ManageEngine
Exchange Reporter Plus

PERMISSIONS GUIDE

www.exchangereporterplus.com

Table of Contents

1. Overview

This document lists all the necessary permissions for reporting, monitoring, and auditing your Exchange Server, Exchange Server Subscription Edition (SE), Exchange Online tenant, and Skype for Business Server using Exchange Reporter Plus. Assign these permissions, based on the capabilities you need, to a service account, and use that account while configuring your Exchange environment in Exchange Reporter Plus.

2. Permissions required to perform specific tasks in Exchange Reporter Plus

Exchange Server tasks	Required privileges
Essential Data Gathering - This is a mandatory task to conduct other tasks	• LDAP Read privilege over all GC Objects • Invoke-Command PowerShell Read privilege • WMI Query Read privilege • Database files Read privilege
Exchange Server Distribution List Membership	• LDAP Read privilege • View-Only Recipients RBAC
Exchange Server Mailbox Account Properties	• LDAP Read privilege • View-Only Recipients RBAC
Exchange Server Public Folder Properties	• LDAP Read privilege • View-Only Recipients 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 Recipients RBAC for Active Sync Reports
Exchange Server Mailbox Permission	• LDAP Read privilege • View-Only Recipients RBAC
Exchange Server Distribution Group Permission	• LDAP Read privilege • View-Only Recipients RBAC

Exchange Server Content Reports Generation	• LDAP Read privilege • Exchange Web Services Read privilege
Exchange Server Audit Reports	• Exchange Server Event Logs Read privilege • Domain Controller Event Logs Read privilege
Exchange Server Advanced Audit Reports	• View-Only Audit Logs RBAC • View-Only Configuration RBAC
Exchange Server Monitoring	• WMI Query Read privilege • Database Folder path Read access • Invoke-Command PowerShell Read Access - Storage Monitoring • View-Only Configuration - All Other Categories
Exchange Server Content Search	• Full access permissions for all mailboxes or • ApplicationImpersonation roles.

Module	Role Name	Scope
Exchange Online reporting	Global Reader	Get reports on all Microsoft 365 services.
	Security Reader	Get audit logs and mailbox reports.
Exchange Online auditing and alerting	Security Reader	Get audit logs and sign-in reports.

Module	API Name	Permission	Scope
Reporting	Microsoft Graph	User.Read.All Group.Read.All Organization.Read.All	Get user and group member reports.
		Reports.Read.All	Get usage reports.
		Calendars.Read	Get users' calendar details.

Auditing and Alerting	Office 365 Management	ActivityFeed.Read	Read the activity data for the organization.
Content Search		Mail.Read	Read the mail content data
Configuration	Microsoft Graph	Application.ReadWrite.All	Modify the application details.

Skype for Business Server Tasks	Required privileges
Skype for Business Server Reporting	• CsAdministrator (Read privilege) or • CsViewOnlyAdministrator role (Read privilege)

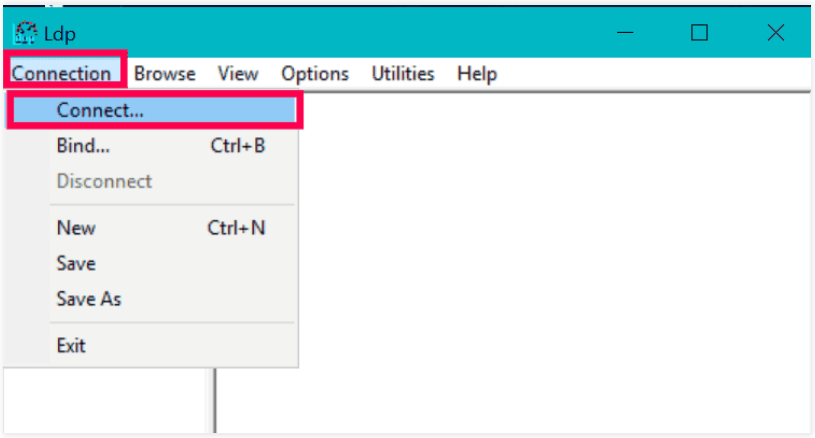
3. Configuring domain permissions

The first step in configuring domain permissions is to create a new service account called erpServiceAcc (you may select a different name as well) under the Domain Users group, and add this user to the Event Log Readers group. Then, provide read permissions for the Exchange Services container and Domain Partitions container as explained below:

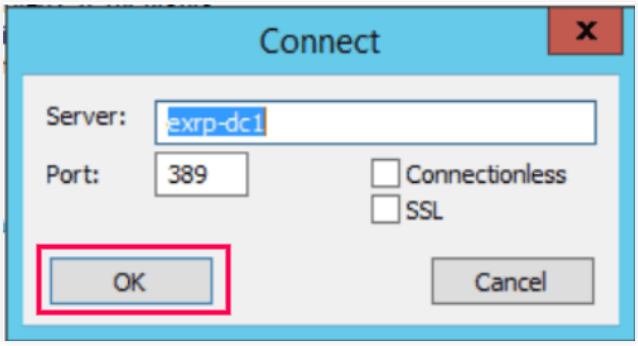
Note:
To ensure optimal functionality and network access for the service, it is recommended to use a specific user account instead of the Local System account. The Local System account has extensive local privileges but limited network access, which can cause connectivity issues with network resources. A specific user account provides the necessary permissions and reliable authentication for seamless operation.
The Local System account has inherent limitations regarding network access because it operates under the machine's credentials rather than a specific user's. While you can extend its network privileges to some degree, it generally lacks the ability to authenticate effectively and access resources across a network. However, there are workarounds available, but they come with potential security risks.

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

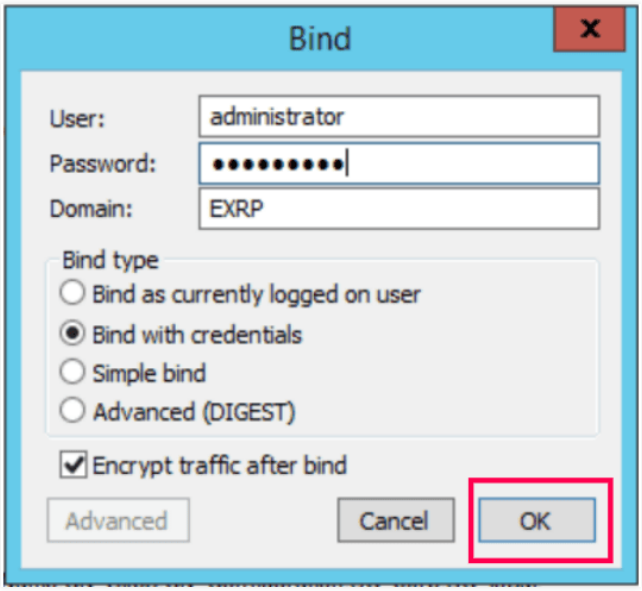
1. Open **Command Prompt** with administrator rights and type **ldp.exe.** Press the **Enter** key to start the ldp.exe utility.
2. Navigate to **Connection** and click **Connect** to open the connect dialog box.



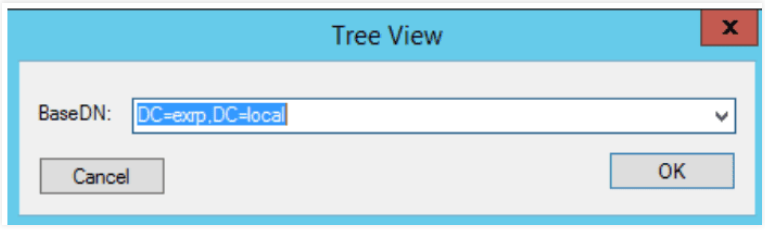
3. Enter the server name in the Server field and the port number as 389 and click **OK.**



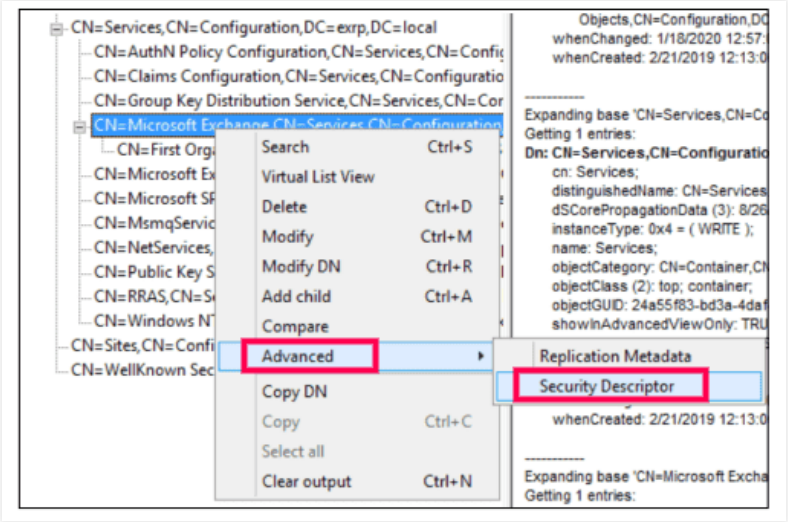
4. Navigate to **Connection** and click **Bind** to open the bind dialog box.
5. Under the *Bind type* field, select **Bind with credentials**. Apply a bind connection using administrative credentials to give permission to the service account you created and click **OK.**



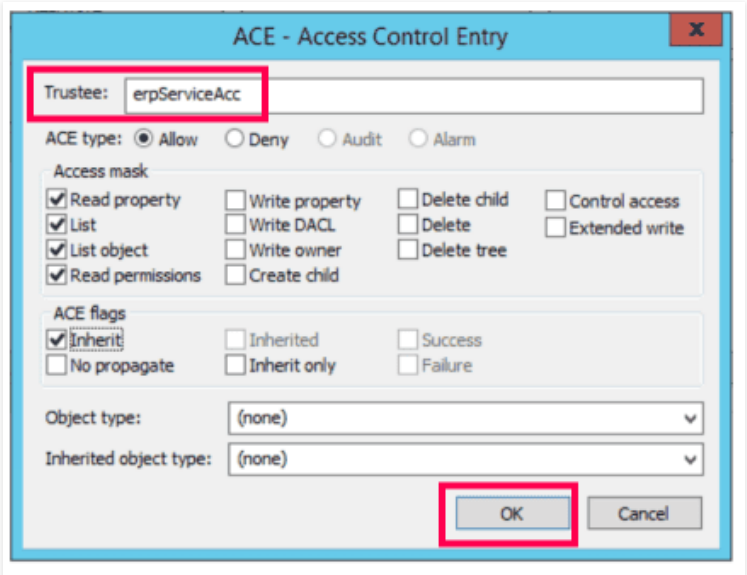
6. Navigate to **View > Tree** to open the **Tree View** window. Provide the distinguished name of the server in the *BaseDN* field. In this case, *DC=exrp,DC=local.*



7. Right-click **CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=exrp,DC=local > Advanced > Security Descriptor** and click **OK.**

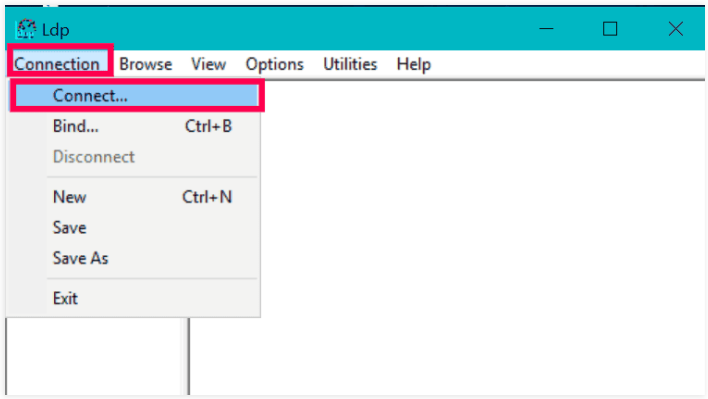


8. In the new window that opens, click **Add** on the right-hand side of the *DACL* field.
9. Add the service account as a trustee by entering the service account name in the *Trustee* field. Click **OK** to save the changes.

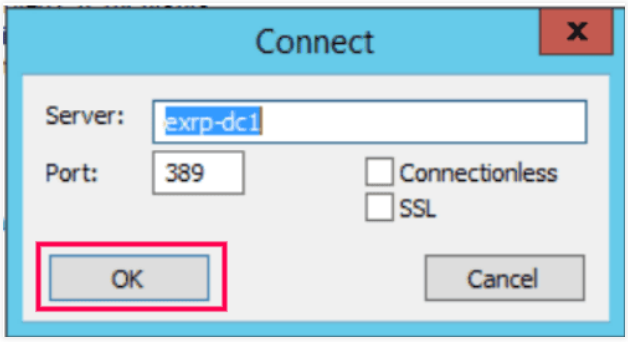


B. Follow the steps given below to provide read permissions to the Domain Partition container:

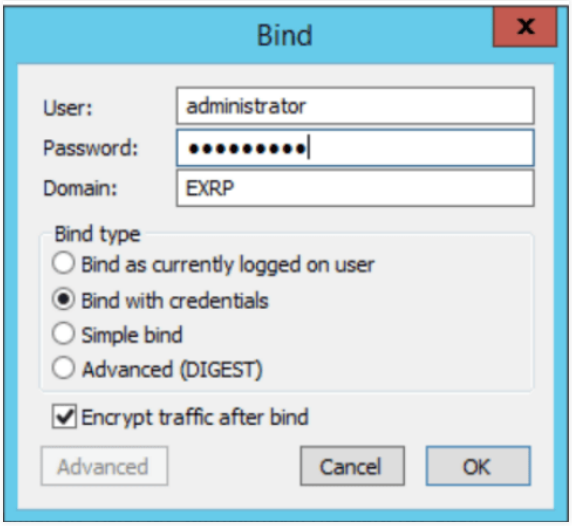
1. Open **Command Prompt** with administrator rights and type **ldp.exe**. Press the Enter key to start the ldp.exe utility.
2. Navigate to **Connection** and click **Connect** to open the connect dialog box.



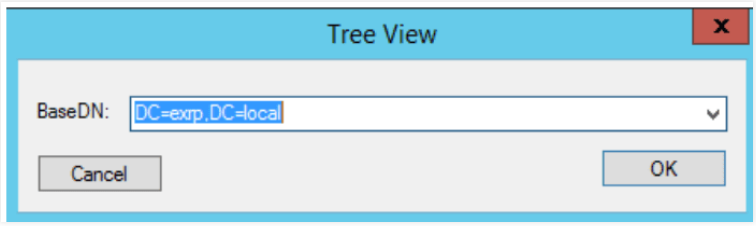
3. Enter the server name in the Server field and the port number as 389 and click **OK.**



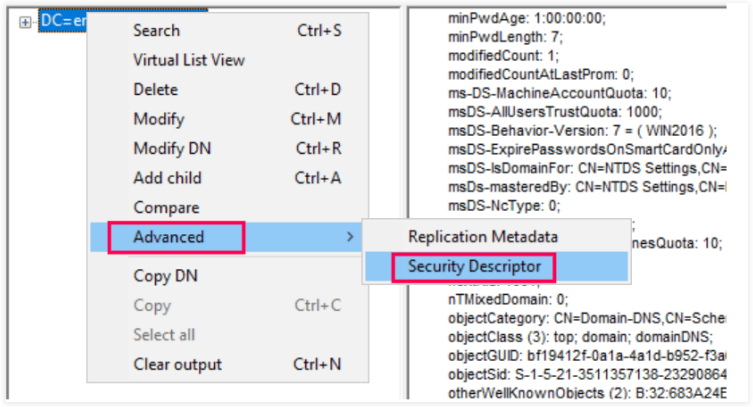
4. Navigate to **Connection** and click **Bind** to open the bind dialog box.
5. Under the *Bind type* field, select **Bind with credentials**. Apply a bind connection using administrative credentials to give permission to the service account you created and click **OK.**



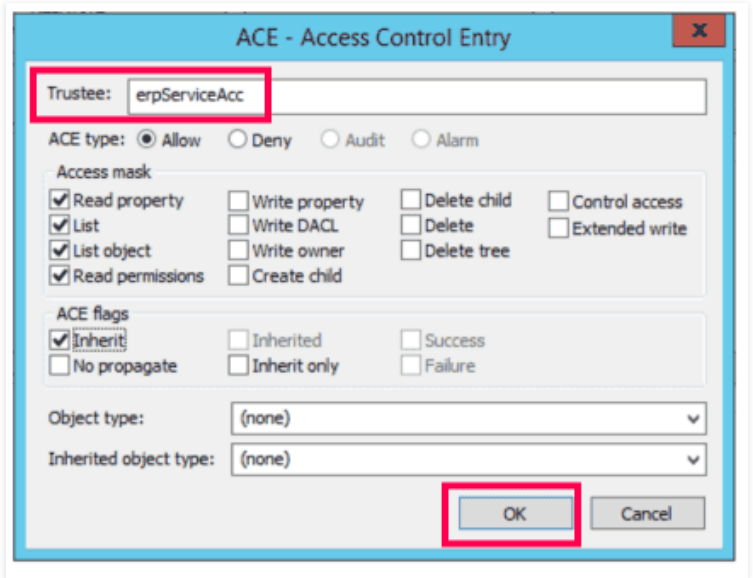
6. Navigate to **View > Tree** to open the **Tree View** window. Provide the distinguished name of the server in the *BaseDN* field. In this case, *DC=exrp,DC=local.*



7. Right-click **DC=exrp, DC=local > Advanced > Security Descriptor.**



8. In the new window that opens, click **Add** on the right-hand side of the *DACL* field.
9. Add the service account as a trustee by entering the service account name in the *Trustee* field. Click **OK** to save the changes.



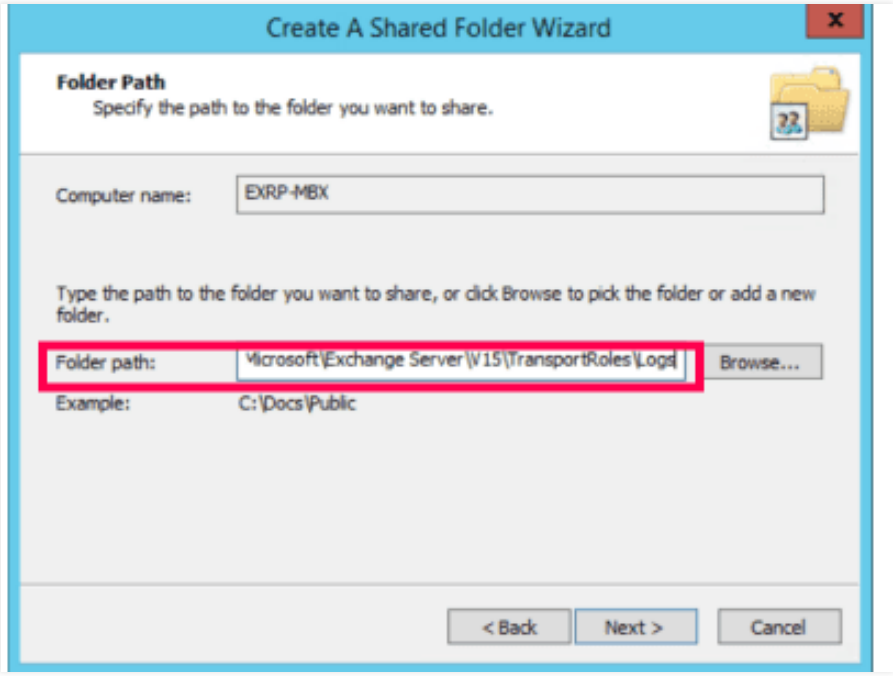
4. Configuring folder read permission for message tracking, IIS logs, and database files

A. Configuring the traffic log path

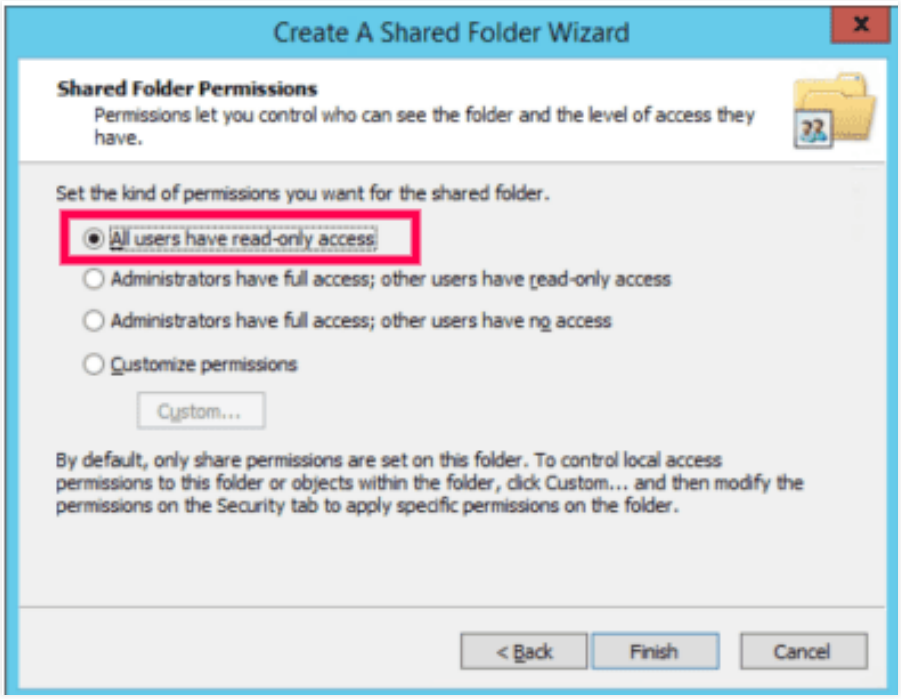
1. Log in to the Exchange Server (the mailbox server or the server which contains the traffic log files). Select **Computer Management.**

Note: If you are using Exchange Server versions before Exchange Server 2013, you need to log in using the mailbox server. For Exchange Server 2013 and later versions, log in using the server that contains the traffic log files.

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.**



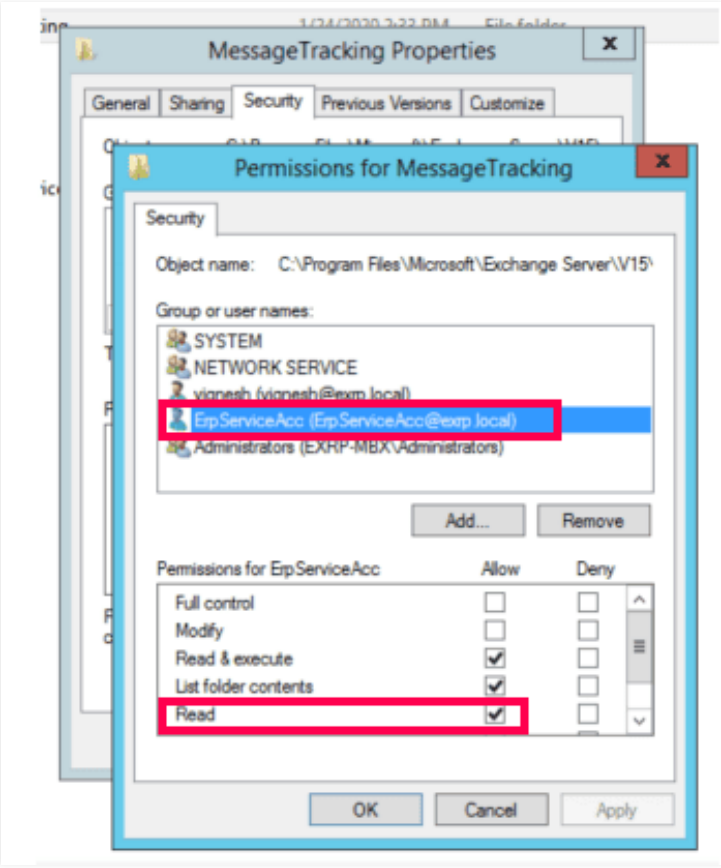
4. Provide the Share name as T$ and click **Next.**
5. You can provide read-only access or full permissions, or you can customize user permissions as per your requirements.



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

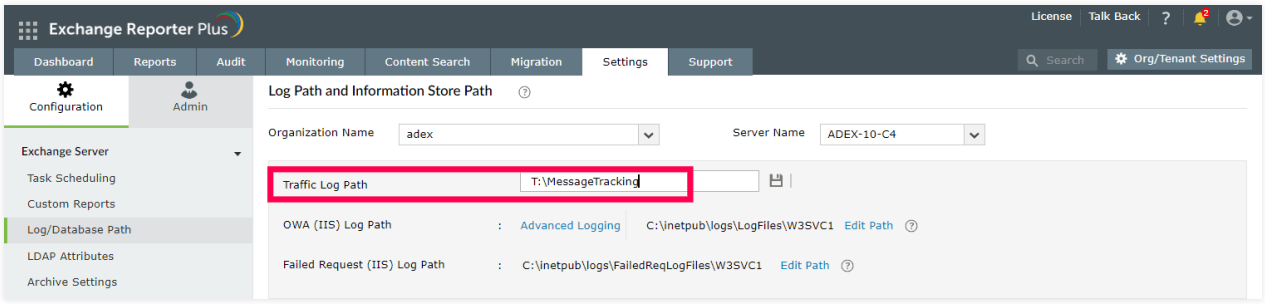
7. Right-click the **MessageTracking** folder and select **Properties.**

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



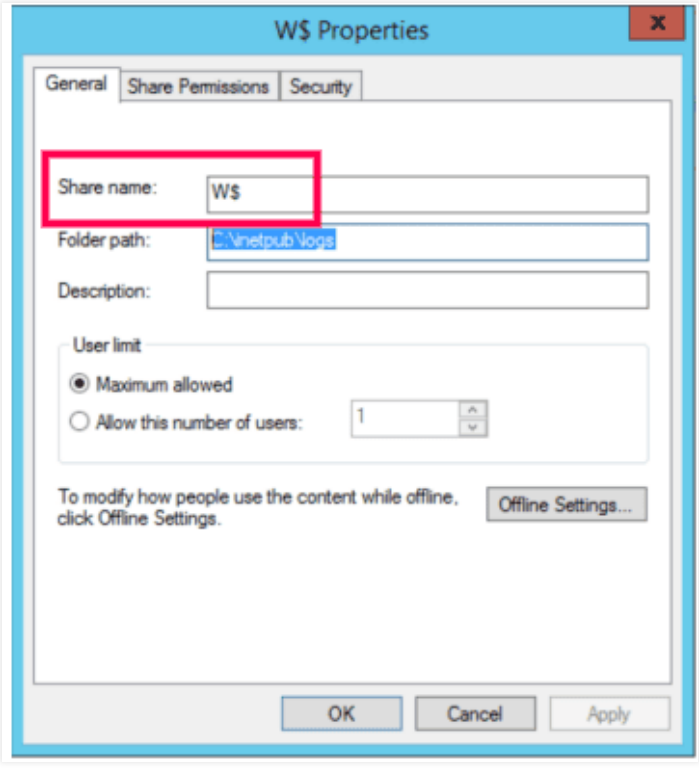
Configuring the traffic log path in Exchange Reporter Plus

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 **Save.**



B. Configuring the IIS log path

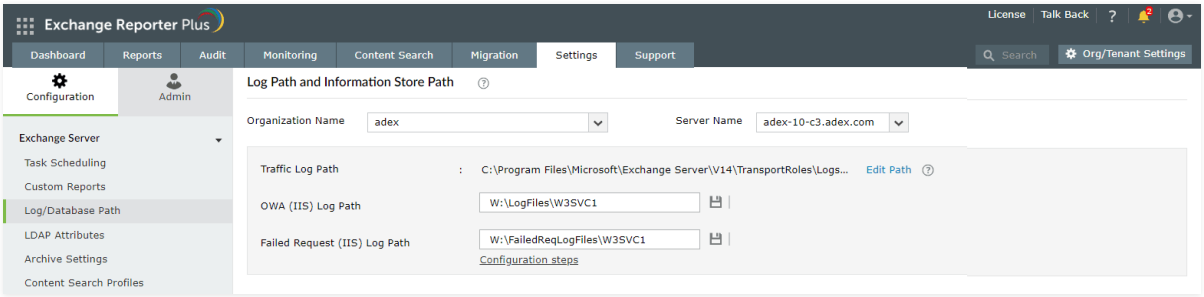
1. Log in to the Client Access Server. Select the **Computer Management** option.
2. Navigate to **System Tools > Shared Folders > Shares.**
3. Create a new share, and choose the folder path as **C:\inetpub\logs.**
4. Provide the *Share name* as *W$* and click **Next.**



5. Navigate to C:\inetpub\logs. Right-click the W3SVC1 folder and go to **Properties.**
6. Click **Edit**, add the service account, and delegate read privileges to the user.

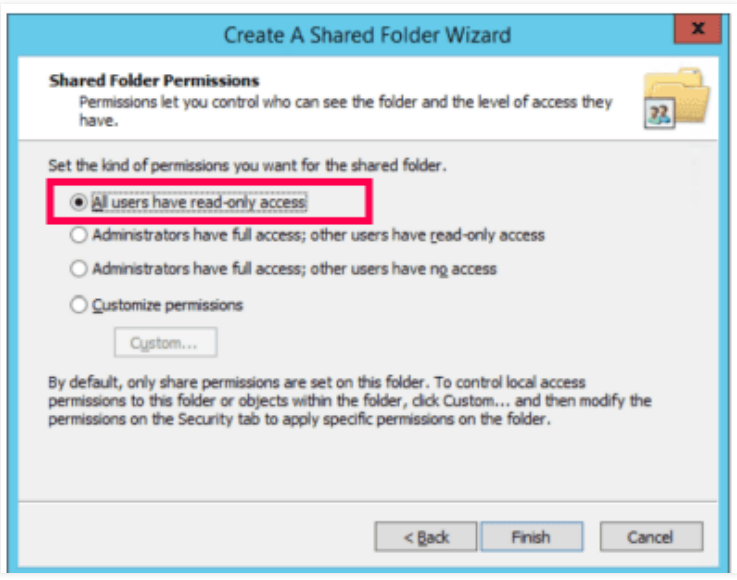
Configuring the OWA (IIS) log path in Exchange Reporter Plus:

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 **Save.**



C. Configuring the information store path

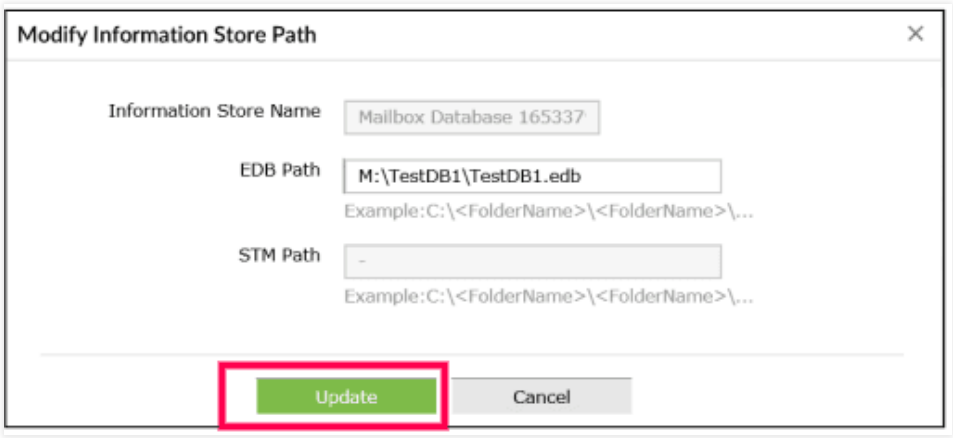
1. Log in to the Client Access Server. Select the **Computer Management** option.
2. Navigate to **System Tools > Shared Folders > Shares.**
3. Create a new share and choose the folder path as **C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox database Name.**
4. Provide the *Share name* as *M$* and click **Next.**
5. ou 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 the service account, and delegate read privileges to the user.

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

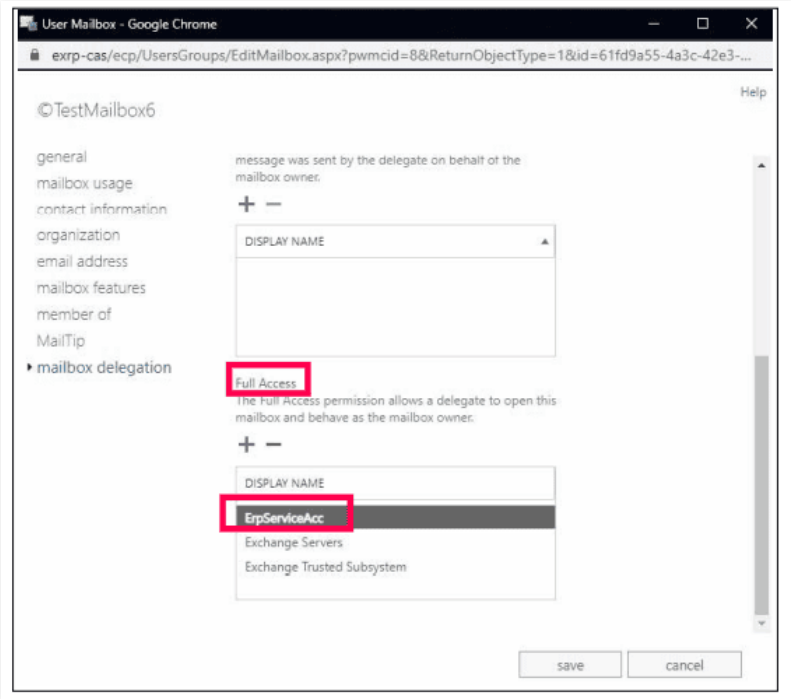
1. Log in to Exchange Reporter Plus as an administrator.
2. Navigate to **Settings > Configuration > Exchange Server > Log/Database Path.**
3. Go to the **Database path** and click the edit icon.
4. Update the database path for all databases in the selected server in the format **M:\<DB Name>\<DB Name>.edb.**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



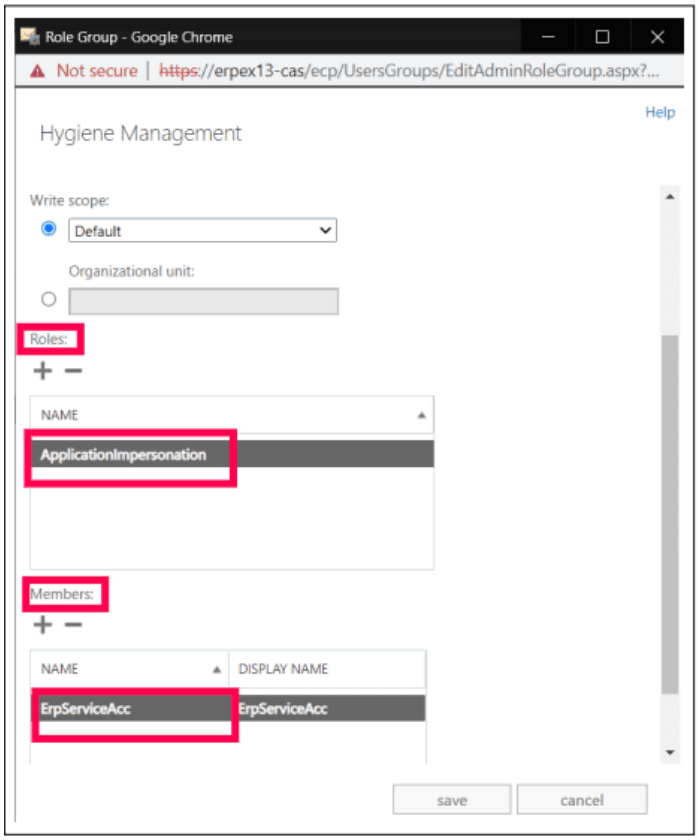
5. Configuring permissions required for content reports

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 permission to that mailbox or should be assigned the ApplicationImpersonation role.

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



To configure the ApplicationImpersonation role for user service account, navigate to **Exchange Admin Center > Permissions > Admin roles > Hygiene Management > Roles.** Add the **ApplicationImpersonation** and the *Members*. Add the service account.

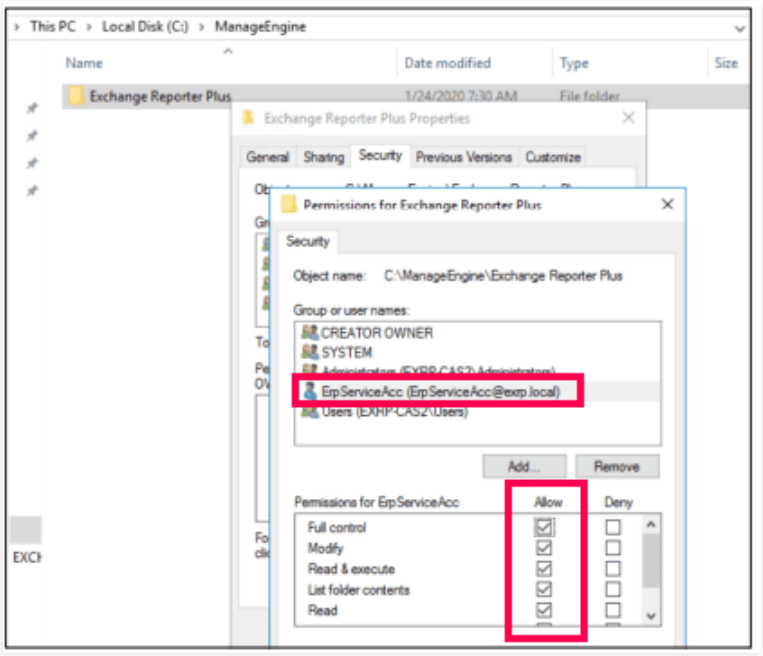


Execute the command below in Exchange PowerShell to equip the user with calendar folder permissions required for the content reports. Replace **<serviceaccname>** with the name of the service account:

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

6. Permissions required for restoration and archiving

The service account created for this purpose 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 service account must 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 is done using remote PowerShell sessions by executing Exchange health commandlets, so it's vital that the created user or service account has permission to execute these commandlets in PowerShell.

Follow the steps given below to delegate the necessary role for advanced auditing and monitoring:

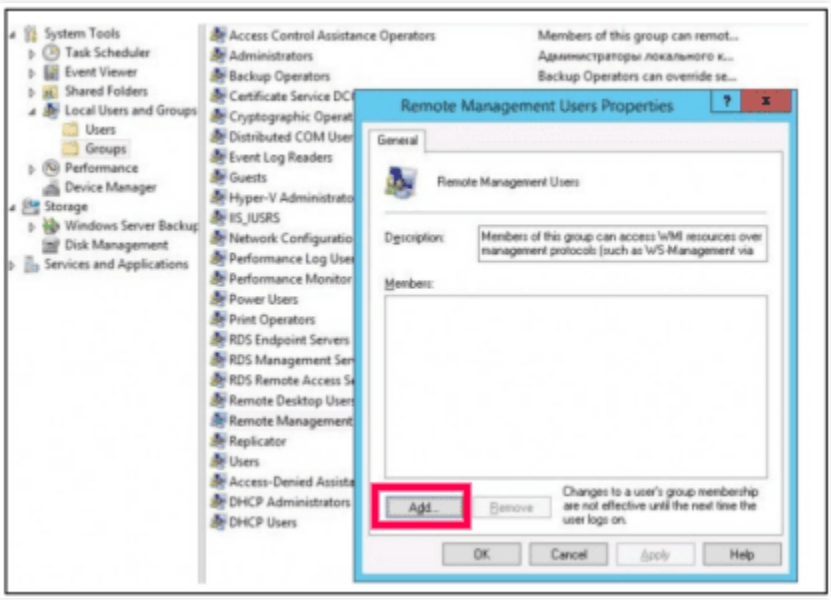
1. Create a new role group called *ERP* in the Exchange Admin Center.
2. Assign the following roles to this *ERP* role group:
   Monitoring
   View-Only Audit Logs
   View-Only Configuration
   View-Only Recipients
3. Add the service account as a member of the *ERP* role group.

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 service account 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 in 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 policy found at **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.

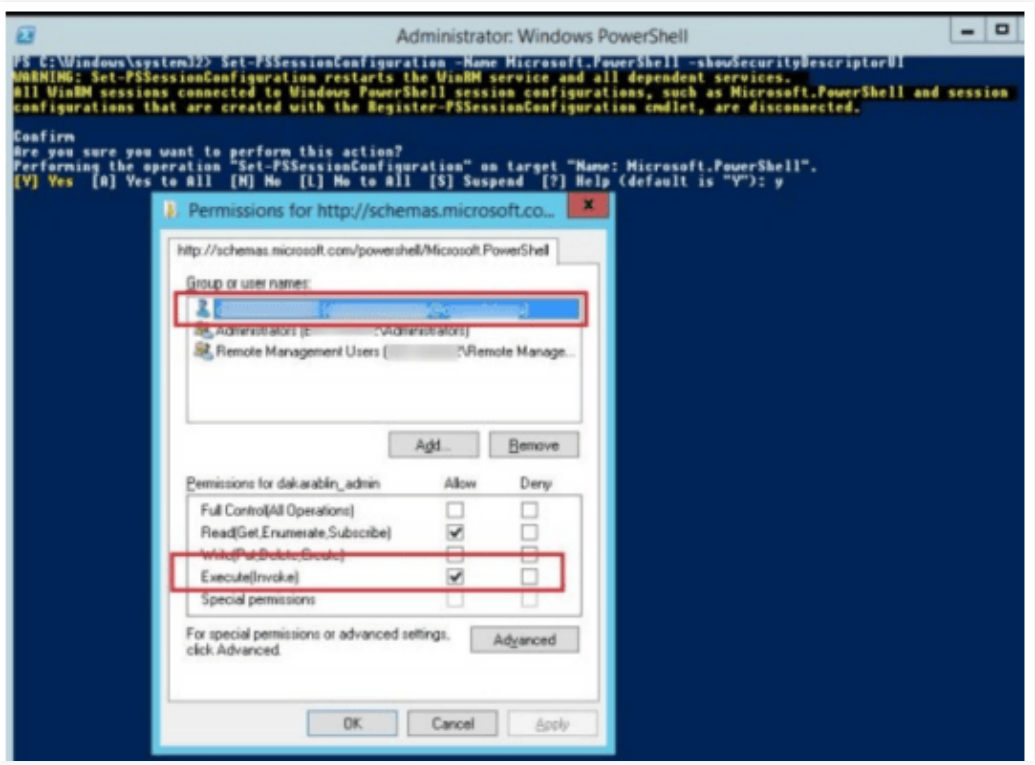
A. Security descriptor of a PowerShell session

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 command below 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 the 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.

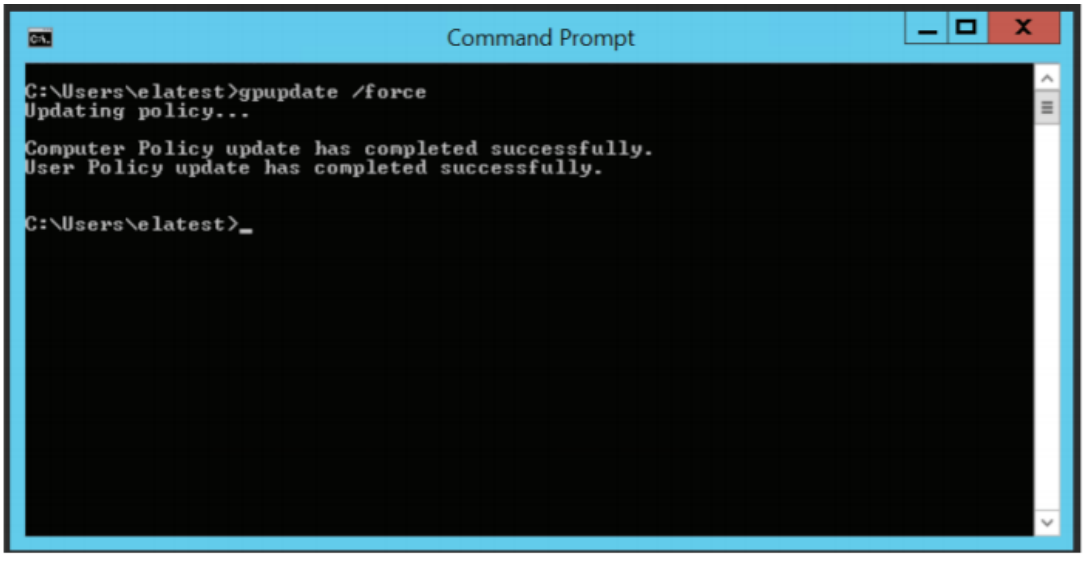
1. Create a non-admin domain user in Active Directory.

   Navigate to **Active Directory Users and Computers.**

   Click **Users > New User.**

   Enter the mandatory user details. Type the first name as the name of the service account.

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 click **Properties**. The rights to be granted are as follows:
      i. Act as part of the operating system
      ii. Log on as a batch job
      iii. Log on as a service
      iv. Replace a process level token
      v. 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 **Run** 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 settings 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 and add the created user by clicking **Add.**
   d. Grant all the permissions and click **OK.**

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus

ADSelfService Plus | M365 Manager Plus

About Exchange Reporter Plus

Exchange Reporter Plus is a reporting, change auditing, monitoring and content search tool for hybrid Exchange environments and Skype for Business. It features over 450 comprehensive reports on various Exchange objects, such as mailboxes, public folders and distribution lists as well as on Outlook Web Access and ActiveSync. Admins can configure alerts in Exchange Reporter Plus to receive instant notifications on critical changes that require immediate attention. Migrate from Exchange on-premises to Exchange Online without hassles.

For more information about Exchange Reporter Plus, visit www.manageengine.com/products/exchange-reports.

$ Get Quote Download