

Service account configuration for Log360



www.manageengine.com/log-management/

Create a new user

Log in to your domain controller with domain admin privileges \rightarrow Open Active Directory Users and Computers \rightarrow Right-click on your domain \rightarrow New \rightarrow User \rightarrow Name the user as "Log360".

Grant the user full control over the product installation folder

Log360 requires full control over the product installation folder.

- 1. Log in to the computer where Log360 is installed with domain admin privileges.
- Locate the product installation folder; right-click Properties and navigate through Security → Edit; add the new Log360 user and edit permissions to check the "full control" box. Click Apply to apply the changes.

Note:

Other than the product installation folder, the Log360 user must be given full control permission for locations used in product configuration such as **archives**, **Elasticsearch**, **and reporting**.

Please refer to the link here to know the detailed configurable paths of each of these modules mentioned above.

Create a new group

- Log in to your domain controller with domain admin privileges → Open Active Directory Users and Computers → Right-click on your domain → New → Group → Name the group "Log360 Group".
- Add all the audited computers as members of the "Log360 Group": Right-click "Log360 Group" → Properties → Members → Add all the domain controllers, Windows servers, and workstations that you wish to audit.

File Action View Help					
🗢 🔿 🙋 💼 🔏 🗶 🗊 🗉	è 🛛 🖬 🗏 🐮 🔻	2 &			
Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers Computers Domain Controllers Computers Users	Name Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Users Enterprise Admins Enterprise Read-only Do Group Policy Creator O Group Policy Creator O Group Policy Creator O Guest Key Admins Test Read-only Domain Cont Schema Admins Test2 waadmin Log3600 Log3600Group	Type Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group User Security Group User Security Group Security Group User Security Group User Security Group User Security Group	Description Designated administrators of the domain All workstations and servers joined to the do All domain controllers in the domain All domain guests All domain users Designated administrators of the enterprise Members of this group can perform adminis Members of this group can perform adminis Members of this group can modify group po Built-in account for guest access to the com Members of this group can perform adminis Members of this group can setforded addition Servers in this group can access remote acce Members of this group are Read-Only Doma Designated administrators of the schema		

Create a new domain level GPO and link it to all the audited computers

Since configuring permissions on individual computers is an elaborate process, a domain level GPO is created and applied on all monitored computers.

- Log in to your domain controller with domain admin privileges.
- Create a new domain level GPO

Open the Group Policy Management Console \rightarrow Right-click on your domain \rightarrow Create a GPO in this domain and link it here \rightarrow Name the GPO "Log360 Permission GPO".

Image: File Action View Window Help Image: File Action View Help	Group Policy Management				-	□ ×			
Image: Security Policy Management ✓ ✓ Forest: log360Cart.com ✓ Image: log360	📓 File Action View Window Help								
Image: Group Policy Management LOg360PermissionGPO ✓ Morains Coga60CART-GPO Image: Dog360cart.com Image: Dog360cart.com Image: Dog360Cart.com Image: Dog360Cart.com									
Add Remove Properties WMI Filtering This GPO is Inked to the following WMI filter:	 Group Policy Management Forest: log360cart.com Gomains Iog360Cart.com Iog360PermissionGPO Iog360PermissionGPO	Log360PermissionGPO Scope Details Settings Dele Links Display links in this location: The following sites, domains, and Location I log360cart.com Security Filtering The settings in this GPO can only Name Add WMI Filtering This GPO is linked to the following	gation OUs are linked to this GPO: Enforced No apply to the following groups, us emove Properties g WMI filter:	Unk Enabled Yes ers, and computers:	Path log360cart.com	× ×			

Remove Apply group policy permission for Authenticated Users group

 Click "Log360 Permission GPO" → Navigate to the right panel, click the Delegation tab → Advanced → Click Authenticated Users → Remove the Apply group policy permission.

Course Dallas Management		
Group Policy Management		
File Action View Window Help		_ 8 ×
📓 Group Policy Management	Log360PermissionGPO	
✓ ▲ Forest: log360cart.com	Scope Details Settings Delegation	
V 🙀 Domains	These groups and users have the specified permission for this GPO	
✓ Im log360cart.com	Groups and users:	
LOG360CART-GPO		
a cat	Name	Allowed Permissions
> Domain Controllers	Authenticated Users Advice (LOC2000ABT) Densis Advice)	Edit settings, delete, modify
> Group Policy Objects	Domain Admine (LOG360CART (Domain Admine)	Edit settings, delete, modify
> 📑 WMI Filters	RENTERPRISE DOMAIN CONTROLLERS	Read
> 🛅 Starter GPOs	& Log360Group Group Policy Management	Edit settings, delete, modify
> 📑 Sites	& SYSTEM	Edit settings, delete, modify
🔯 Group Policy Modeling		
Group Policy Results	Do you want to remove this delegation privilege?	
	OK Cancel	
	<	>
	Add Remove Properties	Advanced

- 2. Add "Log360 Permission Group" to the security filter settings of the "Log360 Permission GPO".
- Open the Group Policy Management Console → Domain → Select "Log360 Permission GPO" → Navigate to the right panel, click the Delegation tab → Advanced → Add "Log360 Permission Group".



Privileges/permissions required for event log collection

Grant the user the Manage auditing and security log right

The Manage auditing and security log right allows the user to define object level auditing.

- Log in to your Domain Controller with Domain Admin privileges→ Open the Group Policy Management Console → Right click on the "Log360PermissionGPO" → Edit.
- 2. In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.
- 3. Navigate to the right panel, right click on Manage auditing and security $\log \rightarrow$ Properties \rightarrow Add the "Log360" user.

1	Group Policy Management Editor		-		×
Fil	e Action View Help				
(🔿 🖄 📷 🗙 🗐 🔒 🛛 🗊				
~	Log360PermissionGPO [LOG360CART-DC1.LOG3(∧ Computer Configuration Policies Software Settings Software Settings Scripts (Startup/Shutdown) Deployed Printers Deployed Printers Deployed Printers Account Policies Account Policies Account Policies Security Options Event Log System Services System Services Registry Sign Kristed Groups Wired Network (IEEE 802.3) Policies Wireless Network (IEEE 802.1) F Wireless Network (IEEE 802.1) F Deploties Wireless Network (IEEE 802.1) F Deplotes Network (IEEE 802.1)	Policy Policy Deny log on through Remote Desktop Services Enable computer and user accounts to be trusted for delega Force shutdown from a remote system Generate security audits Impersonate a client after authentication Increase a process working set Increase scheduling priority Load and unload device drivers Log on as a batch job Log on as a service Manage auditing and security log Modify firmware environment values Obtain an impersonation token for another user in the same Perform volume maintenance tasks Profile single process Profile single process Profile system performance Remove computer from docking station Replace a process level token Restore files and directories	Policy Not E Not E Not C Not C	y Setting Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined Defined	
<	>	<			>

I	Group Po	licy Mana	igement Ec	litor								_		×
Fil	e Action	View	Help	Manage a	uditing and	security	log Properties		?	×				
~	🔿 🖄			Security F	olicy Setting	Explain								
~	Log360Pe Comp Comp 2 2 2 2 2 2 2 2 2 2 2 2 2	ermission/ puter Con olicies Softwar Window Man Scrip Dep Scrip Secu > 20 Secu > 20 Secu Secu Secu Secu Secu Secu Secu Secu	GPO [LOG figuration e Settings vs Settings ne Resoluti ots (Startup loyed Print urity Setting Account Pol cocal Polici	☑ Defir LOG36	Manage au ne these polic; OCART\Log3	v settings	d security log				for delega	Policy Not D Not D Not D Not D Not D Not D Not D Not D Not D	Setting efined efined efined efined efined efined efined efined efined	
		L.	User Rig									Not D	efined	
1			Security									LOG36	50CART\	Log
1			Restricted (System Sen Registry File System Wired Netw Windows F Network Lis Wireless Ne Public Key	Ad	d User or Gro	ир	Remove	Cancel		Apply	the same	Not D Not D Not D Not D Not D Not D Not D Not D	efined efined efined efined efined efined efined efined	
-												_		-

Make the user a member of the Event Log Readers group, Distributed COM and Power Users

Members of the event log readers group will be able to read the event logs of all the audited computers.

For Domain Controllers :

 Log in to your Domain Controller with Domain Admin privileges → Open Active Directory Users and Computers → Built-in Container → Navigate to the right panel, right click on Event Log Readers → Properties → Members → Add the "Log360" user.

For other computers (Windows servers and workstations):

- Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click "Log360 Permission GPO" → Edit.
- In the Group Policy Management Editor → Computer Configuration → Preferences → Control Panel Settings → Right-click Local Users and Groups → New → Local Group → Select Event Log Readers group under group name → Add the "Log360" user.
- In the Group Policy Management Editor → Computer Configuration → Preferences → Control Panel Settings → Right-click Local Users and Groups → New → Local Group → Select Distributed COM User group under group name → Add the "Log360" user.
- 4. In the Group Policy Management Editor → Computer Configuration → Preferences → Control Panel Settings → Right-click Local Users and Groups → New → Local Group → Select Power Users group under group name → Add the "Log360" user





Group Policy Management Editor	New Local Group Properties X – 🗆 X
File Action View Help (= = =) (2) <td< td=""><td>Local Group Common</td></td<>	Local Group Common
Computer Configuration Computer Configuration Policies Defenses	Sroup name: Event Log Readers (built+in)
 Preteraces Windows Settings Control Panel Settings Data Sources Devices Folder Options Local Users and Groups Network Options Power Options 	Rename to: ction Full Name Description: Local Group Member in this view. Members: Name: LOG360CART\Log360Group Name LOG360CART\Log360Group
 Scheduled Tasks Scheduled Tasks Services ✓ ⁽¹⁾ User Configuration ○ Policies > ○ Preferences 	OK Cancel
< >>	Preferences / Extended / Standard /
Local Osers and Groups	





Group Policy Management Edit	or	- 🗆 🗙
File Action View Help		
🗢 🔿 🙇 🔜 🔏 🖎 [Distributed COM Users (built-in) Properties X	
Log360PermissionGPO [LOG36	Local Group Common	
 Policies Preferences 	Action: Update V	tion Full Name D
 Windows Settings Control Panel Settin Data Sources 	Group name: Distributed COM Users (built-in) V Upo	date N/A date N/A
📕 Devices	Description:	date N/A
Local Users and Metwork Option We Power Options	Delete all member users Delete all member groups	
🖉 Printers	Members:	
Screduled lasks	Name Action SID	
 ✓ [®] User Configuration > [™] Policies > [™] Preferences 	LOG360CART (LOG360 ADD 5-1-5-21-1235)	
	< >	
	Add Remove Change	
	OK Cancel Apply Help	>
< >	Preferences Extended Standard	
Last changed: 12/26/2023 6:29:16 A	N	



Group Policy Management Editor		- 🗆	×
File Action View Help			
🗢 🔿 📩 💼 📋 👼 🙆 New Local Group Properties X			
Image: Consistence of the constraint of the properties Image: Constraint of the constraint of the properties Image: Constraint of the constraint of	Action Update Update	Full Name N/A N/A	De
Preferences / Extended > Standard /			
Local Users and Groups			

Terms:

Event Log Readers: Members of this group can read event logs.

Distributed COM Users: Members of this group can launch, activate, and use Distributed COM objects on the computer.

Power Users: Members of this group can discover shares residing on Windows file servers.

Make user to read Event logs:

To read the event logs, you also need to grant the "Log360" users Read permission over HKLM\SYSTEM\ CurrentControlSet\Services\Eventlog\Security.

- Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click "Log360PermissionGPO" → Edit.
- 2. In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Right-click Registry → Add Key.
- In the Select Registry Key Window, navigate to MACHINE → SYSTEM → CurrentControlSet → Services → EventLog → Security → Click OK → Grant Read permission to "Log360" user → Click Apply.
- 4. In the Add Object window, select Configure this key then → Replace existing permissions on all subkeys with inheritable permissions → Click OK.

Group Policy Management Editor	- 🗆 X
File Action View Help	
(+ +) 🖄 📷 🔒 🖬 🖬	
 Windows Settings Mame Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Local Policies Setticted Groups System Services Restricted Groups Software Kestriction Polici Pu Help Software Kestriction Polici Min Policies on Act Monicubared OnS 	Name Windows Settings Control Panel Settings
Adds a new key to this template	







🗐 Gr	oup Policy Management Editor		-	×
File	Action View Help			
(=	🚈 📆 🛃 🖬			
<	 Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Event Log Event Log System Services Restricted Groups System Services Registry File System Windows Firewall with Ad Network List Manager Pol Windows Firewall with Ad Network List Manager Pol Windows Firewall with Ad Network List Manager Policies Software Restriction Policie Software Restriction Policie Application Control Policie Advanced Audit Policy Co 	Object Name MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security		

Enable WMI and Remote Event Log Management traffic through Firewall:

- Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click "Log360 Permission GPO" → Edit.
- 2. Select Computer configuration → Policies → Windows Settings → Security Settings → Windows Firewalls with Advanced Security → Inbound Rules
- 3. Right-click Inbound Rules → New Rule and select WMI in predefined field → select all rules → Allow connection.
- 4. To allow Remote Event Log Management connection, repeat step 4 by selecting Remote Event Log Management in the predefined field.





Note:

These rules open ports of the range, 49152 - 65535, that are exclusive for WMI communication and so these cannot be accessed by other applications.

Grant the user Read permission on all audited shares

There are two ways to grant the user Read permission on all the audited shares:

- Make the user a Member of the Local Administrators group.
 - Login to any computer with domain admin privileges → Open MMC console → File → Add/ Remove Snap-in → Select Local Users and Groups → Add → Another computer → Add target computer
 - 2. Select target computer → Open Local Users and Groups → Select Groups → Right-click Administrators → Properties → Add "Log360" user.
 - 3. Repeat the above steps for every audited Windows file server/cluster.

ſ	-	Console1 - [Console Root\Local	Jsers an	d Groups (log360cart-w	-ws1)\Groups]	
		File Action View Favorites	Wind	low Help	Administrators Properties ? ×	
	(=	• 🔿 🚈 📰 🔀 🕅 🔂 🚺				
	1	Console Root		Name	General	^
	~	Local Users and Groups (log3	300cart	Name Access Control Assii Administrators Certificate Service D Cryptographic Oper Distributed COM Us Event Log Readers Guests Hyper-V Administra Event Log Readers Network Configurat Performance Log U: Performance Monit Power Users Print Operators RDS Endpoint Serve RDS Endpoint Serve RDS Remote Access Remote Desktop Us Remote Desktop Us Remote Desktop Us	Administrators Description: Administrators have complete and unrestricted access to the computer/domain Members: Members: Administrator Administrator AD360260CART.Domain Admins DG360CART.Log360 (Log360@log360cart.com) Interview Filest Add Remove Changes to a user's group membership are not effective until the next time the user logs on. Supports file replication in a dom	
				System Managed Ac	Acc Members of this group nave com	
U	<		>	🙊 Users	Users are prevented from making	×

- Grant the user both Share and NTFS Read permission on every audited share.
 - Login to any computer with domain admin privileges → Open MMC console → File → Add/ Remove Snap-in → Select Shared Folders → Add → Another computer → Add target computer.
 - 2. Select target computer \rightarrow Select share \rightarrow Right-click \rightarrow Properties \rightarrow Security \rightarrow Edit \rightarrow Add the "Log360" user \rightarrow Provide both Share and NTFS, Read permission.
 - 3. Repeat the above steps for every audited share.

Console1 - [Console Root\Shared Folders (\)	LOG360CART-WS1)\Shares]	
File Action View Favorites Window	Help	
	•	
	est Properties	
Console Root s	s	Permissions for Test (\\log360cart-ws1)
Shared Folders (\LOG360CART-WS	General Publish Share Permissions Security	Security
😥 Shares	Object name: \\log360cart-ws1\Test	Object name: \\log360cart-ws1\Test
Sessions Open Files	Group or user names:	Group or user names:
84	SYSTEM .	SYSTEM
	Administrator (LOG360CART-WS1\Administrator)	Administrator (LOG360CART-WS1\Administrator)
	Administrators (LOG360CART-WS1\Administrators)	Administrators (LOG360CART-WS1\Administrators)
		Log360 (Log360@log360cart.com)
	To change permissions, click Edit. Edit	
	Permissions for SYSTEM Allow Deny	All During
	Full control 🗸 ^	Add Remove
	Modify 🗸	Permissions for Log360 Allow Deny
	Read & execute 🗸	Full control
	List folder contents 🗸	Modify D
	Read 🗸 🗸	Read & execute
	For special permissions or advanced settings, click	List folder contents
	Advanced.	Read 🗹 🗆 🗸
	OK Cancel Apply	OK Cancel Apply

Granting WMI permission:

- Log in to any computer with domain admin privileges → Run wmimgmt.msc → Right-click on WMI Control (Local) → Connect to target computer.
- Right-click WMI Control (target computer) → Properties → Security → +Root → CIMV2 → Security → Add the "Log360" user and grant the following permissions: Execute Methods | Enable Account | Remote Enable





- 3. Click OK.
- 4. Navigate to +Root → +RSOP → Computer → Security → Add the "Log360" user and grant the following permissions:

Execute Methods | Enable Account | Remote Enable

Windo	ws Management Instrume	ntation (W	11)	WMI Control
Configures and	WMI Control Properties		Security for ROOT\RSOP	X
	General Backup/Restore	Security /	dv Security	
	Namespace navigation allow Image: A second state of the second st	ve you to set re Directory 2 ation	Group or user names: Authenticated Users Log360 (Log360@log360cart.com) System Authenticated Users Log360 (Log360@log360cart.com) Authenticated Users Administrators (LOG360CART\Admi Administrators (LOG360CART\Admi Administrators (LOG360 Execute Methods Full Write Partial Write Provider Write Enable Account Remote Enable For special permissions or advanced setti	istrators) id Remove Allow Deny
			click Advanced.	Advanced
		OK	OK	Cancel Apply

- 5. Click OK.
- 6. Repeat the steps for every audited computer.

Grant WMI Namespace Security Rights using GPO (PowerShell script)

Script download link

- 1. Add the script WMIrights.ps1 file in the shared location in the domain.
- 2. Create a new GPO WMI NameSpace Security Rights and Right-click \rightarrow Edit.
- 3. Navigate to Computer Configuration \rightarrow Policies \rightarrow Windows Settings \rightarrow Scripts \rightarrow Startup \rightarrow Rightclick and open Properties \rightarrow PowerShell Scripts \rightarrow Add.
- 4. In the Add Script dialog box, click Browse and select the PowerShell script (WMIrights.ps1) file from the shared location and set the parameter as "domainname\username".

🗐 🗐 Group Policy Management Edito	or		- 🗆 X
File Action View Help			
🗢 🔿 🙋 📆 🗟 🔒 🛛 5			
WMI NameSpace Security Right Will NameSpace Security Right Difference Policies Software Settings Windows Settings Scripts (Statup/S Script	Scripts (Startup/Shutdown) Startup Display Properties, Description: Contains computer startup scripts.	Name Startup Shutdown	Startup Properties ? Scripts PowerShell Scripts Windows PowerShell Startup Scripts for WMI NameSpace Script Rame: Vog380bcart.dc1WWMigta Browse
Preferences Solution Preferences Preferences	Extended / Standard /		Script Farameters: bg360cart Vog360[Fc OK Cancel Not configured PowerShell scripts require at least Windows 7 or Windows Server Show Files OK Cancel Apply

5. Click OK to return to the Startup Properties dialog box \rightarrow Apply \rightarrow OK

Configuring Administrative Template Settings

- 1. On the left pane of the Group Policy Management Editor, navigate to Computer Configuration Administrator Templates System.
- 2. Under System, select Scripts.
- 3. On the right pane of the GPO Editor, double-click Run logon scripts synchronously, and enable it \rightarrow Apply \rightarrow OK.



4. Enable Maximum wait time for Group Policy scripts and set the maximum time at 10 seconds.

Specify maximum	wait time for Gro	oup Policy scripts			—		×
Specify maximum	wait time for Gro	up Policy scripts		Previous Setting	Next Setting		
 Not Configured Enabled 	Comment:						^
O Disabled	Supported on:	At least Windov	vs 2000				* *
Options:			Help:				
Seconds: 10 Range is 0 to 32000, 1	use 0 for infinite v	vait time	This policy scripts app This setting startup, any running. If specified ti records an If you enable a number fi the system system to v long they t This interva must wait v script must the ""Run I system to v the desktop	setting determines how lied by Group Policy to d shutdown scripts appl the scripts have not fini me expires, the system series error event. It this setting, then, in t rom 1 to 32,000 for the to wait for the set of sc vait until the scripts hav ake, type 0. It is particularly importa while the scripts complet complete before the n ogon scripts synchrono vait for the logon script b.	v long the system w run. lowed for all logon, lied by Group Policy shed running when stops script process the Seconds box, yo number of seconds ripts to finish. To di re finished, no matt ant when other syste ete. By default, each ext one runs. Also, y usly"" setting to dir s to complete befor	vaits for logoff, y to finish t the ing and ou can typ you wan rect the er how em tasks o startup you can u rect the re loading	e t
				OK	Cancel	Арр	y _a nan

5. Navigate to Logon under System, on the right pane double-click Always wait for the network at startup and logon, and enable it \rightarrow Apply \rightarrow OK

Group Policy Management Editor		-	- 🗆	×
File Action View Help				
Early Launch Antimalware Access	Logon	Setting	State	^
File Classification Infrastructure	computer startup and logon	E Turn off picture password sign-in	Not configure	ed
> 🧮 Filesystem 🧮 Folder Redirection	Edit policy setting	E Assign a default credential provider E Assign a default domain for logon	Not configure Not configure	ed ed
S Group Policy S Internet Communication Mana S ISCS KDC	Requirements: At least Windows Server 2003 operating systems or Windows XP Professional	E Exclude credential providers E Block user from showing account details on sign-in D on ot process the legacy run list D on ot process the run once list	Not configure Not configure Not configure Not configure	ed ed ed
Kerberos Locale Services Locale Services Locale Services Locale Mitigation Options Net Logon Net Logon Remore Management Recovery Remote Assistance Remote Procedure Call Removable Storage Access Scripts Scripts Stutdown Shutdown	Description: This policy setting determines whether Group Policy processing is synchronous (that is, whether computers wait for the network to be fully initialized during computer startup and user logon). By default, on client computers, Group Policy processing is not synchronous; client computers typically do not wait for the network to be fully initialized at startup and logon. Existing users are logged on using cached credentials, which results in shorter loagn times. Group Policy	Turn off app notifications on the lock screen Turn off Windows Startup sound Do not display network selection UI Do not enumerate connected users on domain-joined com Show first sign-in animation Enumerate local users on domain-joined computers Hide entry points for Fast User Switching Always use classic logon Do not display the Getting Started welcome screen at logon Run these programs at user logon Always wait for the network at computer startup and logon Always use custom logon background	Not configure Not configure Not configure Not configure Not configure Not configure Not configure Not configure Not configure Enabled Not configure	≥d ≥d ed ed ed ed ed ed ed
<	Extended Standard /			

6. Navigate to Group Policy under System, on the right pane double-click Configure Group Policy slow link detection, and enable it \rightarrow Apply \rightarrow OK.

Group Policy Management Editor		-	- 🗆	×
System Access-Denied Assistance App-V Audr Process Creation Credentials Delegation Device Guard Device Installation Disk Outas Disk Quotas Disk Quota	Configure Group Policy Configure Group Policy slow link detection Edit policy setting Requirements: At least Windows 2000 Description: This policy setting defines a slow connection for purposes of applying and updating Group Policy. If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this setting, the system considers the connection to be slow.	Setting Configure Internet Explorer Maintenance policy processing Configure Internet Explorer Maintenance policy processing Configure registry policy processing Configure scripts policy processing Configure wireds policy Clent Service AOAC optimization Turn off Group Policy Clent Service AOAC optimization Configure Group Policy Clent Service AOAC optimized for up Policy Clent Service AOAC optimized for Universes Configure Group Policy Caching of Servers Configure Group Policy Caching Grevers Configure Group Policy colow link detection Set Group Policy refresh interval for computers Control policy refresh interval for domain controllers Configure Servers Configure Group Policy Clent Service AOAC optimized for Computers Configure Group Policy Clent Service Configure Group Policy Clent Service Configure Group Policy I aching for Servers Configure Group Policy refresh interval for computers Configure Group Policy refresh interval for Computers Configure Group Policy Clent Servers Configure Control Clent Servers Configure Group Policy Clent Servers Configure Group Policy I aching for Servers Configure ServerServ	State Not configu Not configu	red red red red red red red red red red
< >>	\Extended \Standard /			

Apply the GPO

1. On the left pane of the Group Policy Management Editor, right-click the required GPO → Properties.

Group Policy Management Editor	_	×
File Action View Heln		-
WMI NameSpace Security Pights II View	,	
item to view its description. Name		
> Preferen		
✓ K User Config Properties K User Configuration		
> Capeform Help		
< > Extended / Standard /		
Opens the properties dialog box for the current selection.		

2. Navigate to the Security tab and unselect the "Apply Group Policy" permissions for Authenticated Users → Add.

Group Policy Management Edite	10	– 🗆 X
File Action View Help		
🏟 📰 🖼 😨 🖬	WMI NameSpace Security Rights [LOG360CART-DC1.L ? ×	
WMI NameSpace Security Right Secur	General Links Security Comment	F.COM] Policy
> 🦰 Policies	Group or user names:	
> Preferences	REATOR OWNER	
Oser Configuration		
> Preferences	Domain Admins (LOG360CART\Domain Admins)	
,	Enterprise Admins (LOG360CART\Enterprise Admins)	
	SenterPrise Domain Controllers	
	Add Remove	
	Permissions for Authenticated Users Allow Deny	
	Write	
-	Create all child objects	
	Delete all child objects	
	Special pemissions	
	For special permissions or advanced settings, click Advanced Advanced.	
	OK Cancel Apply	
< >	Extended (Standard /	

- 3. In the dialog box that appears, click Object Types.
- 4. Enter the names of the required computers and groups and click Check Names.
- 5. Select the required computers and groups and click OK to return to the properties dialog box.

Group Policy Management Edite	pr	_	×
File Action View Help			
	WMI NameSpace Security Rights [LOG360CART-DC1.L ? ×		
WMI NameSpace Security Righ	Select Users, Computers, Service Accounts, or Groups	imes icy	
> Policies	Select this object type:		
> Preferences	Users, Computers, Groups, or Built-in security principals Object Type	es	
 V Ser Configuration Policies 	From this location:		
> 🧮 Preferences	log360cart.com Locations	s	
	Enter the object names to select (<u>examples</u>):		
	Log360Group Check Nam	mes	
	Advanced OK Cance	el .:	
1	Delete all child objects		
	Apply group policy		
	Special permissions		
	Advanced.		
<	> Extended Standard		

6. In the Security tab, grant "Apply group policy" permissions to the selected computers and groups \rightarrow Apply \rightarrow OK.

I	Group Policy Management Edit	or	_	\times
File	Action View Help			
\$	🔶 🔲 📓 📓 🖬	WMI NameSpace Security Rights [LOG360CART-DC1.L ? X		
~	WMI NameSpace Security Righ Policies Policies User Configuration Preferences Policies Policies Preferences	General Links Security Comment Group or user names: SYSTEM SQ Domain Admins (LOG360CART\Domain Admins) Enterprise Admins (LOG360CART\Enterprise Admins) Enterprise Admins (LOG360CART\Enterprise Admins) ENTERPRISE DOMAIN CONTROLLERS Log360Group (LOG360CART\Log360Group) Add Remove Permissions for Log360Group Allow Deny Write Create all child objects Delete all child objects Delete all child objects Special permissions For special permissions or advanced settings, click Advanced OK Cancel	T.COM] Policy	
		Lxtended _Standard /		

7. Restart the computers and execute the command gpupdate/force



Note:

After all the required devices are given WMI permissions, remove the script from Computer Configuration Policies Windows Settings Scripts (Startup/Shutdown) \rightarrow Startup or the scripts will run every time during startup.

Grant the user read permission over the C\$ share (\\server_name\C\$):

Read permission over C\$ share (\\server_name\C\$) is needed to access NetApp C-Mode log files.

Privileges/permissions required for automatic audit policy and object level auditing configuration

Privileges/permissions required for domain controller auditing configuration

Granting the service account the following privileges/permissions, allows ADAudit Plus to automatically configure the required audit policy and object level auditing settings in your environment. ADAudit Plus does this by pushing the required settings via GPO, to the group which contains all the monitored computers.

 Log in to your domain controller with domain admin privileges
 → Open the Group Policy Management Console
 → click Default domain controllers Policy
 → Navigate to the right panel, click the Delegation tab
 → Add the Log360 User
 → Provide permission to Edit settings.



🞼 Group Policy Results

<

Add... Remove Properties

>

Advanced...

Privileges/permissions required for member server, workstation, and file server auditing configuration

Make the user a member of the Group Policy Creator Owners group

 Log in to your domain controller with domain admin privileges > Open Active Directory Users and Computers > Click Users > Navigate to the right panel, Right-click Group Policy Creator Owners group > Add the "Log360" user as a member.

Active Directory Users and Computers				\times
File Action View Help				
🗢 🔿 🖄 📆 🤞 🖬 🙆 🧔	🖻 🛛 🖬 🐮 📚 🛍 🍸 💆 🐍			
Active Directory Users and Computers [I	lc Name	Туре	Description	-
> 📔 Saved Queries	🛃 admin	User		
✓ III log360cart.com	Administrator	User	Built-in account for administering the comp	
> Builtin	Allowed RODC Password Replication Group	Security Group	Members in this group can have their passw	
> cart	🐁 baskie	User		
> Computers	A Cert Publishers	Security Group	Members of this group are permitted to pub	
EoreignSecurityPrincipals	Rection Controllers	Security Group	Members of this group that are domain cont	
Kevs	DefaultAccount	User	A user account managed by the system.	
> CostAndFound	Replication Group	Security Group	Members in this group cannot have their pa	
Managed Service Accounts	A DnsAdmins	Security Group	DNS Administrators Group	
> 📔 Program Data	A DnsUpdateProxy	Security Group	DNS clients who are permitted to perform d	
> 🧮 System	Admins Admins	Security Group	Designated administrators of the domain	
C Users	A Domain Computers	Security Group	All workstations and servers joined to the do	
> MTDS Quotas	A Domain Controllers	Security Group	All domain controllers in the domain	
> I TPM Devices	A Domain Guests	Security Group	All domain guests	
	💐 Domain Users	Security Group	All domain users	
	Admins & Enterprise Admins	Security Group	Designated administrators of the enterprise	
	A Enterprise Key Admins	Security Group	Members of this group can perform adminis	
	Read-only Domain Controllers	Security Group	Members of this group are Read-Only Doma	
	Sroup Policy Creator Owners	Security Group	Members in this group can modify group po	
	🛃 Guest	User	Built-in account for guest access to the com	
	A Key Admins	Security Group	Members of this group can perform adminis	
	🛃 krbtgt	User	Key Distribution Center Service Account	
	🛃 Log360	User		
	🖧 Log360Group	Security Group		
	Reprotected Users	Security Group	Members of this group are afforded addition	
	RAS and IAS Servers	Security Group	Servers in this group can access remote acce	
	a readonly	User		
	Read-only Domain Controllers	Security Group	Members of this group are Read-Only Doma	
< >	Schema Admins	Security Group	Designated administrators of the schema	~
	-D			

Active Directory Users and Computers		X
File Action View Help ← → ∑ ☆ △ ☆ ○ △ ☐ Active Directory Users and Com ∑ ∑ <td>Group Policy Creator Owners Properties ? × General Members Member Of Managed By Members: Name Active Directory Domain Services Folder Active Directory Domain Services Folder Cog 560 log 560cart.com/Users</td> <td>domain ed to the do nain</td>	Group Policy Creator Owners Properties ? × General Members Member Of Managed By Members: Name Active Directory Domain Services Folder Active Directory Domain Services Folder Cog 560 log 560cart.com/Users	domain ed to the do nain
 > Computers > Domain Controllers > ForeignSecurityPrincipal: > Managed Service Accourt ≥ Ent ≥ Users ≥ Gu ≥ Gu 		enterprise orm adminis -Only Doma ify group po to the com orm adminis
して 選 Pro 選 Pro 選 Rea 選 Sch 選 Sch 選 Sch 工 ES 工 ES Tes 選 Tes	Add Remove	ded addition remote acce -Only Doma : schema
Contraction Contr	OK Cancel Apply 380 User 360Group Security Group	↓

Grant the user, group management permissions

- Log in to your domain controller with domain admin privileges → Open Active Directory User and Computers. Click View and ensure that Advanced Features is enabled. This will display the advanced security settings for selected objects in Active Directory Users and Computers.
- Right-click Users → Properties → Security → Advanced → Permissions → Add → In the Permissions Entry for Users window, Select a principal: Log360 user → Type: Allow → Applies to: This object and all descendant objects → Select permissions: Create Group objects and Delete Group objects.

Note:

Use Clear all to remove all permissions and properties before selecting the mentioned permissions.

Active Directory Users a	nd Computers		-	×
File Action View He	Users Properties	? ×		
(+ +) 2 📰 📋				
Active Directory Users a Active Directory Users a Barrier Strategy of the series of	General Object Security Attribute Editor Group or user names: Group or user names: Group or user names: GREATOR OWNER SELF Attribute Editor Gast Authenicated Users System Security Add Domain Admins (LOG360CART\Domain Admins) Add Permissions for CREATOR OWNER Allow Full control Read OK Cancel OK Cancel Apply	aded computer ac ain controllers rity identifiers (SID bjects aned objects aged service acco ainer e of application d aded user accounts		
<	>			
Active 📕 Advanced Se	curity Settings for Users	>	<	×
File Act				
Owner:	Domain Admins (LOG360CART\Domain Admins) Change			
> Sa Permissions	Auditing Effective Access			
For additional	information, double-click a permission entry. To modify a permission entry, se	elect the entry and click Edit (if available).		

lype	Principal	Access	Inherited from	Applies to 2
Allow	Log360 (Log360@log360cart		None	Descendant Group objects
Allow	Log360 (Log360@log360cart	Create/delete Group o	None	This object and all descendan
Allow	Account Operators (LOG360	Create/delete InetOrg	None	This object only
Allow	Account Operators (LOG360	Create/delete Group o	None	This object only
Allow	Print Operators (LOG360CAR	Create/delete Printer o	None	This object only
Allow	Account Operators (LOG360	Create/delete User obj	None	This object only
Allow	Domain Admins (LOG360CA	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatib	Special	DC=log360cart,DC=co	Descendant InetOrgPerson o v
A <u>d</u> d Disable	<u>R</u> emove <u>V</u> iew			Restore defaults

ManageEngine) Log360

Permission	n Entry for Users		
Principal:	Select a principal		
Туре:	Allow		
Applies to:	This object and all descendant objects $\qquad \qquad \lor$		
Permissions	5:		
	Full control	Create msDS-ManagedServiceAccount objects	
	✓ List contents	Delete msDS-ManagedServiceAccount objects	
	Read all properties	Create msDS-PasswordSettingsContainer objects	
	Write all properties	Delete msDS-PasswordSettingsContainer objects	
	Delete	Create msDS-ResourceProperties objects	
	Delete subtree	Delete msDS-ResourceProperties objects	
	Read permissions	Create msDS-ResourcePropertyList objects	
	Modify permissions	Delete msDS-ResourcePropertyList objects	
	Modify owner	Create msDS-ShadowPrincipalContainer objects	
	All validated writes	Delete msDS-ShadowPrincipalContainer objects	
	Create all child objects	Create msDS-ValueType objects	
	Delete all child objects	Delete msDS-ValueType objects	
	Create account objects	Create msieee80211-Policy objects	
	Delete account objects	Delete msieee80211-Policy objects	
	Create aCSResourceLimits objects	Create msImaging-PSPs objects	
	Delete aCSResourceLimits objects	Delete mslmaging-PSPs objects	

Permission	n Entry for Users			
Principal:	Log360 (Log360@log360cart.com) Select a principal			
Туре:	Allow			
Applies to:	This object and all descendant objects $\qquad \lor$			
Permission:	5:			
	Full control	Create msDS-ManagedServiceAccount objects		
	✓ List contents	Delete msDS-ManagedServiceAccount objects		
	Read all properties	Create msDS-PasswordSettingsContainer objects		
	Write all properties	Delete msDS-PasswordSettingsContainer objects		
	Delete	Create msDS-ResourceProperties objects		
	Delete subtree	Delete msDS-ResourceProperties objects		
	Read permissions	Create msDS-ResourcePropertyList objects		
	Modify permissions	Delete msDS-ResourcePropertyList objects		
	Modify owner	Create msDS-ShadowPrincipalContainer objects		
	All validated writes	Delete msDS-ShadowPrincipalContainer objects		
	Create all child objects	Create msDS-ValueType objects		
	Delete all child objects	Delete msDS-ValueType objects		
	Create account objects	Create msieee80211-Policy objects		
	Delete account objects	Delete msieee80211-Policy objects		
	Create aCSResourceLimits objects	Create msImaging-PSPs objects		
		Delete melace size DCDs altients		

	<u> </u>	
Read msDS-IsPrimaryComputerFor	Write msDS-ReplValueMetaData	
Read msDS-KrbTgtLinkBl	Read msDS-RepIValueMetaDataExt	
Read msDS-LastKnownRDN	✓ Write msDS-RepIValueMetaDataExt	
Write msDS-LastKnownRDN	Read msDS-RevealedDSAs	
Read msDS-LocalEffectiveDeletionTime	Read msDS-RevealedListBL	
Write msDS-LocalEffectiveDeletionTime	✓ Write msDS-RevealedListBL	
Read msDS-LocalEffectiveRecycleTime	Read msDS-SourceAnchor	
Write msDS-LocalEffectiveRecycleTime	Write msDS-SourceAnchor	
Read msDs-masteredBy	Read msDS-TasksForAzRoleBL	
Read msds-memberOfTransitive	Read msDS-TasksForAzTaskBL	
Write msds-memberOfTransitive	Read msDS-TDOEgressBL	
Read msDS-MembersForAzRoleBL	Read msDS-TDOIngressBL	
Read msDS-MembersOfResourcePropertyListBL	Read msDS-ValueTypeReferenceBL	
Read msds-memberTransitive	Read msSFU30PosixMemberOf	
Write msds-memberTransitive	Read name	
Read msDS-NCRepICursors	✓ Write name	
Write msDS-NCRepICursors	Read Name	
Read msDS-NCReplInboundNeighbors	🗹 Write Name	
Write msDS-NCReplInboundNeighbors	Read ownerBL	
Read msDS-NCReplOutboundNeighbors	Read structuralObjectClass	
Write msDS-NCRepIOutboundNeighbors	Write structuralObjectClass	
Read msDS-NC-RO-Replica-Locations-BL		
Only apply these permissions to objects and/or containers within this	container	Clear all
		OK Cancel

Permission Entry for Users		— 🗆	×
Read msDS-IsPrimaryComputerFor			^
Read msDS-KrbTgtLinkBl	Read msDS-ReplValueMetaDataExt		
Read msDS-LastKnownRDN	Write msDS-RepIValueMetaDataExt		
Write msDS-LastKnownRDN	Read msDS-RevealedDSAs		
Read msDS-LocalEffectiveDeletionTime	Read msDS-RevealedListBL		
Write msDS-LocalEffectiveDeletionTime	Write msDS-RevealedListBL		
Read msDS-LocalEffectiveRecycleTime	Read msDS-SourceAnchor		
Write msDS-LocalEffectiveRecycleTime	Write msDS-SourceAnchor		
Read msDs-masteredBy	Read msDS-TasksForAzRoleBL		
Read msds-memberOfTransitive	Read msDS-TasksForAzTaskBL		
Write msds-memberOfTransitive	Read msDS-TDOEgressBL		
Read msDS-MembersForAzRoleBL	Read msDS-TDOIngressBL		
Read msDS-MembersOfResourcePropertyListBL	Read msDS-ValueTypeReferenceBL		
Read msds-memberTransitive	Read msSFU30PosixMemberOf		
Write msds-memberTransitive	Read name		
Read msDS-NCRepICursors	Write name		
Write msDS-NCRepICursors	Read Name		
Read msDS-NCReplInboundNeighbors	Write Name		
Write msDS-NCReplInboundNeighbors	Read ownerBL		
Read msDS-NCReplOutboundNeighbors	Read structuralObjectClass		
Write msDS-NCRepIOutboundNeighbors	Write structuralObjectClass		
Read msDS-NC-RO-Replica-Locations-BL			
Only apply these permissions to objects and/or containers within this	container	Clear all	
			-
		OK Cance	el

rincipal:	Log360 (Log360@log360cart.com) Select a principal		
/ne:	Allow		
, per			
pplies to:	This object and all descendant objects ~		
ermissions			
	Full control	Create msDS-ManagedServiceAccount objects	
	List contents	Delete msDS-ManagedServiceAccount objects	
	Read all properties	Create msDS-PasswordSettingsContainer objects	
	Write all properties	Delete msDS-PasswordSettingsContainer objects	
	Delete	Create msDS-ResourceProperties objects	
	Delete subtree	Delete msDS-ResourceProperties objects	
	Read permissions	Create msDS-ResourcePropertyList objects	
	Modify permissions	Delete msDS-ResourcePropertyList objects	
	Modify owner	Create msDS-ShadowPrincipalContainer objects	
	All validated writes	Delete msDS-ShadowPrincipalContainer objects	
	Create all child objects	Create msDS-ValueType objects	
	Delete all child objects	Delete msDS-ValueType objects	
	Create account objects	Create msieee80211-Policy objects	
	Delete account objects	Delete msieee80211-Policy objects	
	Create aCSResourceLimits objects	Create msImaging-PSPs objects	
	Delete aCSResourceLimits objects	Delete msImaging-PSPs objects	
	Create applicationVersion objects	Create msKds-ProvRootKey objects	
	Delete applicationVersion objects	Delete msKds-ProvRootKey objects	
	Create certificationAuthority objects	Create msKds-ProvServerConfiguration objects	
	Delete certificationAuthority objects	Delete msKds-ProvServerConfiguration objects	
	Create Computer objects	Create MSMQ Queue Alias objects	
	Delete Computer objects	Delete MSMQ Queue Alias objects	
	Create Contact objects	Create ms-net-ieee-80211-GroupPolicy objects	
	Delete Contact objects	Delete ms-net-ieee-80211-GroupPolicy objects	
	Create document objects	Create ms-net-ieee-8023-GroupPolicy objects	
	Delete document objects	Delete ms-net-ieee-8023-GroupPolicy objects	
	Create documentSeries objects	Create msPKI-Enterprise-Oid objects	
	Delete documentSeries objects	Delete msPKI-Enterprise-Oid objects	
	Create Group objects	Create msPKI-Key-Recovery-Agent objects	
	Delete Group objects	Delete msPKI-Key-Recovery-Agent objects	

From the Active Directory User and Computers console → Right-click Users → Properties → Security

 Advanced → Permissions → Add → In the Permission Entry for Users window → Select a principal:
 Log360 user → Type: Allow → Applies to: Descendant Group objects → Select property: Write
 Members.

Note:

Use Clear all to remove all permissions and properties before selecting the mentioned property.

File Active Were Program Data System System System System System System System TPM Devices Full only on a diverse of advanced settings, click Adduser accounts	Active Directory Users and Computers				_	×
For special permissions or advanced settings, click Advanced OK Cancel Apply Help	Active Directory Users and Computers File Action View Help Active Directory Users and Computers [Ic Active Directory Users and Computers [Ic Active Directory Users and Computers [Ic Bayed Queries Bayed Queries Builtin Socart Builtin Computers Domain Controllers Domain Controllers Computers Computers Computers Socart Computers Computers Socart Socart Computers Socart Socart Computers Socart Computers Socart	Users Properties General Object Security Attribute Editor Group or user names: CEEATOR OWNER State State State SYSTEM Log300 (log300Cat com) Domain Admins (LOG300CART\Domain Admins) Add Pemissions for CREATOR OWNER Allon Full control Read Create all child objects Delete all child objects Dele	? ×	aded computer ac ain controllers rity identifiers (SID bjects aned objects aged service acco ainer re of application d		×
		For special permissions or advanced settings, click Advanced. OK Cancel Apply	Advanced	raoed user accounts		

(Ac	tive	Ad	lvanced S	ecurity Settings for U	lsers			_		×		×
	File	Act	Ow	ner:	Domain Admins	(LOG360CAF	R\Domain Admins) Char	nge					
Ľ	> AC	Sa	Pe	rmissions	Auditing	Effective A	ccess						
	× 1		For Peri	addition	al information, doubl	e-click a pen	mission entry. To modify a	permission entry, select th	e entry and click Edit (if av	/ailable).			
	>			Type	Principal		Access	Inherited from	Applies to		^		
	~		2	Allow	Log360 (Log360@lo	og360cart		None	Descendant Group obje	cts			
	Ś		2	Allow	Log360 (Log360@lo	og360cart	Create/delete Group o	None	This object and all desce	endan			
	>		52	Allow	Account Operators	(LOG360	Create/delete InetOrg	None	This object only				
	>		52	Allow	Account Operators	(LOG360	Create/delete Group o	None	This object only				
	>		<u>82</u>	Allow	Print Operators (LO	G360CAR	Create/delete Printer o	None	This object only				
	>		82	Allow	Account Operators	(LOG360	Create/delete User obj	None	This object only				
	>		52	Allow	Domain Admins (L	OG360CA	Special	None	This object only				
	>		52	Allow	Authenticated User	s	Special	None	This object only				
	>		<u>82</u>	Allow	SYSTEM		Full control	None	This object only				
			<u>88</u>	Allow	Pre-Windows 2000	Compatib	Special	DC=log360cart,DC=co	Descendant InetOrgPers	on o	~		
				A <u>d</u> d Disable <u>i</u> n	<u>R</u> emove heritance	View			Restore	defaults			
L	¢								OK Cancel	<u>А</u> рр	ly etc		
												1	

Principal:	Select a principal		
Туре:	Allow		
Applies to:	This object and all descendant objects		
Permission	5:		
	Full control	Create msDS-ManagedServiceAccount objects	
	✓ List contents	Delete msDS-ManagedServiceAccount objects	
	Read all properties	Create msDS-PasswordSettingsContainer objects	
	Write all properties	Delete msDS-PasswordSettingsContainer objects	
	Delete	Create msDS-ResourceProperties objects	
	Delete subtree	Delete msDS-ResourceProperties objects	
	Read permissions	Create msDS-ResourcePropertyList objects	
	Modify permissions	Delete msDS-ResourcePropertyList objects	
	Modify owner	Create msDS-ShadowPrincipalContainer objects	
	All validated writes	Delete msDS-ShadowPrincipalContainer objects	
	Create all child objects	Create msDS-ValueType objects	
	Delete all child objects	Delete msDS-ValueType objects	
	Create account objects	Create msieee80211-Policy objects	
	Delete account objects	Delete msieee80211-Policy objects	
	Create aCSResourceLimits objects	Create msImaging-PSPs objects	
	Delete aCSResourceLimits objects	Delete ms/maging-PSPs objects	

Permission	Entry for Users				×
Principal:	Log360 (Log360@log360cart.com) Select a principal				
Type.					
Applies to:	Descendant Group objects 🗸 🗸				
Permissions	Descendant group objects Descendant group ofUniqueNames objects Descendant groupPolicyContainer objects Descendant ieee802Device objects				
	Descendant inetUrgPerson objects Descendant IntelliMirror Service objects Descendant IntelliMirror Service objects Descendant iphots objects Descendant ipPortoscol objects Descendant ipService objects Descendant msAuthz-CentralAccessPolicies objei Descendant msAuthz-CentralAccessPolicy object Descendant msAuthz-CentralAccessRule objects Descendant msAuthz-CentralAccessRule objects Descendant msCuth2-Partition objects Descendant msCOM-Partition Set policets	Modify owner MI validated writes AII validated writes Call extended rights Create all child objects Delete all child objects Add/remove self as member Send to			
Properties:	Descendant msDFS-DeletedLinkv2 objects Descendant msDFS-DeletedLinkv2 objects Descendant msDFS-NamespaceAnchor objects Descendant msDFS-Namespacev2 objects Descendant msDFS-Namespacev2 objects Descendant msDFSR-Connection objects Descendant msDFSR-Content objects Descendant msDFSR-ContentSet objects Descendant msDFSR-CocalSettings objects Descendant msDFSR-Member objects Descendant msDFSR-Member objects	Read msDS-NCRepIInboundNeighbors Write msDS-NCRepIInboundNeighbors Read msDS-NCRepIOutboundNeighbors Write msDS-NCRepIOutboundNeighbors Read msDS-NC-R0-RepIca-Locations-BL Read msDS-NC-R0-RepIca-Locations-BL Read msDS-NCType			
	Descendant msDFSR-Subscriber objects		ОК	Car	ncel

· •	Permission Entry for Users				×
	Read gidNumber	Write msDS-NcType			^
	Write gidNumber	Read msDS-NonMembers			
	Read Group name (pre-Windows 2000)	Write msDS-NonMembers			
	Write Group name (pre-Windows 2000)	Read msDS-NonMembersBL			
	Read groupAttributes	Read msDS-ObjectReferenceBL			
	Write groupAttributes	Read msDS-ObjectSoa			
	Read groupType	Write msDS-ObjectSoa			
	Write groupType	Read msDS-OIDToGroupLinkBI			
	Read isRecycled	Read msDS-OperationsForAzRoleBL			
	Write isRecycled	Read msDS-OperationsForAzTaskBL			
	Read labeledURI	Read msDS-parentdistname			
	Write labeledURI	Write msDS-parentdistname			
	Read Managed By	Read msDS-PrimaryComputer			
	Write Managed By	Write msDS-PrimaryComputer			
	Read memberOf	Read msDS-PrincipalName			
	Read Members	Write msDS-PrincipalName			
	Write Members	Read msDS-PSOApplied			
	Read memberUid	Read msDS-ReplAttributeMetaData			
	Write memberUid	Write msDS-ReplAttributeMetaData			
	Read msCOM-PartitionSetLink	Read msDS-RepIValueMetaData			
	Read msCOM-UserLink	Write msDS-ReplValueMetaData			
	Read msDFSR-ComputerReferenceBL	Read msDS-RepIValueMetaDataExt			
	Read msDFSR-MemberReferenceBL	Write msDS-ReplValueMetaDataExt			
	Read msDS-Approx-Immed-Subordinates	Read msDS-RevealedDSAs			
	Write msDS-Approx-Immed-Subordinates	Read msDS-RevealedListBL			~
			ОК	Car	ncel

	ci.	Domain Admins (LOG360CAF	RT\Domain Admins) <u>C</u> har	nge	
Perr	nissions	Auditing Effective A	ccess		
or a erm	dditiona nission e	I information, double-click a per ntries:	mission entry. To modify a	permission entry, select the	e entry and click Edit (if available).
	Туре	Principal	Access	Inherited from	Applies to
2	Allow	Domain Admins (LOG360CA	Special	None	This object only
8	Allow	Authenticated Users	Special	None	This object only
2	Allow	SYSTEM	Full control	None	This object only
8	Allow	Log360 (Log360@log360cart		None	Descendant Group objects
2	Allow	Log360 (Log360@log360cart	Create/delete Group o	None	This object and all descendan
2	Allow	Account Operators (LOG360	Create/delete InetOrg	None	This object only
2	Allow	Account Operators (LOG360	Create/delete Group o	None	This object only
2	Allow	Print Operators (LOG360CAR	Create/delete Printer o	None	This object only
2	Allow	Account Operators (LOG360	Create/delete User obj	None	This object only
8	Allow	Enterprise Admins (LOG360C	Full control	DC=log360cart,DC=co	This object and all descendan
	A <u>d</u> d	<u>R</u> emove <u>E</u> dit			Restore defaults
	Allow Allow Allow Allow Allow Allow	Log360 (Log360@log360cart Account Operators (LOG360 Account Operators (LOG360 Print Operators (LOG360CAR Account Operators (LOG360C Enterprise Admins (LOG360C	Create/delete Group o Create/delete InetOrg Create/delete Group o Create/delete Printer o Create/delete User obj Full control	None None None None DC=log360cart,DC=co	This object and all descenda This object only This object only This object only This object only This object and all descenda

Grant the user Read permission over the SYSVOL folder

Read permission over the SYSVOL folder is needed for GPO Settings change auditing.

Note:

By default, all Authenticated Users have read permission over the sysvol folder, if the "Log360" user does not, the Read permission has to be provided by following the steps listed below.

1. Navigate to the sysvol folder (C:\Windows\SYSVOL\sysvol) \rightarrow Right-click \rightarrow Properties \rightarrow Sharing \rightarrow Advanced sharing \rightarrow Permissions \rightarrow Add the "Log360" user \rightarrow Provide Share Read permission.

Permissions for SYSVOL		\times
Share Permissions		
Group or user names:		
Image: Second contract of the second		
	Add	Remove
Permissions for Log360	Allow	Deny
Full Control Change Read		
ОК	Cancel	Apply

For ADMP component,

To carry out the desired Active Directory (AD) management and reporting operations without a domain admin user account, follow the steps using the document below. We can use the Log360 user and group for the below mentioned steps,

https://download.manageengine.com/products/ad-manager/permissions-required-for-the-ad-account-configured-in-admanager-plus.pdf

For Exchange Reporter Plus component,

We can use the Log360 user and group for the below mentioned steps,

https://download.manageengine.com/products/exchange-reports/erp-permission-document.pdf

Configurable Paths

If the configurations below are changed rather than using the default path, kindly provide NTFS Read and Execute permissions to Log360 users for the same,

- Log360 → Admin → General Settings → Database Settings → Database Backup → Click the pencil icon to edit Component Settings → Backup Storage Path
- EventLog Analyzer → Settings → Admin Settings → General → Product Settings → Product Configurations → Reporting mode → If "Save to Location" is selected → Click the Settings Icon next to it.
- EventLog Analyzer → Settings → Admin Settings → Data Storage → Archives → Settings icon on top
 right corner of the tab → Archive Location

- ADAudit Plus \rightarrow Admin \rightarrow Archive Events \rightarrow Scroll down to see the location.
- ADAudit Plus → Admin → Schedule Reports → Modify Schedule Report → Scroll down to see the location.
- ADAudit Plus \rightarrow Configuration \rightarrow Modify Alert Profile \rightarrow Scroll down to see the location.
- $M365 \rightarrow Settings \rightarrow Configuration \rightarrow Audit Configuration \rightarrow Archive Settings \rightarrow Archive Folder Path$
- DataSecurity Plus → Admin → Configurations → Archive Configuration
- DataSecurity Plus → Admin → Schedule Reports → Modify Schedule Report. You can see the location under After Execution
- DataSecurity Plus → Configuration → Alerts → Modify Alert Profile

Grant the user Modify permissions over files for which Move/Delete responses are configured (DSP)

- 1. Log in to the target computer with domain admin privileges. Locate the file for which Move/Delete responses are configured.
- 2. Right-click the file, go to Properties \rightarrow Security \rightarrow Edit, add the Log360 user, and provide Modify permissions.
- 3. Repeat the steps for all the files for which the specified responses are configured.

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus Exchange Reporter Plus | M365 Manager Plus

ManageEngine)

ManageEngine Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. It combines threat intelligence, machine learning-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks, and offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/

\$ Get Quote

↓ Download