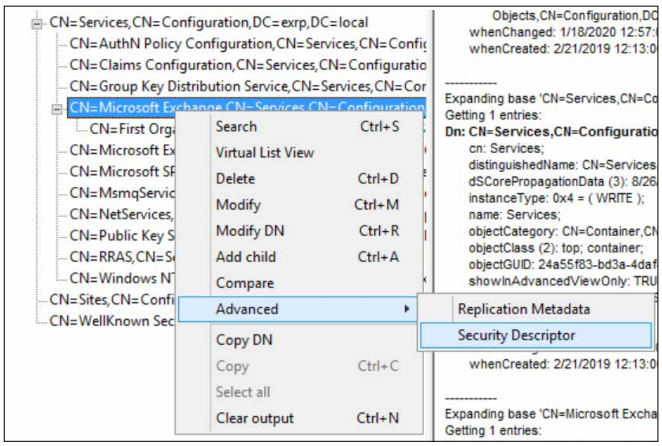
3. Open the configuration **Tree View.**

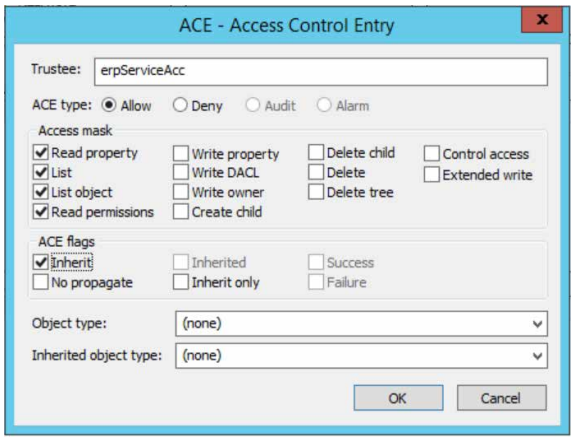
4. Right-click on **CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=exrp,DC=local > Advanced > Security Descriptor.**



5. In the bottom-left corner, select the **Access Control Entries (ACE)** option and add a **Trustee.**

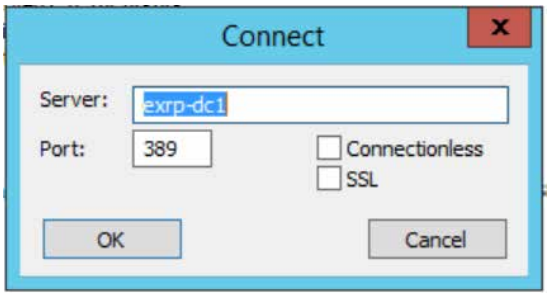
6. Add erpServiceAcc as a **Trustee.**



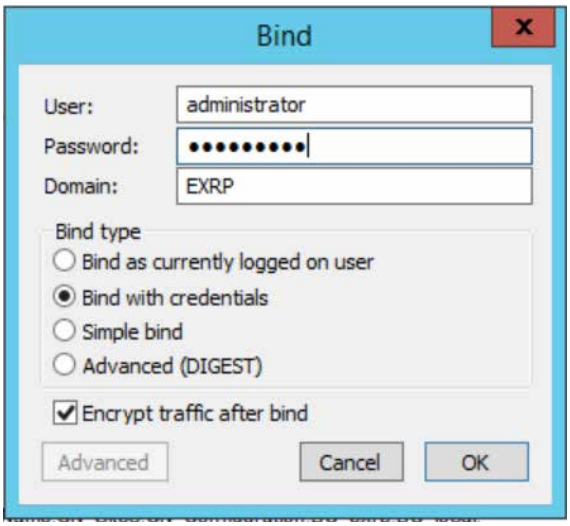


B. Follow the steps given below to provide read permissions to the Domain Partition container:

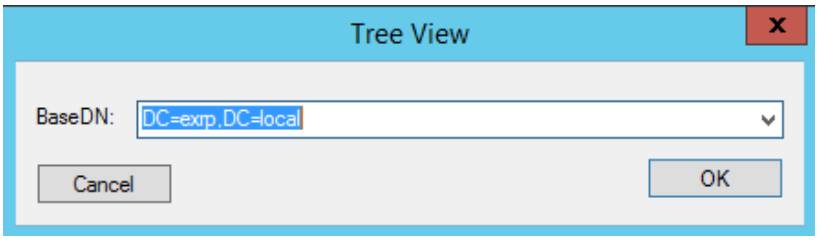
1. Open the **ldp.exe** file that acts as a lightweight directory access protocol client and connect to the primary domain controller.



2. Apply a bind connection using administrative credentials to give permission to the **erpServiceAcc** account.



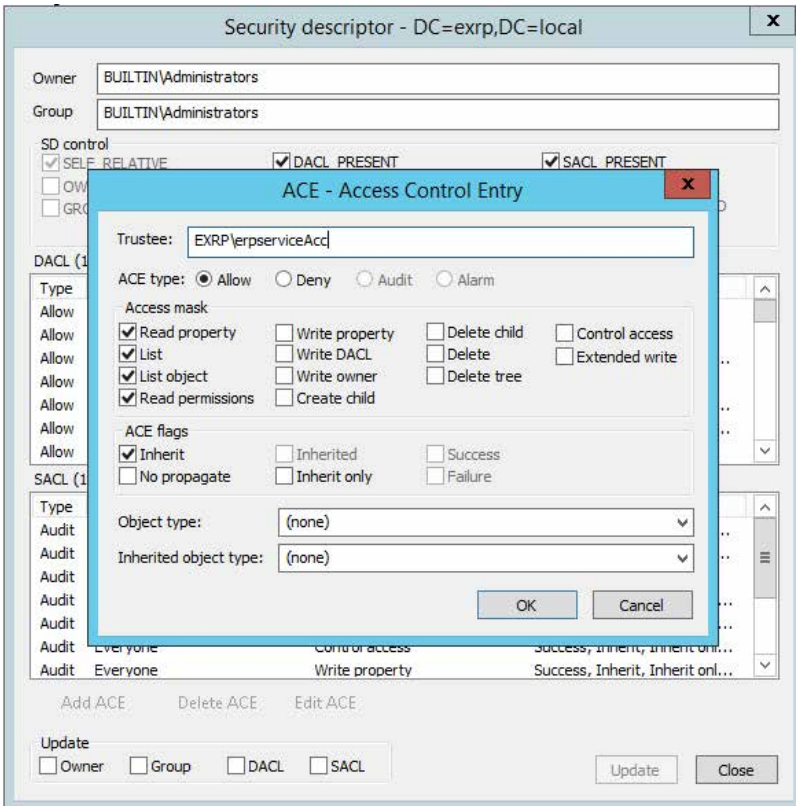
3. Open the configuration Tree View.



4. Right-click on **CN=exrp,DC=local > Advanced > Security Descriptor.**

5. In the bottom-left corner, select the **Access Control Entries (ACE)** option and add a Trustee.

6. Add **erpServiceAcc** as a Trustee.



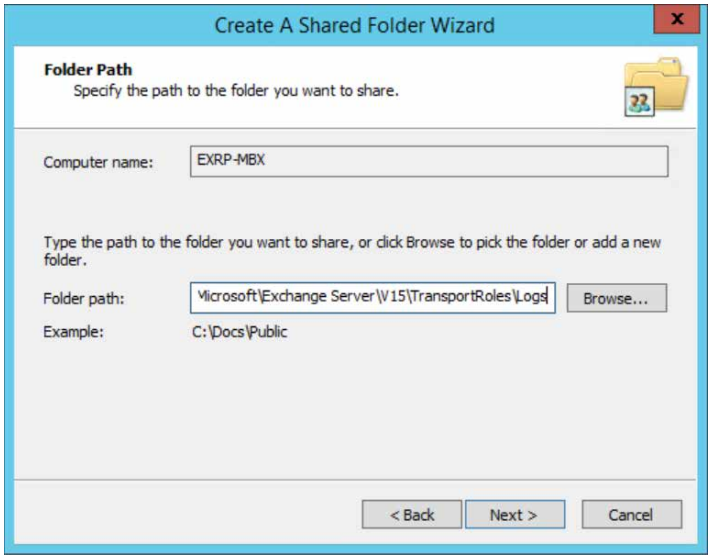
4. Configuring folder read permission for message tracking, IIS logs, and database files

A. Configuring the traffic log path

1. Log in to the Exchange Server (mailbox role). Select **Computer Management.**

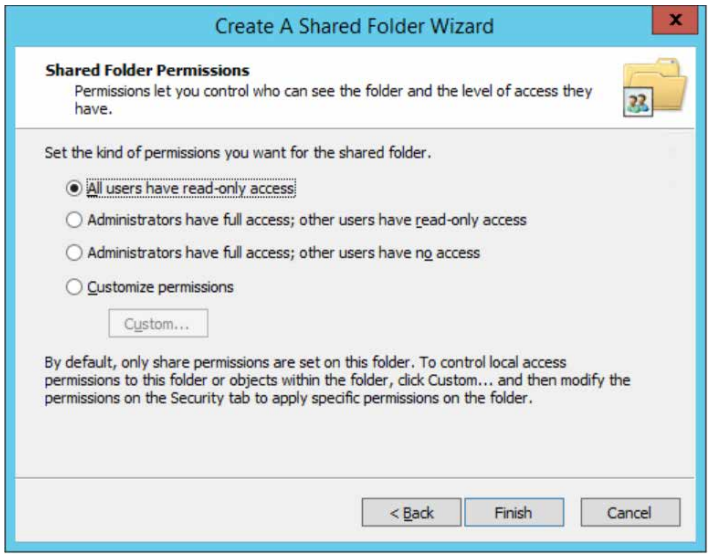
2. Navigate to **System Tools** > **Shared Folders** > **Shares.**

3. Create a new share, and choose the folder path as **C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs.**



4. Provide the **Share name** as T$ and click **Next.**

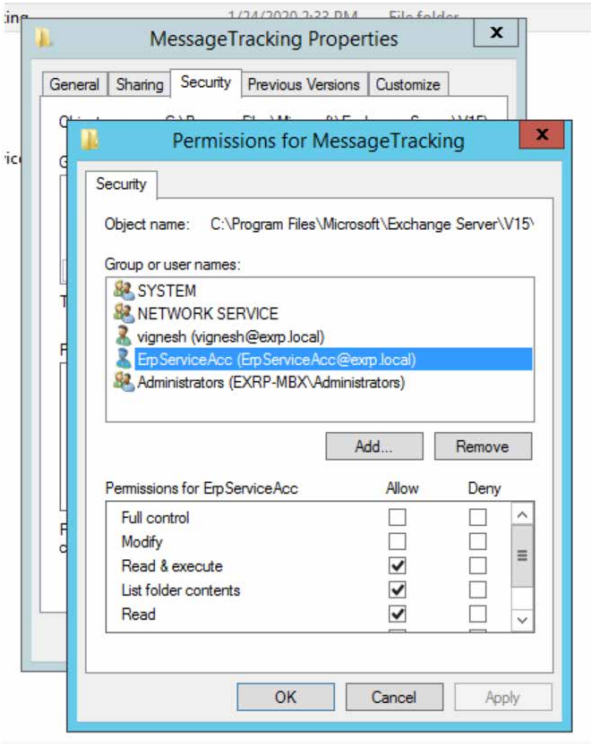
5. You can provide read-only access or full permissions, or you can customize user permissions as per your requirement.



6. Navigate to **C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs.**

7. Right-click the **MessageTracking** folder and select **Properties.**

8. Click **Edit**, add **erpServiceAcc**, and delegate read privileges to the user.



Configuring the traffic log path in Exchange Reporter Plus:

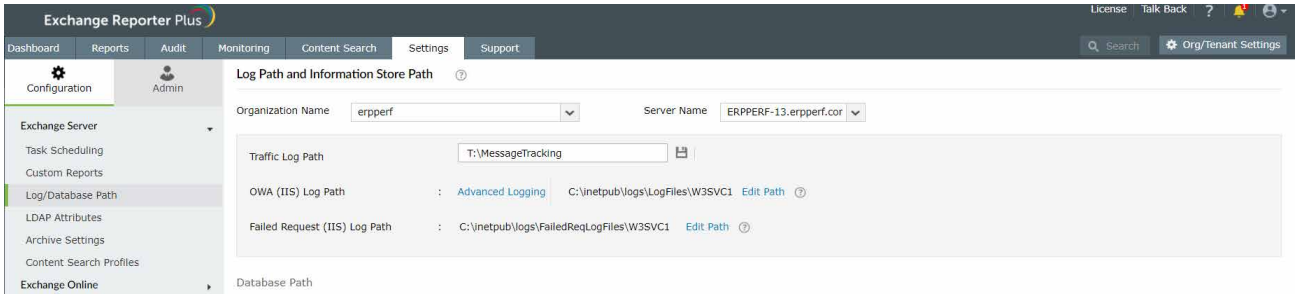
1. Log in to Exchange Reporter Plus as an administrator.

2. Navigate to **Settings > Configuration > Exchange Server > Log/Database Path.**

3. Go to **Traffic Log Path** and click **Edit Path.**

4. Update the path to **T:\MessageTracking.**

5. Click the **save icon.**



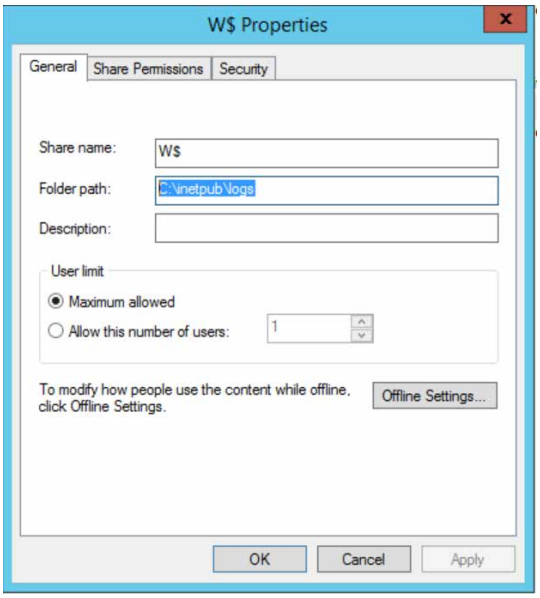
B. Configuring the IIS log path

1. Log in to the **Client Access Server.** Select the **Computer Management** option.

2. Navigate to **System Tools > Shared Folders > Shares.**

3. Create a new share, and choose the folder path as **C:\inetpub\logs.**

4. Provide the **Share name** as W$ and click **Next.**



5. Navigate to C:\inetpub\logs. Right-click the **W3SVC1** folder and go to **Properties.**

6. Click **Edit,** add **erpServiceAcc,** and delegate read privileges to the user.

Configuring the OWA (IIS) log path in Exchange Reporter Plus:

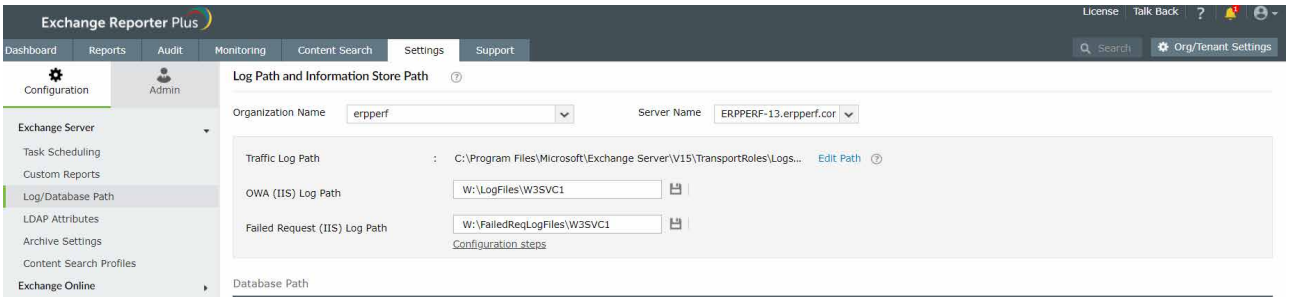
1. Log in to Exchange Reporter Plus as an administrator.

2. Navigate to **Settings > Configuration > Exchange Server > Log/Database Path.**

3. Go to **OWA (IIS) Log path** and click **Edit Path.**

4. Update the path to **W:\LogFiles\W3SVC1**. Also, update **Failed Request (IIS) Log Path** to **W:\FailedReqLogFiles\W3SVC1.**

5. Click the save icon.



C. Configuring the information store path

1. Log in to the Client Access Server. Select the **Computer Management** option.

2. Navigate to **System Tools > Shared Folders > Shares.**

3. Create a new share and choose the folder path as **C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox database Name.**

4. Provide the **Share name** as M$ and click **Next.**

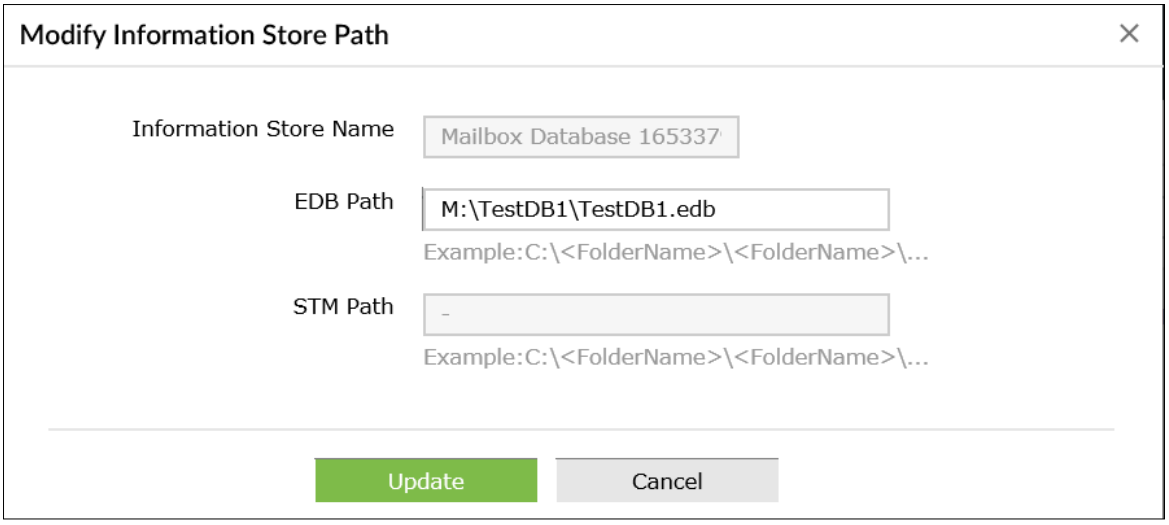
5. You can customize the permissions to be given to the user or simply delegate read-only permissions for all users.

6. Navigate to **C:\Program Files\Microsoft\Exchange Server\V15.** Right-click the Mailbox folder and go to Properties.

7. Click **Edit**, add **erpServiceAcc**, and delegate read privileges to the user.

Configuring the database (information store) path in Exchange Reporter Plus:

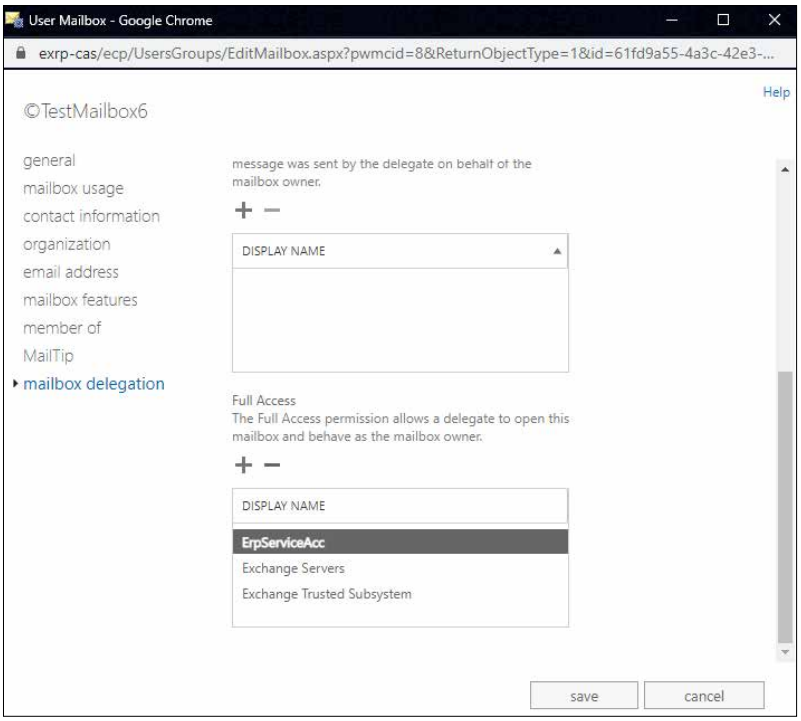
1. Log in to **Exchange Reporter Plus** as an administrator.
2. Navigate to **Settings > Configuration > Exchange Server > Log/Database Path.**
3. Go to **Database path** and click the edit icon.
4. Update the database path for all databases in the selected server in the **format M:\<DB Name>\<DB Name>.edb.**
5. Click **Update.**
6. Repeat these steps for all mailbox servers.



5. Configuring permissions required for content reports

The data required for content reports is collected from Exchange Web Services. To bind and retrieve information from any mailbox, the user service account used must have full access permissions to that mailbox.

To give full access permissions to the user account, navigate to **Exchange Admin Center > Mailboxes > <Name of the mailbox> > mailbox delegation > Full Access.** Add the **erpServiceAcc** user here.

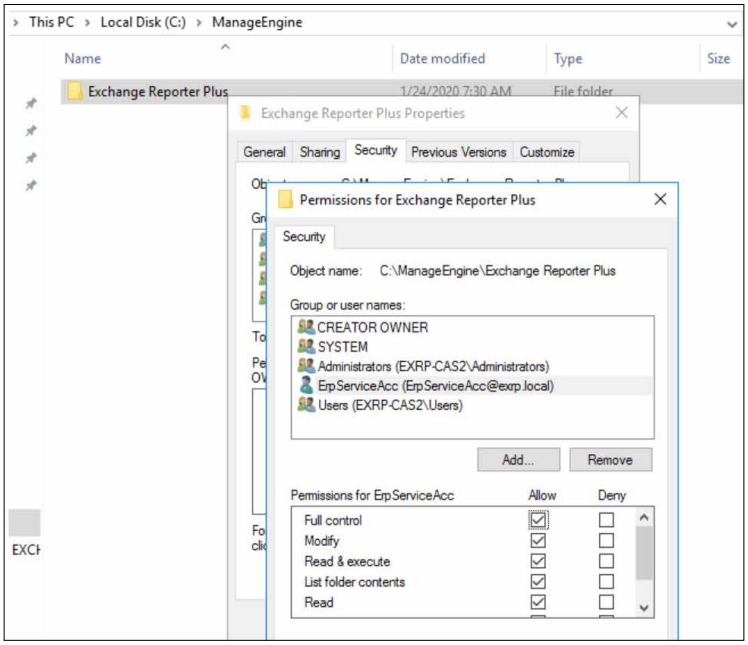


Execute the command below in Exchange PowerShell to equip the user with calendar folder permissions required for the content reports.

add-mailboxfolderpermission -identity <roommailboxname>:\calendar -user erpserviceacc -accessrights reviewer

6. Permissions required for backup restoration and archiving

The user or service account created for this purpose (here, the **erpServiceAcc** user) must have **full access** permissions to the Exchange Reporter Plus installation folder. (By default, the product is installed under C:\ManageEngine\Exchange Reporter Plus.)



7. Configuring permissions required for auditing and monitoring

The user or service account configured (erpSericeAcc) should be a member of the **Domain Admins** group for **auditing.** Otherwise, the user needs to enable the auditing function manually. Refer to the links given below for more detailed information on how to configure Exchange Server and domain controllers for auditing.

Configuring Exchange Server auditing:

https://www.manageengine.com/products/exchange-reports/help/audit/configuring-exchange-server.html

Configuring default domain controller auditing:

https://www.manageengine.com/products/exchange-reports/help/audit/configuring-default-domain-controller-policy.html

Configuring object level auditing:

https://www.manageengine.com/products/exchange-reports/help/audit/configuring-object-level-auditing.html

In Exchange Reporter Plus, Exchange Server monitoring of is done using remote PowerShell sessions by executing Exchange health commandlets, so it's vital that the created user or service account (erpServiceAcc) has permission to execute these commandlets in PowerShell. Follow the steps given below to delegate the necessary role for advanced auditing and monitoring:

1. Create a new role group called ERP in the Exchange Admin Center.
2. Assign the following roles to this ERP role group:

   Monitoring

   View-Only Audit Logs

   View-Only Configuration

   View-Only Recipents

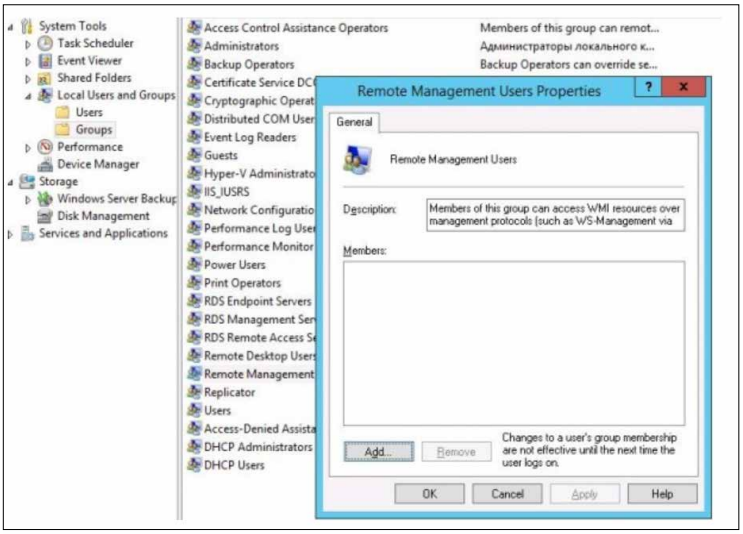
3. Add **erpServiceAcc** as a member of the ERP role group.

8. Permissions for Powershell command execution

Exchange Reporter Plus uses the remote invoke-command script in PowerShell to get reports on various services under Exchange. This remote invoke-command script requires permissions for the destination server (remote machine).

For this, you need to add the erpServiceAcc user as a member of the built-in Administrators local group or the Remote Management Users security group (this group is created by default starting from PowerShell 4.0). This group also has access to WMI resources via management protocols (e.g., WS-Management).

A user can be added to the Administrator or Remote Management Users group using the Computer Management option under the Exchange Admin center:



> **Tip:** If you need to provide such permissions on multiple computers, you can use Group Policy. To do this, assign the GPO to the computers you need, and add the new Remote Management Users group to the Computer Configuration > Windows Settings > Security Settings > Restricted Groups policy. Users or groups that need to be granted access to WinRM can be added to the policy.

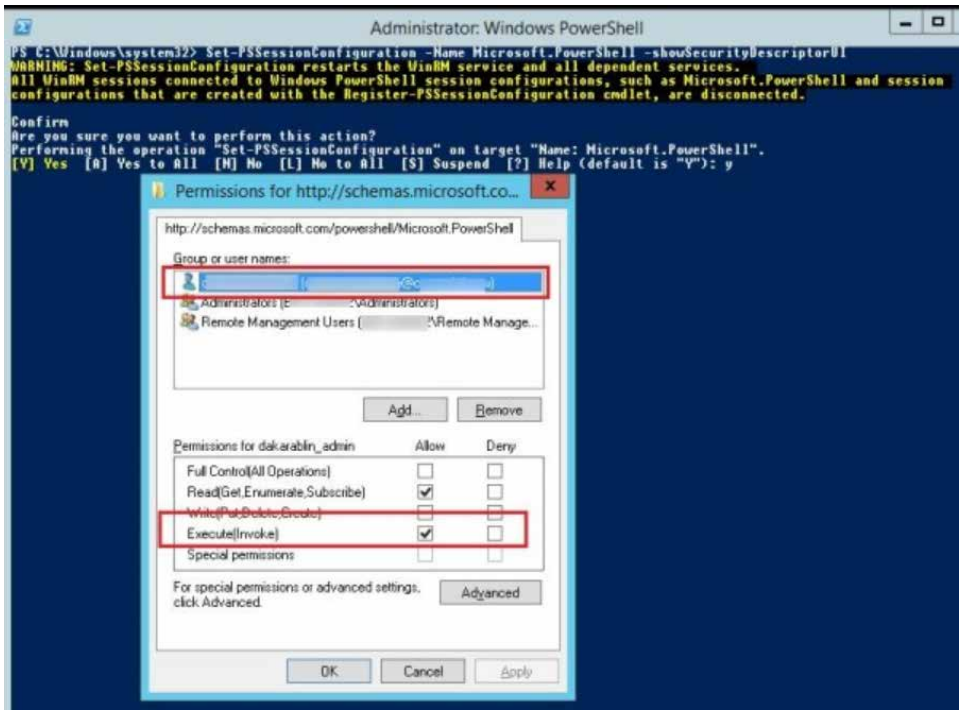
A. Security Descriptor of a PowerShell session

Another easy way to give a user access to remote PowerShell without including the user account to the local security group is by modifying the security descriptor of the current Windows PowerShell session on the local computer. This method will allow you to quickly grant temporary (until the next restart) remote connection rights to a user via PowerShell.

The following command displays the list of current permissions a service account has:

Set-PSSessionConfiguration -Name Microsoft.PowerShell-showSecurityDescriptorUI

In this dialog window, add a user or group and grant them Execute (Invoke) permissions.

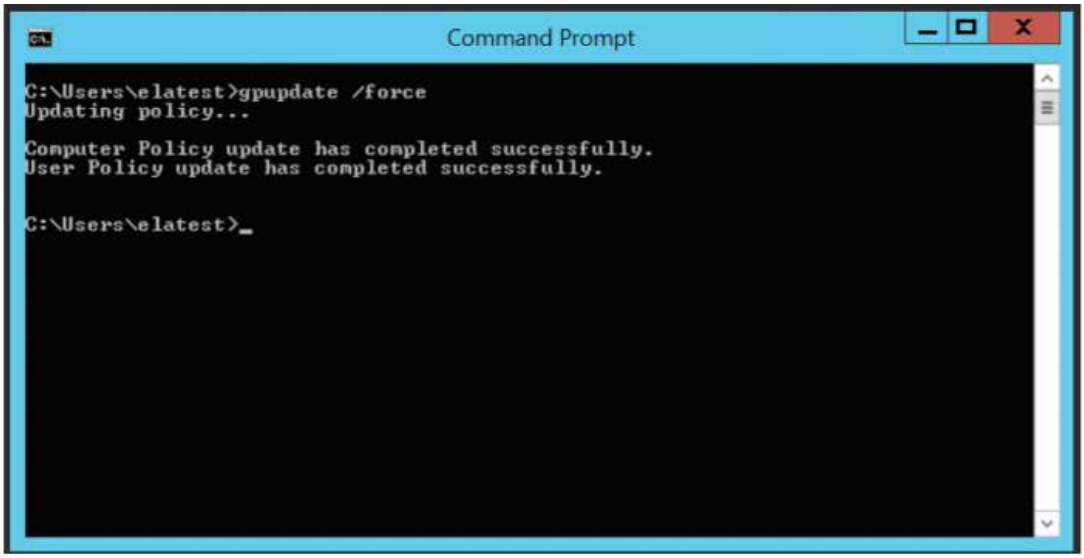


After you save the changes, the system will prompt for confirmation and restart of WinRM service.

9. Permissions required for storage reports (WMI access permissions)

It's necessary for the user or service account created to have Domain admin permissions in order to have access to WMI. Alternatively, you can also follow the steps given below to equip the users with just enough permissions for WMI access if they don't have the domain admin rights.

1. Create a non-admin domain user in Active Directory.
    a. Navigate to **Active Directory Users and Computers.**
    b. Click **Users** > **New User.**
    c. Enter the mandatory user details. Type the first name as **erpServiceAcc.**
2. Add the user to the following groups: **Event Log Readers, Performance Log Users,** and **Distributed COM Users.**
3. Create a new **Group Policy** in the **Group Policy Management** console.
4. Assign rights to the created users.
    a. Right-click the created Group Policy and click **Edit.**
    b. Navigate to **Computer Configurations** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment.**
    c. Right-click the specific right and then click **Properties.** The rights to be granted are as follows:
        - Act as part of the operating system
        - Log on as a batch job
        - Log on as a service
        - Replace a process level token
        - Manage Auditing and Security Log Properties
    d. Enable **Define these policy settings**, click **Add User or Group,** select the created user, and click Apply.
5. Enforce the created Group Policy and run **gpupdate\force** in the Command Prompt.



6. Grant **WMI Namespace Security Rights** and **COM Permissions** to the user.

    a. In the domain controller from which the logs are to be collected, open the **Run** command and type **wmimgmt.msc** to open the WMI Management Console.

    b. Right-click **WMI Control (Local)** and click **Properties.**

    c. In the WMI Control Properties pop-up that opens, click the **Security tab.**

    d. In the Security tab, expand the **Root NameSpace** and select **CIMV2 Namespace.**

    e. Click the Security button that appears on the bottom right corner to open the **Security for ROOT\CIMV2.**

    f. Click **Add** and select the created user.

    g. The user now needs to be granted permissions. To do this, click the user and check the **Allow** boxes beside all required permissions.

    h. Apply the permissions given below and click **OK** to exit the WMI Management console.

        i. Execute Methods

        ii. Enable Account

        iii. Remote Enable

        iv. Read Security

7. Grant COM permissions to the created user.

    a. In the domain controller from which the logs are to be collected, navigate to Start **Administrative Tools Component Services.**

    b. Expand the Computers folder and navigate to **My Computer Properties COM SECURITY.**

c. Under Access Permissions, click **Edit Limits** and add the created user by clicking **Add.**

d. Grant all the permissions and click **OK.**