



Service account configuration

for Log360



Create a new user

Log in to your domain controller with domain admin privileges → Open Active Directory Users and Computers → Right-click on your domain → New → User → 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.
2. 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.

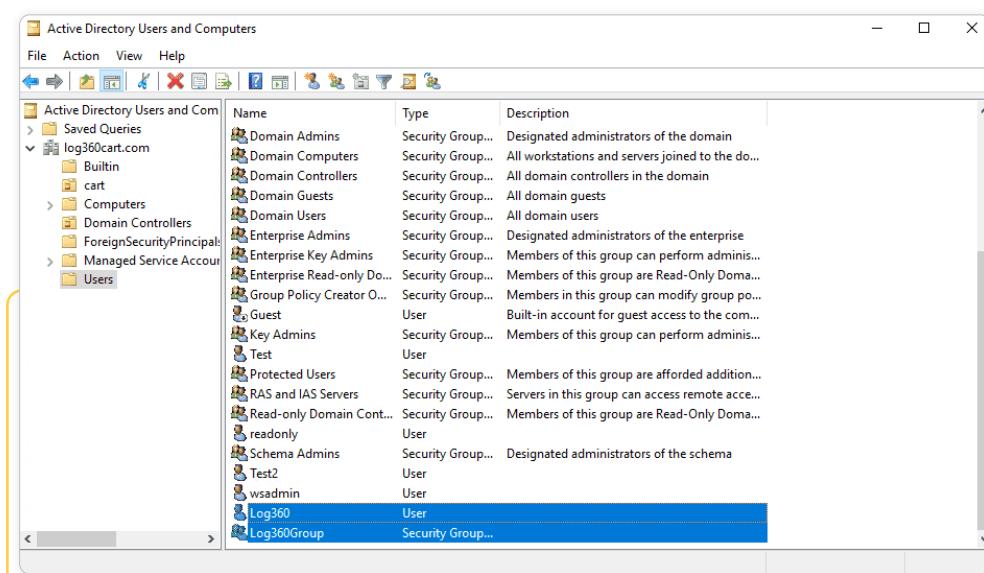
Note:

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

1. 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”.
2. 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.

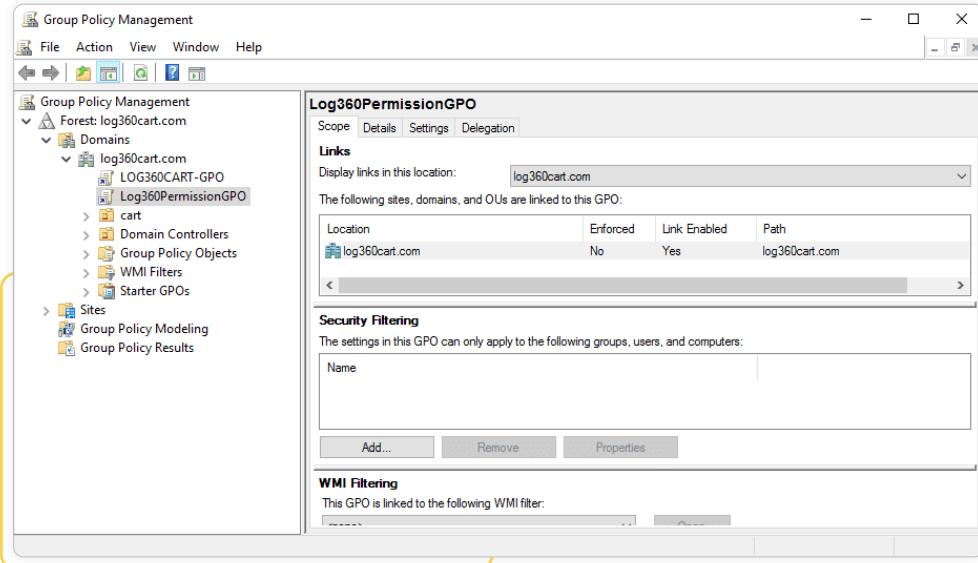


Create a new domain level GPO and link it to all the audited computers

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

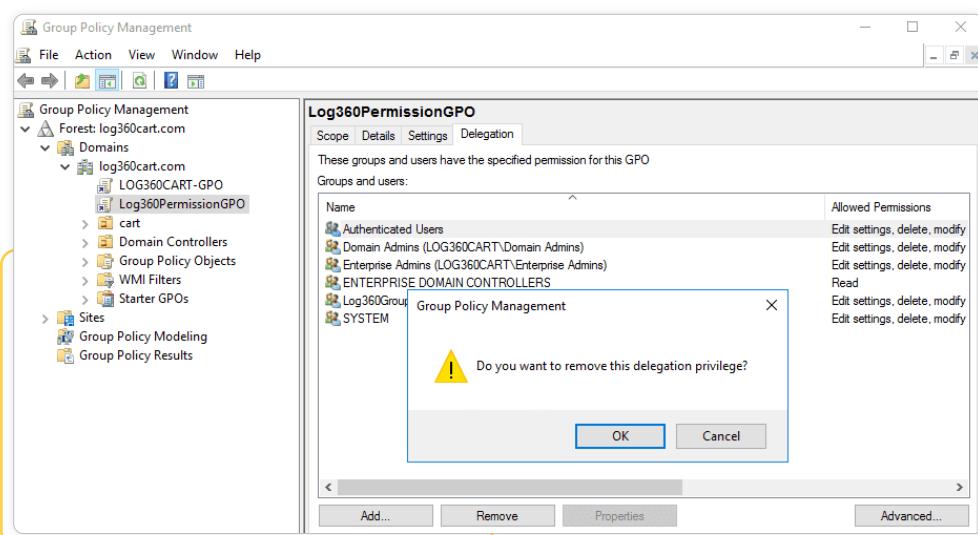
- Log in to your domain controller with domain admin privileges.
- **Create a new domain level GPO**

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

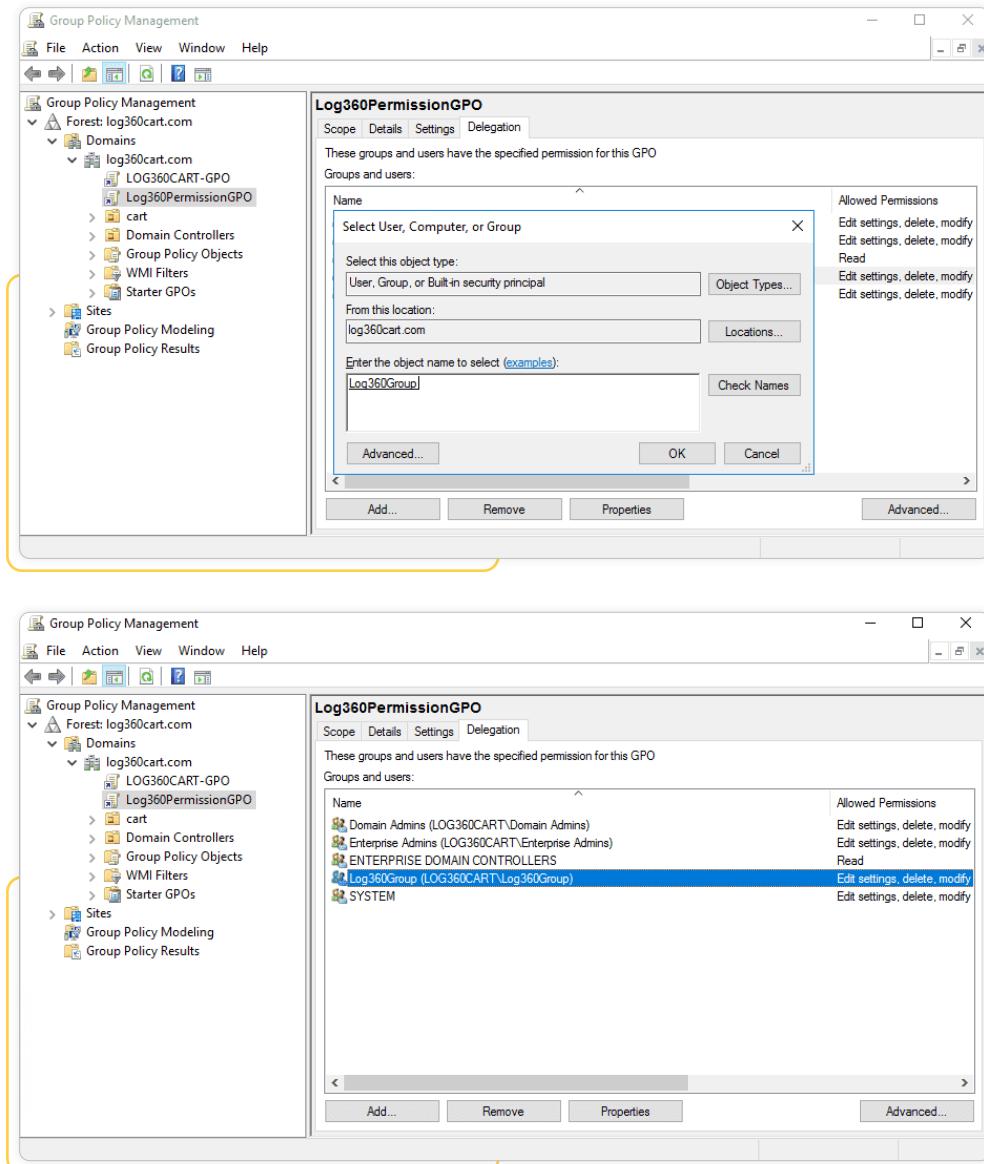


Remove Apply group policy permission for Authenticated Users group

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



2. Add “Log360 Permission Group” to the security filter settings of the “Log360 Permission GPO”.
3. 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”.

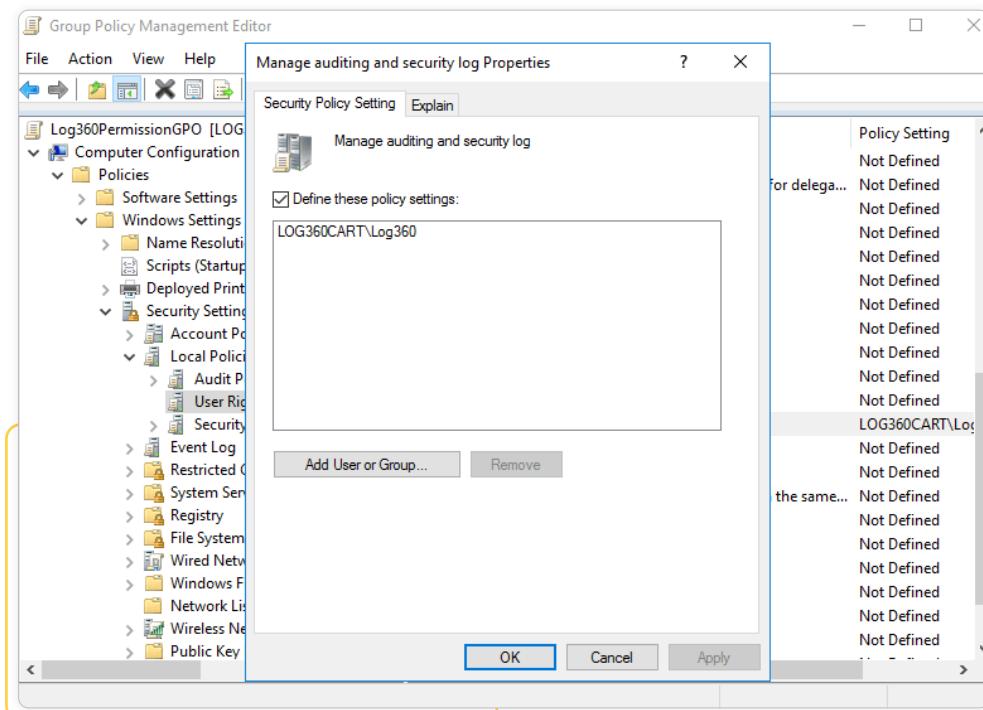
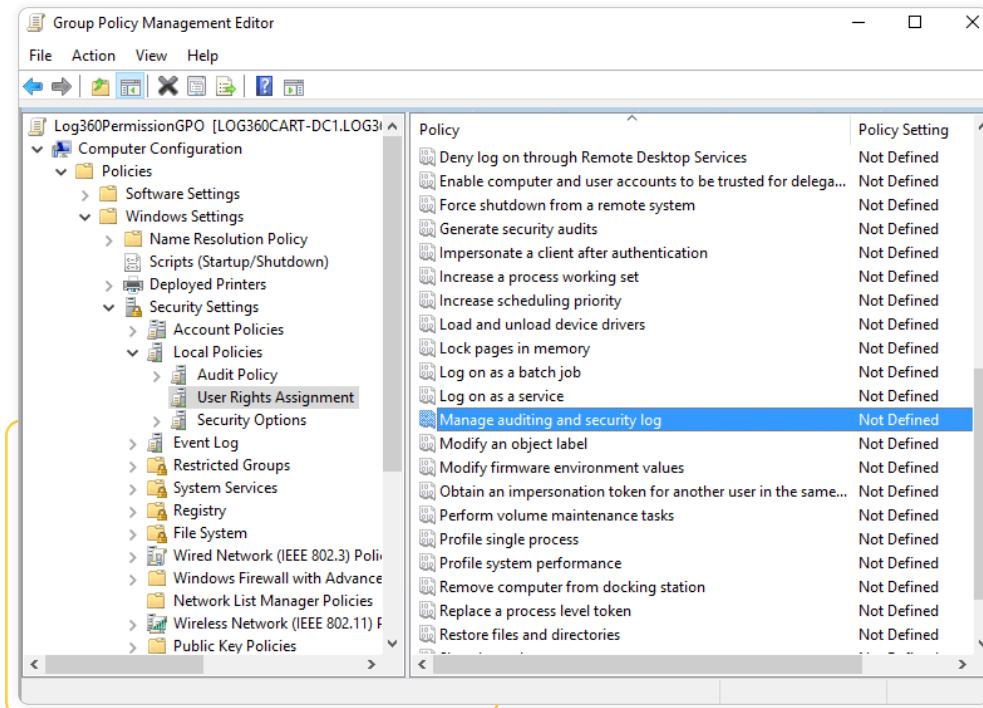


Privileges/permissions required for event log collection

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.

1. 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 → Properties → Add the "Log360" user.



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

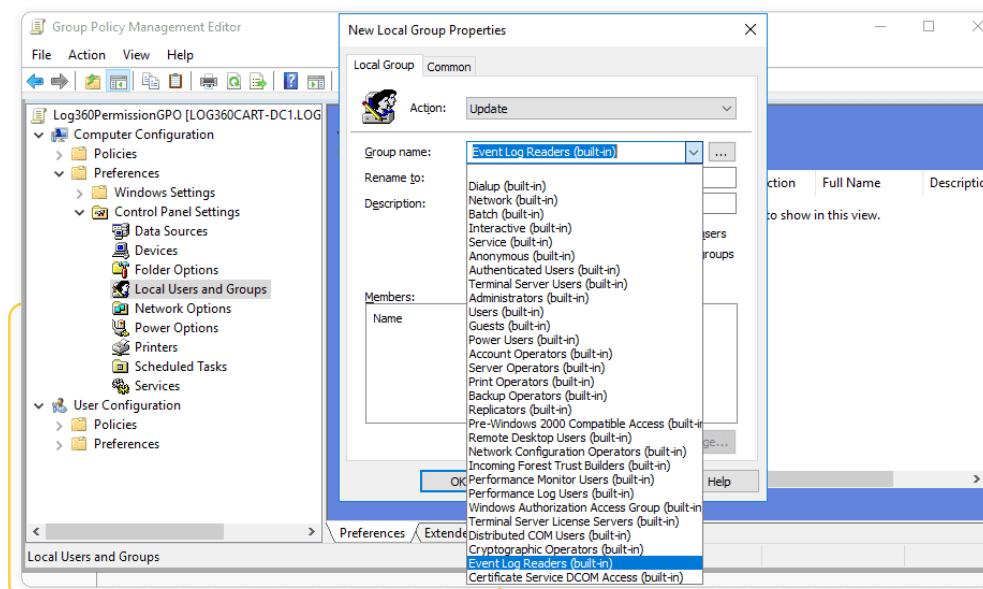
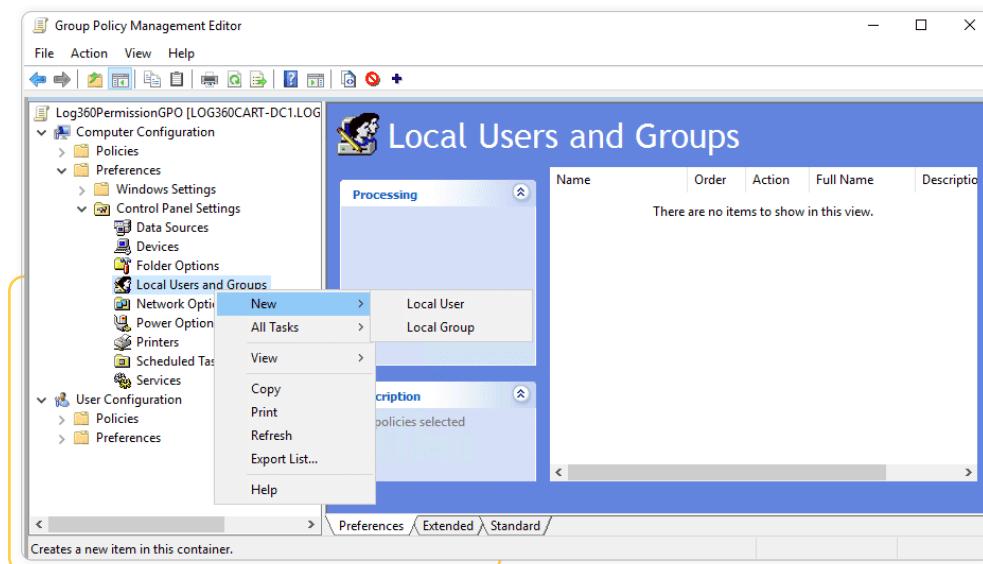
Members of the event log readers group will be able to read the event logs of all the audited computers.

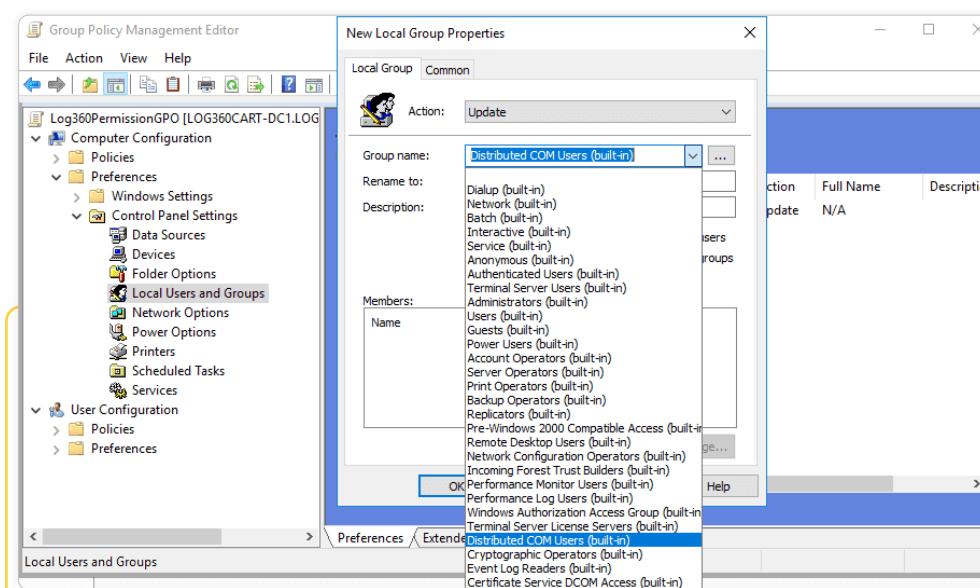
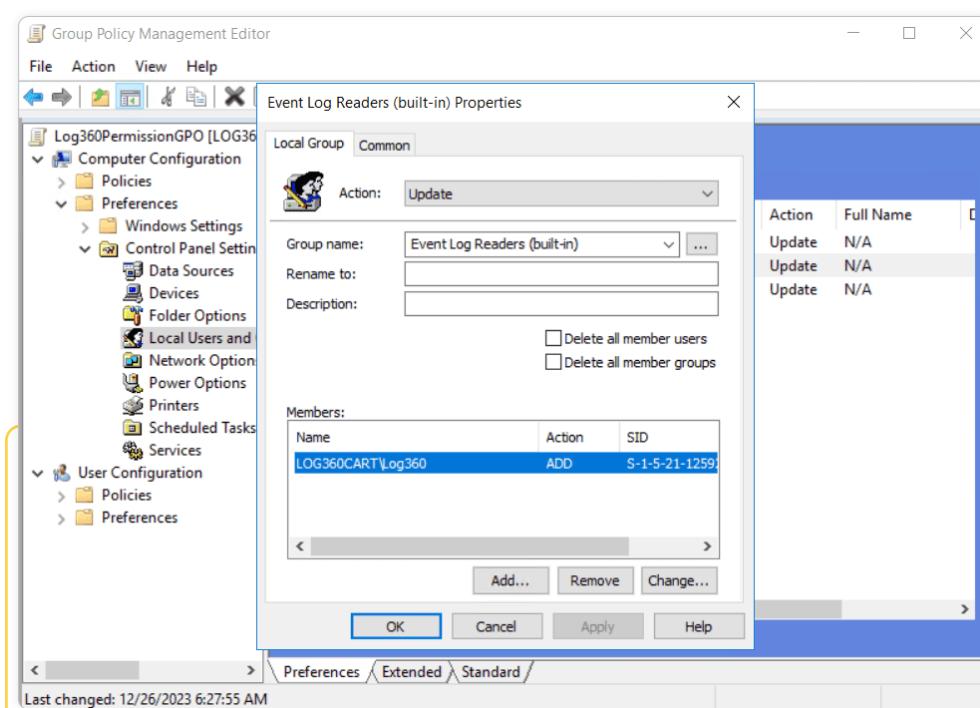
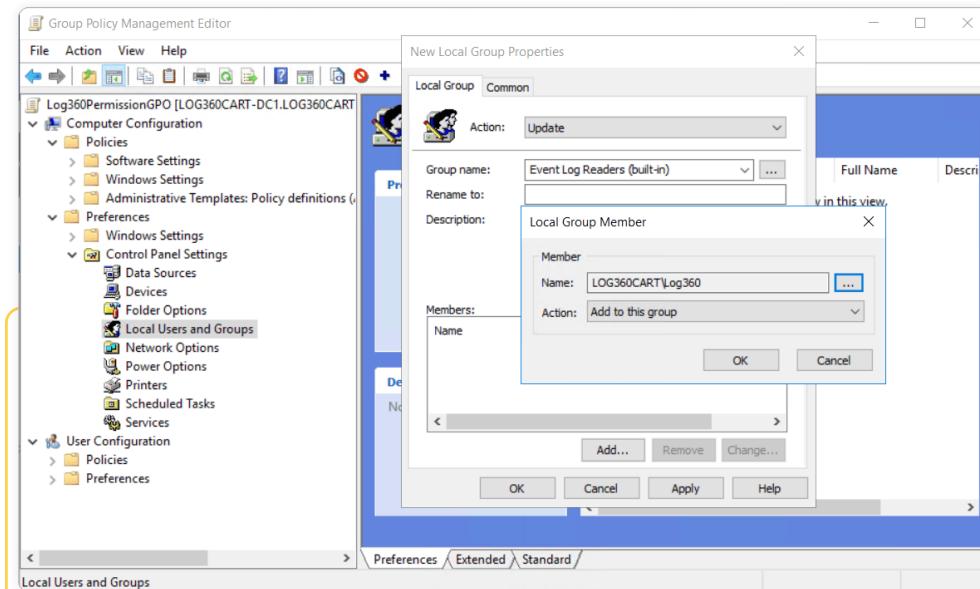
For Domain Controllers :

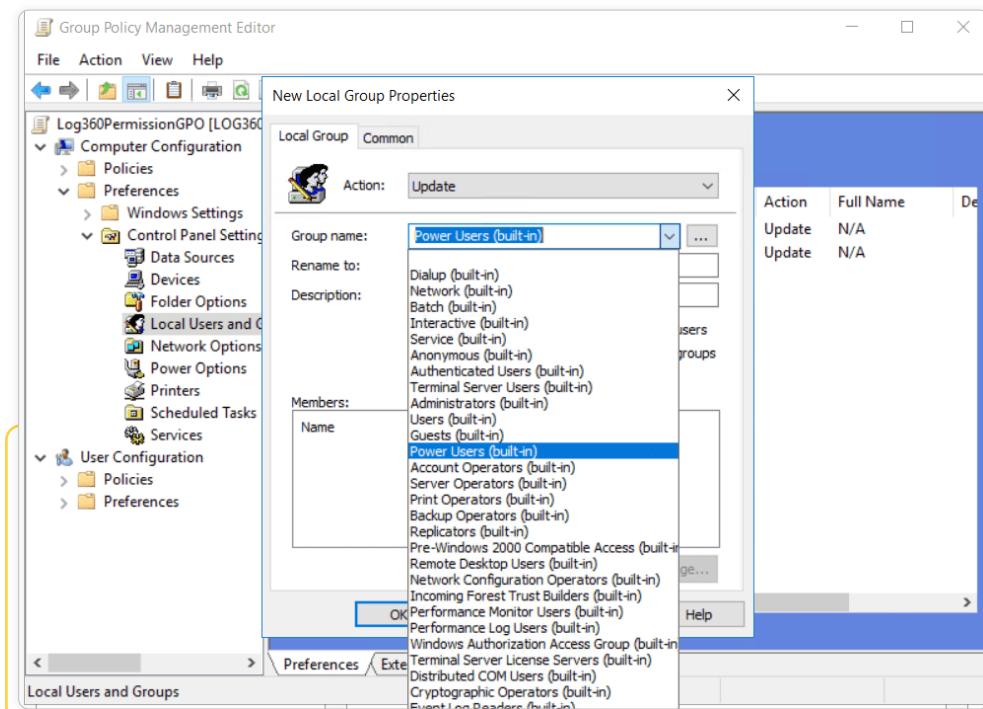
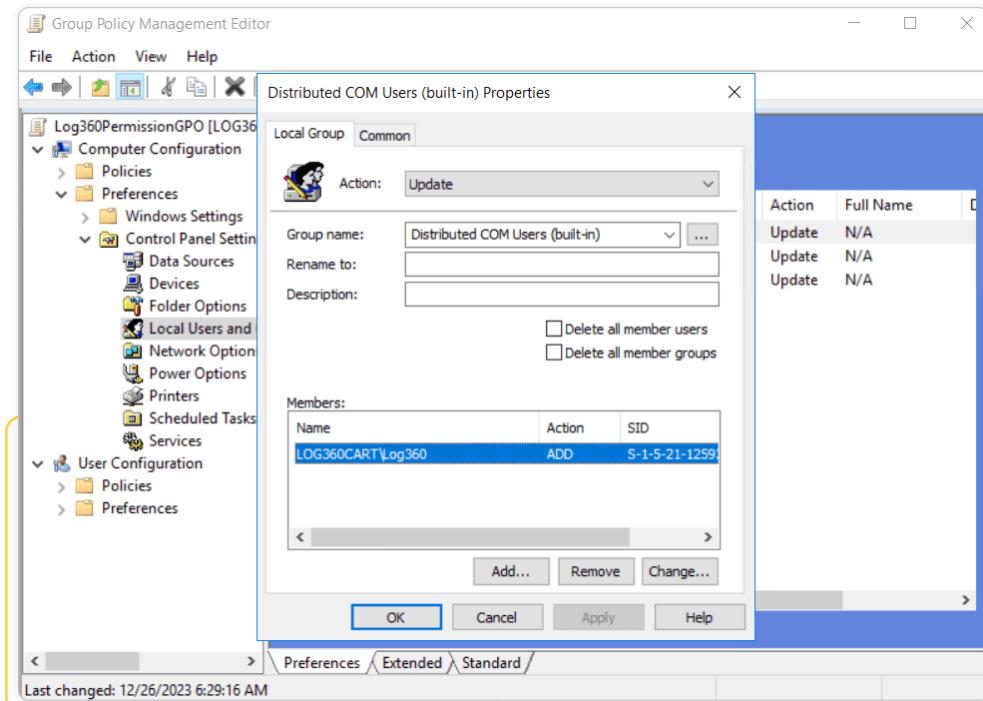
1. Log in to your Domain Controller with Domain Admin privileges → Open Active Directory Users and Computers → Built-in Container → Navigate to the right panel, right click on Event Log Readers → Properties → Members → Add the "Log360" user.

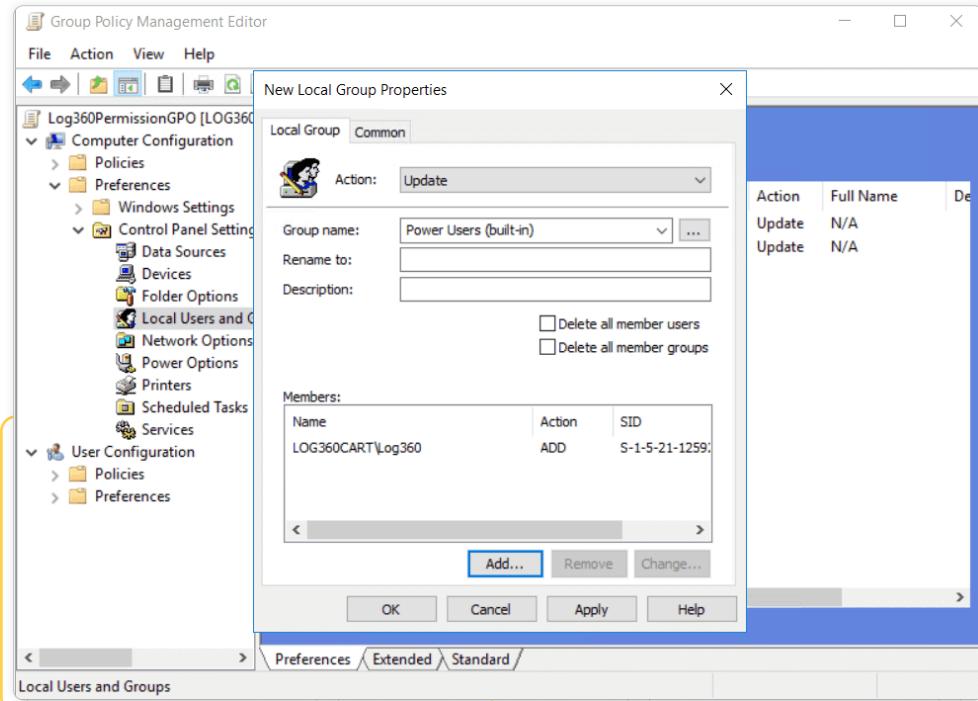
For other computers (Windows servers and workstations):

1. Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click “Log360 Permission GPO” → Edit.
2. 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.
3. 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









Terms:

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

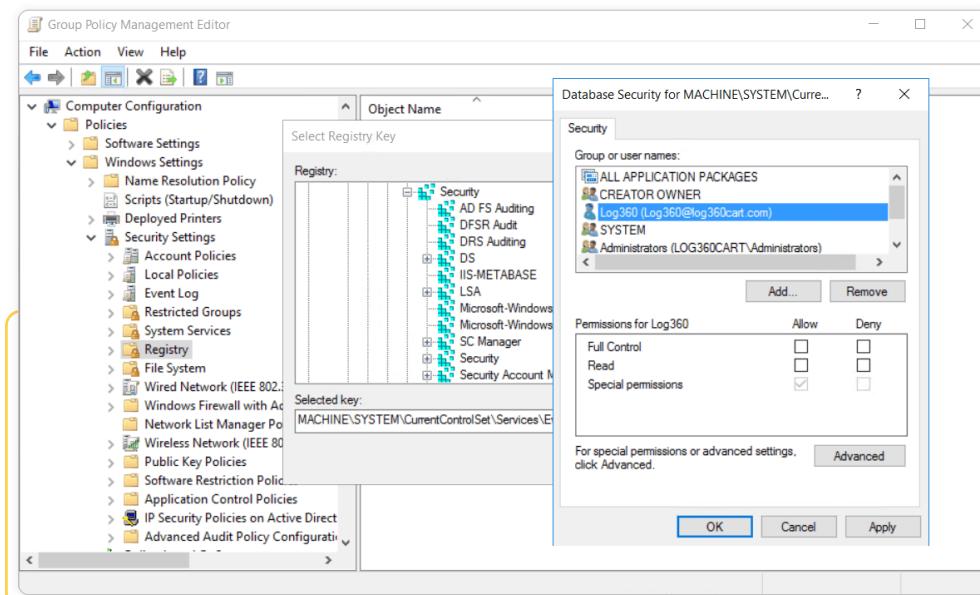
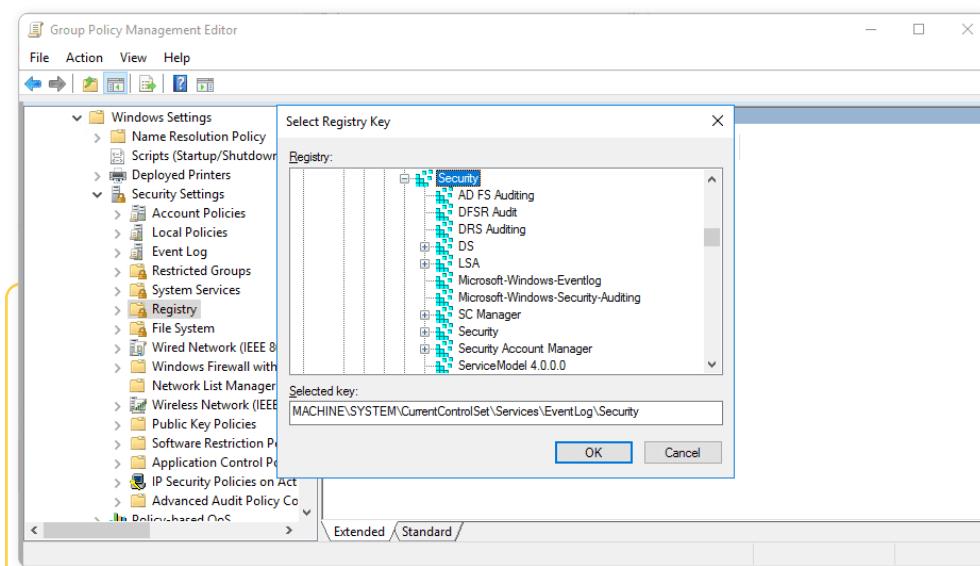
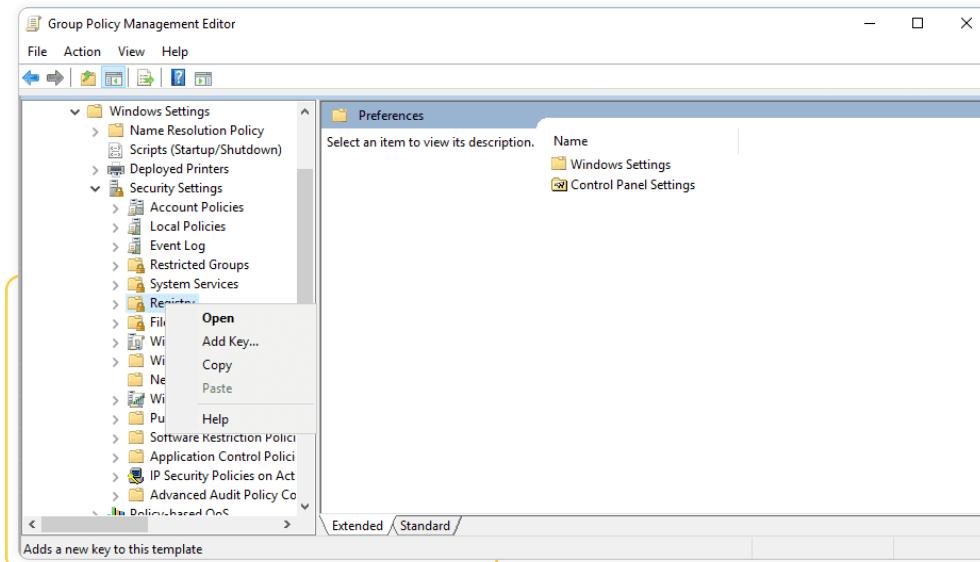
Distributed COM Users: Members of this group can launch, activate, and use Distributed COM objects on the computer.

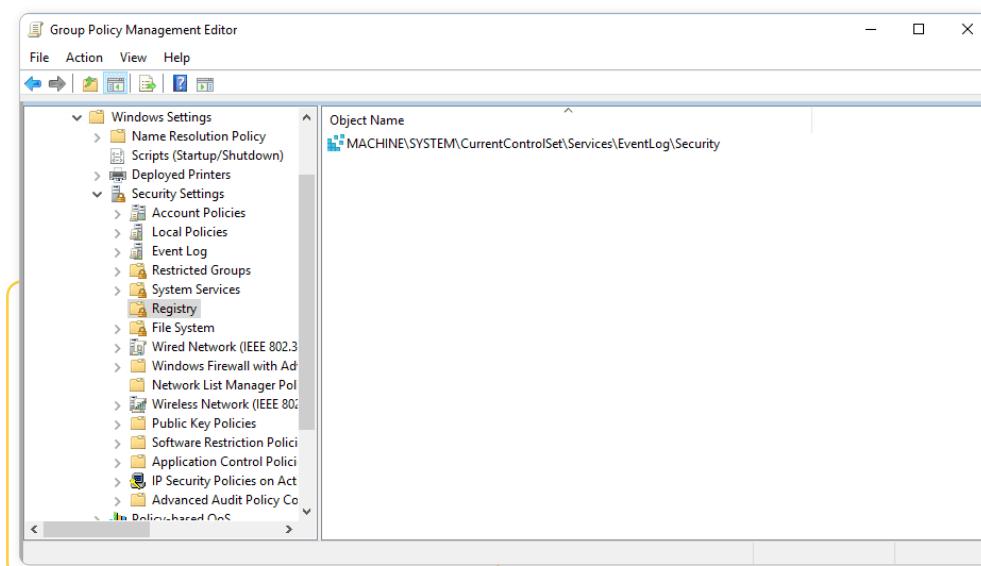
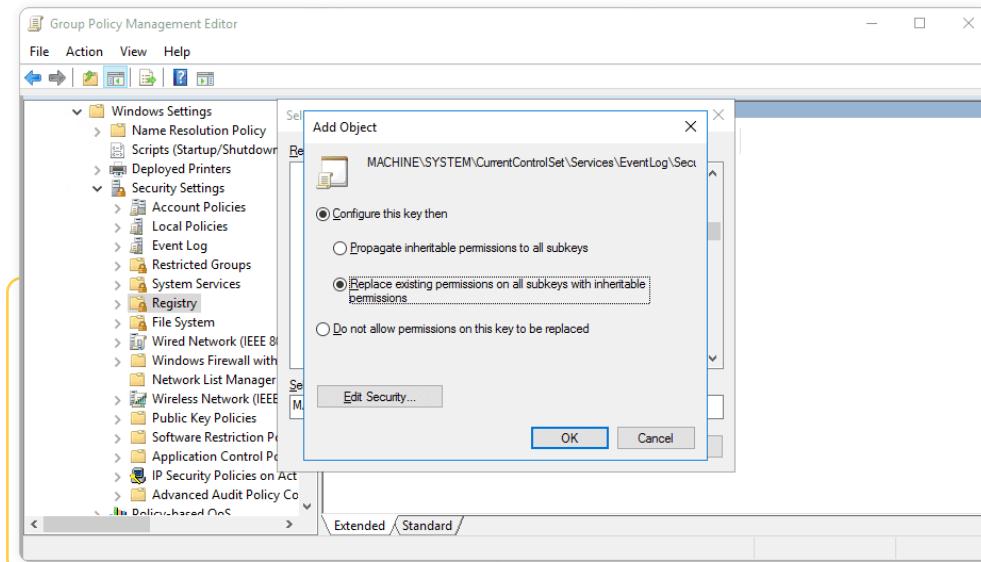
Power Users: Members of this group can discover shares residing on Windows file servers.

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.

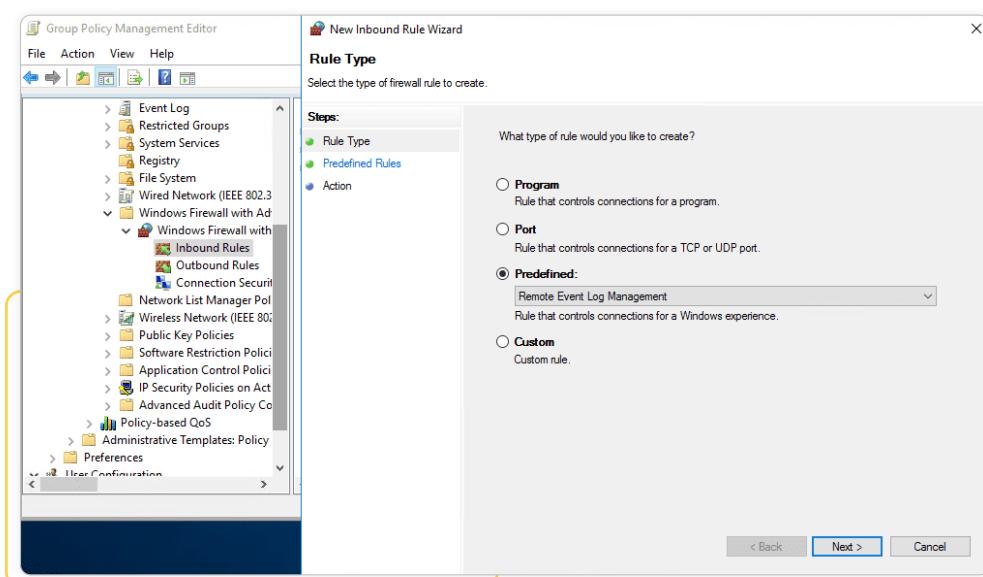
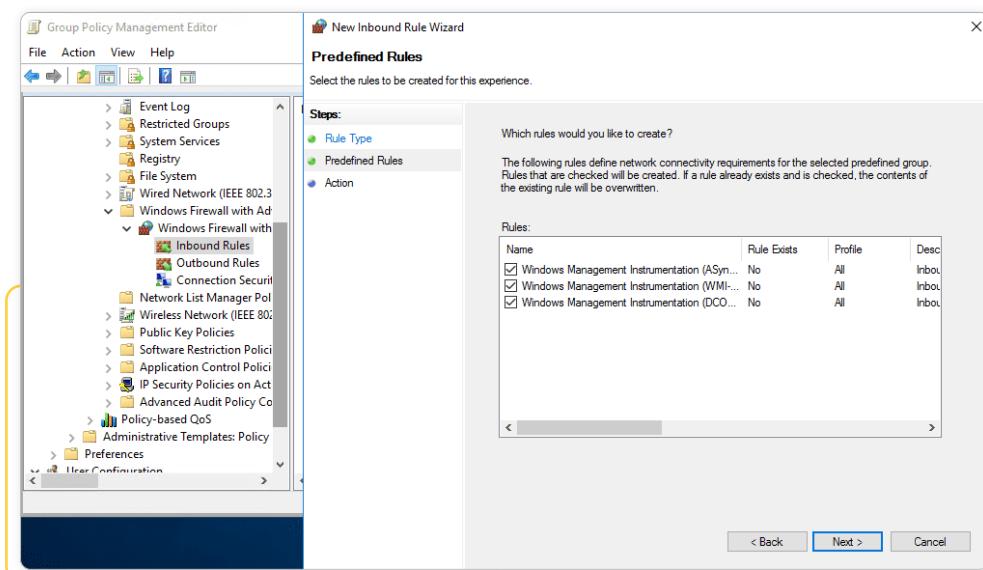
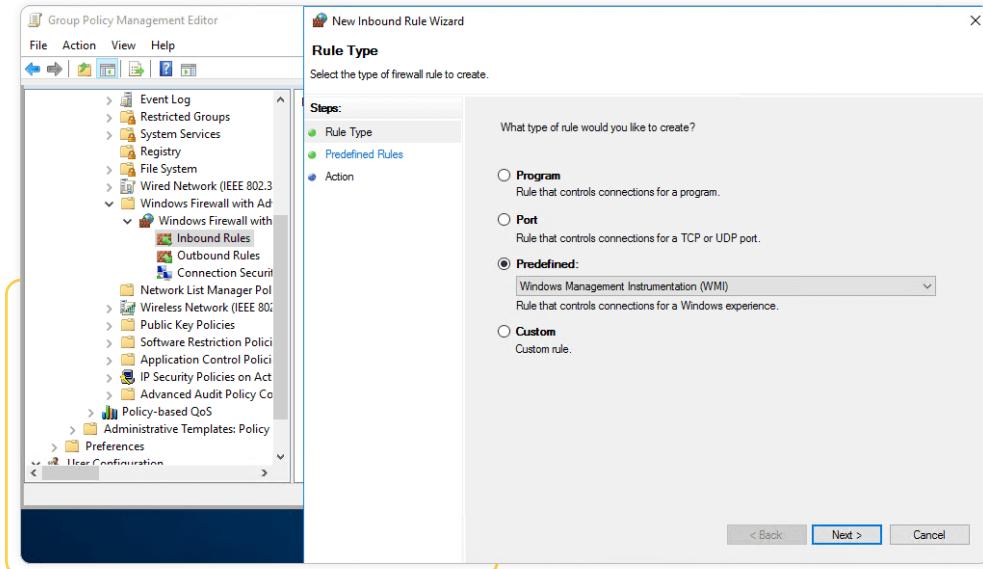
1. Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click "Log360PermissionGPO" → Edit.
2. In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Right-click Registry → Add Key.
3. 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.

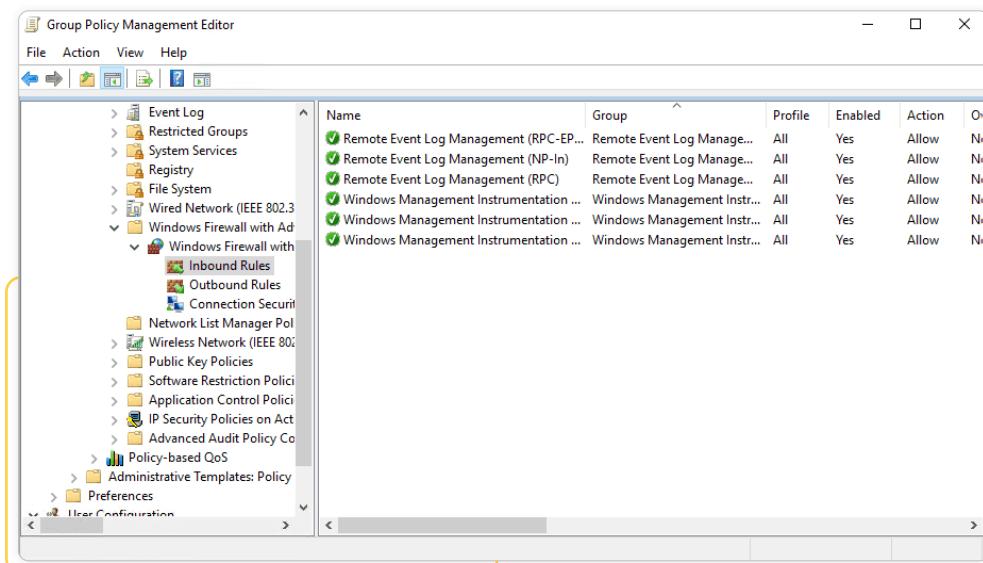
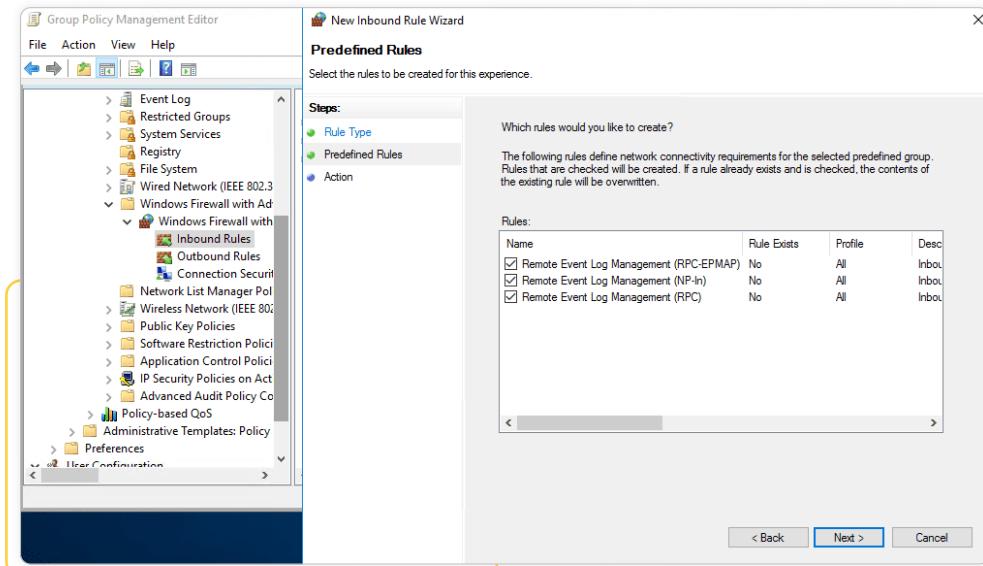




Enable WMI and Remote Event Log Management traffic through Firewall:

1. 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.





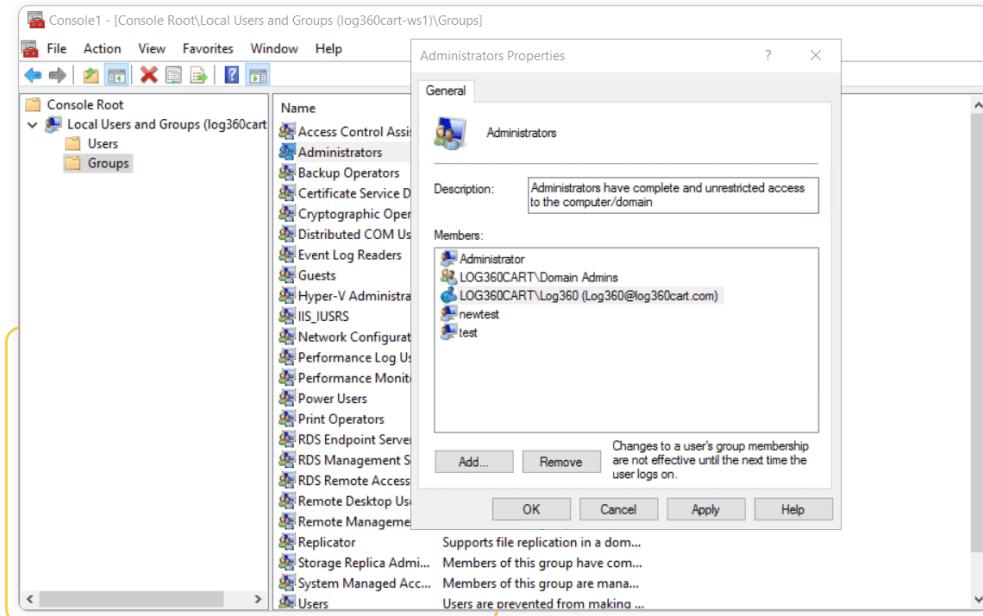
Note:

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

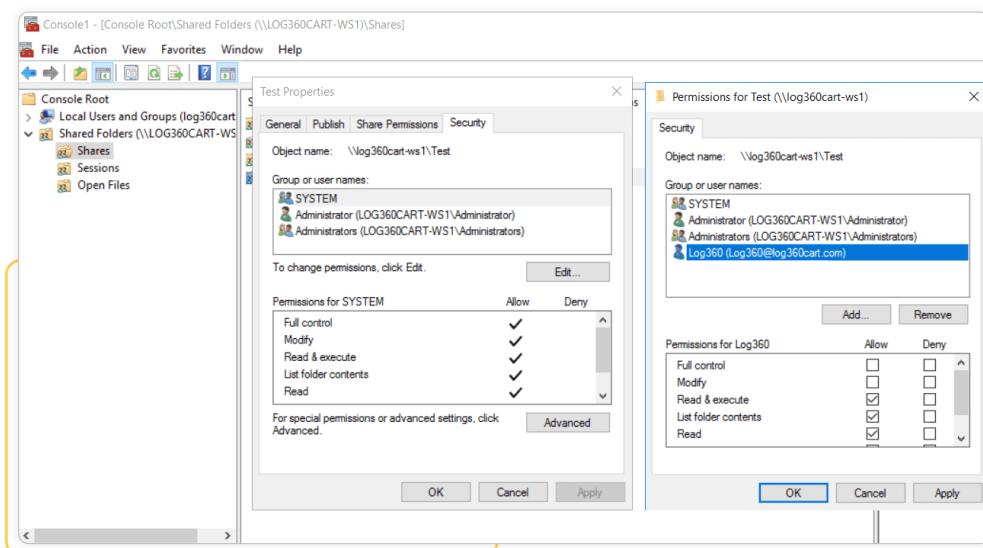
There are two ways to grant the user Read permission on all the audited shares:

- **Make the user a Member of the Local Administrators group.**
 1. 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.



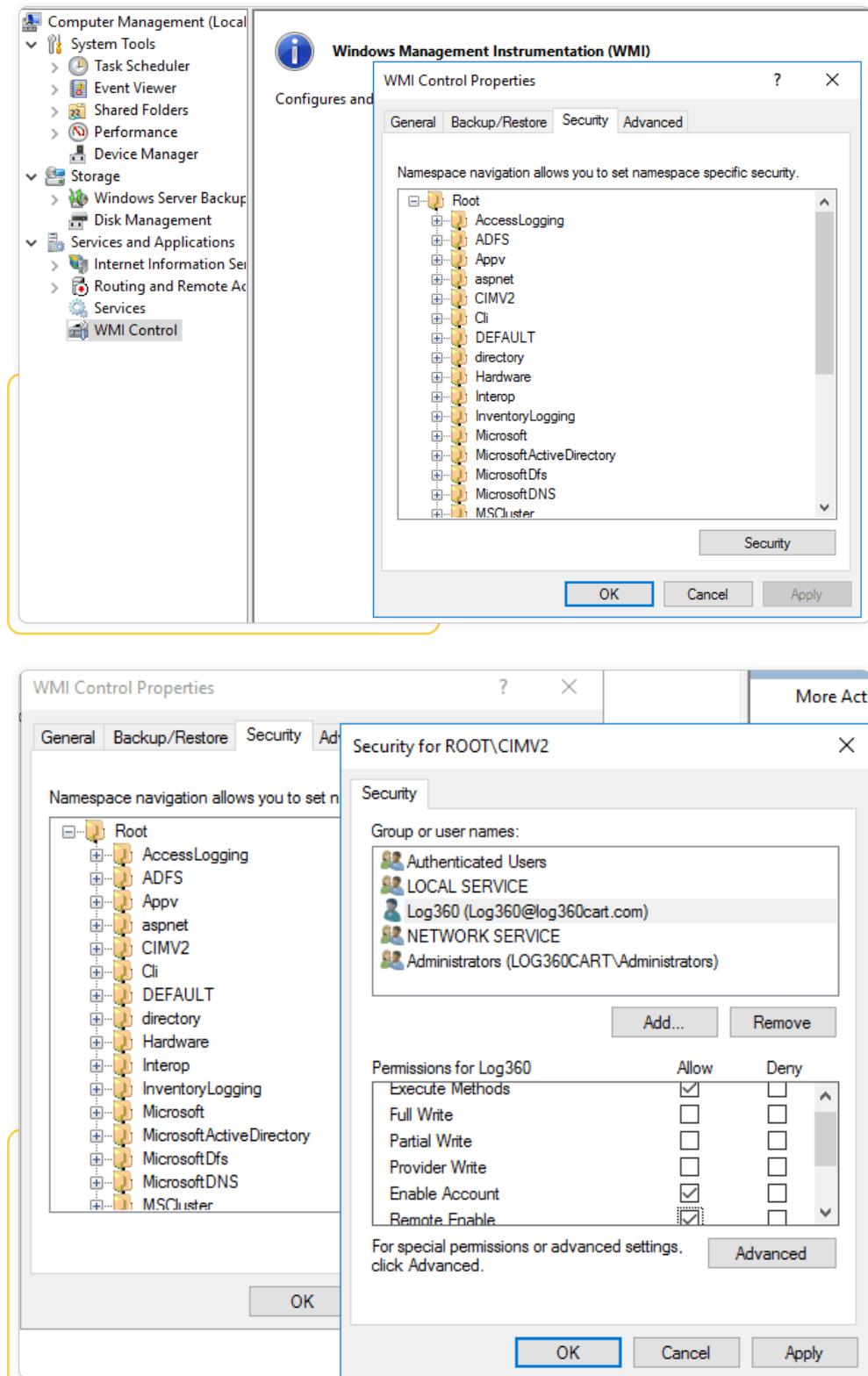
- Grant the user both Share and NTFS Read permission on every audited share.

1. 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 → Select share → Right-click → Properties → Security → Edit → Add the “Log360” user → Provide both Share and NTFS, Read permission.
3. Repeat the above steps for every audited share.

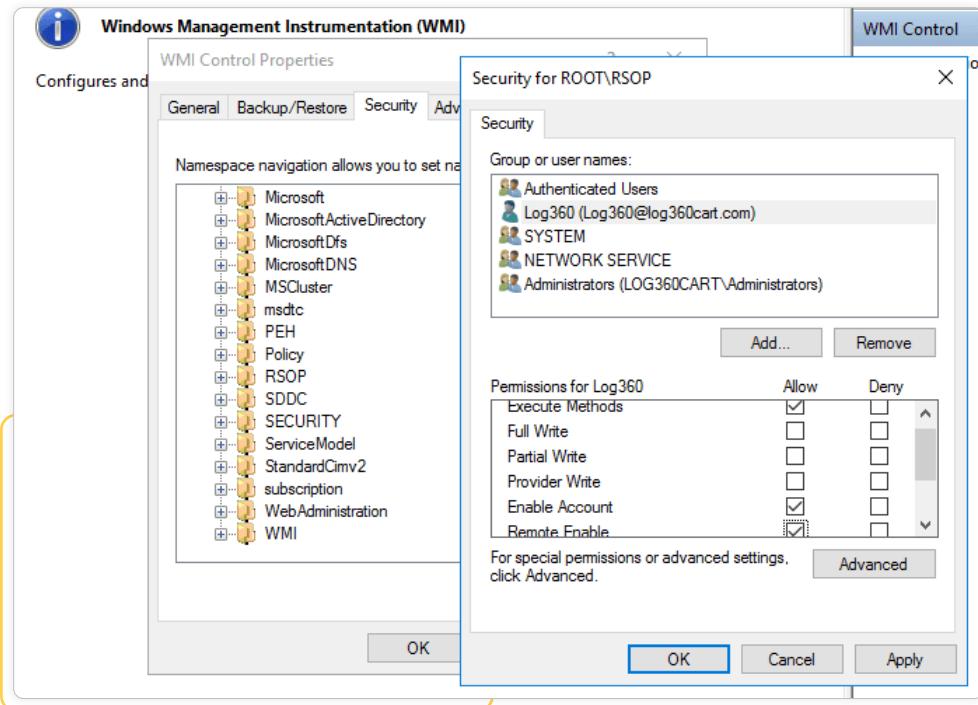


Granting WMI permission:

1. Log in to any computer with domain admin privileges → Run `wmimgmt.msc` → Right-click on WMI Control (Local) → Connect to target computer.
2. 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

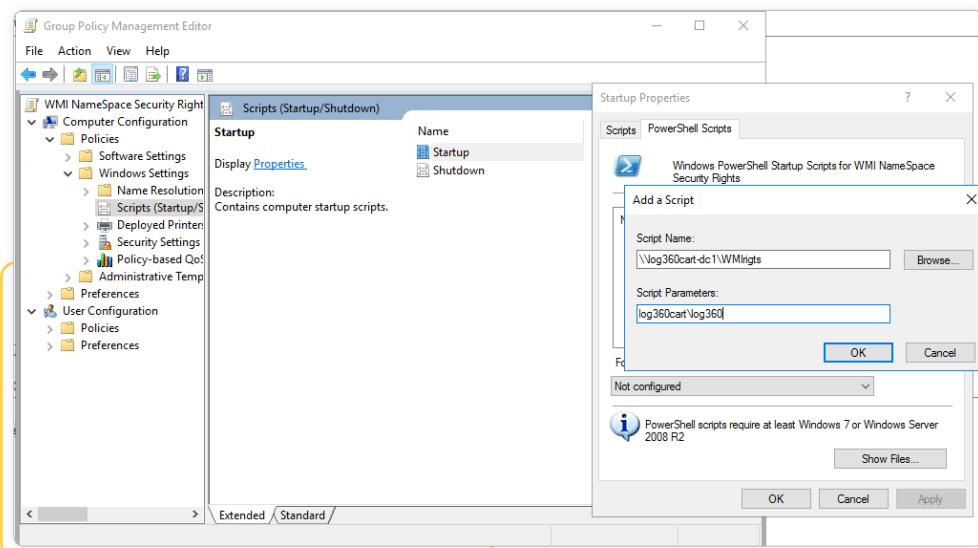


5. Click OK.
6. Repeat the steps for every audited computer.

Grant WMI Namespace Security Rights using GPO (PowerShell script)

[Script download link](#)

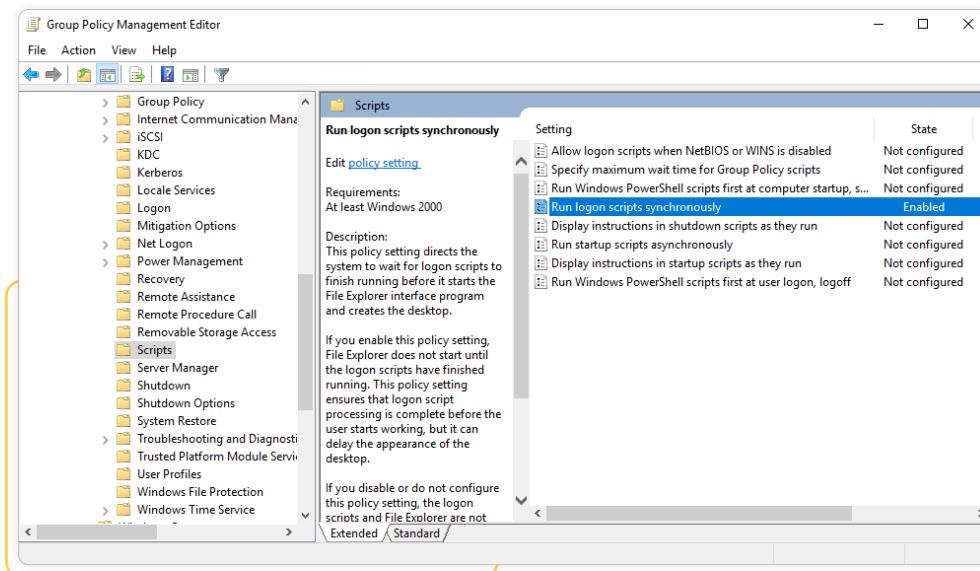
1. Add the script WMIRights.ps1 file in the shared location in the domain.
2. Create a new GPO WMI NameSpace Security Rights and Right-click → Edit.
3. Navigate to Computer Configuration → Policies → Windows Settings → Scripts → Startup → Right-click and open Properties → PowerShell Scripts → Add.
4. 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”.



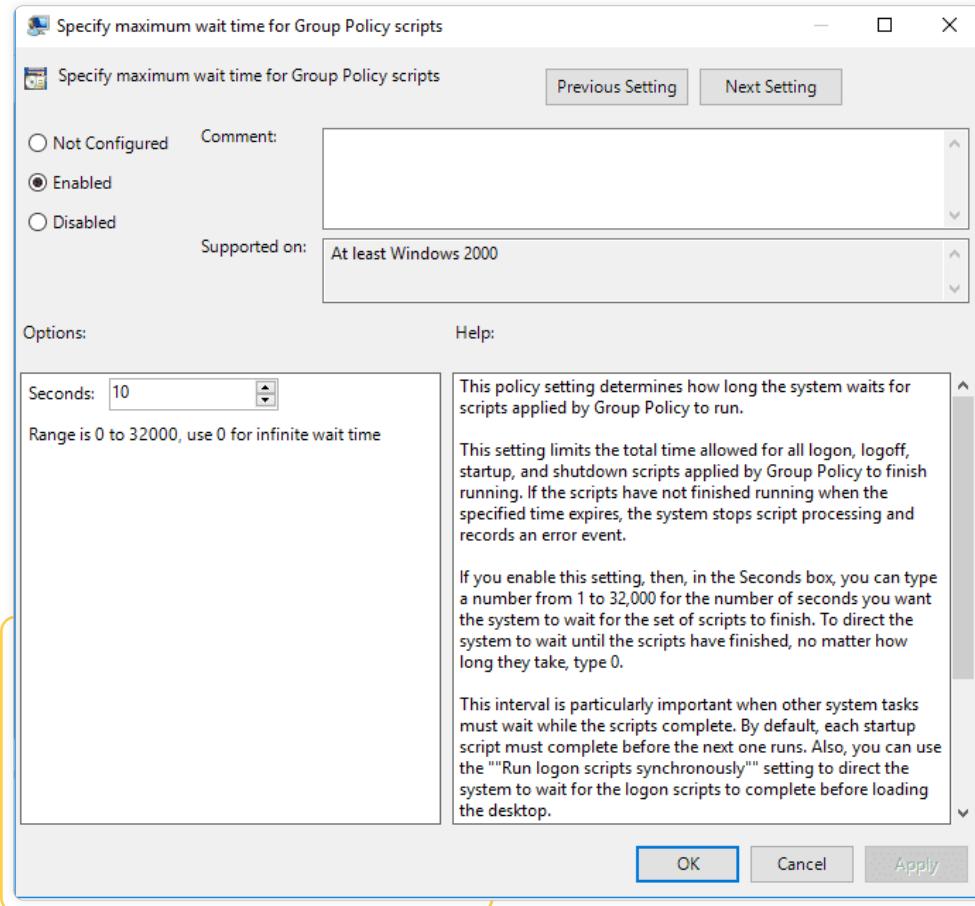
5. Click OK to return to the Startup Properties dialog box → Apply → OK

Configuring Administrative Template Settings

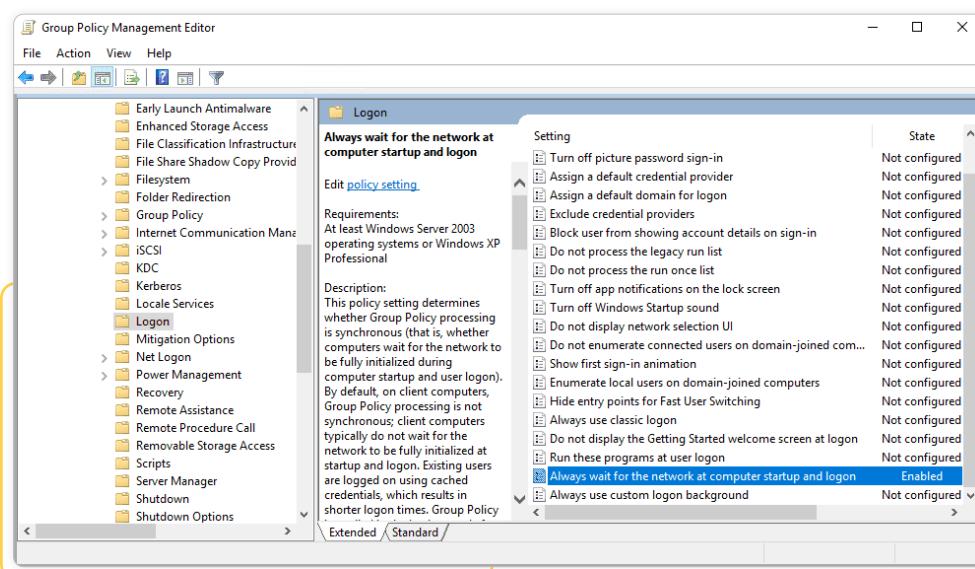
1. On the left pane of the Group Policy Management Editor, navigate to Computer Configuration Administrator Templates System.
2. Under System, select Scripts.
3. On the right pane of the GPO Editor, double-click Run logon scripts synchronously, and enable it → Apply → OK.



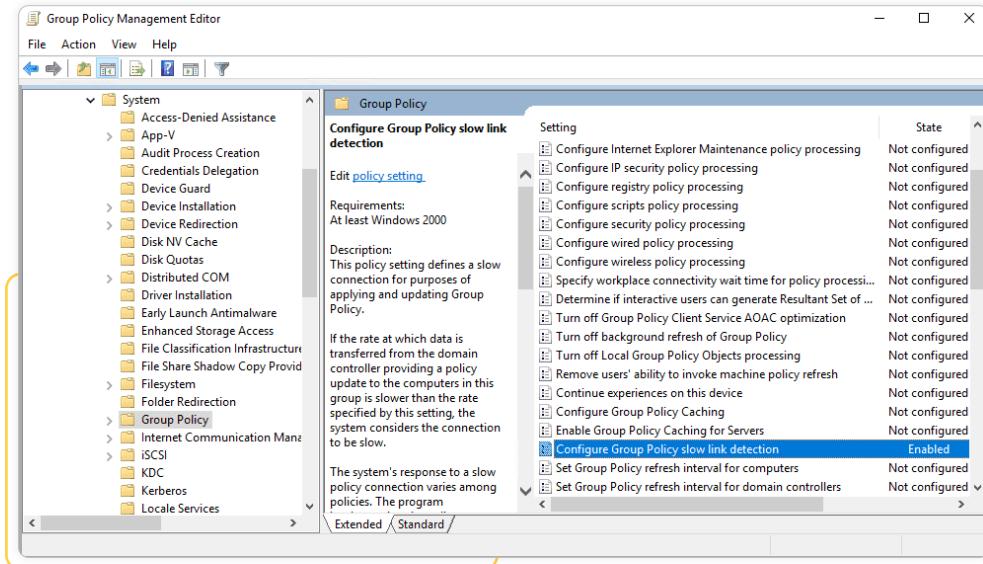
4. Enable Maximum wait time for Group Policy scripts and set the maximum time at 10 seconds.



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

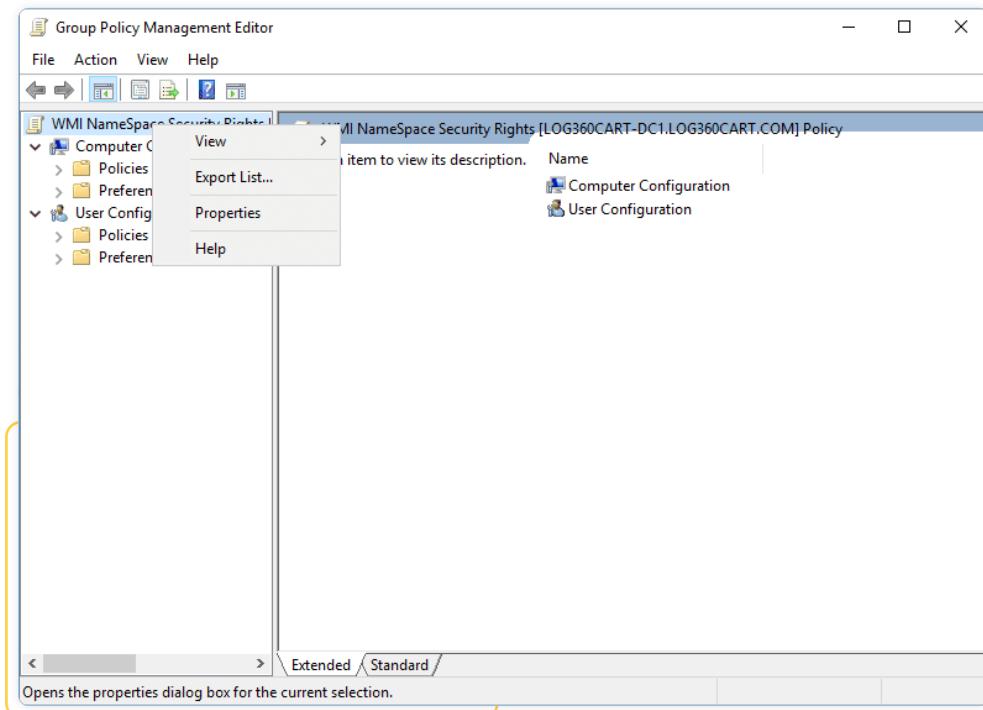


6. Navigate to Group Policy under System, on the right pane double-click Configure Group Policy slow link detection, and enable it → Apply → OK.

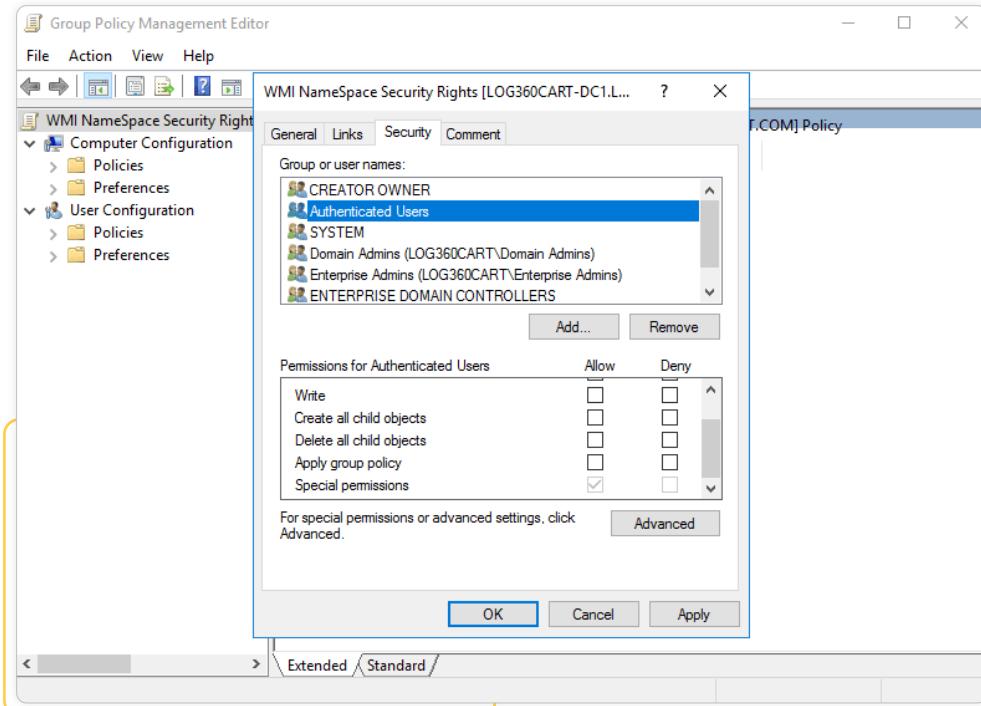


Apply the GPO

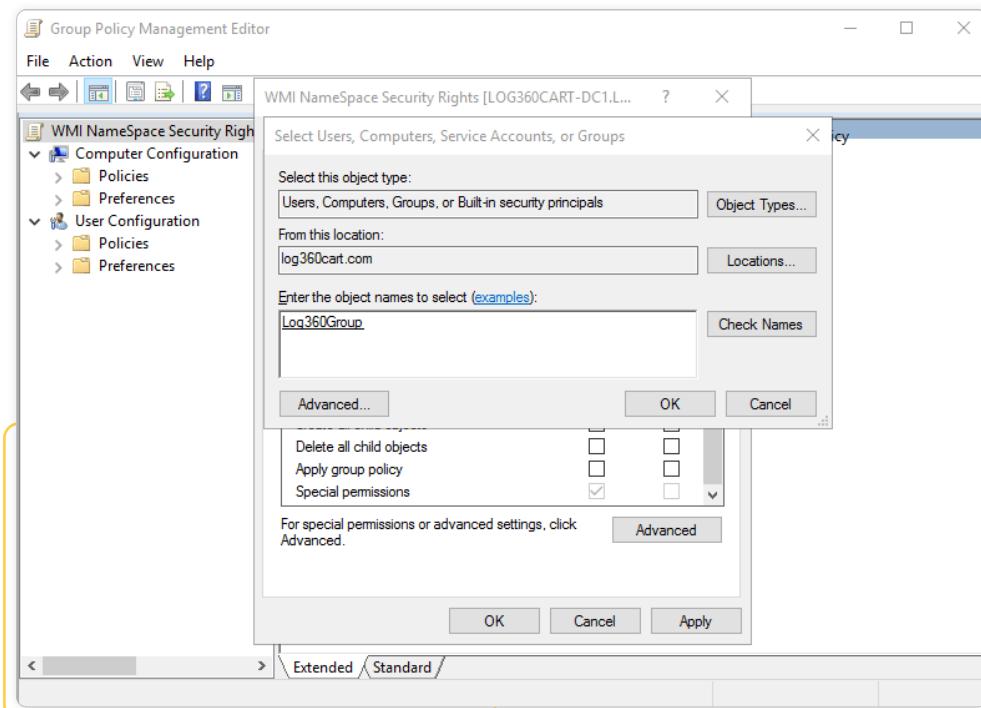
1. On the left pane of the Group Policy Management Editor, right-click the required GPO → Properties.



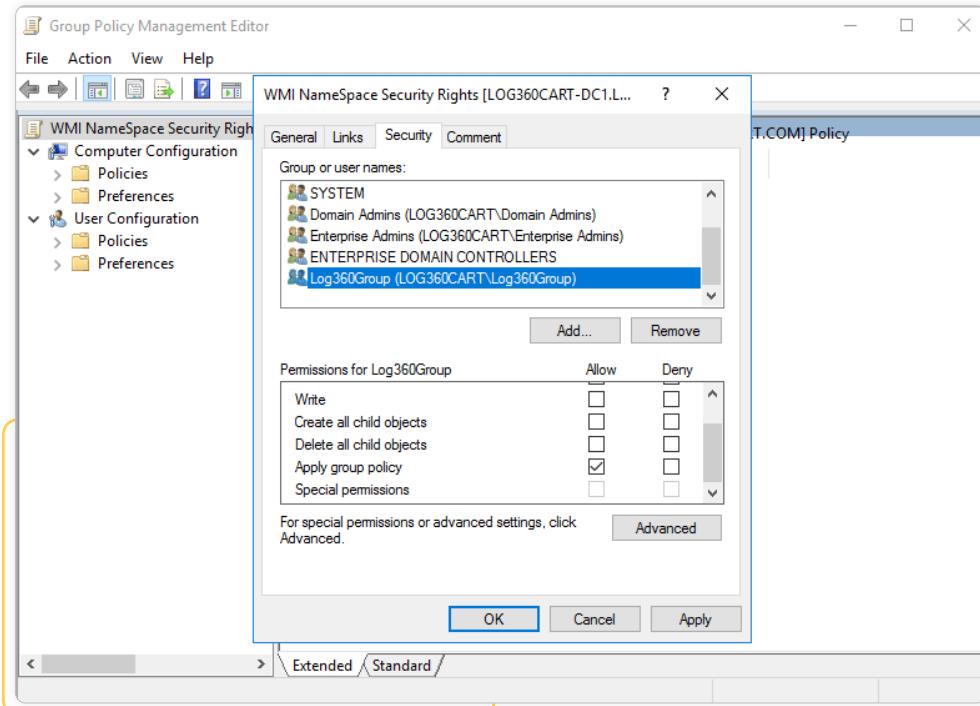
2. Navigate to the Security tab and unselect the "Apply Group Policy" permissions for Authenticated Users → Add.



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.



6. In the Security tab, grant “Apply group policy” permissions to the selected computers and groups
→ Apply → OK.



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

```
C:\Users\Administrator>gpupdate/force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Note:

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

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

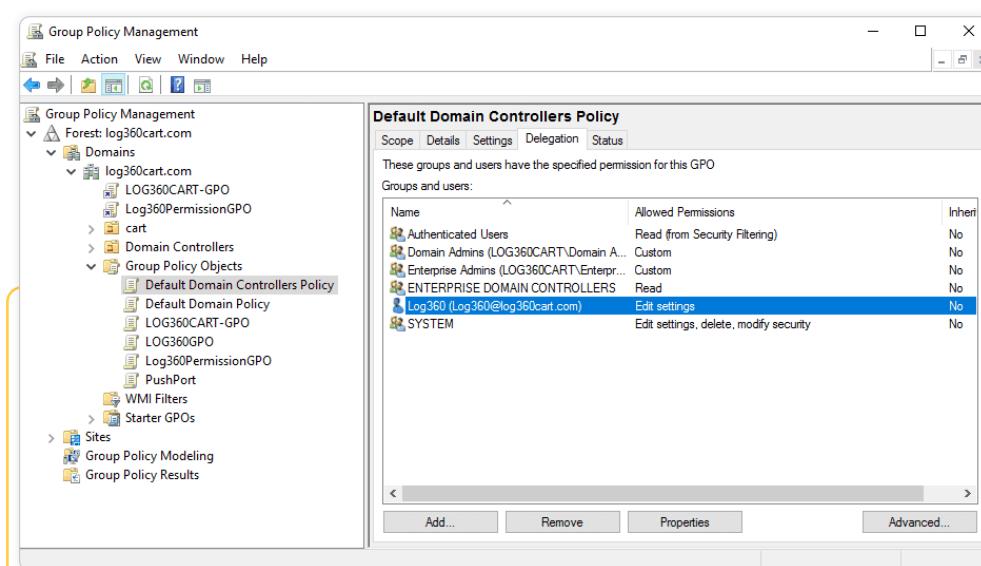
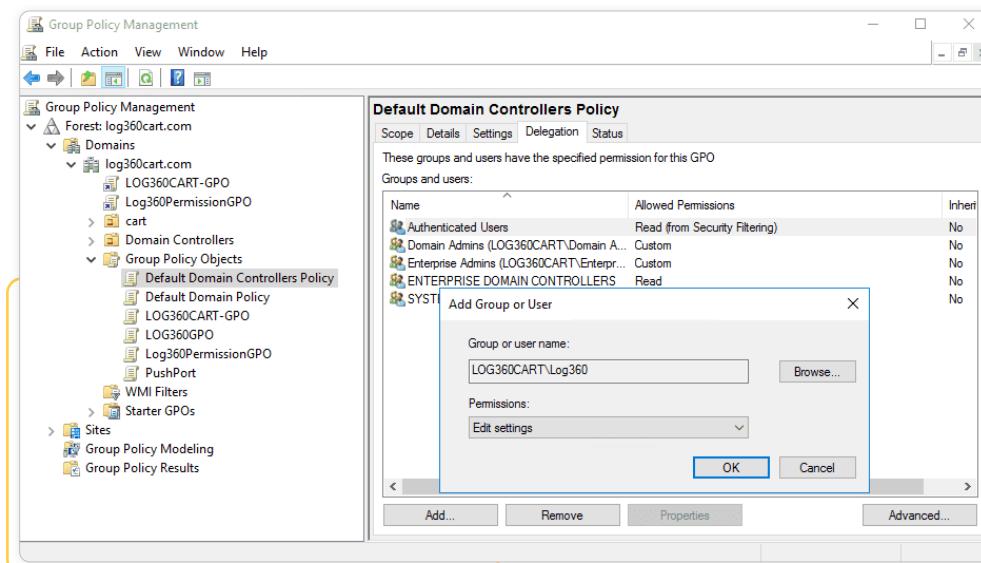
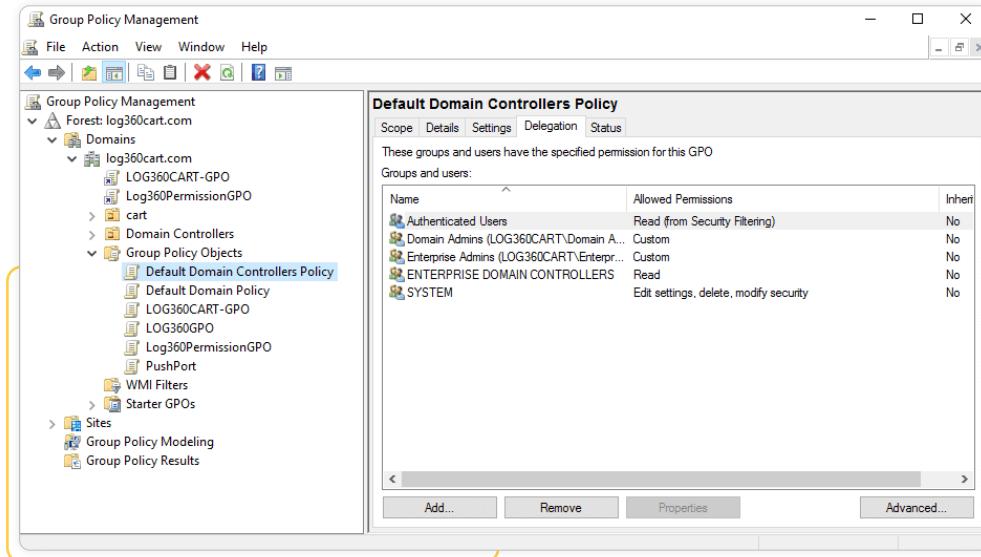
Read permission over C\$ share (\server_name\C\$) is needed to access NetApp C-Mode log files.

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.

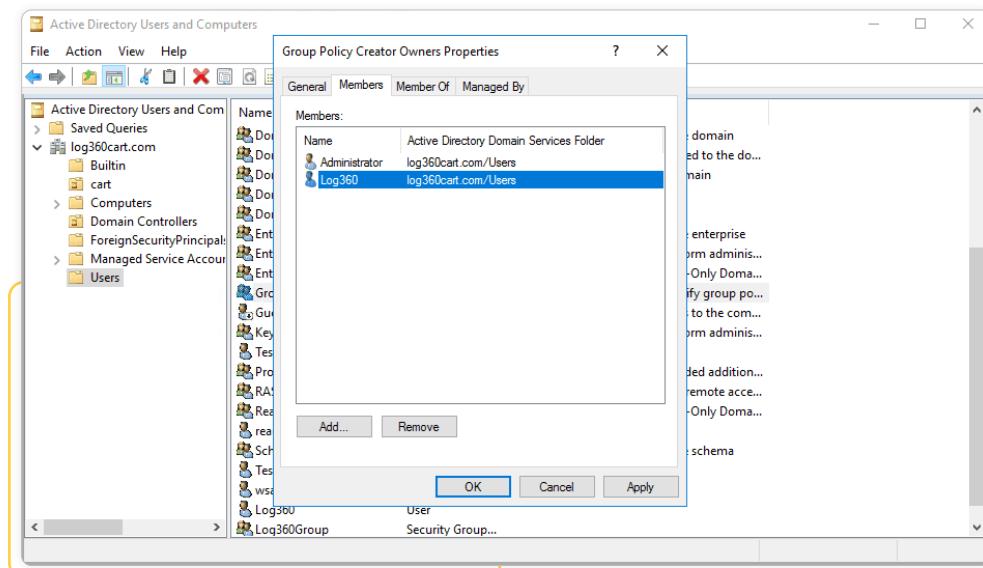
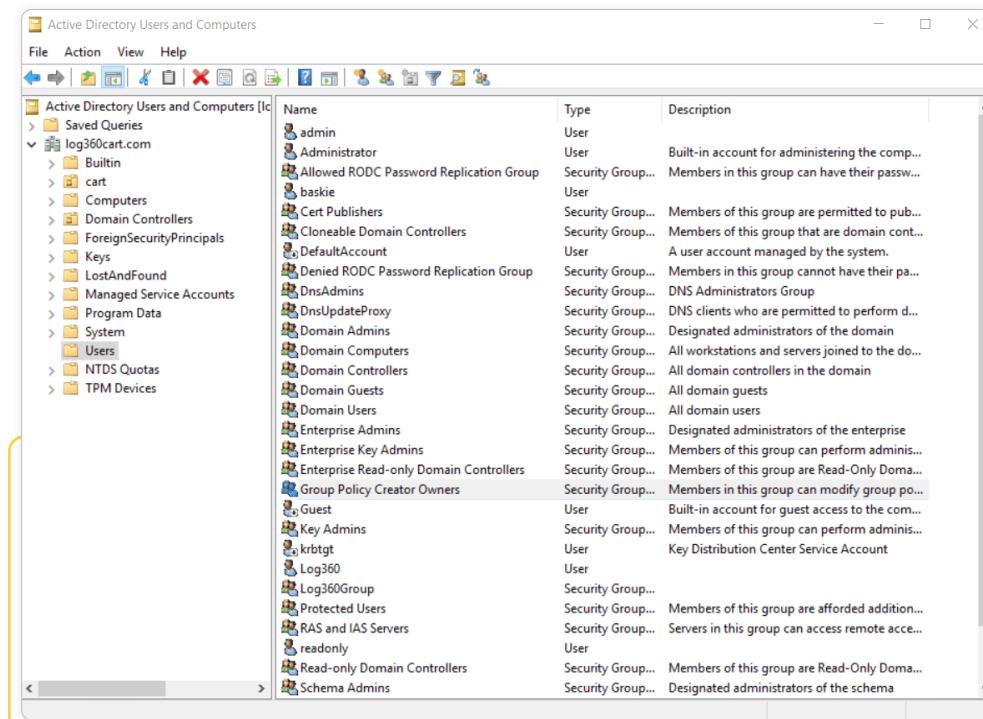
- Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → click Default domain controllers Policy → Navigate to the right panel, click the Delegation tab → Add the Log360 User → Provide permission to Edit settings.



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.

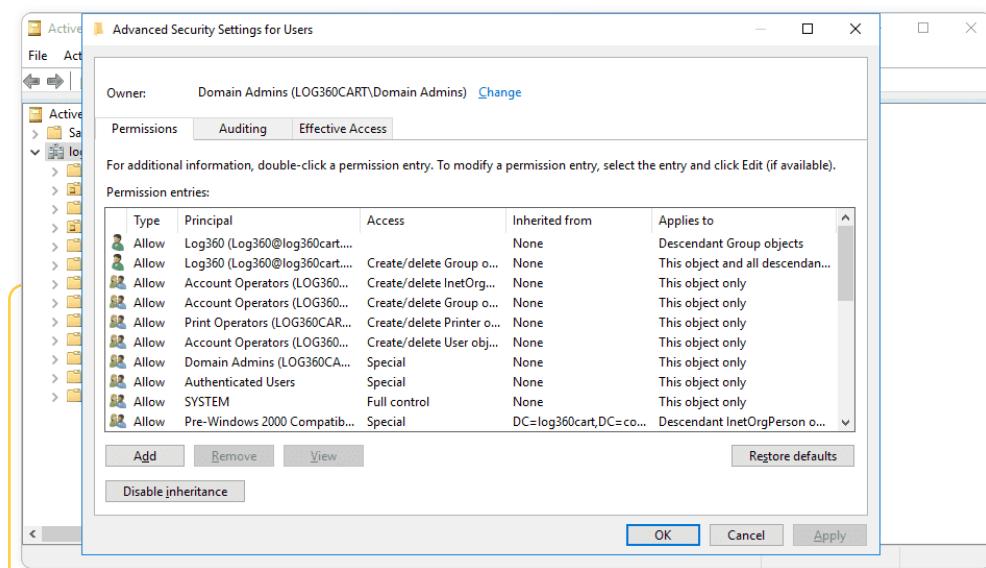
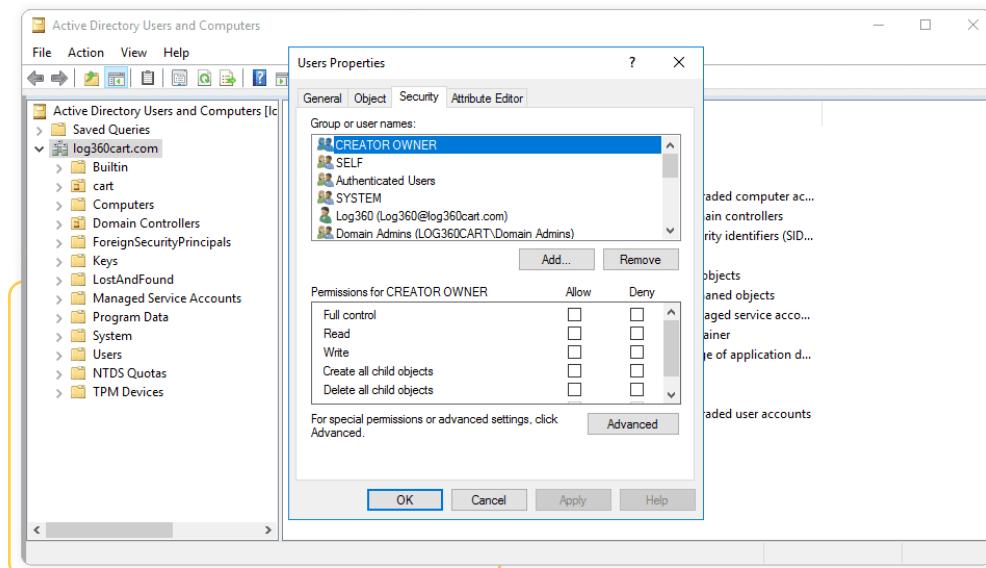


Grant the user, group management permissions

1. 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.
2. 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.



Permission Entry for Users

Principal: [Select a principal](#)

Type: [Allow](#)

Applies to: [This object and all descendant objects](#)

Permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Create msDS-ManagedServiceAccount objects
<input checked="" type="checkbox"/> List contents	<input type="checkbox"/> Delete msDS-ManagedServiceAccount objects
<input checked="" type="checkbox"/> Read all properties	<input type="checkbox"/> Create msDS-PasswordSettingsContainer objects
<input type="checkbox"/> Write all properties	<input type="checkbox"/> Delete msDS-PasswordSettingsContainer objects
<input type="checkbox"/> Delete	<input type="checkbox"/> Create msDS-ResourceProperties objects
<input type="checkbox"/> Delete subtree	<input type="checkbox"/> Delete msDS-ResourceProperties objects
<input checked="" type="checkbox"/> Read permissions	<input type="checkbox"/> Create msDS-ResourcePropertyList objects
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Delete msDS-ResourcePropertyList objects
<input type="checkbox"/> Modify owner	<input type="checkbox"/> Create msDS-ShadowPrincipalContainer objects
<input type="checkbox"/> All validated writes	<input type="checkbox"/> Delete msDS-ShadowPrincipalContainer objects
<input type="checkbox"/> Create all child objects	<input type="checkbox"/> Create msDS-ValueType objects
<input type="checkbox"/> Delete all child objects	<input type="checkbox"/> Delete msDS-ValueType objects
<input type="checkbox"/> Create account objects	<input type="checkbox"/> Create msieee80211-Policy objects
<input type="checkbox"/> Delete account objects	<input type="checkbox"/> Delete msieee80211-Policy objects
<input type="checkbox"/> Create aCSResourceLimits objects	<input type="checkbox"/> Create msImaging-PSPs objects
<input type="checkbox"/> Delete aCSResourceLimits objects	<input type="checkbox"/> Delete msImaging-PSPs objects

[OK](#) [Cancel](#)

Permission Entry for Users

Principal: [Log360 \(Log360@log360cart.com\) Select a principal](#)

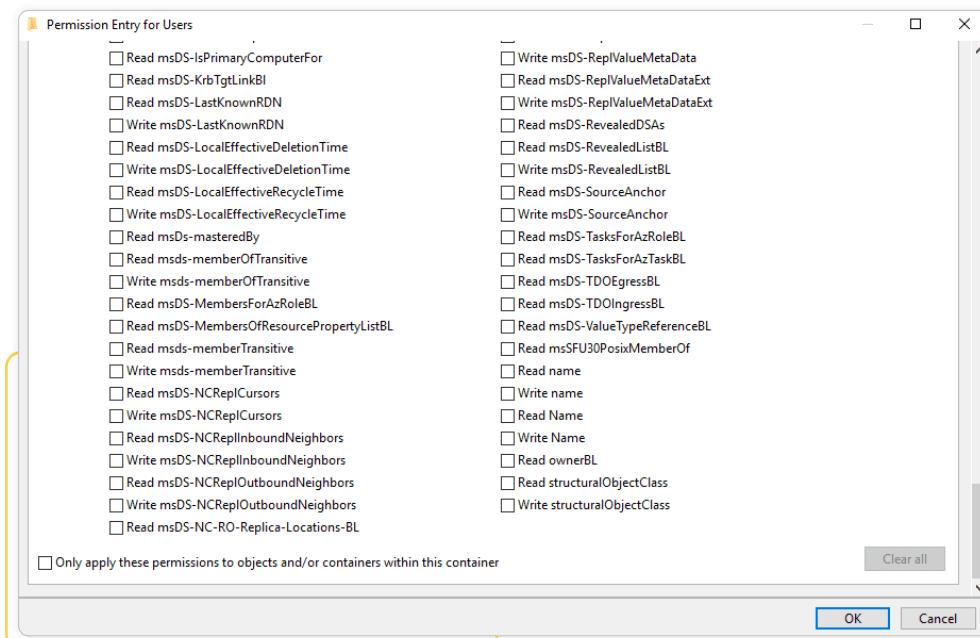
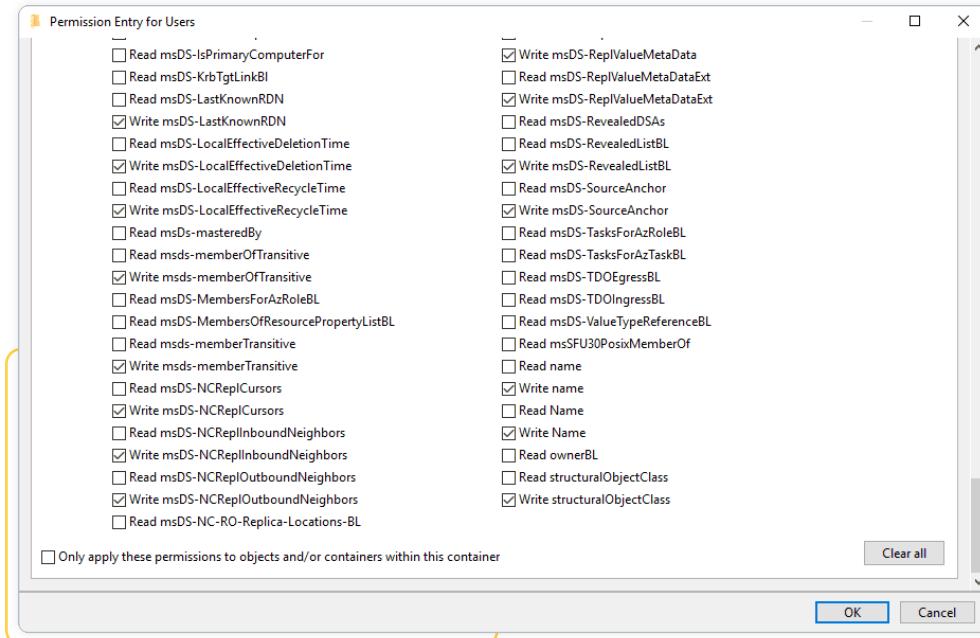
Type: [Allow](#)

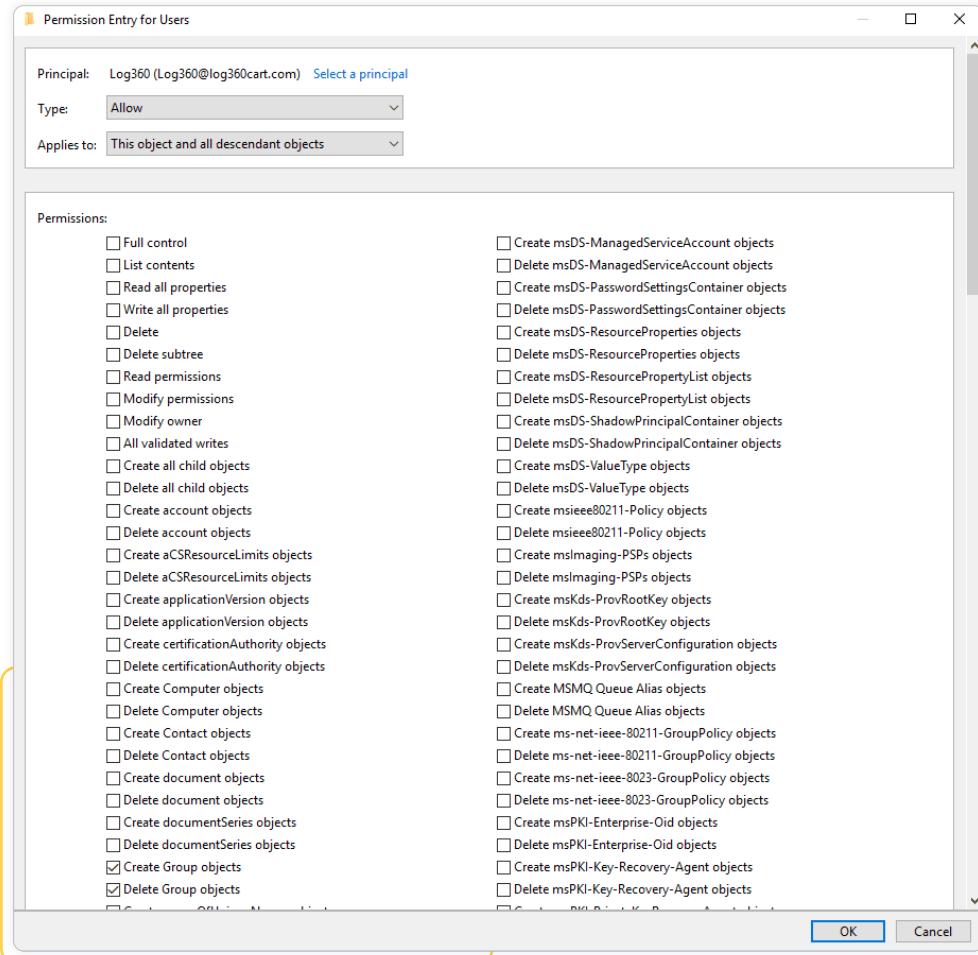
Applies to: [This object and all descendant objects](#)

Permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Create msDS-ManagedServiceAccount objects
<input checked="" type="checkbox"/> List contents	<input type="checkbox"/> Delete msDS-ManagedServiceAccount objects
<input checked="" type="checkbox"/> Read all properties	<input type="checkbox"/> Create msDS-PasswordSettingsContainer objects
<input type="checkbox"/> Write all properties	<input type="checkbox"/> Delete msDS-PasswordSettingsContainer objects
<input type="checkbox"/> Delete	<input type="checkbox"/> Create msDS-ResourceProperties objects
<input type="checkbox"/> Delete subtree	<input type="checkbox"/> Delete msDS-ResourceProperties objects
<input checked="" type="checkbox"/> Read permissions	<input type="checkbox"/> Create msDS-ResourcePropertyList objects
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Delete msDS-ResourcePropertyList objects
<input type="checkbox"/> Modify owner	<input type="checkbox"/> Create msDS-ShadowPrincipalContainer objects
<input type="checkbox"/> All validated writes	<input type="checkbox"/> Delete msDS-ShadowPrincipalContainer objects
<input type="checkbox"/> Create all child objects	<input type="checkbox"/> Create msDS-ValueType objects
<input type="checkbox"/> Delete all child objects	<input type="checkbox"/> Delete msDS-ValueType objects
<input type="checkbox"/> Create account objects	<input type="checkbox"/> Create msieee80211-Policy objects
<input type="checkbox"/> Delete account objects	<input type="checkbox"/> Delete msieee80211-Policy objects
<input type="checkbox"/> Create aCSResourceLimits objects	<input type="checkbox"/> Create msImaging-PSPs objects
<input type="checkbox"/> Delete aCSResourceLimits objects	<input type="checkbox"/> Delete msImaging-PSPs objects

[OK](#) [Cancel](#)

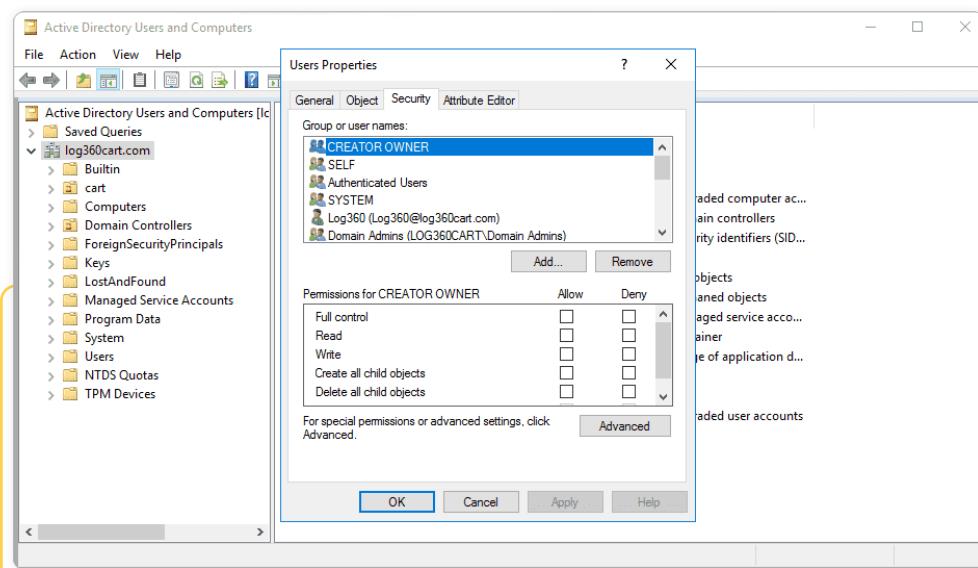




3. From the Active Directory User and Computers console → Right-click Users → Properties → Security → Advanced → Permissions → Add → In the Permission Entry for Users window → Select a principal: Log360 user → Type: Allow → Applies to: Descendant Group objects → Select property: Write Members.

Note:

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



Advanced Security Settings for Users

Owner: Domain Admins (LOG360CART\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Log360 (Log360@log360cart....)	None	None	Descendant Group objects
Allow	Log360 (Log360@log360cart....)	Create/delete Group o...	None	This object and all descendant...
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...

Add Remove View Restore defaults

Disable inheritance

OK Cancel Apply

Permission Entry for Users

Principal: [Select a principal](#)

Type: Allow

Applies to: This object and all descendant objects

Permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Create msDS-ManagedServiceAccount objects
<input checked="" type="checkbox"/> List contents	<input type="checkbox"/> Delete msDS-ManagedServiceAccount objects
<input checked="" type="checkbox"/> Read all properties	<input type="checkbox"/> Create msDS-PasswordSettingsContainer objects
<input type="checkbox"/> Write all properties	<input type="checkbox"/> Delete msDS-PasswordSettingsContainer objects
<input type="checkbox"/> Delete	<input type="checkbox"/> Create msDS-ResourceProperties objects
<input type="checkbox"/> Delete subtree	<input type="checkbox"/> Delete msDS-ResourceProperties objects
<input checked="" type="checkbox"/> Read permissions	<input type="checkbox"/> Create msDS-ResourcePropertyList objects
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Delete msDS-ResourcePropertyList objects
<input type="checkbox"/> Modify owner	<input type="checkbox"/> Create msDS-ShadowPrincipalContainer objects
<input type="checkbox"/> All validated writes	<input type="checkbox"/> Delete msDS-ShadowPrincipalContainer objects
<input type="checkbox"/> Create all child objects	<input type="checkbox"/> Create msDS-ValueType objects
<input type="checkbox"/> Delete all child objects	<input type="checkbox"/> Delete msDS-ValueType objects
<input type="checkbox"/> Create account objects	<input type="checkbox"/> Create msieee80211-Policy objects
<input type="checkbox"/> Delete account objects	<input type="checkbox"/> Delete msieee80211-Policy objects
<input type="checkbox"/> Create aCSResourceLimits objects	<input type="checkbox"/> Create msImaging-PSPs objects
<input type="checkbox"/> Delete aCSResourceLimits objects	<input type="checkbox"/> Delete msImaging-PSPs objects

OK Cancel

Permission Entry for Users

Principal: Log360 (Log360@log360cart.com) [Select a principal](#)

Type: Allow

Applies to: Descendant Group objects

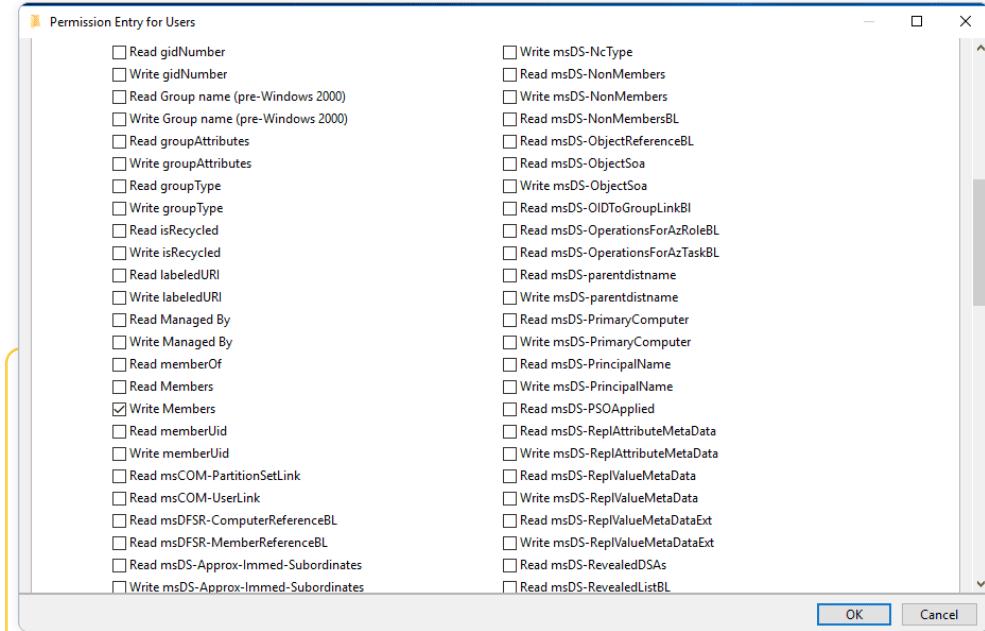
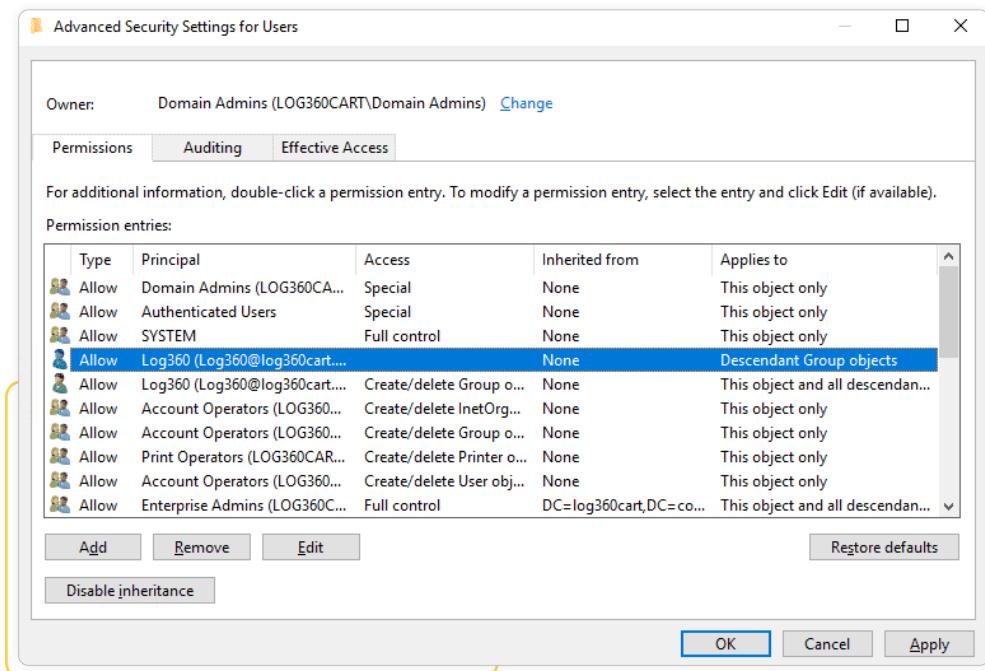
Permissions:

<input type="checkbox"/> Modify owner
<input type="checkbox"/> All validated writes
<input type="checkbox"/> All extended rights
<input type="checkbox"/> Create all child objects
<input type="checkbox"/> Delete all child objects
<input type="checkbox"/> Add/remove self as member
<input type="checkbox"/> Send to

Properties:

<input type="checkbox"/> Read msDS-NCRepInboundNeighbors
<input type="checkbox"/> Write msDS-NCRepInboundNeighbors
<input type="checkbox"/> Read msDS-NCRepOutboundNeighbors
<input type="checkbox"/> Write msDS-NCRepOutboundNeighbors
<input type="checkbox"/> Read msDS-NC-RO-Replica-Locations-BL
<input type="checkbox"/> Read msDS-NcType

OK Cancel

The 'Advanced Security Settings for Users' dialog box shows the following permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (LOG360CART\Domain Admins)	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Log360 (Log360@log360cart....)	None		Descendant Group objects
Allow	Log360 (Log360@log360cart....)	Create/delete Group o...	None	This object and all descendant...
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	Enterprise Admins (LOG360C...	Full control	DC=log360cart,DC=co...	This object and all descendant...

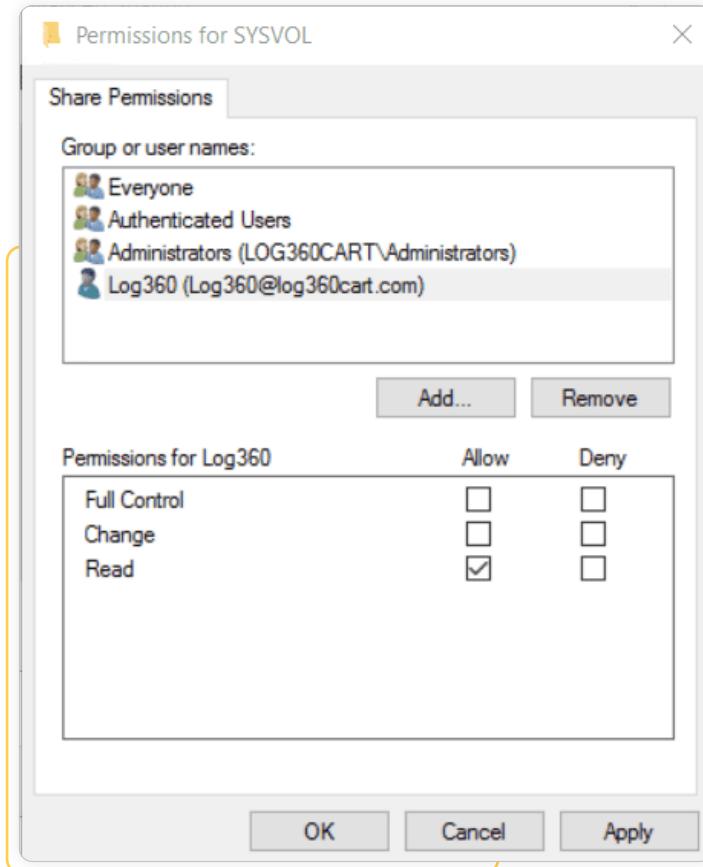
Grant the user Read permission over the SYSVOL folder

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) → Right-click → Properties → Sharing → Advanced sharing → Permissions → Add the "Log360" user → Provide Share Read permission.



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 → Admin → Archive Events → Scroll down to see the location.
- ADAudit Plus → Admin → Schedule Reports → Modify Schedule Report → Scroll down to see the location.
- ADAudit Plus → Configuration → Modify Alert Profile → Scroll down to see the location.
- M365 → Settings → Configuration → Audit Configuration → Archive Settings → 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 → Security → 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 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](#)