ManageEngine
Log360

Service account configuration for Log360

www.manageengine.com/log-management/

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.

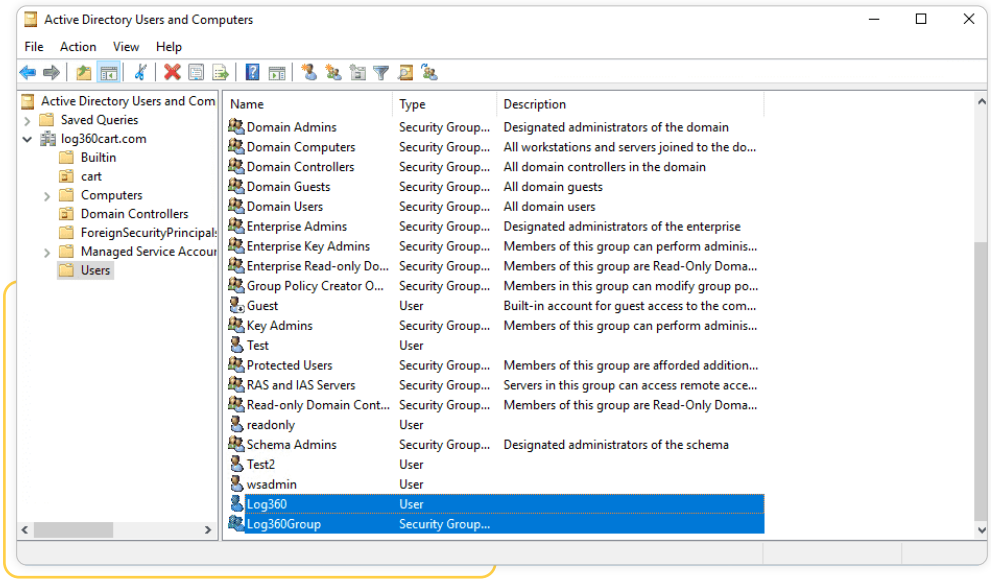
Note:

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.

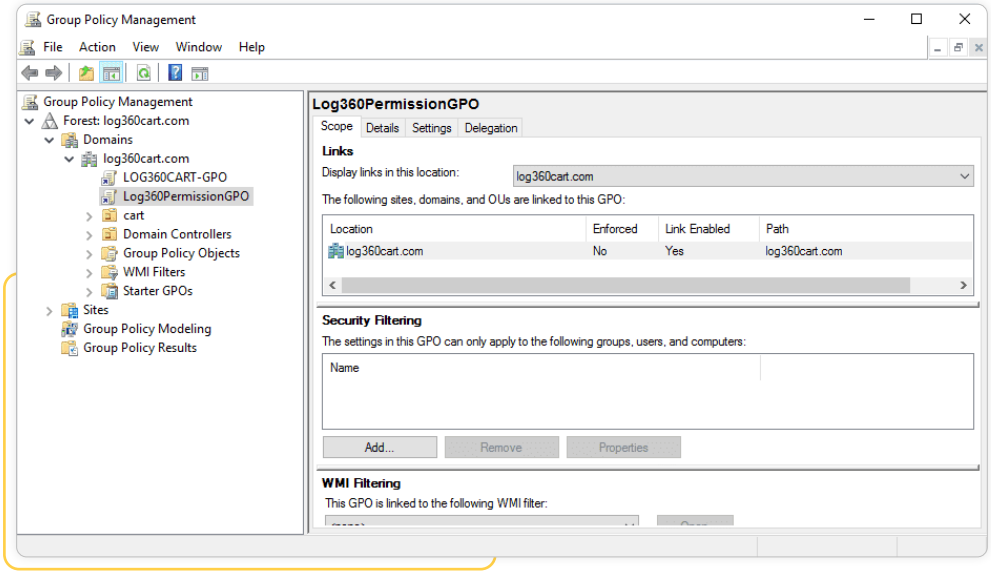


Create a new domain level GPO and link it to all the audited computers

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

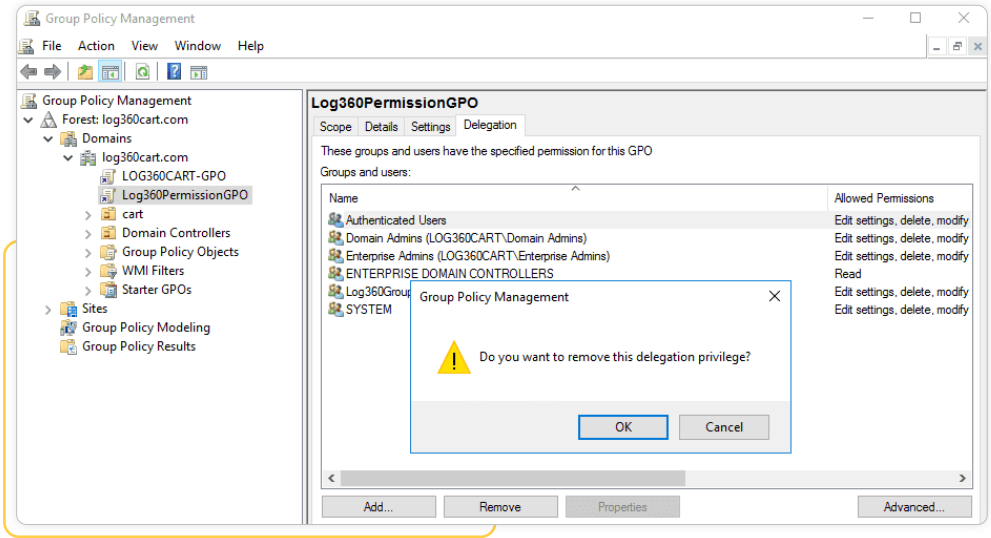
- Log in to your domain controller with domain admin privileges.
- **Create a new domain level GPO**

  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".

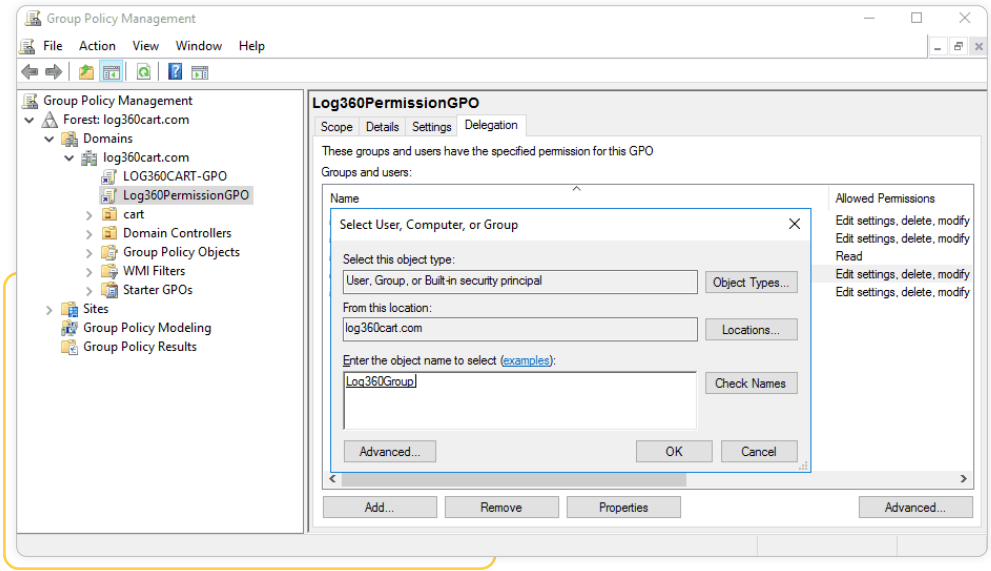


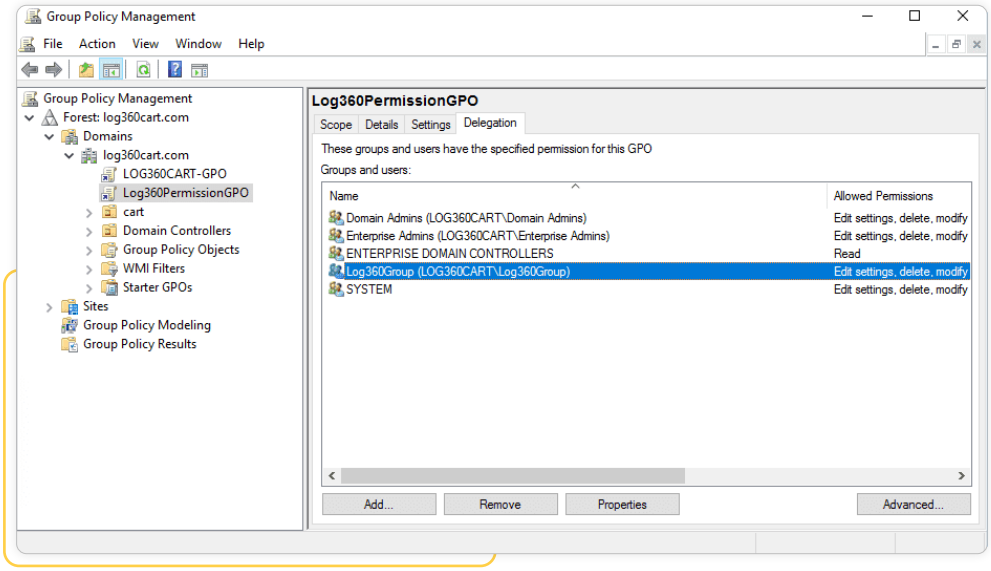
Remove Apply group policy permission for Authenticated Users group

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".



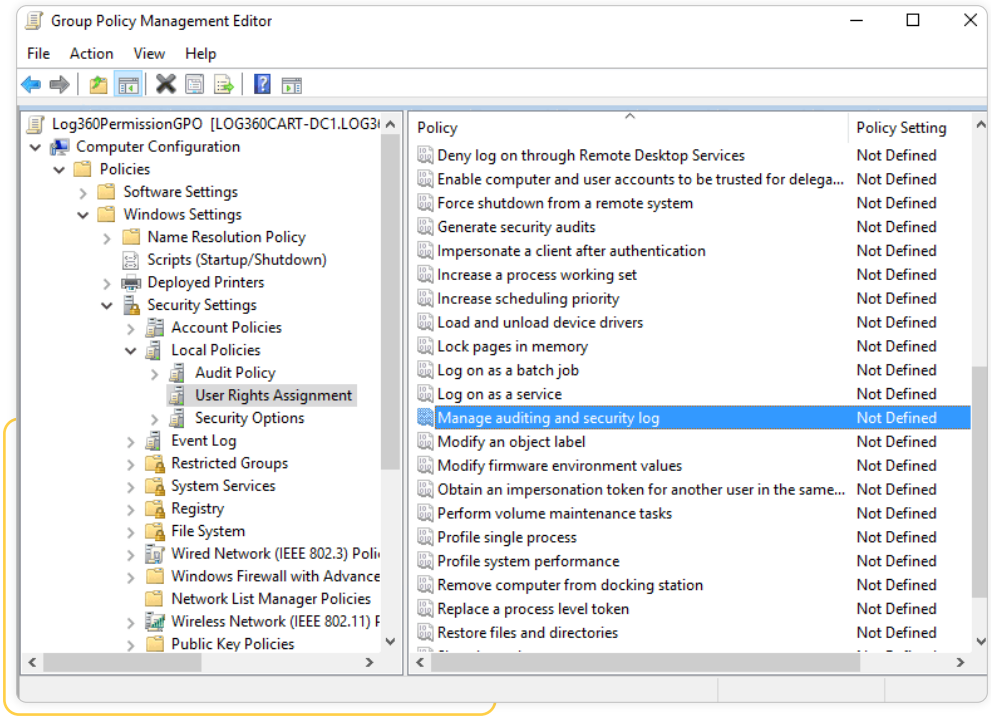


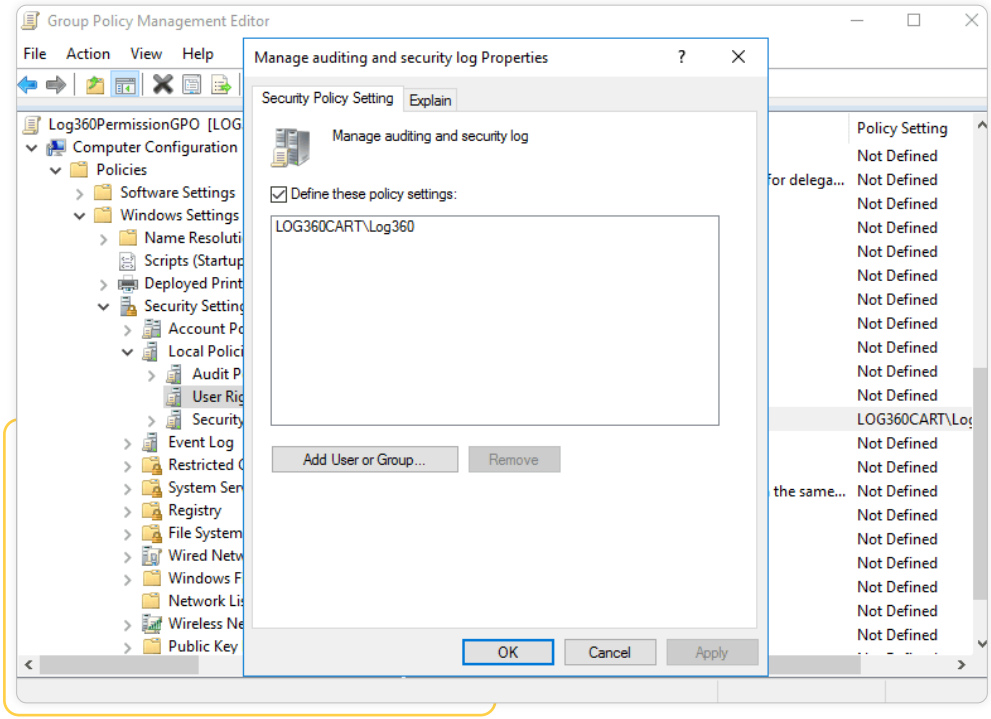
Privileges/permissions required for event log collection

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

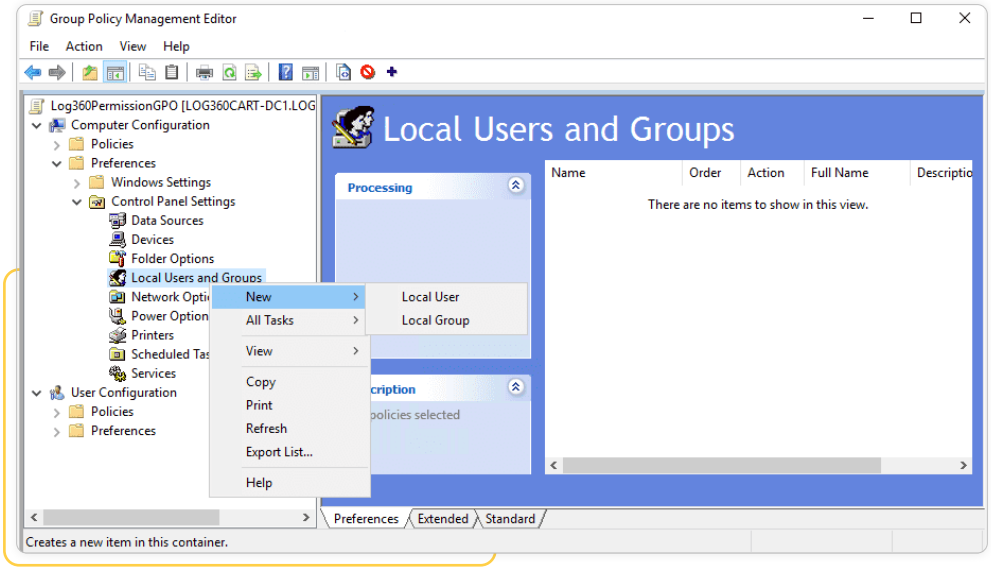
Members of the event log readers group will be able to read the event logs of all the audited computers.

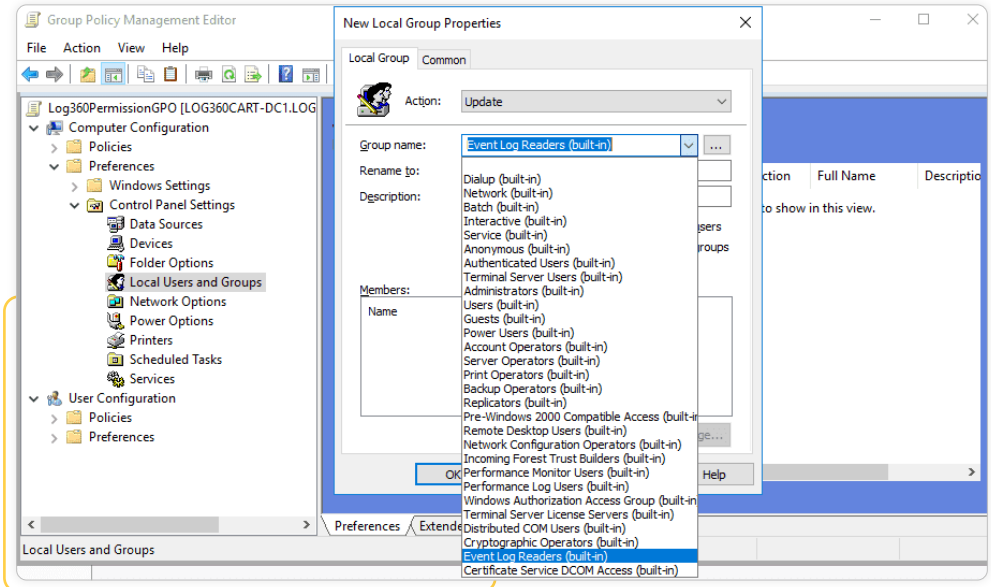
For Domain Controllers :

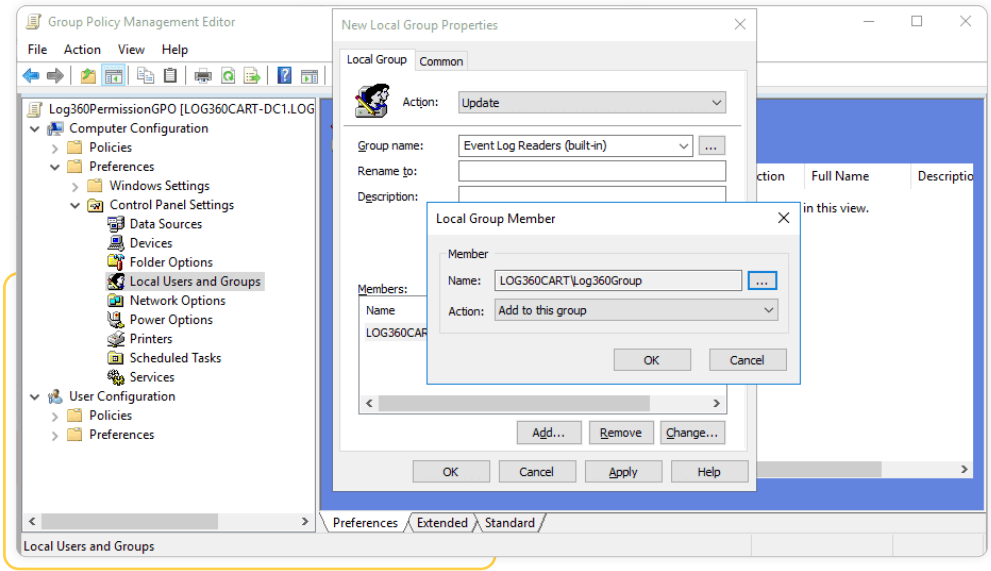
1. Log in to your Domain Controller with Domain Admin privileges → Open Active Directory Users and Computers → Built-in Container → Navigate to the right panel, right click on Event Log Readers → Properties → Members →Add the "Log360" user.

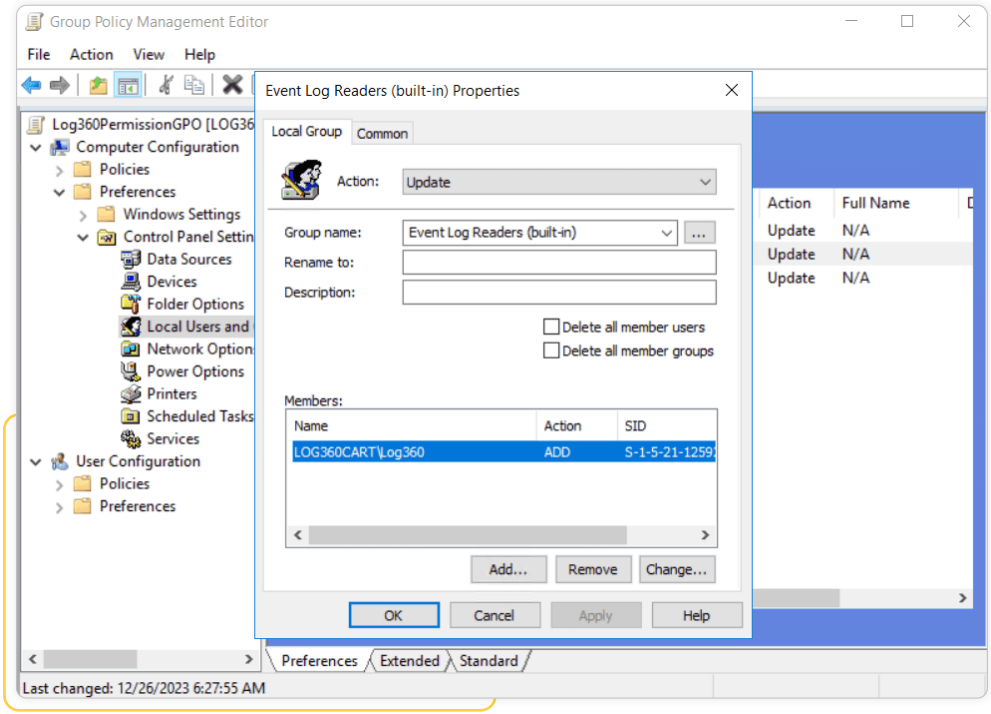
For other computers (Windows servers and workstations):

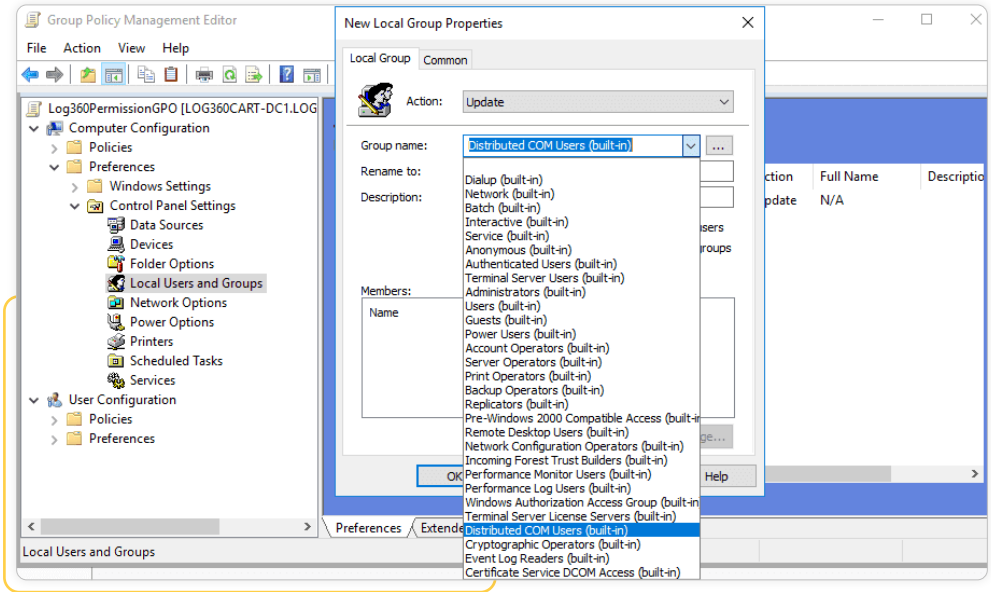
1. Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click "Log360 Permission GPO" → Edit.
2. In the Group Policy Management Editor → Computer Configuration → Preferences → Control Panel Settings → Right-click Local Users and Groups → New → 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

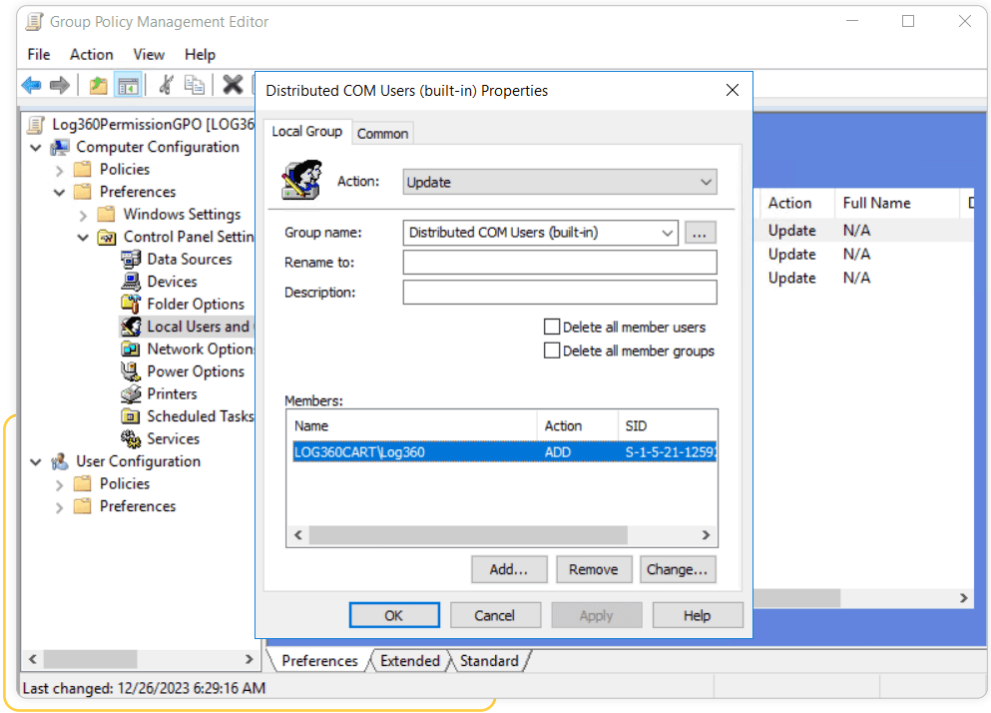


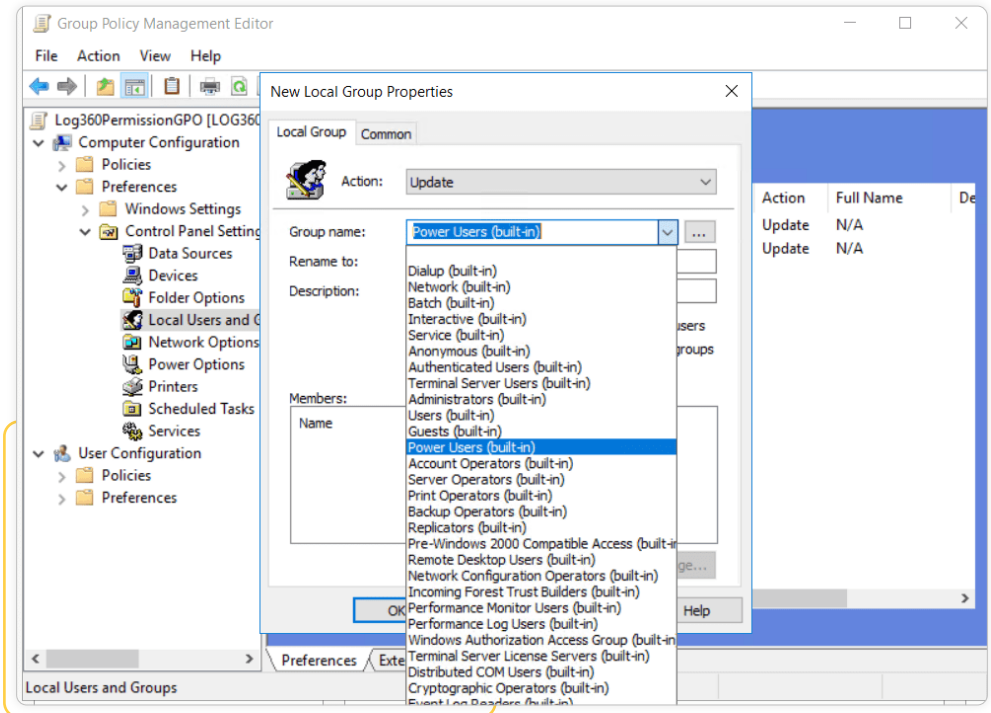


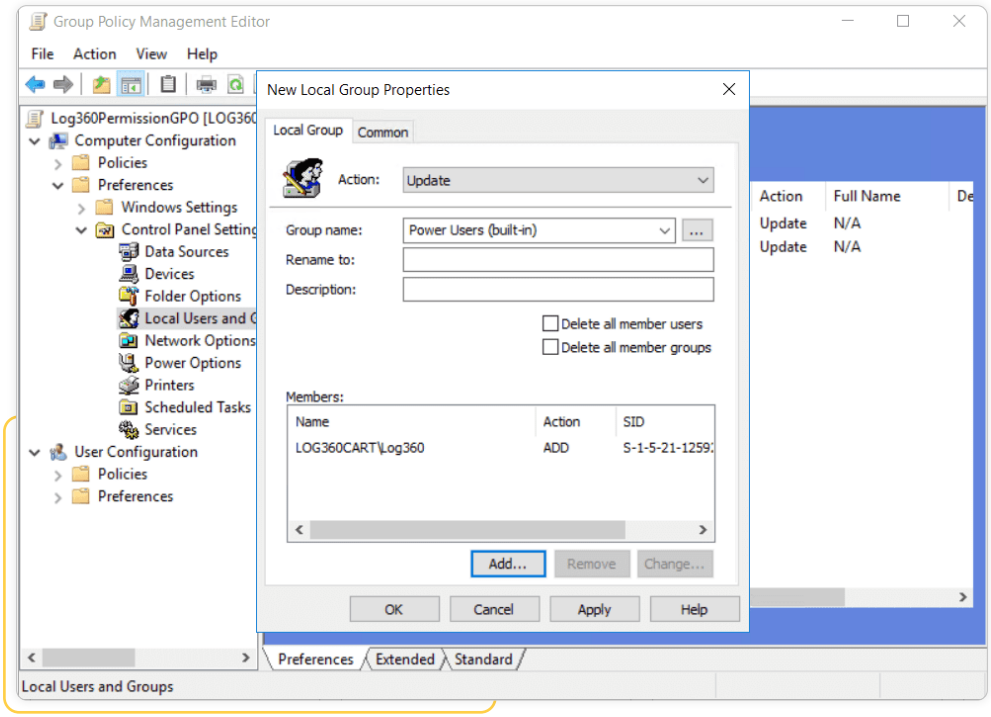

Group Policy Management Editor
File Action View Help
Log360PermissionGPO [LOG360CART-DC1.LOG
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Settings
Data Sources
Devices
Folder Options
Local Users and Groups
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
New Local Group Properties
Local Group
Common
Action:
Update
Group name:
Event Log Readers (built-in)
Rename to:
Description:
Local Group Member
Member
Name:
LOG360CART\Log360Group
Action:
Add to this group
OK
Cancel
Members:
Name
LOG360CAR
Add...
Remove
Change...
OK
Cancel
Apply
Help
Full Name
Descriptio
in this view.
Preferences
Extended
Standard
Local Users and Groups


Group Policy Management Editor
File Action View Help
Log360PermissionGPO [LOG36
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Settin
Data Sources
Devices
Folder Options
Local Users and
Network Option
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
Event Log Readers (built-in) Properties
Local Group
Common
Action:
Update
Group name:
Event Log Readers (built-in)
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name
Action
SID
LOG360CART\Log360
ADD
S-1-5-21-1259
Add...
Remove
Change...
OK
Cancel
Apply
Help
Action
Full Name
Update
N/A
Update
N/A
Update
N/A
Preferences
Extended
Standard
Last changed: 12/26/2023 6:27:55 AM


Group Policy Management Editor
File Action View Help
Log360PermissionGPO [LOG360CART-DC1.LOG
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Settings
Data Sources
Devices
Folder Options
Local Users and Groups
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
New Local Group Properties
Local Group
Common
Action:
Update
Group name:
Distributed COM Users (built-in)
Rename to:
Description:
Members:
Name
Dialup (built-in)
Network (built-in)
Batch (built-in)
Interactive (built-in)
Service (built-in)
Anonymous (built-in)
Authenticated Users (built-in)
Terminal Server Users (built-in)
Administrators (built-in)
Users (built-in)
Guests (built-in)
Power Users (built-in)
Account Operators (built-in)
Server Operators (built-in)
Print Operators (built-in)
Backup Operators (built-in)
Replicators (built-in)
Pre-Windows 2000 Compatible Access (built-in)
Remote Desktop Users (built-in)
Network Configuration Operators (built-in)
Incoming Forest Trust Builders (built-in)
Performance Monitor Users (built-in)
Performance Log Users (built-in)
Windows Authorization Access Group (built-in)
Terminal Server License Servers (built-in)
Distributed COM Users (built-in)
Cryptographic Operators (built-in)
Event Log Readers (built-in)
Certificate Service DCOM Access (built-in)
Help
Full Name
Descriptio
N/A
Preferences
Local Users and Groups


Group Policy Management Editor
File Action View Help
Distributed COM Users (built-in) Properties
Local Group Common
Action: Update
Group name: Distributed COM Users (built-in)
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name Action SID
LOG360CART\Log360 ADD S-1-5-21-1259
Add... Remove Change...
OK Cancel Apply Help
Log360PermissionGPO [LOG36
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Settin
Data Sources
Devices
Folder Options
Local Users and
Network Option
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
Action Full Name
Update N/A
Update N/A
Update N/A
Preferences Extended Standard
Last changed: 12/26/2023 6:29:16 AM


Group Policy Management Editor
File Action View Help
New Local Group Properties
Local Group Common
Action: Update
Group name: Power Users (built-in)
Rename to:
Description:
Members:
Name
Dialup (built-in)
Network (built-in)
Batch (built-in)
Interactive (built-in)
Service (built-in)
Anonymous (built-in)
Authenticated Users (built-in)
Terminal Server Users (built-in)
Administrators (built-in)
Users (built-in)
Guests (built-in)
Power Users (built-in)
Account Operators (built-in)
Server Operators (built-in)
Print Operators (built-in)
Backup Operators (built-in)
Replicators (built-in)
Pre-Windows 2000 Compatible Access (built-in)
Remote Desktop Users (built-in)
Network Configuration Operators (built-in)
Incoming Forest Trust Builders (built-in)
Performance Monitor Users (built-in)
Performance Log Users (built-in)
Windows Authorization Access Group (built-in)
Terminal Server License Servers (built-in)
Distributed COM Users (built-in)
Cryptographic Operators (built-in)
OK Help
Log360PermissionGPO [LOG360
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Setting
Data Sources
Devices
Folder Options
Local Users and G
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
Action Full Name
Update N/A
Update N/A
Preferences
Local Users and Groups



Terms:

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

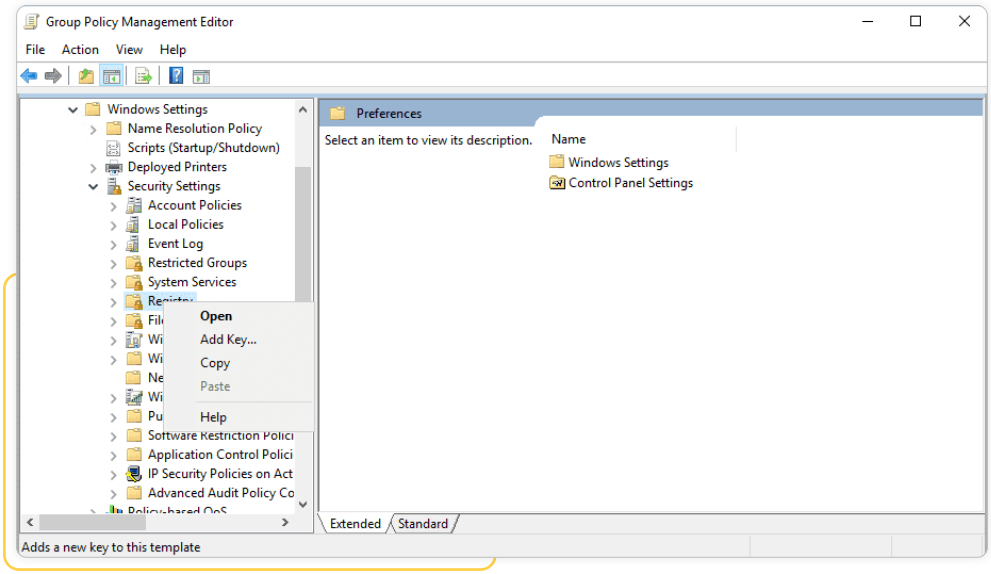
Distributed COM Users: Members of this group can launch, activate, and use Distributed COM objects on the computer.

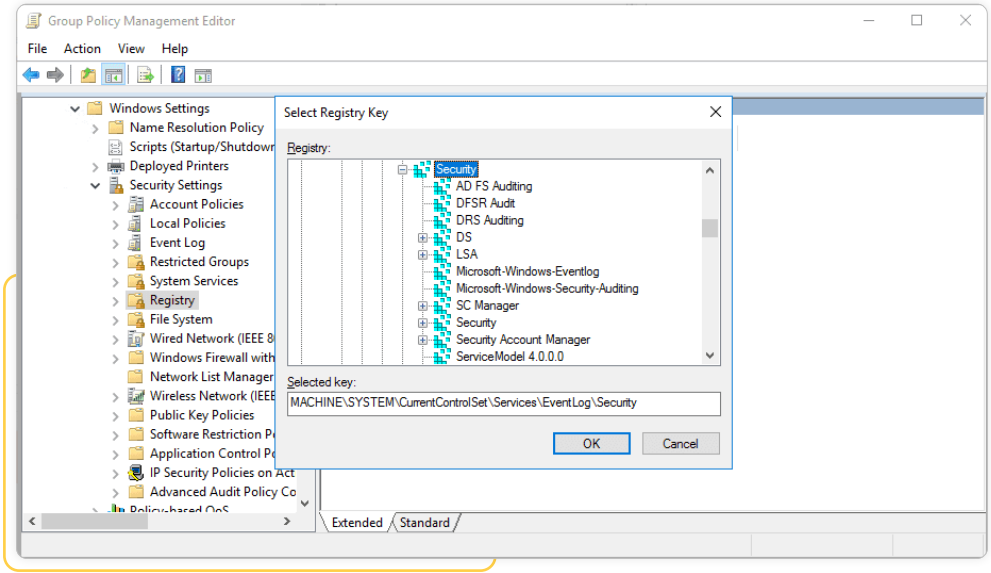
Power Users: Members of this group can discover shares residing on Windows file servers.

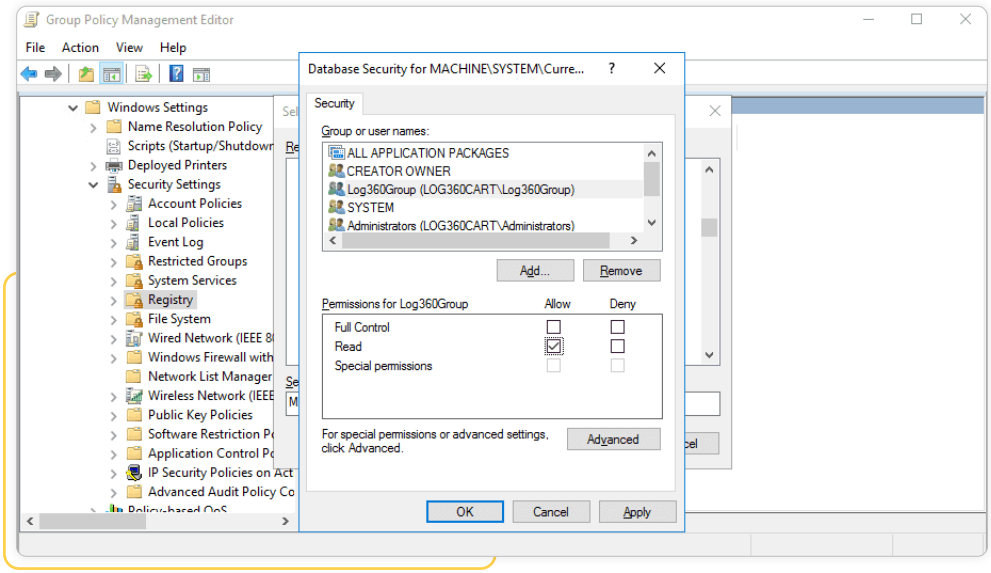
Make user to read Event logs:

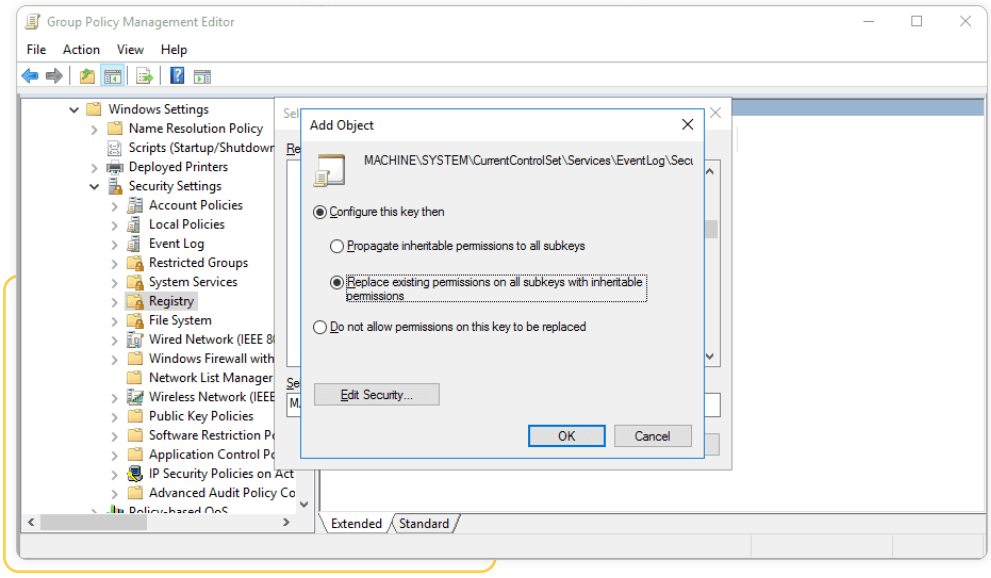
To read the event logs, you also need to grant the "Log360" users Read permission over HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security.

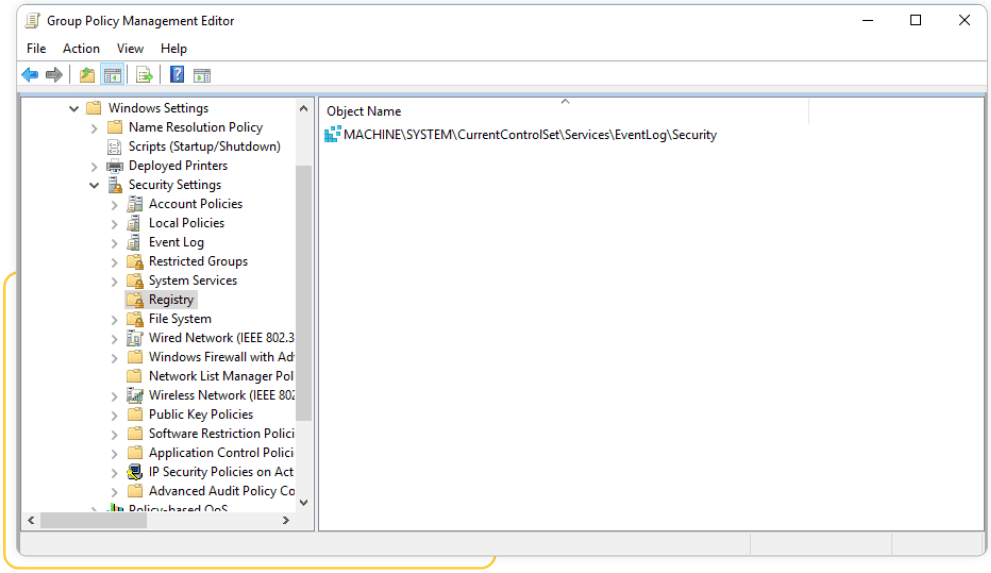
1. Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click "Log360PermissionGPO" → Edit.
2. In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Right-click Registry → Add Key.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


Group Policy Management Editor
File Action View Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Open
Add Key...
Copy
Paste
Help
Preferences
Select an item to view its description.
Name
Windows Settings
Control Panel Settings
Extended
Standard
Adds a new key to this template


Group Policy Management Editor
File Action View Help
Select Registry Key
Registry:
Security
AD FS Auditing
DFSR Audit
DRS Auditing
DS
LSA
Microsoft-Windows-Eventlog
Microsoft-Windows-Security-Auditing
SC Manager
Security
Security Account Manager
ServiceModel 4.0.0.0
Selected key:
MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security
OK
Cancel
Extended
Standard

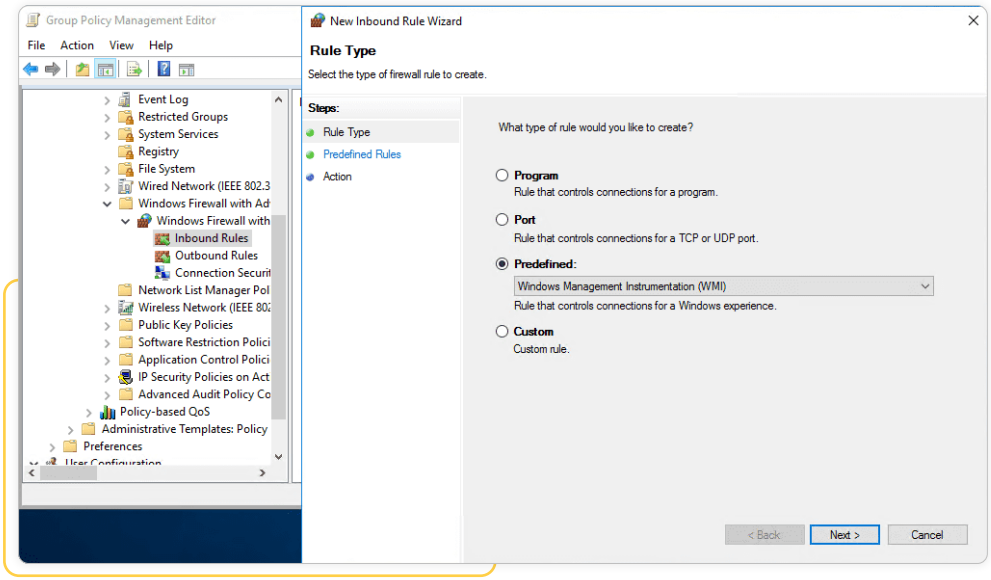

Group Policy Management Editor
File Action View Help
Database Security for MACHINE\SYSTEM\Curre...
Security
Group or user names:
ALL APPLICATION PACKAGES
CREATOR OWNER
Log360Group (LOG360CART\Log360Group)
SYSTEM
Administrators (LOG360CART\Administrators)
Add...
Remove
Permissions for Log360Group
Allow
Deny
Full Control
Read
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

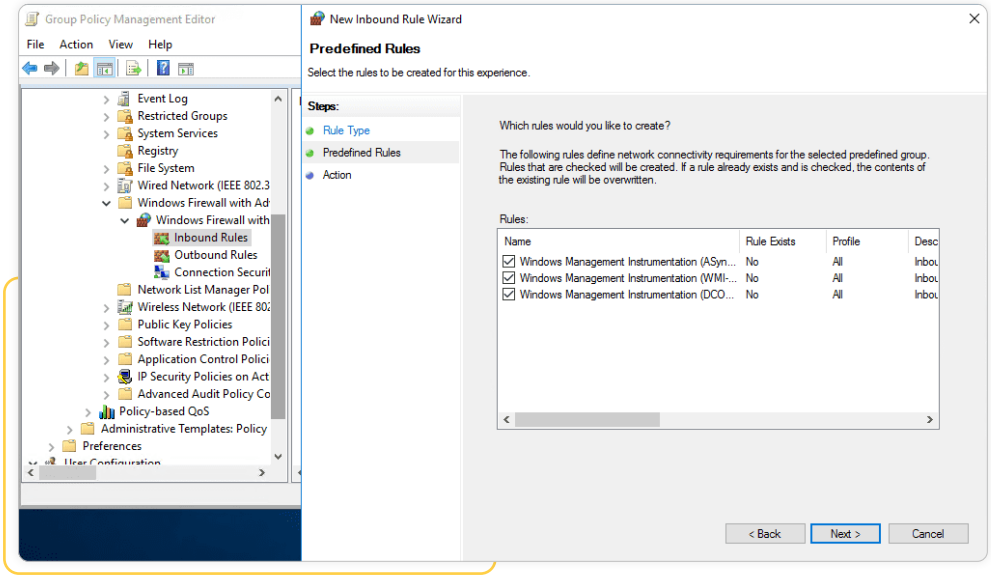


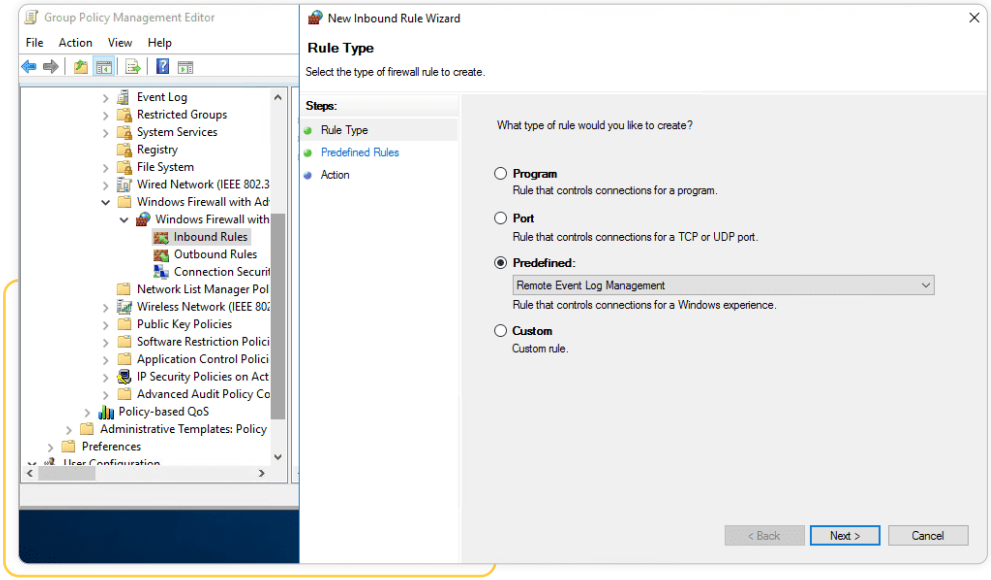


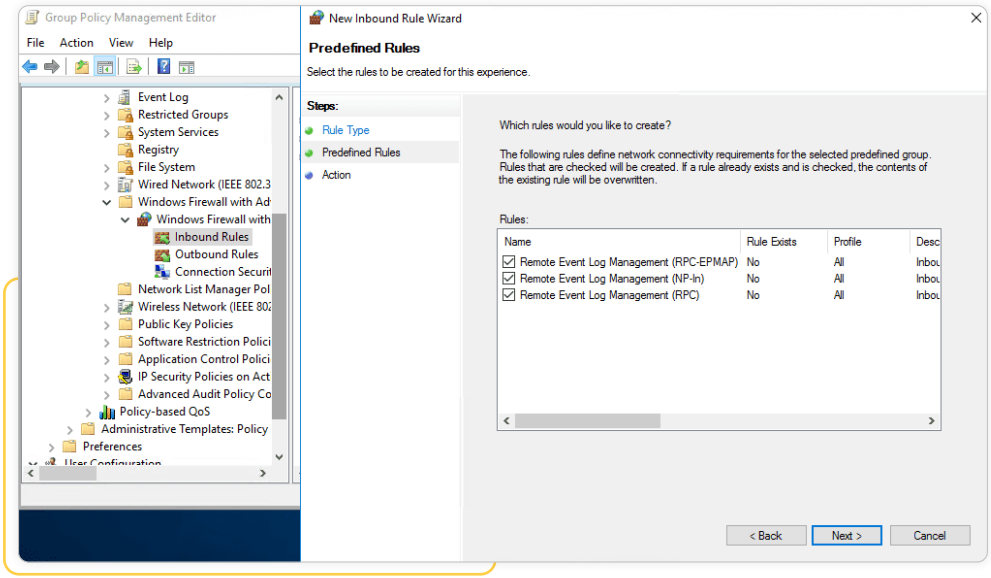
Enable WMI and Remote Event Log Management traffic through Firewall:

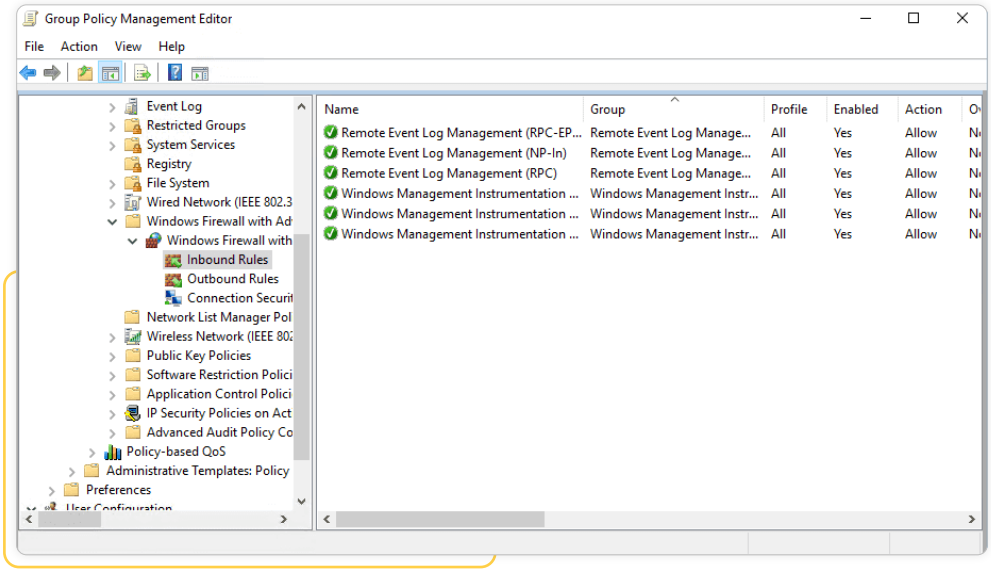
1. Log in to your domain controller with domain admin privileges → Open the Group Policy Management Console → Right-click "Log360 Permission GPO" → Edit.
2. Select Computer configuration → Policies → Windows Settings → Security Settings → Windows Firewalls with Advanced Security → Inbound Rules
3. Right-click 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.


Group Policy Management Editor
File Action View Help
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3
Windows Firewall with Ad
Windows Firewall with
Inbound Rules
Outbound Rules
Connection Securit
Network List Manager Pol
Wireless Network (IEEE 80
Public Key Policies
Software Restriction Polici
Application Control Polici
IP Security Policies on Act
Advanced Audit Policy Co
Policy-based QoS
Administrative Templates: Policy
Preferences
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Predefined Rules
Action
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Windows Management Instrumentation (WMI)
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


Group Policy Management Editor
File Action View Help
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3
Windows Firewall with Ad
Windows Firewall with
Inbound Rules
Outbound Rules
Connection Securit
Network List Manager Pol
Wireless Network (IEEE 80
Public Key Policies
Software Restriction Polici
Application Control Polici
IP Security Policies on Act
Advanced Audit Policy Co
Policy-based QoS
Administrative Templates: Policy
Preferences
New Inbound Rule Wizard
Predefined Rules
Select the rules to be created for this experience.
Steps:
Rule Type
Predefined Rules
Action
Which rules would you like to create?
The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.
Rules:
Name
Rule Exists
Profile
Desc
Windows Management Instrumentation (ASyn...
No
All
Windows Management Instrumentation (WMI-...
No
All
Windows Management Instrumentation (DCO...
No
All
< Back
Next >
Cancel


Group Policy Management Editor
File Action View Help
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3
Windows Firewall with Ad
Windows Firewall with
Inbound Rules
Outbound Rules
Connection Securit
Network List Manager Pol
Wireless Network (IEEE 80
Public Key Policies
Software Restriction Polici
Application Control Polici
IP Security Policies on Act
Advanced Audit Policy Co
Policy-based QoS
Administrative Templates: Policy
Preferences
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Predefined Rules
Action
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Remote Event Log Management
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel





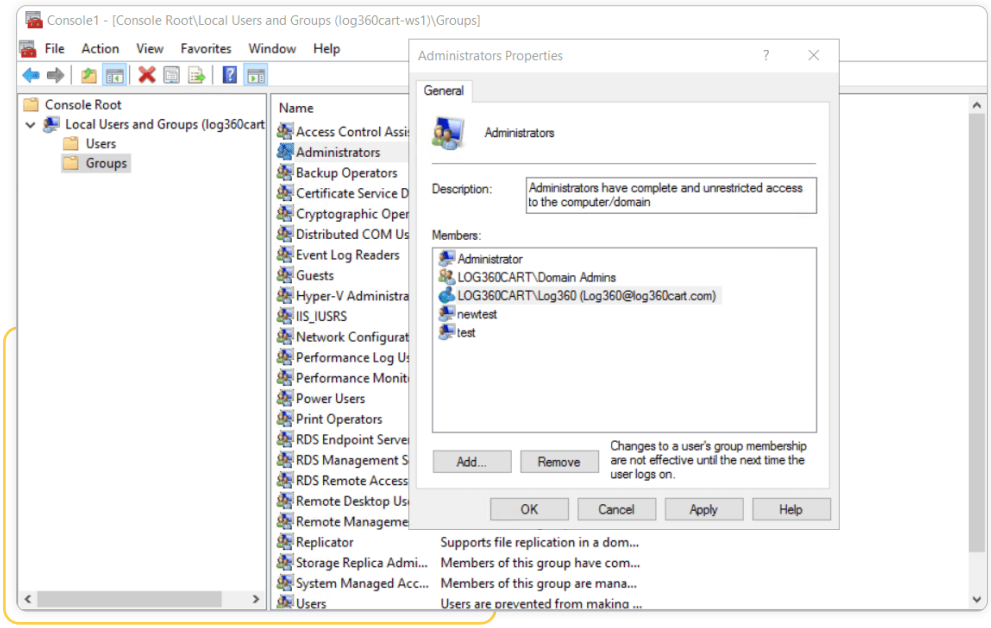
Note:

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

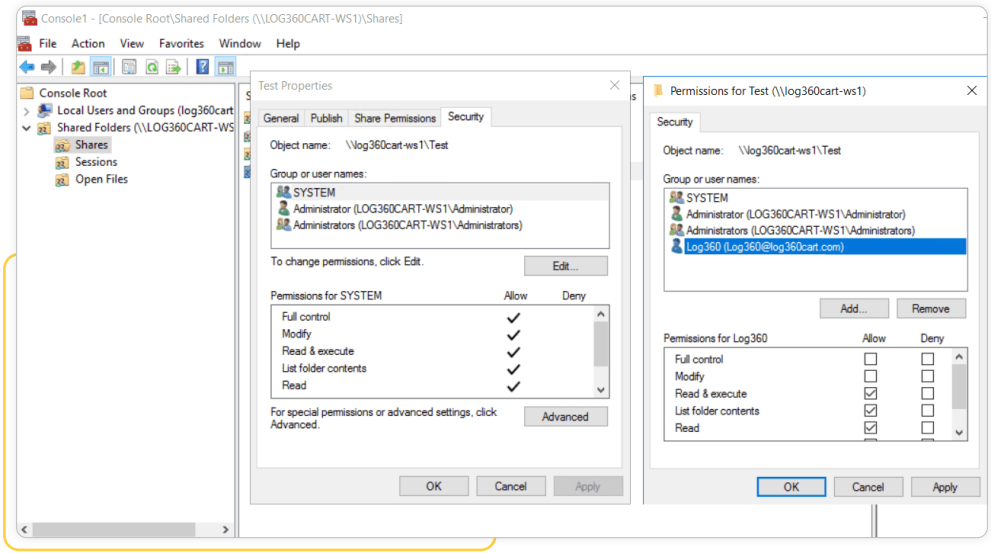
There are two ways to grant the user Read permission on all the audited shares:

- **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.



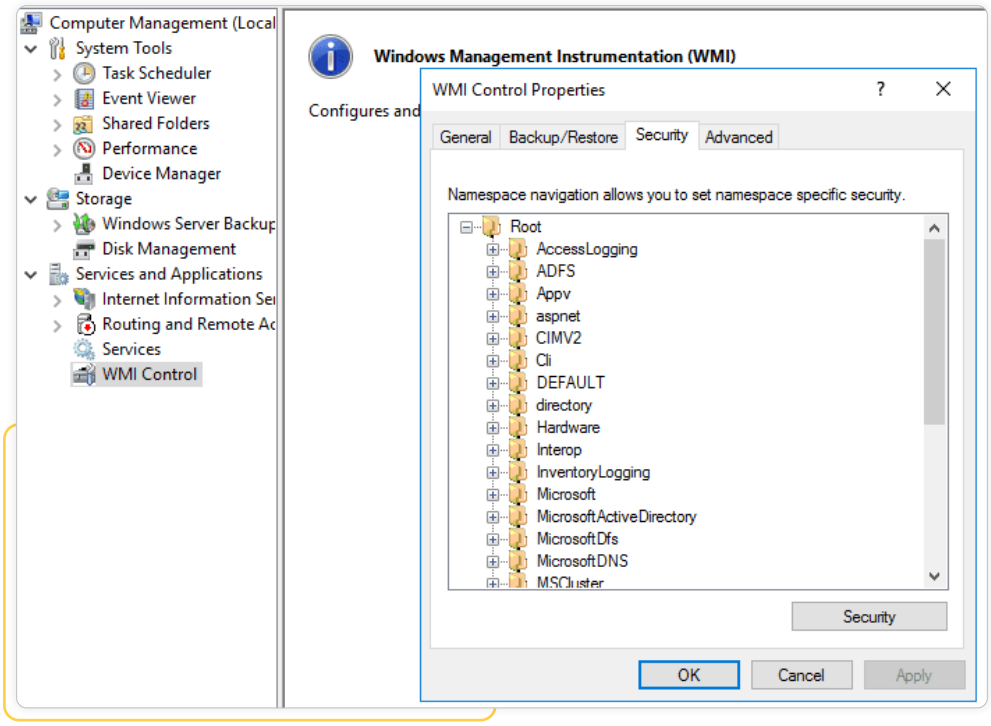
- **Grant the user both Share and NTFS Read permission on every audited share.**

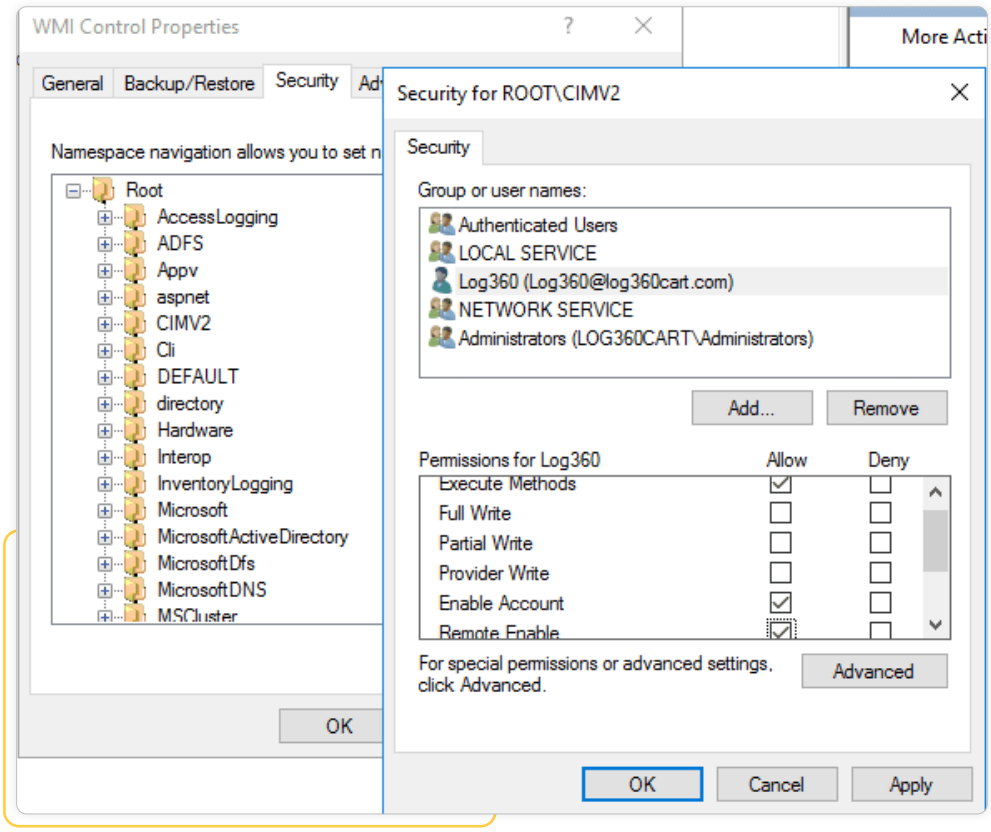
1. Login to any computer with domain admin privileges → Open MMC console → File → Add/ Remove Snap-in → Select Shared Folders → Add → Another computer → Add target computer.
2. Select target computer → Select share → Right-click → Properties → Security → Edit → Add the "Log360" user → Provide both Share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



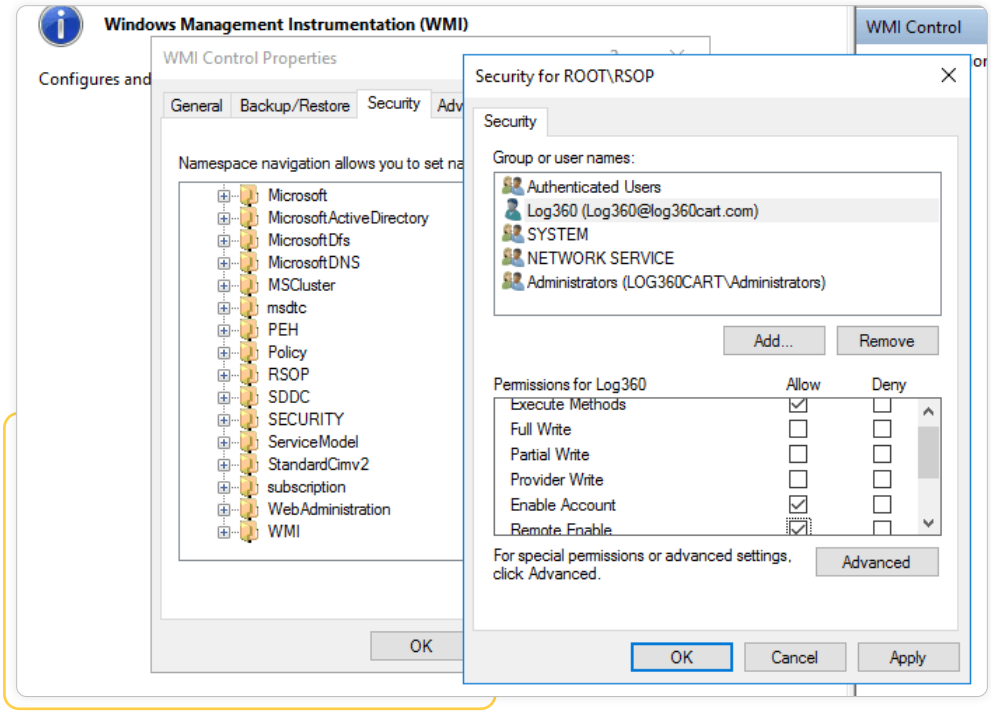
Granting WMI permission:

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

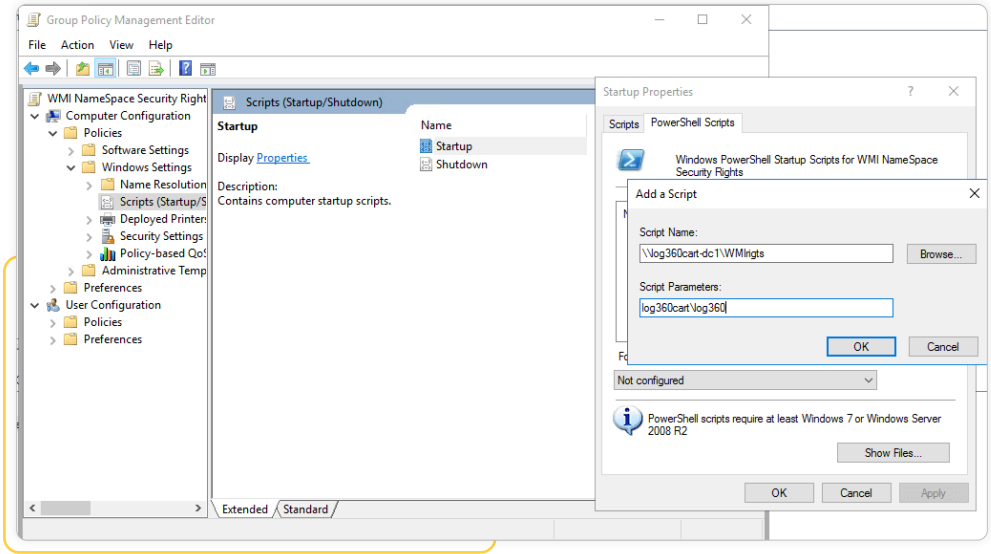


5. Click OK.
6. Repeat the steps for every audited computer.

Grant WMI Namespace Security Rights using GPO (PowerShell script)

Script download link

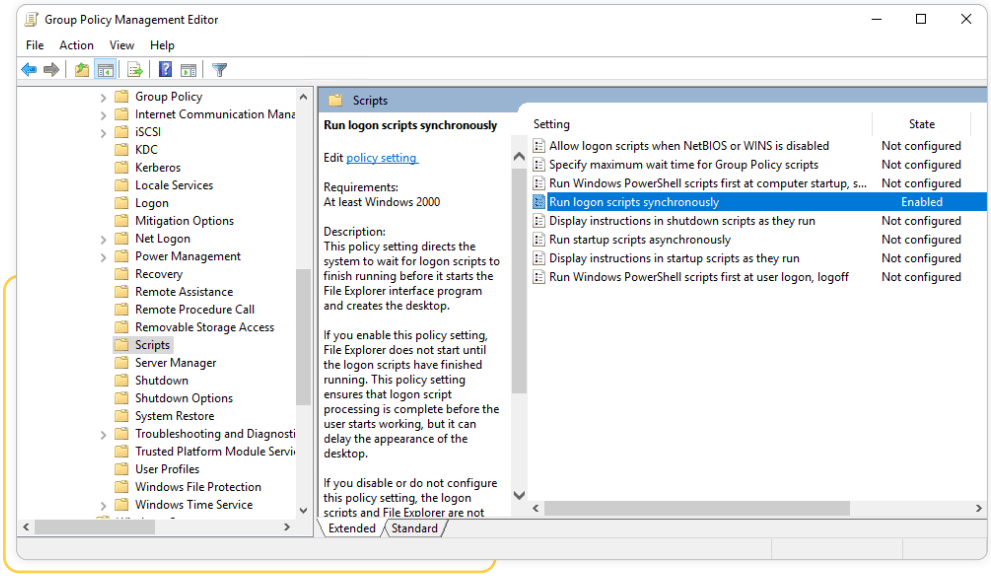
1. Add the script WMIrights.ps1 file in the shared location in the domain.
2. Create a new GPO WMI NameSpace Security Rights and Right-click → Edit.
3. Navigate to Computer Configuration → Policies → Windows Settings → Scripts → Startup → Right-click and open Properties→PowerShell Scripts → Add.
4. In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



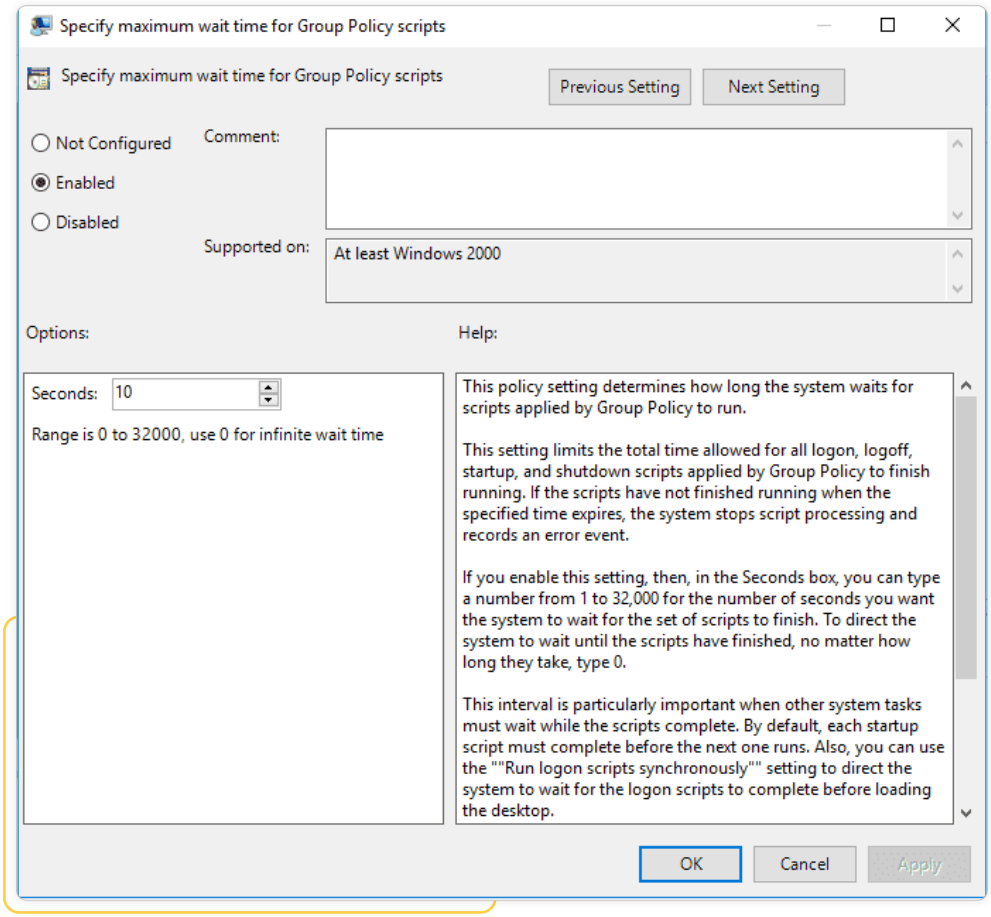
5. Click OK to return to the Startup Properties dialog box → Apply → OK

Configuring Administrative Template Settings

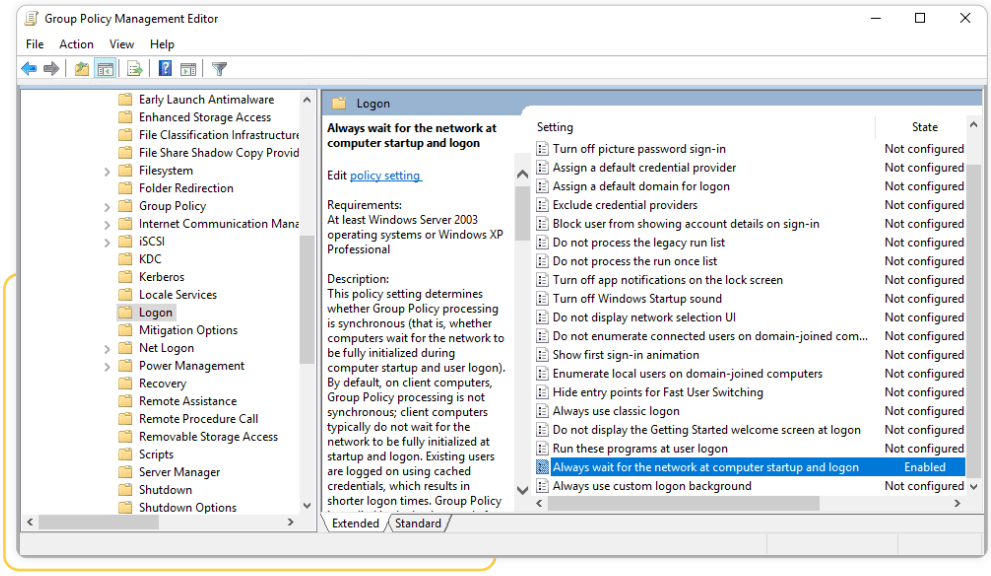
1. On the left pane of the Group Policy Management Editor, navigate to Computer Configuration Administrator Templates System.
2. Under System, select Scripts.
3. On the right pane of the GPO Editor, double-click Run logon scripts synchronously, and enable it → Apply → OK.



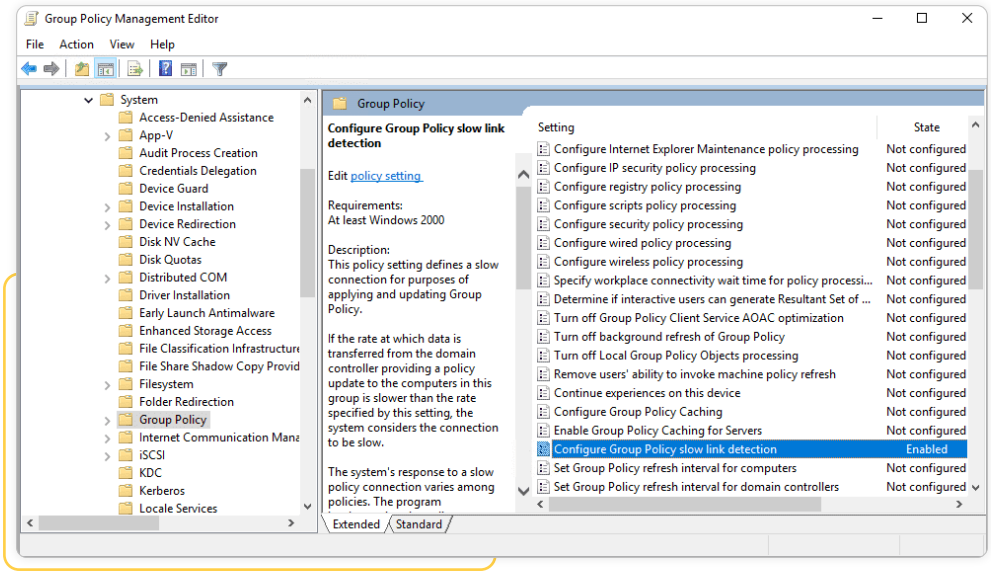
4. Enable Maximum wait time for Group Policy scripts and set the maximum time at 10 seconds.



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

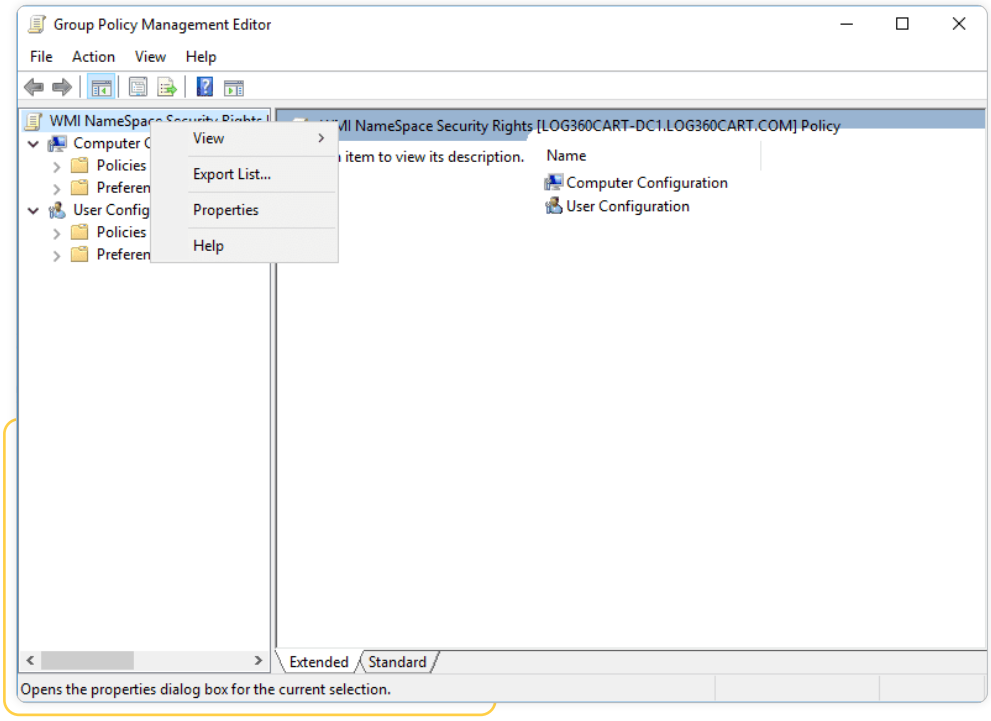


6. Navigate to Group Policy under System, on the right pane double-click Configure Group Policy slow link detection, and enable it → Apply → OK.

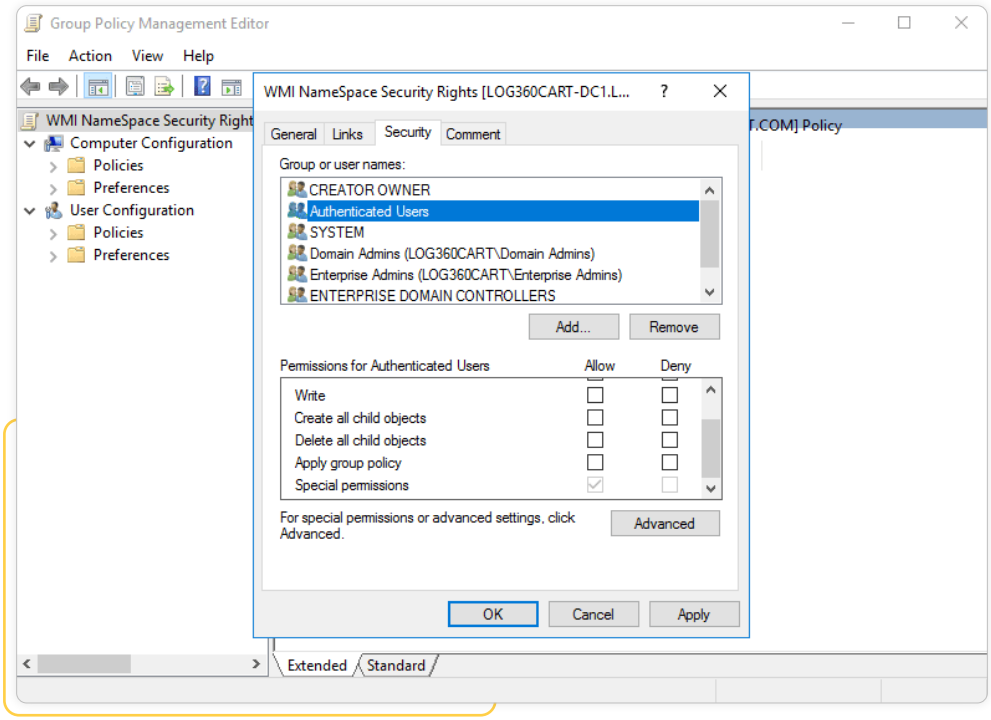


Apply the GPO

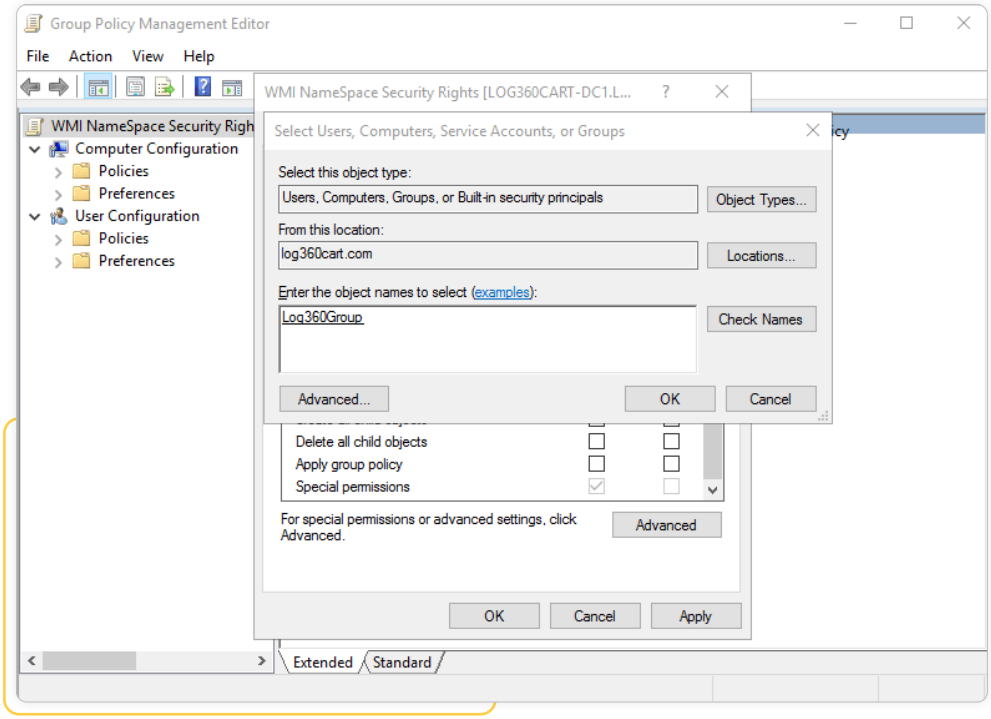
1. On the left pane of the Group Policy Management Editor, right-click the required GPO → Properties.



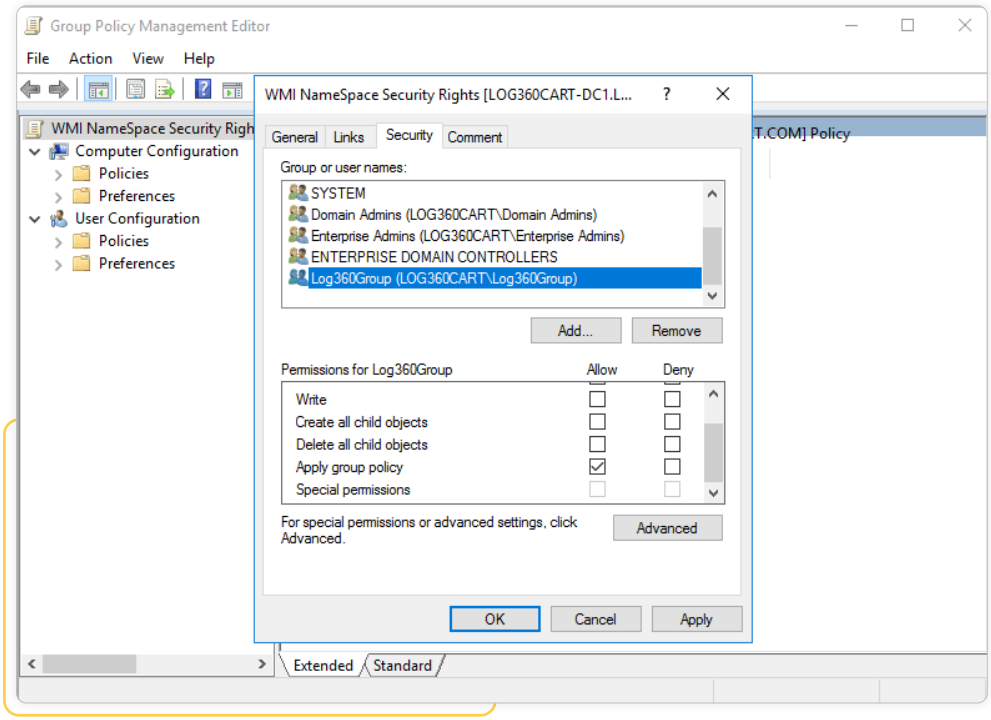
2. Navigate to the Security tab and unselect the “Apply Group Policy” permissions for Authenticated Users → Add.



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$):

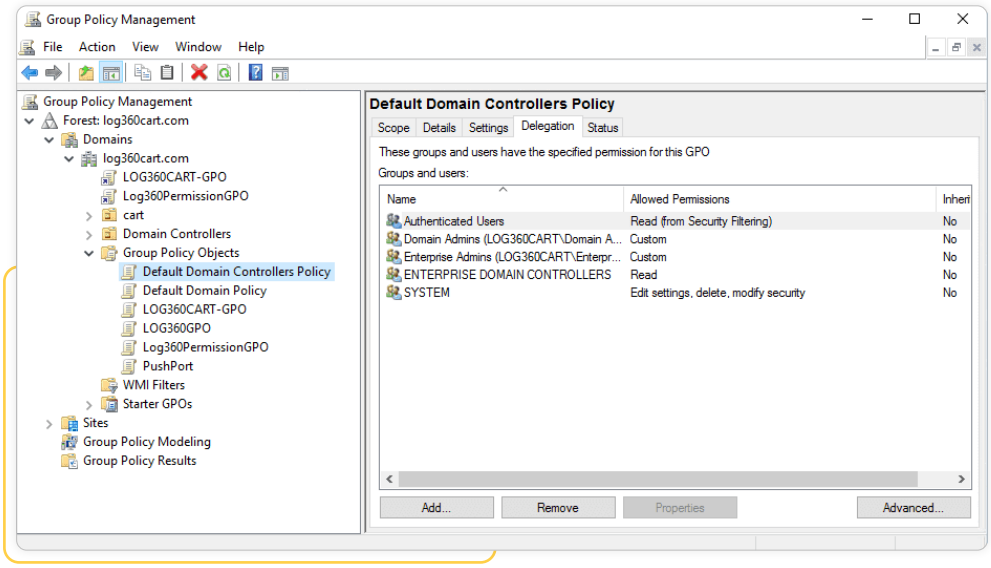
Read permission over C$ share (\\server_name\C$) is needed to access NetApp C-Mode log files.

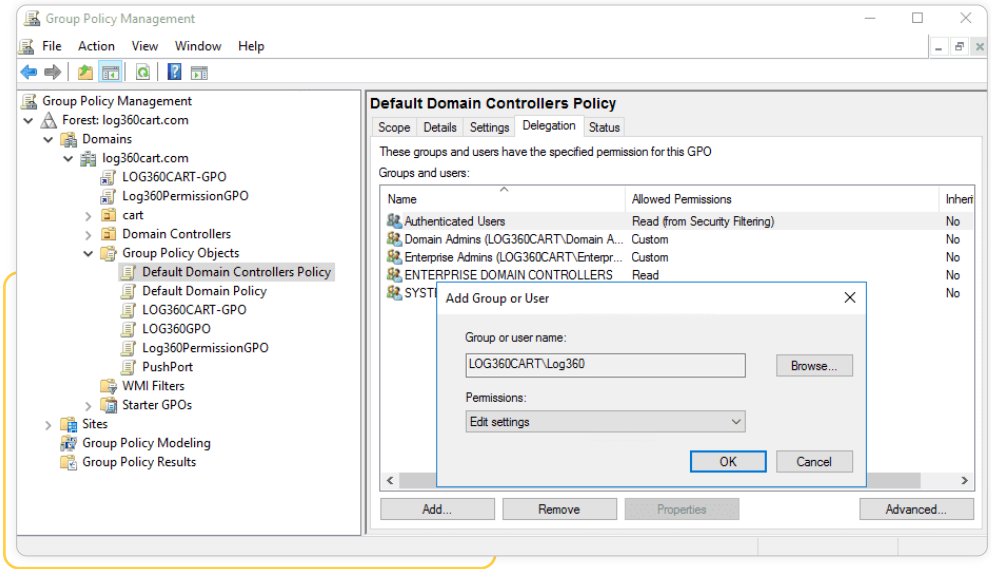
Privileges/permissions required for automatic audit policy and object level auditing configuration

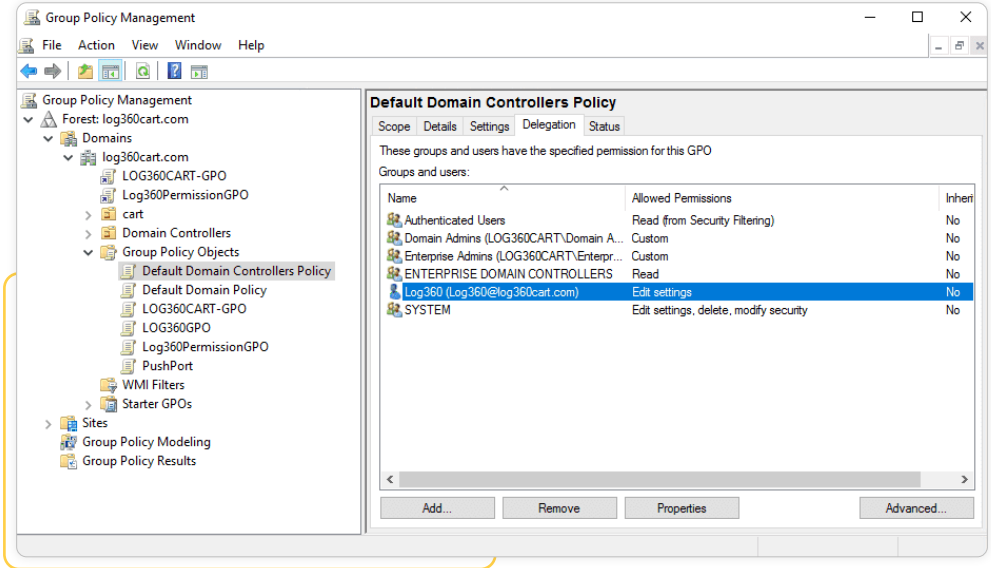
Privileges/permissions required for domain controller auditing configuration

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.



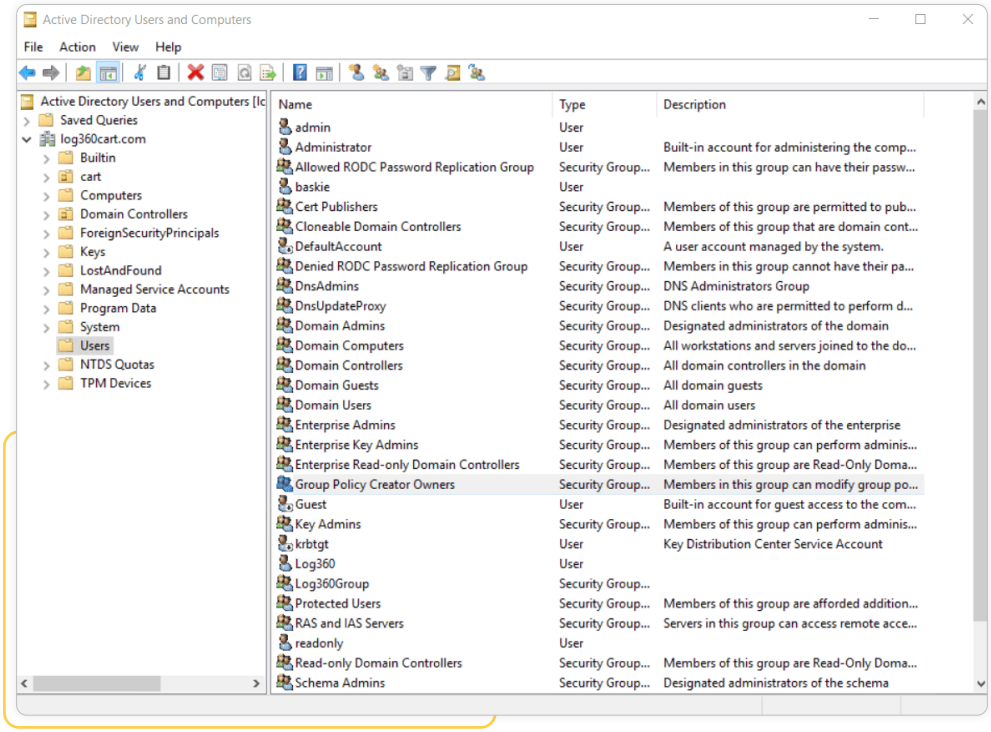


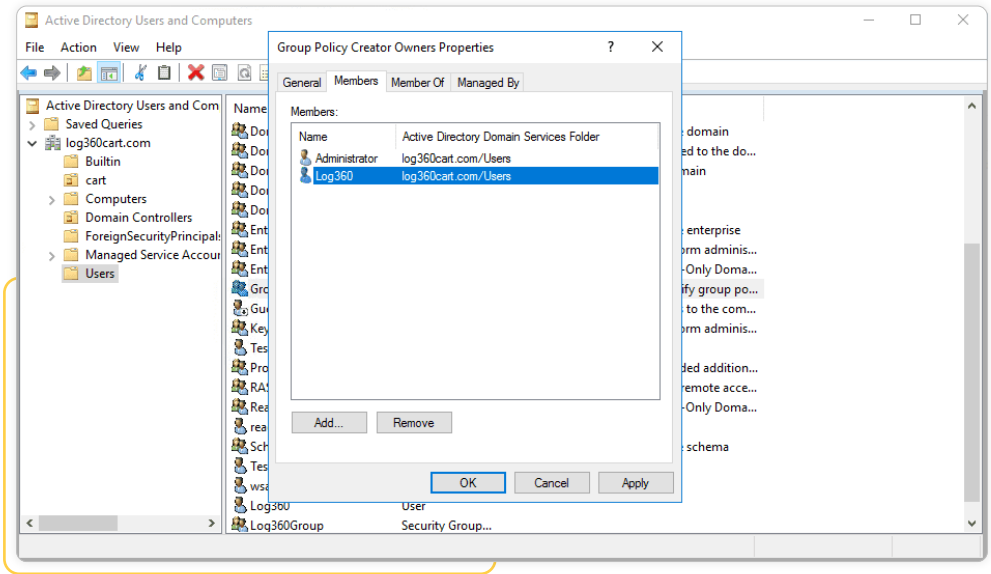


Privileges/permissions required for member server, workstation, and file server auditing configuration

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.



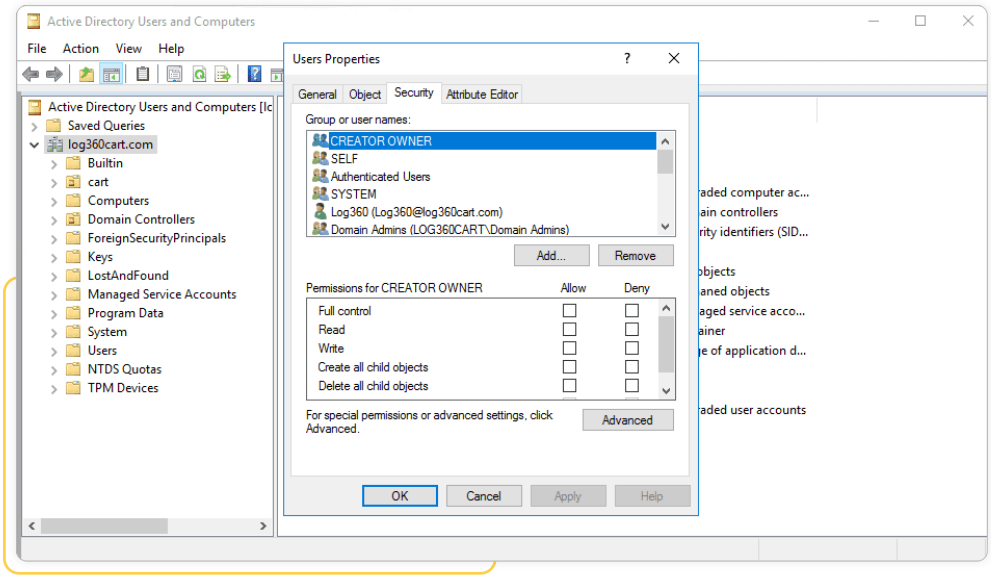


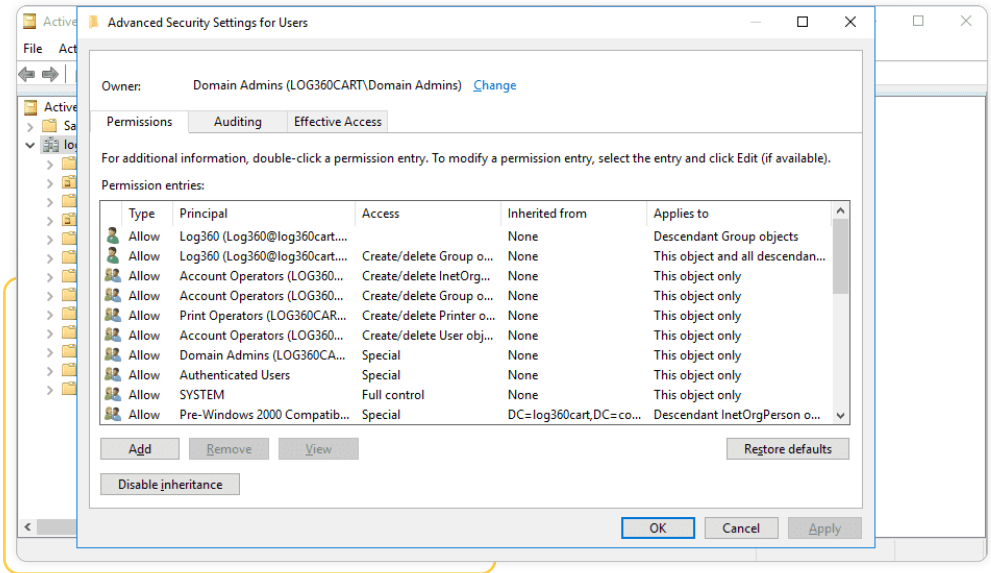
Grant the user, group management permissions

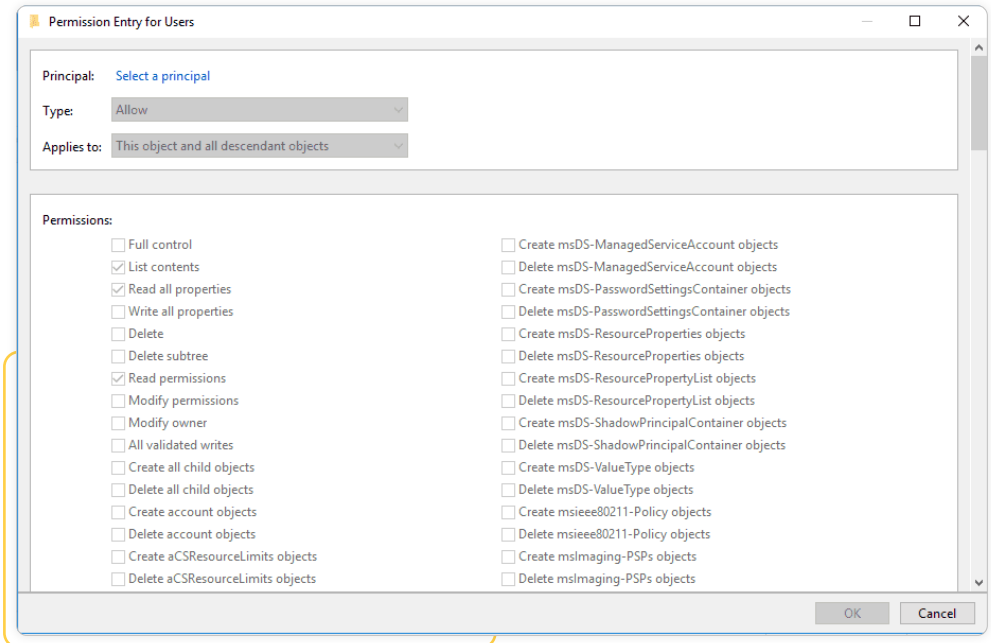
1. Log in to your domain controller with domain admin privileges → Open Active Directory User and Computers. Click View and ensure that Advanced Features is enabled. This will display the advanced security settings for selected objects in Active Directory Users and Computers.
2. Right-click Users → Properties → 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.

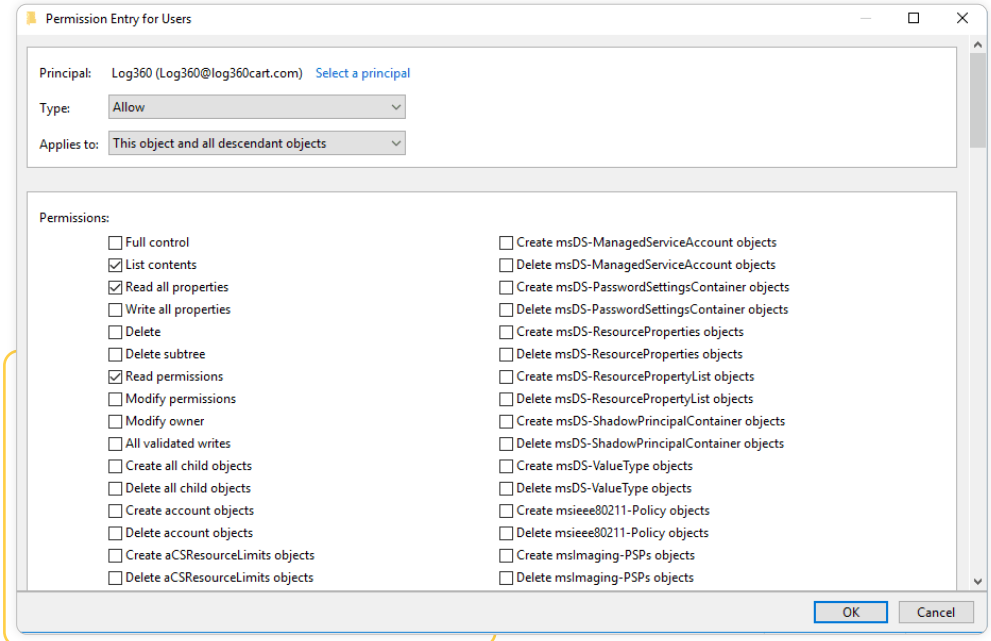
Note:

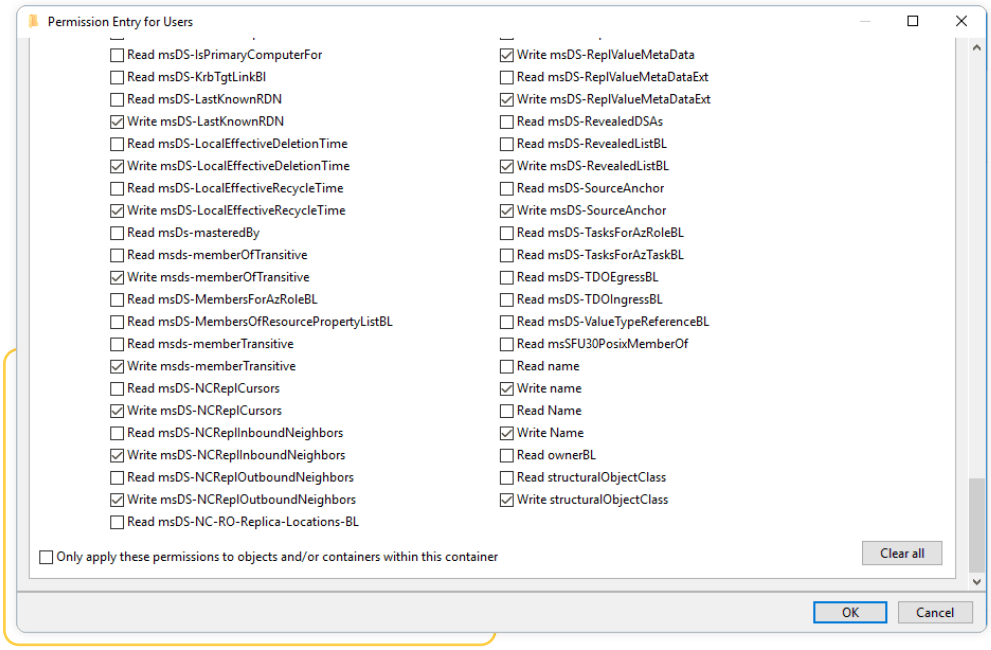
Use Clear all to remove all permissions and properties before selecting the mentioned permissions.

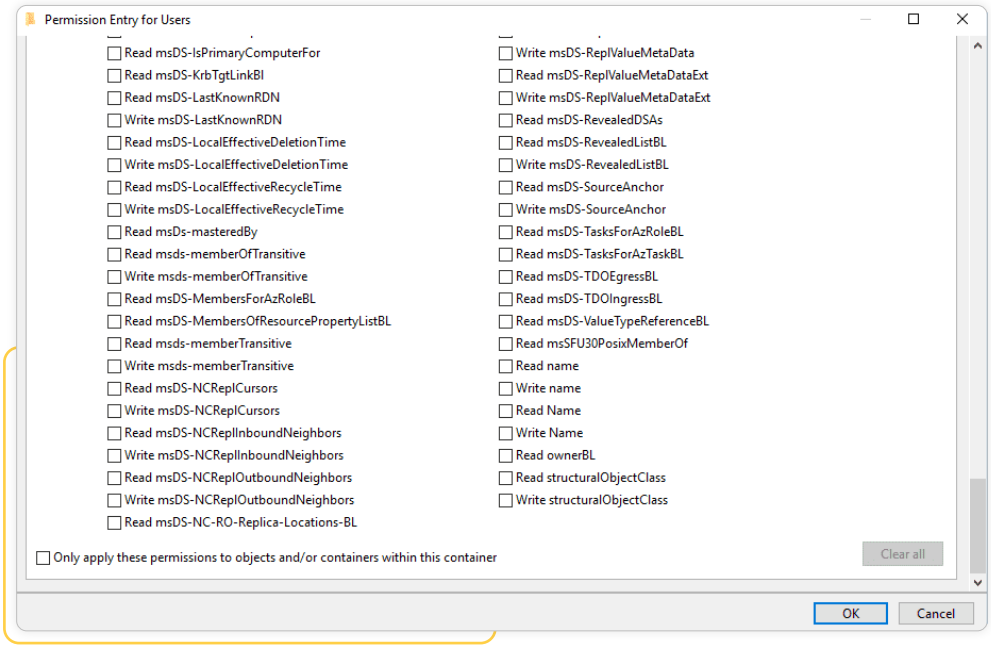


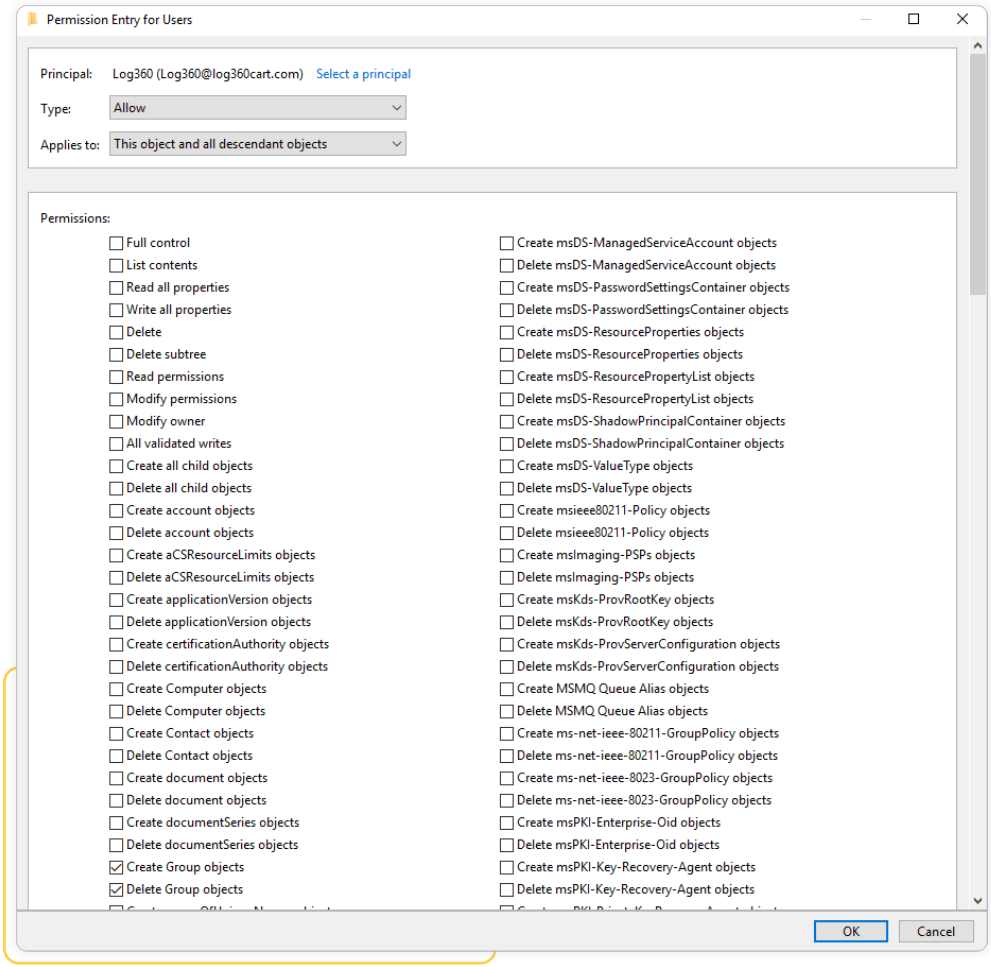



Permission Entry for Users
Principal: Select a principal
Type: Allow
Applies to: This object and all descendant objects
Permissions:
Full control
List contents
Read all properties
Write all properties
Delete
Delete subtree
Read permissions
Modify permissions
Modify owner
All validated writes
Create all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


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

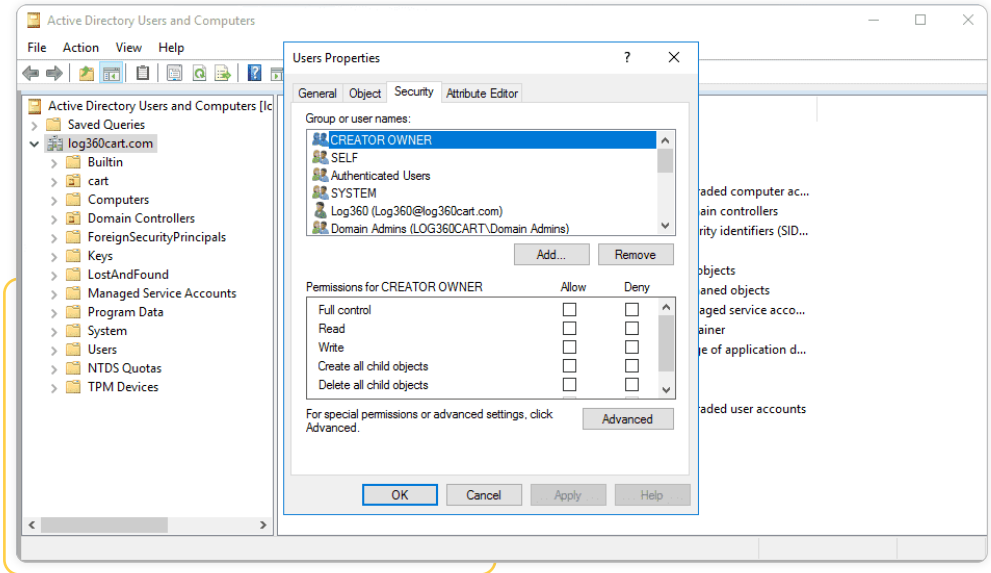

Permission Entry for Users
Read msDS-IsPrimaryComputerFor
Read msDS-KrbTgtLinkBl
Read msDS-LastKnownRDN
Write msDS-LastKnownRDN
Read msDS-LocalEffectiveDeletionTime
Write msDS-LocalEffectiveDeletionTime
Read msDS-LocalEffectiveRecycleTime
Write msDS-LocalEffectiveRecycleTime
Read msDs-masteredBy
Read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

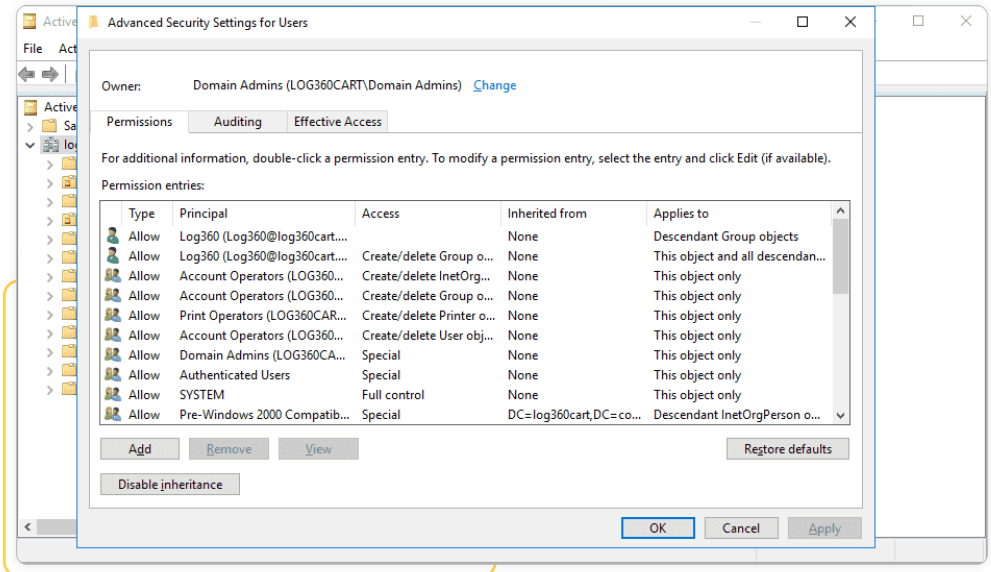


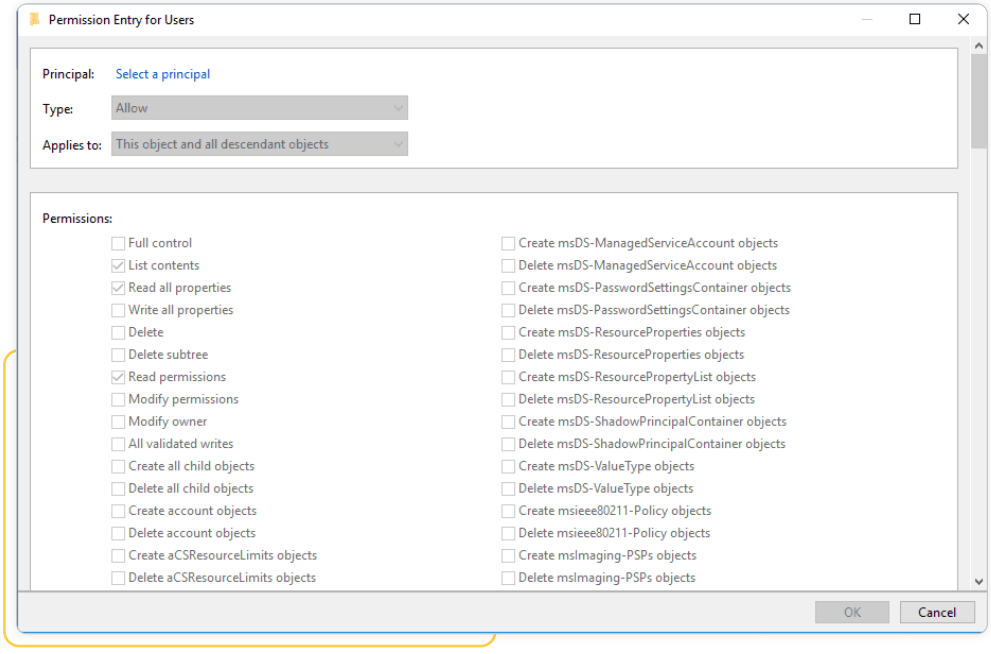
3. From the Active Directory User and Computers console → Right-click Users → Properties → Security → Advanced → Permissions → Add → In the Permission Entry for Users window → Select a principal: Log360 user → Type: Allow → Applies to: Descendant Group objects → Select property: Write Members.

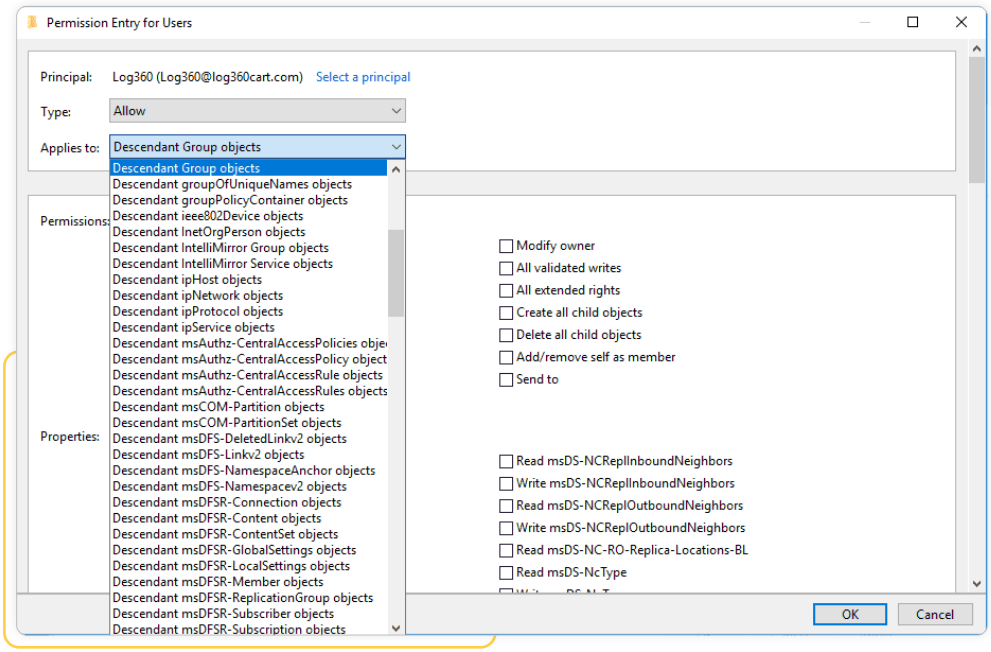
Note:

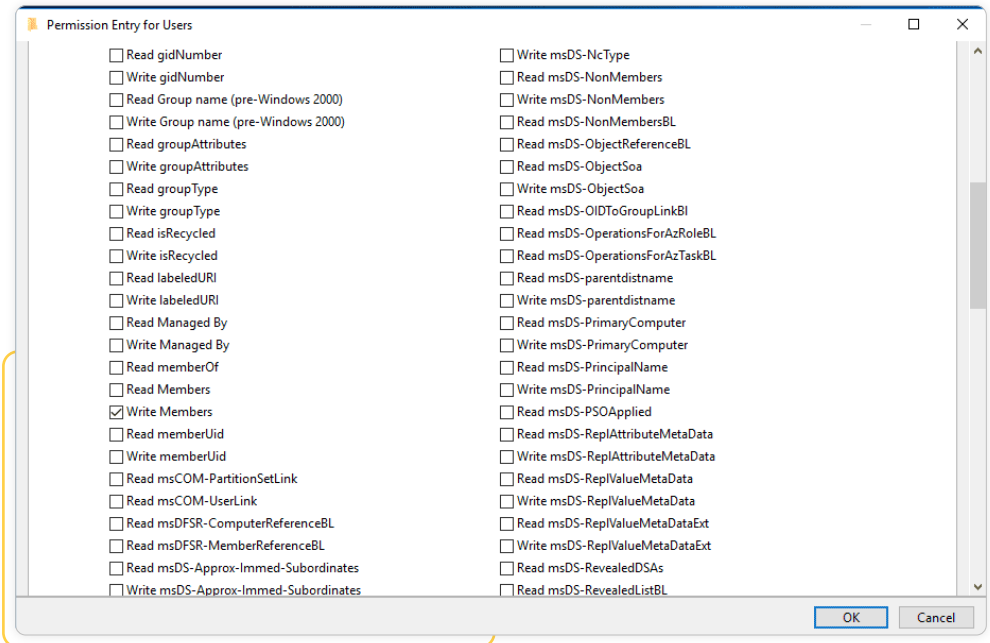
Use Clear all to remove all permissions and properties before selecting the mentioned property.

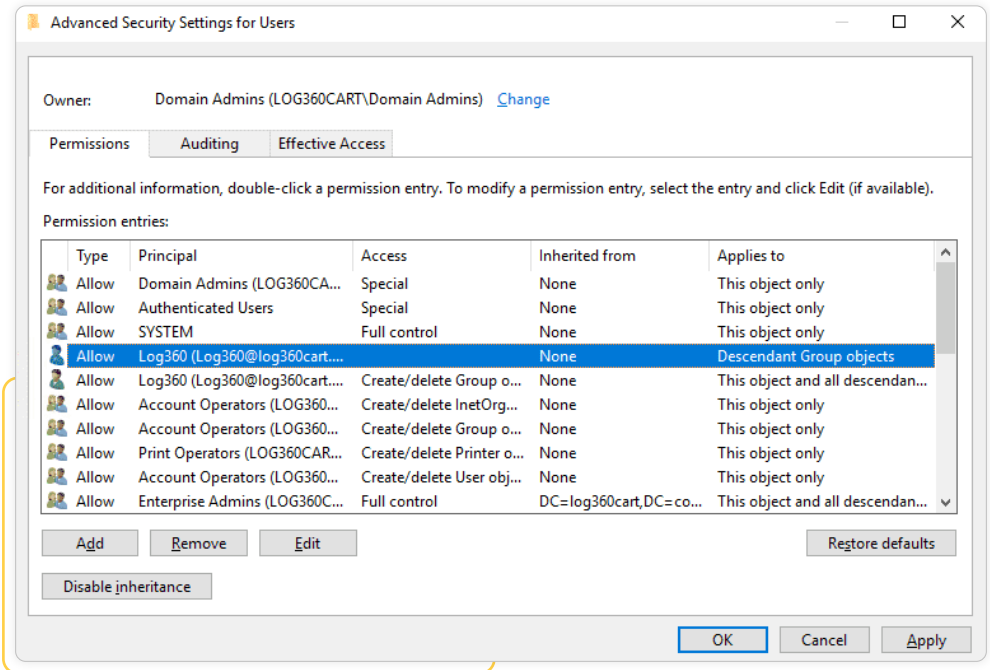



Advanced Security Settings for Users
Owner: Domain Admins (LOG360CART\Domain Admins) Change
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type
Principal
Access
Inherited from
Applies to
Allow Log360 (Log360@log360cart.... None 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...
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:
Full control
List contents
Read all properties
Write all properties
Delete
Delete subtree
Read permissions
Modify permissions
Modify owner
All validated writes
Create all child objects
Delete all child objects
Create account objects
Delete account objects
Create aCSResourceLimits objects
Delete aCSResourceLimits objects
Create msDS-ManagedServiceAccount objects
Delete msDS-ManagedServiceAccount objects
Create msDS-PasswordSettingsContainer objects
Delete msDS-PasswordSettingsContainer objects
Create msDS-ResourceProperties objects
Delete msDS-ResourceProperties objects
Create msDS-ResourcePropertyList objects
Delete msDS-ResourcePropertyList objects
Create msDS-ShadowPrincipalContainer objects
Delete msDS-ShadowPrincipalContainer objects
Create msDS-ValueType objects
Delete msDS-ValueType objects
Create msieee80211-Policy objects
Delete msieee80211-Policy objects
Create msImaging-PSPs objects
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
Descendant Group objects
Descendant groupOfUniqueNames objects
Descendant groupPolicyContainer objects
Descendant ieee802Device objects
Descendant InetOrgPerson objects
Descendant IntelliMirror Group objects
Descendant IntelliMirror Service objects
Descendant ipHost objects
Descendant ipNetwork objects
Descendant ipProtocol objects
Descendant ipService objects
Descendant msAuthz-CentralAccessPolicies obje
Descendant msAuthz-CentralAccessPolicy object
Descendant msAuthz-CentralAccessRule objects
Descendant msAuthz-CentralAccessRules objects
Descendant msCOM-Partition objects
Descendant msCOM-PartitionSet objects
Descendant msDFS-DeletedLinkv2 objects
Descendant msDFS-Linkv2 objects
Descendant msDFS-NamespaceAnchor objects
Descendant msDFS-Namespacev2 objects
Descendant msDFSR-Connection objects
Descendant msDFSR-Content objects
Descendant msDFSR-ContentSet objects
Descendant msDFSR-GlobalSettings objects
Descendant msDFSR-LocalSettings objects
Descendant msDFSR-Member objects
Descendant msDFSR-ReplicationGroup objects
Descendant msDFSR-Subscriber objects
Descendant msDFSR-Subscription objects
Permissions:
Modify owner
All validated writes
All extended rights
Create all child objects
Delete all child objects
Add/remove self as member
Send to
Properties:
Read msDS-NCReplInboundNeighbors
Write msDS-NCReplInboundNeighbors
Read msDS-NCReplOutboundNeighbors
Write msDS-NCReplOutboundNeighbors
Read msDS-NC-RO-Replica-Locations-BL
Read msDS-NcType
OK
Cancel





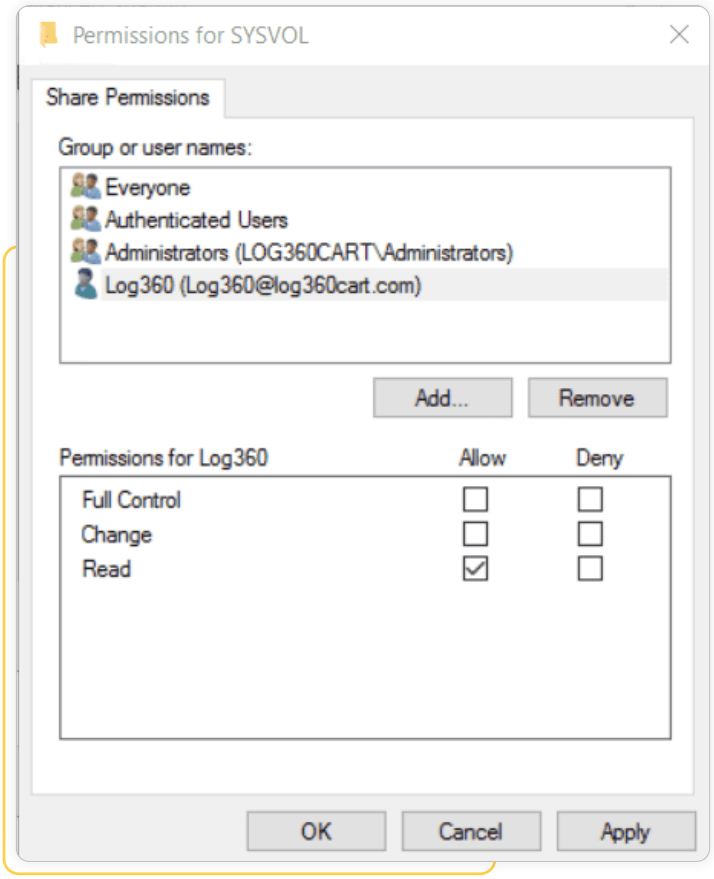
Grant the user Read permission over the SYSVOL folder

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.