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	3
A. Exchange Server container	3
B. Domain Partitions container	5
4. Configuring folder read permissions for message tracking, IIS logs, and database files	7
A. Configuring traffic log path	7
B. Configuring IIS log path	9
C. Configuring information store path	10
5. Configuring permissions required for content reports	12
6. Permissions required for backup restoration and archiving	14
7. Configuring permissions required for auditing and monitoring	14
8. Permissions for Powershell command execution	15
A. Security Descriptor of PowerShell session	16
9. Permissions required for storage reports (WMI access permissions)	17

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

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 privilegeView-Only Recipents RBAC
Exchange Server Mailbox Account Properties	LDAP Read privilegeView-Only Recipents RBAC
Exchange Server Public Folder Properties	LDAP Read privilegeView-Only Recipents RBAC
Exchange Server Traffic Logs	LDAP Read privilegeMessage 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 privilegeView-Only Recipents RBAC
Exchange Server Distribution Group Permission	LDAP Read privilegeView-Only Recipents RBAC

ManageEngine Exchange Reporter Plus

Exchange Server Content Reports Generation	LDAP Read privilegeExchange 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 RBACView-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.

Exchange Online Tasks	Required privileges
Exchange Online Reporting	 View-Only Recipients MailRecipients Read privilege AddressLists Read privilege View-Only Configuration MailboxSearch Read privilege UserOptions role (Read privilege)
Exchange Online Auditing	View-OnlyRecipientsDataLossPrevention role (Read privilege)

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 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.

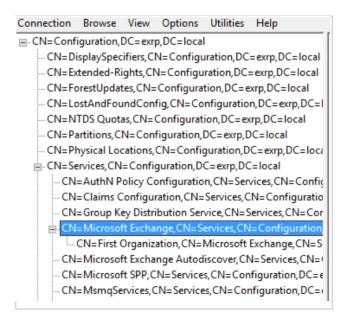
	Con	nect ×
Server:	exrp-dc1	
Port:	389	Connectionless
OK		Cancel

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

	Bind		
User: Password: Domain:	administrator ••••••		
Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST)			
Encrypt tra Advanced	affic after bind Cancel OK		

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.**

· · · · · · · · · · · · · · · · · · ·	figuration, DC= exrp, DC Configuration, CN= Serv uration, CN= Services, Cl	ices,CN=Confi	· I	Objects,CN=Configuration,DC whenChanged: 1/18/2020 12:57: whenCreated: 2/21/2019 12:13:0
CN=Microsoft Eyzl CN=First Org - CN=Microsoft Ey - CN=Microsoft SF - CN=MsmqServic - CN=NetServices, - CN=Public Key S - CN=RAS, CN=Si - CN=Windows N	tribution Service, CN=Se Search CN=Search Virtual List View Delete Modify Modify DN Add child Compare			Expanding base 'CN=Services,CN=Co Getting 1 entries: Dn: CH=Services,CN=Configuratio cn: Services; distinguishedName: CN=Services dSCorePropagationData (3): 8/26 instanceType: 0x4 e (WRITE); name: Services; objectClase(2): top; container,Ch objectClase(2): top; container, objectClase(2): top; container, objectClase(2): top; container, objectClave(3): 24a55/83-bd3a-4daf showNhAdvancedViewOnly: TRU
CN=Sites, CN=Confi CN=WellKnown Sec	Advanced	•		Replication Metadata
erte reliation see	Copy DN			Security Descriptor
	Сору	Ctrl+C		whenCreated: 2/21/2019 12:13:0
	Select all			
	Clear output	Ctrl+N		Expanding base 'CN=Microsoft Excha Getting 1 entries:

ACE - Access Control Entry				
Trustee: erpService/	Acc			
	○ Deny ○ Audit	OAlarm		
Access mask Read property List List object Read permissions	Write property Write DACL Write owner Create child	Delete child Delete Delete tree	Control access	
ACE flags Inherit No propagate	Inherited	Success		
Object type:	(none)		¥	
Inherited object type:	(none)		~	
		ОК	Cancel	

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.

	Con	nect ×
Server:	exrp-dc1	
Port:	389	Connectionless
ОК		Cancel

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

	Bind		
Bind with a	Password: ••••••• Domain: EXRP		
Encrypt tra	affic after bind Cancel OK		

3. Open the configuration Tree View.

Tree View	x
BaseDN: DC=exrp,DC=local	¥
Cancel	ОК

- 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.

	Secu	rity descriptor -	DC=exrp,DC=	local	x
Owner	BUILTIN\Administrators				
Group	BUILTIN\Administrators				
SD contr SELF	ol RELATIVE	✓ DACL PRESENT ACE - Access C	ontrol Entry	SACL PRESENT	
GRO	Trustee: EXRP\erpse		ondorenay		>
DACL (1 Type Allow	ACE type: Allow Access mask	O Deny O Audit	O Alarm		
Allow Allow Allow Allow Allow	 ✓ Read property ✓ List ✓ List object ✓ Read permissions 	Write property Write DACL Write owner Create child	Delete child Delete Delete tree	Control access	
Allow Allow SACL (1	ACE flags Inherit No propagate	Inherited	Success		
Type Audit	Object type:	(none)		~	^
Audit Audit Audit Audit	Inherited object type:	(none)	OK	Cancel	·· =
Audit	Everyone	Control access Write property		Success, Innent, Innent Success, Inherit, Inherit	
Add.	ACE Delete ACE	Edit ACE			
Update	er Group DA			Update	Close

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.

	Create A Shared Folder Wizard
Folder Path Specify the path	to the folder you want to share.
Computer name:	EXRP-MBX
Type the path to the folder.	folder you want to share, or click Browse to pick the folder or add a new
Folder path:	Microsoft\Exchange Server\V15\TransportRoles\Logs Browse
Example:	C:\Docs\Public
	< Back Next > Cancel

- 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.

Create A Shared Folder Wizard	x
Shared Folder Permissions Permissions let you control who can see the folder and the level of access they have.	22
Set the kind of permissions you want for the shared folder.	
All users have read-only access	
\bigcirc Administrators have full access; other users have $\underline{r}ead$ only access	
○ Administrators have full access; other users have no access	
○ <u>C</u> ustomize permissions	
Custom	
By default, only share permissions are set on this folder. To control local access permissions to this folder or objects within the folder, click Custom and then modify the permissions on the Security tab to apply specific permissions on the folder.	e
< <u>B</u> ack Finish Ca	ncel

- 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.

ine				1	124/2020 2	22 DM	Eilo fol		-
1	k		M	essageT	racking l	Prope	rties	X	
	Ge	neral	Sharing	Security	Previous \	/ersions	Customize	e	
					P1 144	015		11/15	<u>.</u>
ice				Permiss	sions for	Mess	ageTrack	ing	x
		S	ecurity						
			Object nar	me: C:\/	Program Files	Micro	soft\Exchan	ge Server\\	/15\
			Group or u	iser names	c				
			SYS"	ГЕМ					
	11		8 NET	WORK SE	RVICE				
			🥈 vigne	sh (vignes	h@exrp.loca	al)			
					(EmpService.				
			🔏 Admi	nistrators (l	EXRP-MBX	Adminis	trators)		
						1	Add	Remove	
			Permission	ns for EnpS	erviceAcc		Allow	Deny	_
			Full con	trol					^
			Modify						=
			Read &	execute			✓		=
			List fold	er contents	s		✓		
			Read				✓		$\overline{}$
									-
L	_								
					OK		Cancel	Арр	у

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.

≡ Exchange Re	porter Plus	Home Reporting Auditing Monitoring Settings Support	😝 Purchase Now License Talk Back ? 😔 🗸 Q Search 🌣 Org/Tenant Settings
Configuration	Admin	Log Path and Information Store Path ③	
Exchange Server	.	Organization Name ERP1 v Server Name ERP1-10A	~
Task Scheduling		Traffic Log Path T:\MessageTracking	
Custom Reports Log/Database Path		OWA (IIS) Log Path : Advanced Logging C:\Inetpub\logs\LogFiles\W3SVC1 Edit Path	3
LDAP Attributes		Failed Request (IIS) Log Path : C:\inetpub\logs\FailedReqLogFiles\W3SVC1 Edit Path ?	
Archive Settings			
Exchange Online Skype for Business	•	Database Path	

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.**

W\$ Properties X
General Share Permissions Security
Share name: W\$
Folder path: C:\inetpub\logs
Description:
User limit
Maximum allowed
○ Allow this number of users: 1
To modify how people use the content while offline, Offline Settings
OK Cancel Apply

- 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.

			😑 Purchase Now 🛛 License	Talk Back 🛛 ? 🛛 🕹 👻
≡ Exchange I	Reporter Plus 🌙	Home Reporting Auditing Monitoring Settings Support	Q Search	Org/Tenant Settings
Configuration	Admin	Log Path and Information Store Path ①		
Exchange Server	Ţ	Organization Name ERP1 v Server Name ERP1-10A	~	
Task Scheduling		Traffic Log Path : C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Log	Edit Path ⑦	
Custom Reports				
Log/Database Pat	h	OWA (IIS) Log Path		
LDAP Attributes		Failed Request (IIS) Log Path W:\FailedReqLogFiles\W3SVC1		
Archive Settings		Configuration steps		
Exchange Online	•			
Skype for Business		Database Path		

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.

Create A Shared Folder Wizard
Shared Folder Permissions Permissions let you control who can see the folder and the level of access they have.
Set the kind of permissions you want for the shared folder.
All users have read-only access
○ Administrators have full access; other users have read-only access
○ Administrators have full access; other users have no access
○ <u>C</u> ustomize permissions
Custom
By default, only share permissions are set on this folder. To control local access permissions to this folder or objects within the folder, click Custom and then modify the permissions on the Security tab to apply specific permissions on the folder.
< <u>B</u> ack Finish Cancel

- 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.

Modify Information Store Path		\times
Information Store Name	Mailbox Database 165337	
EDB Path	M:\TestDB1\TestDB1.edb Example:C:\ <foldername>\<foldername>\</foldername></foldername>	
STM Path	- Example:C:\ <foldername>\<foldername>\</foldername></foldername>	
U	pdate Cancel	

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 **erpServiceAcc** user here.

©TestMailbox6		Hel
general mailbox usage contact information	message was sent by the delegate on behalf of the mailbox owner.	
organization email address mailbox features member of MailTip	DISPLAY NAME	
mailbox delegation	Full Access The Full Access permission allows a delegate to open this mailbox and behave as the mailbox owner.	
	DISPLAY NAME ErpServiceAcc Exchange Servers	
	Exchange Trusted Subsystem	

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 **ErpServiceAcc.**

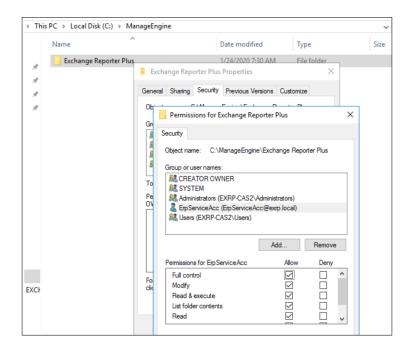
鞽 Role Group - Google Chrome	2		- 🗆 X	
A Not secure https://er	pex13-cas/ecp/Users(Groups/EditAdmi	nRoleGroup.aspx?	
Hygiene Managemer	nt		He	lp
Write scope:				•
Default	~			
Organizational unit:				
Roles:				
+ -				
NAME				
ApplicationImpersonation				
Members:				
NAME	DISPLAY NAME			
ErpServiceAcc	ErpServiceAcc			•
		save	cancel	

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-s erver.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-aud iting.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

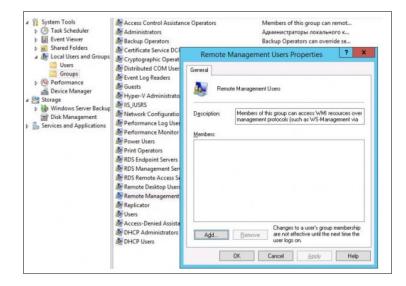
3. Add **erpServiceAcc** as a member of the ERP role group.

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

	ssionConfiguration restarts s connected to Windows Power hat are created with the Regi	ster-PSSes	ion configuration configuration	tions, such as Microsotion cmdlet, are disc	onnected.
firm you sure you forming the op Yes [A] Yes	want to perform this action? eration "Set-PSSessionConfig to All [M] Ho [L] Ho to Al	uration" o 1 [\$] Sus	n target "Nar pend [?] He	ne: Microsoft.PowerSho lp (default is "Y"):	,ıı . .
	Permissions for http://sche	mas.micro	soft.co 🗙		
	http://schemas.microsoft.com/powersh	nell/Microsoft.P	owerShell		
	Group or user names:				
	Sk. Administrators (E. CVAdr	i@c	-)		
	Remote Management Users (:\Ren	note Manage		
		Add	Bemove		
	Permissions for dakarablin_admin	Allow	Deny		
	Full Control(All Operations)				
	Read(Get,Enumerate,Subscribe)	1			
	Write(Put,Delete,Greate)		8		
		~			
	Execute(Invoke)				
	Execute(Invoke) Special permissions				

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**.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus | M365 Manager Plus

ManageEngine) Exchange Reporter Plus

Exchange Reporter Plus is an analysis, monitoring, and change auditing solution for Exchange Online and Exchange Servers. It features over 450 unique reports on various Exchange entities such as mailboxes, public folders, Outlook Web Access, and ActiveSync. Customize reports to track room mailbox usage, break down email response times, and locate messages based on keywords in their content. Configure alerts in Exchange Reporter Plus for instant notifications on critical changes that require your immediate attention.

\$ Get Quote

± Download