APPENDIX C

Active Directory Security Management Pack

Active Directory provides many key components for authenticating users and generating authorization data that controls access to network resources. Active Directory is also used to configure servers and clients by utilizing group policy. A breach in Active Directory security can result in the loss of access to network resources by legitimate clients or the inappropriate disclosure of potentially sensitive information. MOM can be used to help track changes within your Active Directory infrastructure and alert you to any changes that should be validated to ensure that the change is authorized.

MOM is not a security audit tool, but it can be utilized to help monitor the security of your Active Directory infrastructure without compromising the performance of your MOM servers. You should carefully filter events that you wish to capture—for example, auditing user logons in a large enterprise environment should be avoided due to the volume of events that this could generate. This appendix will cover how to monitor for changes to the built-in security groups, changes to organizational units (OUs), and group policy. The steps that are shown in this appendix can be easily modified to monitor other important security events within your Active Directory infrastructure.

Monitoring Changes to Security Groups

Security groups are used to apply permissions to resources and to control access. When Active Directory is installed, a number predefined groups are created. These built-in groups by default have administrative access to various components of the Active Directory infrastructure. They are used heavily by organizations as the basis of their security delegation models. It is therefore important that any changes to these groups are tracked. This section will show you how to create alerts in MOM if memberships of these groups are changed. The process that is used can be adapted to monitor any groups that your organization requires. Table C-1 lists the built-in groups that are defined in Active Directory.

Table C-1. Built-In Groups

Group or Account Name	Description
Enterprise Admins (global)	Enterprise Admins by default is added to the Administrators group in every domain in the forest, providing complete access to the configuration of all domain controllers.
Schema Admins (global)	Schema Admins has full administrative access to the Active Directory schema.
Administrators (built-in local)	Administrators has complete control over all domain controllers and all directory content stored in the domain,

	and it can change the membership of all administrative groups in the domain.
	Domain Admins (global) Domain Admins has complete control over all domain controllers and all directory content stored in the domain.
Server Operators (built-in local)	Server Operators can perform maintenance tasks, such as backup and restore, on domain controllers.
Account Operators (built-in local)	Account Operators can create and manage users and groups in the domain, but it cannot manage service administrator accounts.
Backup Operators (built-in local)	Backup Operators can perform backup and restore operations on domain controllers.

Monitoring for Changes to a Security Group

To enable monitoring of changes to security groups, auditing must be enabled—otherwise, the changes will not be recorded in the event log. You should ensure that the Audit Account Management audit policy is configured to record success and failure events. This will ensure that you can alert on any changes to the groups. The event IDs that MOM will be configured to monitor are shown in Table C-2.

Table C-2. Event IDs

Event ID	Description
632	A member was added to a global group.
633	A member was removed from a global group.
636	A member was added to a local group.
637	A member was removed from a local group.

Creating an Alert for Changes to a Global Group

To enable MOM to monitor changes to the Enterprise Admins, Schema Admins, and Domain Admins groups, an alert needs to be configured. To create the MOM alert for changes to a global group, follow these steps:

1. Create a new rule group, called (for the purposes of this example) Active Directory Security.
2. Associate the Active Directory Security rule group to the Windows Server 2003 Domain Controllers and/or Windows 2000 Domain Controllers computer groups, depending on the version of your domain controllers.
3. Create a new Alert on or Respond to Event rule called Alert on Changes to Global Admins. In the description field, state that it will alert on changes to Domain Admins, Enterprise Admins, and Schema Admins.

4. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-1.

Field: Event Number

Condition: matches regular expression

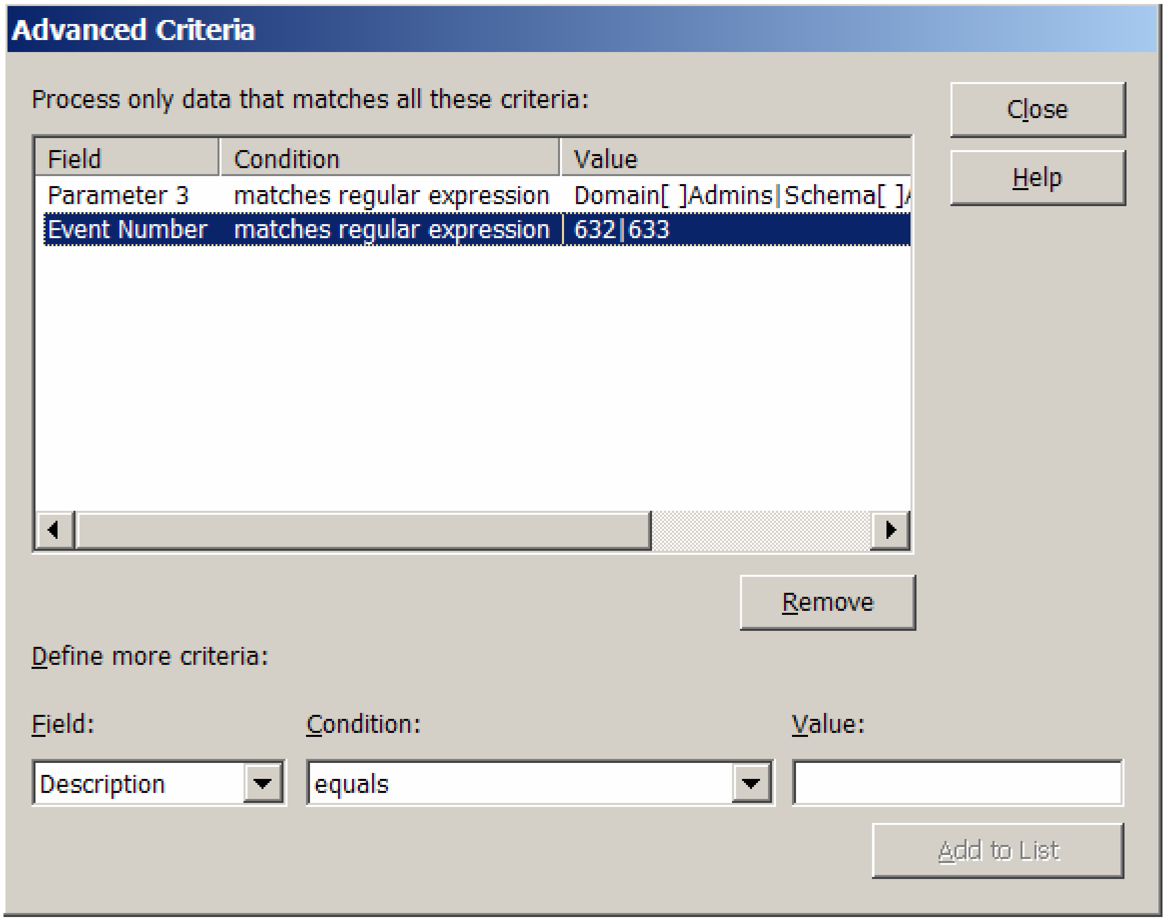
Value: 632|633

Field: Parameter 3

Condition: matches regular expression

Value: Domain[ ]Admins|Schema[ ]Admins|Enterprise[ ]Admins

Note Between the square brackets, there is a single space. This format is required for the regular expression to work.



Process only data that matches all these criteria:

Field	Condition	Value
Parameter 3	matches regular expression	Domain[ ]Admins|Schema[ ]
Event Number	matches regular expression	632|633

Define more criteria:

Field: Description

Condition: equals

Value:

Figure C-1. Advanced critera for global groups

5. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked. This will allow alert to suppression to be active only if the computer names, domains, and descriptions are identical. This will stop changes to the monitored groups being missed, as a new alert will be generated (instead of the repeat count increasing on the existing alert).

6. On the Alert tab, configure the Alert Severity as a Security Issue.

Creating an Alert for Changes to a Built-In Group

To enable MOM to monitor changes to the Administrators, Server Operators, Account Operators, and Backup Operators groups, you need to configure an alert. To create the MOM alert for changes to a built-in group, follow these steps:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on Changes to Built-in Admins. In the description field, state that it will alert on changes to Backup Operators, Administrators, Account Operators, and Server Operators.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-2.

Field: Event Number

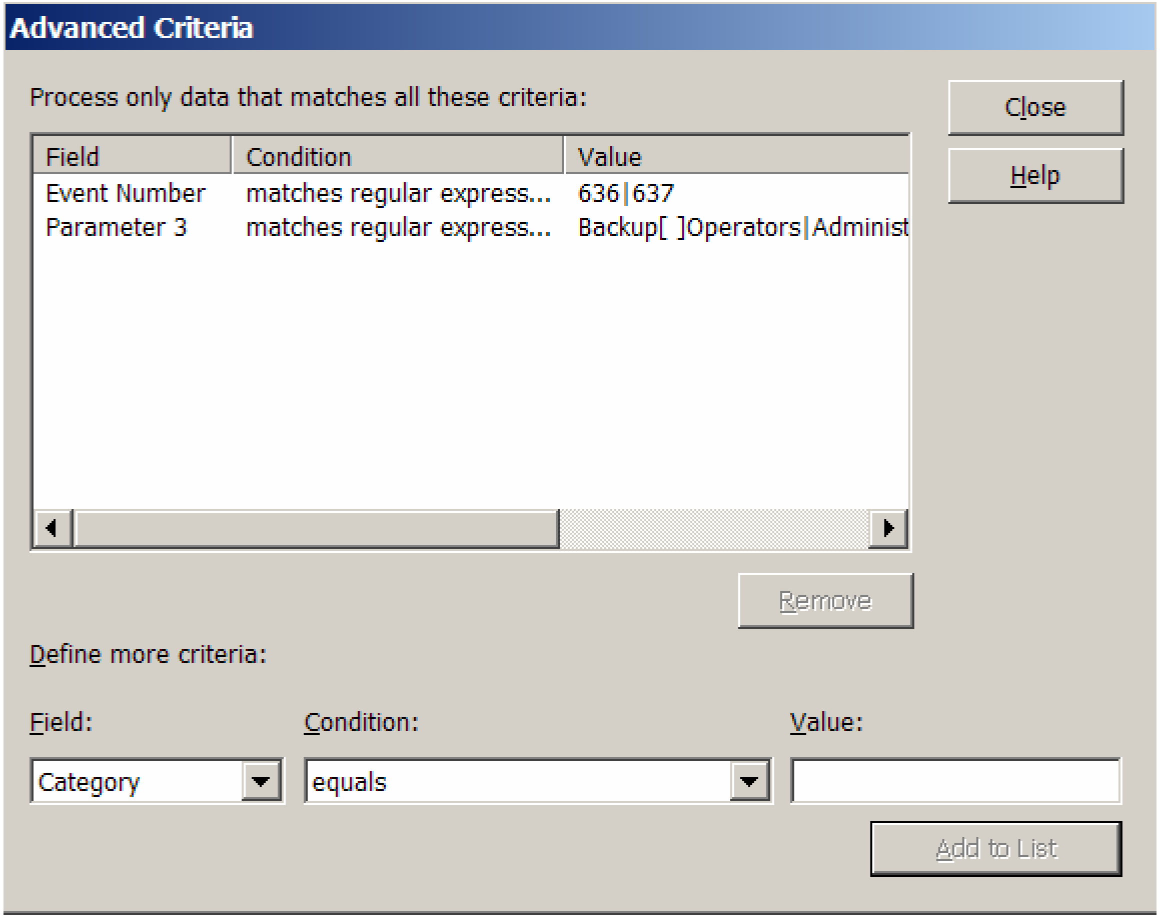
Condition: matches regular expression

Value: 636|637

Field: Parameter 3

Condition: matches regular expression

Value: Backup[ ]Operators|Administrators|Account[ ]Operators|Server[ ]Operators



Advanced Criteria

Process only data that matches all these criteria:

Field	Condition	Value
Event Number	matches regular express...	636|637
Parameter 3	matches regular express...	Backup[ ]Operators|Administ

Define more criteria:

Field: Category

Condition: equals

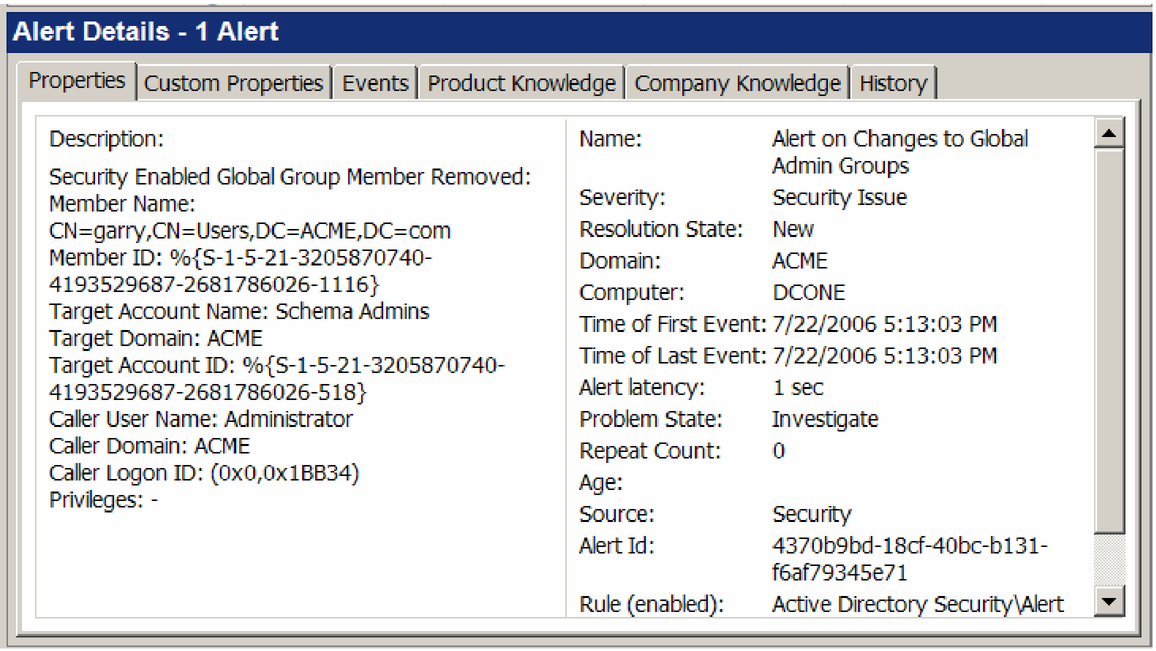
Value:

Figure C-2. Advanced criteria for built-in groups

3. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked. On the Alert tab, configure the Alert Severity as a Security Issue.

Resolving Security GUIDs and SIDs

The output from the alert is shown in Figure C-3. Some fields in the description are not represented correctly. Only the SID/GUID is visible.



Description:

Security Enabled Global Group Member Removed:
Member Name:
CN=garry,CN=Users,DC=ACME,DC=com
Member ID: %{S-1-5-21-3205870740-4193529687-2681786026-1116}
Target Account Name: Schema Admins
Target Domain: ACME
Target Account ID: %{S-1-5-21-3205870740-4193529687-2681786026-518}
Caller User Name: Administrator
Caller Domain: ACME
Caller Logon ID: (0x0,0x1BB34)
Privileges: -

Name:	Alert on Changes to Global Admin Groups
Severity:	Security Issue
Resolution State:	New
Domain:	ACME
Computer:	DCONE
Time of First Event:	7/22/2006 5:13:03 PM
Time of Last Event:	7/22/2006 5:13:03 PM
Alert latency:	1 sec
Problem State:	Investigate
Repeat Count:	0
Age:	
Source:	Security
Alert Id:	4370b9bd-18cf-40bc-b131-f6af79345e71
Rule (enabled):	Active Directory Security\Alert

Figure C-3. An example alert

By default, MOM does not resolve SIDs/GUIDs to their friendly names. You can configure the MOM agent to resolve the SIDs/GUIDs by adding the following registry value to the registry using `regedit`:

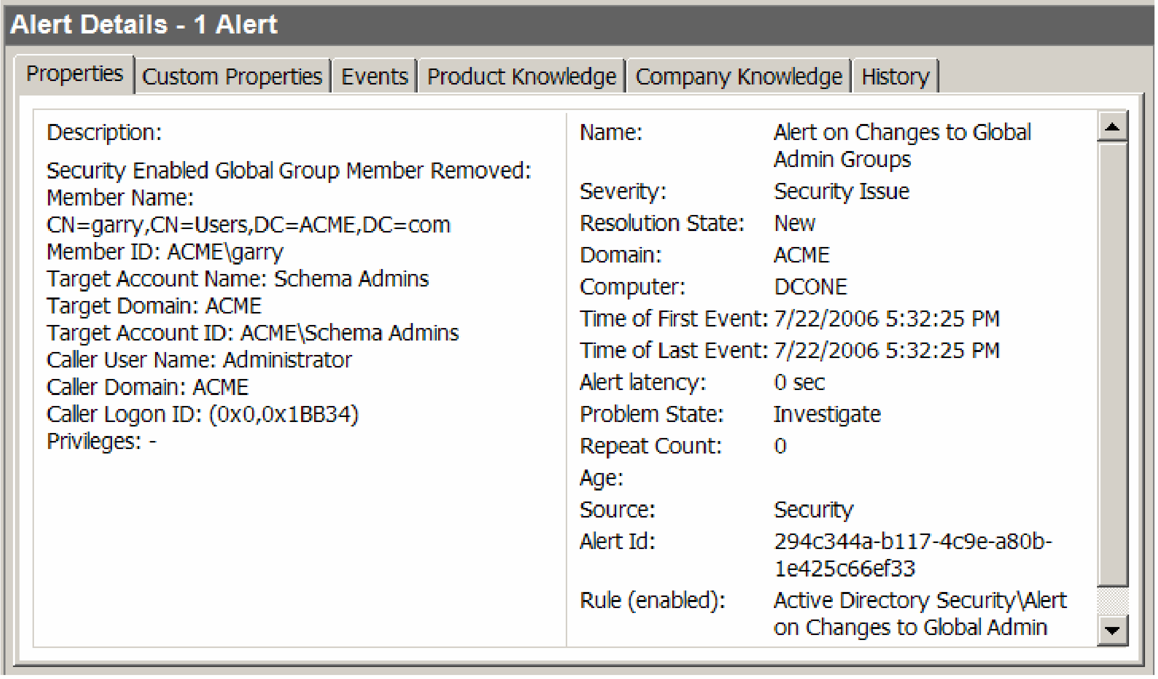
Registry Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Mission Critical Software\OnePoint`

Name: `ResolveGUID`

Type: `Dword`

Value: `00000001`

After adding this key to the registry, be sure to restart the MOM service. Figure C-4 shows the alert once the registry value has been added.



Description:

Security Enabled Global Group Member Removed:
Member Name:
CN=garry,CN=Users,DC=ACME,DC=com
Member ID: ACME\garry
Target Account Name: Schema Admins
Target Domain: ACME
Target Account ID: ACME\Schema Admins
Caller User Name: Administrator
Caller Domain: ACME
Caller Logon ID: (0x0,0x1BB34)
Privileges: -

Name:	Alert on Changes to Global Admin Groups
Severity:	Security Issue
Resolution State:	New
Domain:	ACME
Computer:	DCONE
Time of First Event:	7/22/2006 5:32:25 PM
Time of Last Event:	7/22/2006 5:32:25 PM
Alert latency:	0 sec
Problem State:	Investigate
Repeat Count:	0
Age:	
Source:	Security
Alert Id:	294c344a-b117-4c9e-a80b-1e425c66ef33
Rule (enabled):	Active Directory Security\Alert on Changes to Global Admin

Figure C-4. An example alert after a key has been enabled

If the MOM infrastructure is not at SP1 and it is then upgraded, the registry must be configured again, as the SP1 upgrade can remove the registry key.

Monitoring Changes to Organizational Units (OUs)

OUs within Active Directory provide a way to delegate control over part of the directory to a user or group of users. Every object in Active Directory, including each object within an OU and the OU itself, has an access control list that can be modified to suit the security needs of your environment. Any changes to OUs need to be monitored to ensure that no unauthorized changes are made. Before MOM can monitor these events, the `ResolveGUID` registry key must be configured; otherwise, none of the alerts that you define will work. The preceding “Resolving Security GUIDs and SIDs” section shows how you can enable this key.

Creating an Alert for New OUs Being Created

It is important to monitor for the creation of new OUs to ensure that no unauthorized changes are made to your Active Directory design. The following steps show you how to create an alert to monitor for OU creations:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on New OU Creation. In the description field, state that it will alert on new OUs being created.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-5.

Field: Event Number

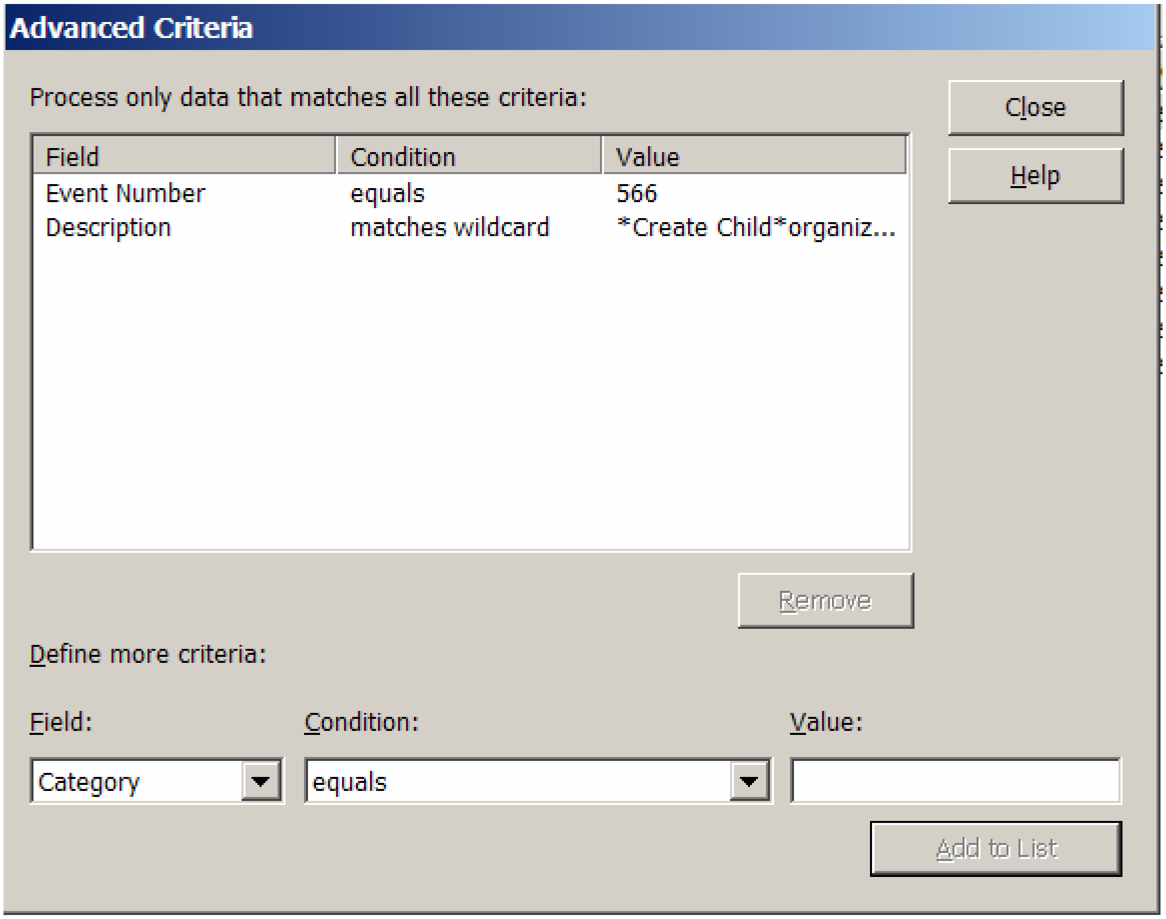
Condition: equals

Value: 566

Field: Description

Condition: matches wildcard

Value: *Create Child*organizationalUnit*



Process only data that matches all these criteria:

Field	Condition	Value
Event Number	equals	566
Description	matches wildcard	*Create Child*organiz...

Define more criteria:

Field: Category

Condition: equals

Value:

Figure C-5. Advanced critera for the New OU Creation alert

3. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked. On the Alert tab, configure the Alert Severity as a Security Issue.

Creating an Alert for OUs Being Deleted

If an OU is deleted, then any Active Directory objects that are located under that OU will also be deleted. Configuring MOM to alert on OU deletions will not stop the deletion from happening, but the alert will tell you what has happened and who carried out the deletion. The following steps show you how to create an alert to monitor for OU deletions:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on OU Deletion. In the description field, state that it will alert on an OU being deleted.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-6.

Field: Event Number

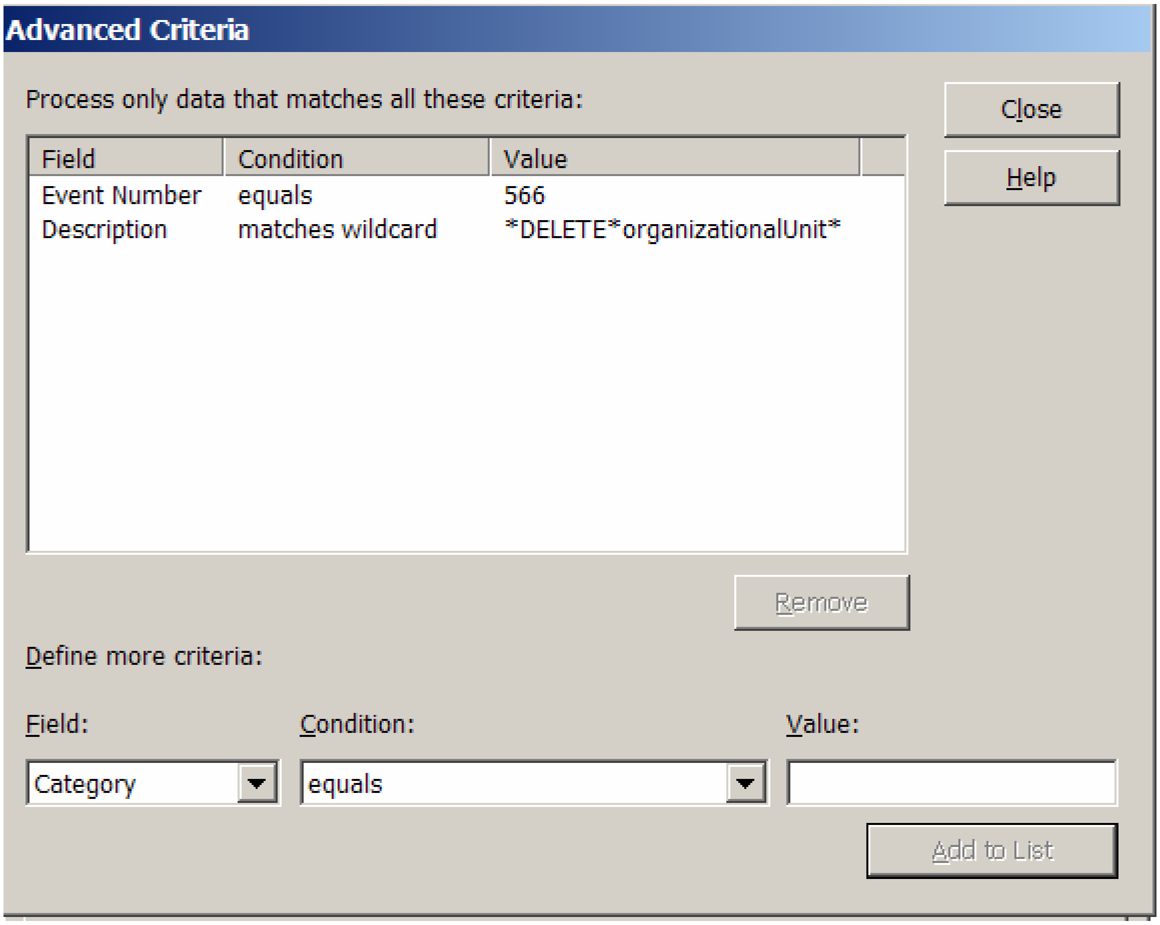
Condition: equals

Value: 566

Field: Description

Condition: matches wildcard

Value: *DELETE*organizationalUnit*



Advanced Criteria

Process only data that matches all these criteria:

Field	Condition	Value
Event Number	equals	566
Description	matches wildcard	*DELETE*organizationalUnit*

Define more criteria:

Field: Category

Condition: equals

Value:

Figure C-6. Advanced critera for the New OU Deletion alert

3. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked. On the Alert tab, configure the Alert Severity as a Security Issue.

Creating an Alert for OUs Whose Security Is Being Modified

Any change to an OU’s security should be monitored, as it could lead to a security hole or cause unexpected problems (e.g., if a change were carried out on a OU that contained user accounts that removed the security attributes that allowed the user to query which group they are a member of). This would mean that any logon scripts that were based on mapping drives based on user group membership would fail for the accounts under that OU. To enable MOM to monitor for changes to OU security, the following steps need to be carried out:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on OU Security Modification. In the description field, state that it will alert on an OU’s security being modified.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-7.

Field: Event Number

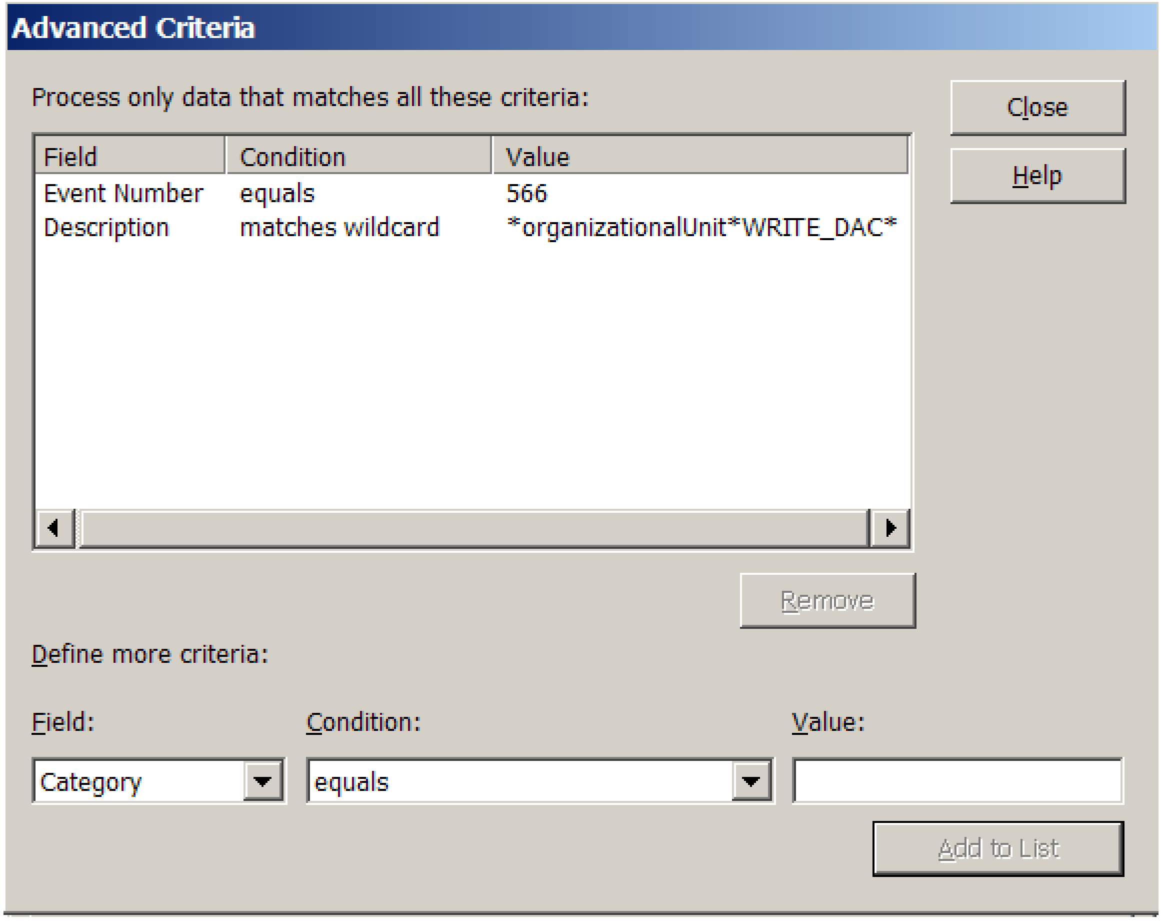
Condition: equals

Value: 566

Field: Description

Condition: matches wildcard

Value: *organizationalUnit*WRITE_DAC*



Process only data that matches all these criteria:

Field	Condition	Value
Event Number	equals	566
Description	matches wildcard	*organizationalUnit*WRITE_DAC*

Define more criteria:

Field: Category

Condition: equals

Value:

Figure C-7. Advanced critera for the New OU Security Modification alert

3. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked. On the Alert tab, configure the Alert Severity as a Security Issue.

Monitoring Changes to a Group Policy Object (GPO)

A group policy object (GPO) is a collection of settings that define what a system will look like and how it will behave for a defined group of users. GPOs can configure registry-based polices, security options, software installation and maintenance options, script options, and folder redirection options.

If a GPO is incorrectly configured, it can result in serious problems with the systems that it has been assigned to. In extreme situations, it can stop those systems from functioning correctly. It is therefore important that GPO creation and modification is controlled and monitored. Before MOM can monitor these events, the `ResolveGUID` registry key must be enabled; otherwise, none of the alerts that you define will work. The earlier “Resolving Security GUIDs and SIDs” section shows how you can enable this key.

Creating an Alert for a GPO Being Created

A misconfigured GPO could potentially cause serious issues on any machine or user that has the GPO applied to it. MOM cannot stop the creation of GPOs, but it can give you an alert on any changes and who made them. The following steps will show you how to create an alert for the creation of any new GPOs:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on New GPO. In the description field, state that it will alert when a new GPO is created.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-8.

Field: Event Number

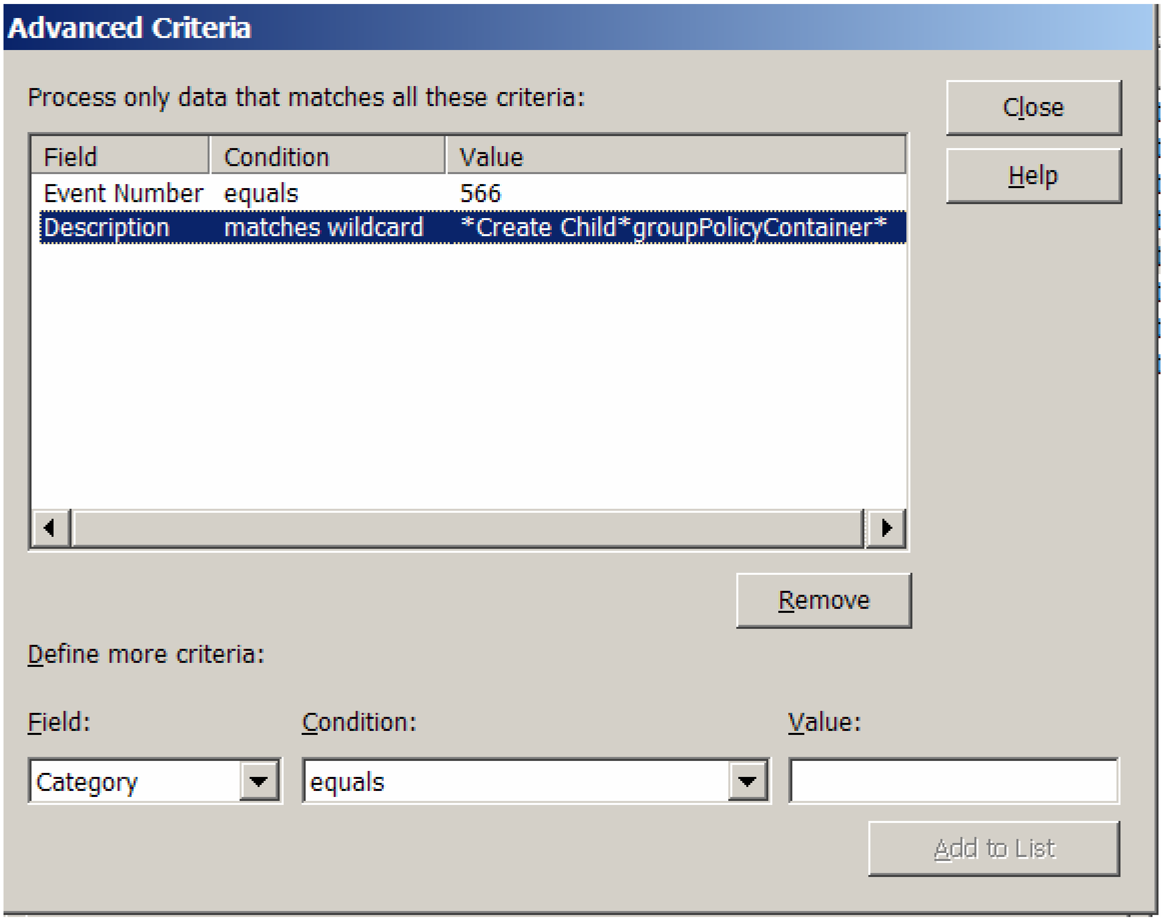
Condition: equals

Value: 566

Field: Description

Condition: matches wildcard

Value: *Create Child*groupPolicyContainer*



Advanced Criteria

Process only data that matches all these criteria:

Field	Condition	Value
Event Number	equals	566
Description	matches wildcard	*Create Child*groupPolicyContainer*

Define more criteria:

Field: Category

Condition: equals

Value:

Figure C-8. Advanced critera for the New GPO alert

3. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked, and configure the Alert Severity as a Security Issue.

When monitoring GPO creation, you will often have four alerts created per GPO. This is normal, as the event ID is created four times with slightly different values each time in the event log.

Creating an Alert for a GPO Being Modified

Modifications to GPOs should be monitored, as the alerts can be used to track unauthorized changes and also help in troubleshooting. If, for example, a GPO linked to all clients in the New York OU has been changed, and the users in New York are now raising help desk calls, then the GPO change could be the root cause of the issue. The following steps will show you how to create an alert for the modification of a GPO:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on a GPO Being Modified. In the description, field state that it will alert when a GPO is modified.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-9.

Field: Event Number

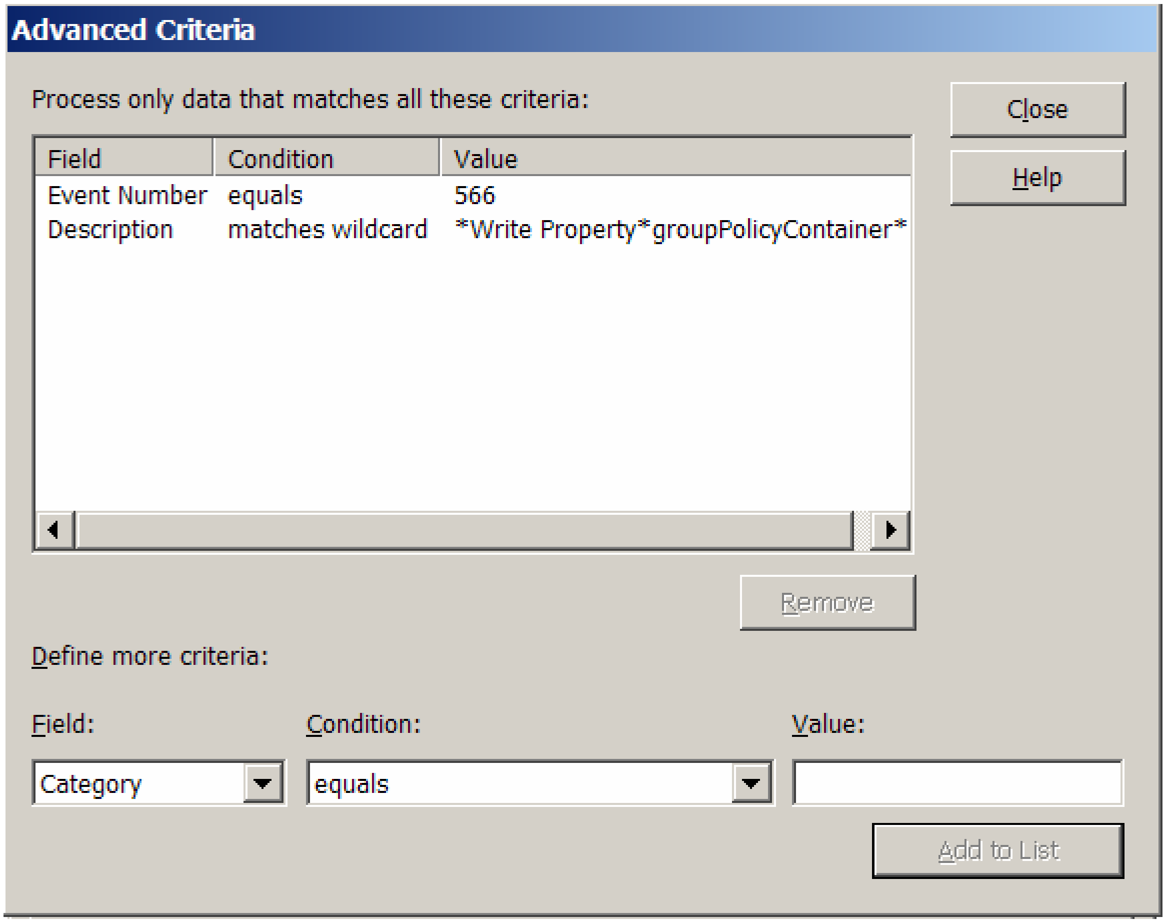
Condition: equals

Value: 566

Field: Description

Condition: matches wildcard

Value: *Write Property*groupPolicyContainer*



Process only data that matches all these criteria:

Field	Condition	Value
Event Number	equals	566
Description	matches wildcard	*Write Property*groupPolicyContainer*

Define more criteria:

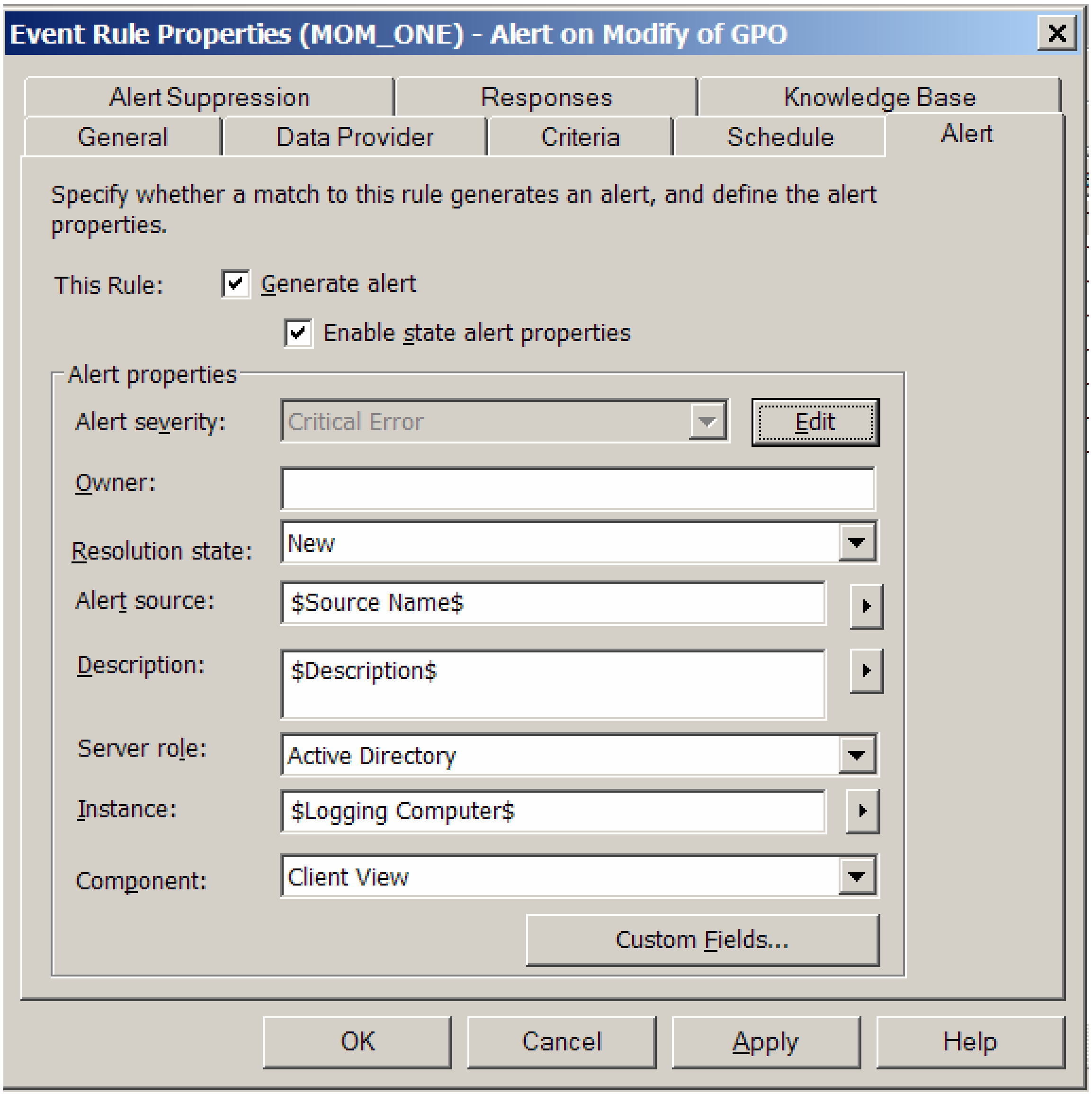
Field: Category

Condition: equals

Value:

Figure C-9. Advanced critera for the Modify GPO alert

3. On the Alert tab, check "Enable state alert properties" (as shown in Figure C-10), and then click Edit.



Event Rule Properties (MOM_ONE) - Alert on Modify of GPO

Specify whether a match to this rule generates an alert, and define the alert properties.

This Rule: ☑ Generate alert

☑ Enable state alert properties

Alert properties

Alert severity: Critical Error

Owner:

Resolution state: New

Alert source: $Source Name$

Description: $Description$

Server role: Active Directory

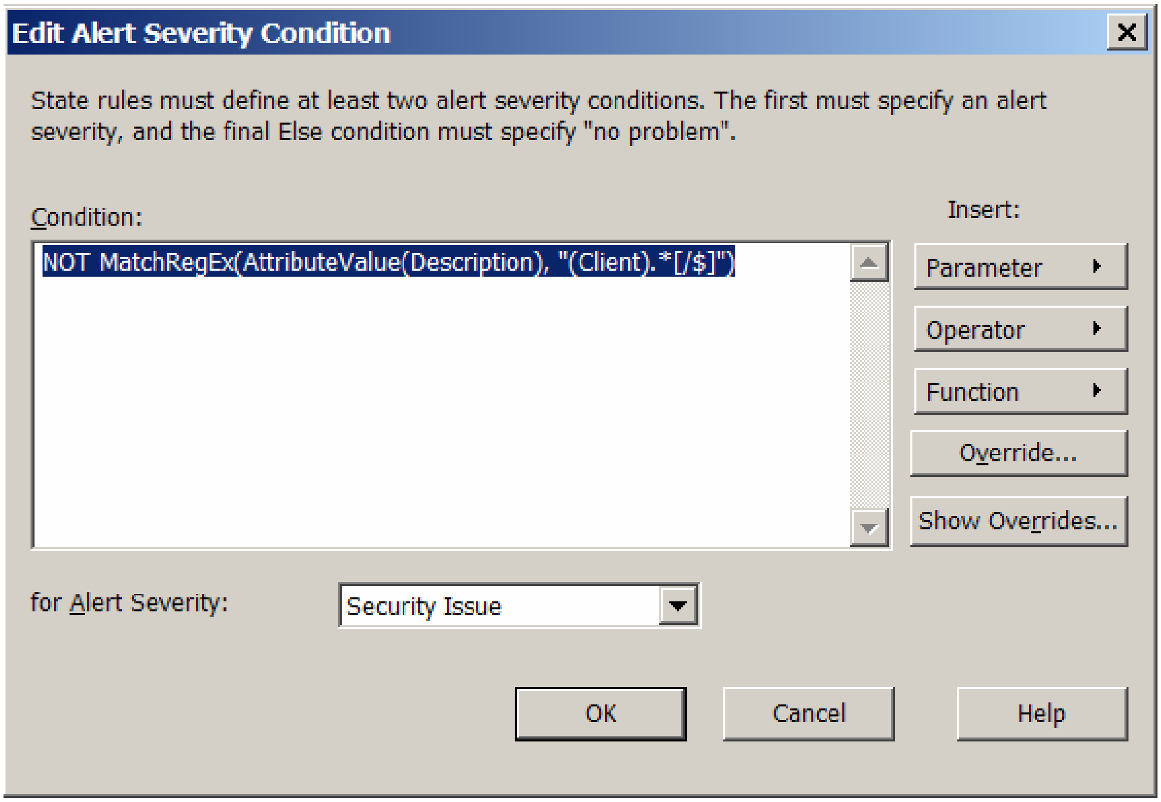
Instance: $Logging Computer$

Component: Client View

Figure C-10. Alert properties for the Modify GPO alert

4. On the Alert Severity Calculation for State rule, click Add.

5. Add NOT MatchRegEx(AttributeValue(Description), "(Client).*[/$") to the Condition field. On the Alert tab, configure the Alert Severity as a Security Issue (as shown in Figure C-11), and then click OK.



State rules must define at least two alert severity conditions. The first must specify an alert severity, and the final Else condition must specify "no problem".

Condition:

```
NOT MatchRegEx(AttributeValue(Description), "(Client).*[/$]")
```

for Alert Severity: Security Issue

Figure C-11. Severity condition for the Modify GPO alert

6. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked.

By enabling the matching regular expression in the alert state, you will prevent alerts from being generated by the domain controller if the domain controller itself updates a GPO (e.g., the Default Domain Controllers policy).

Creating an Alert for a GPO Being Deleted

If a GPO is deleted, then the configuration settings that were applied via the GPO will be lost. This could introduce security or configuration issues on the machines or users that the GPO was applied to. It is therefore very important that any GPO deletions are tracked. The following steps should be carried out to configure an alert for GPO deletions:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on GPO being deleted. In the description field, state that it will alert when a GPO is deleted.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-12.

Field: Event Number

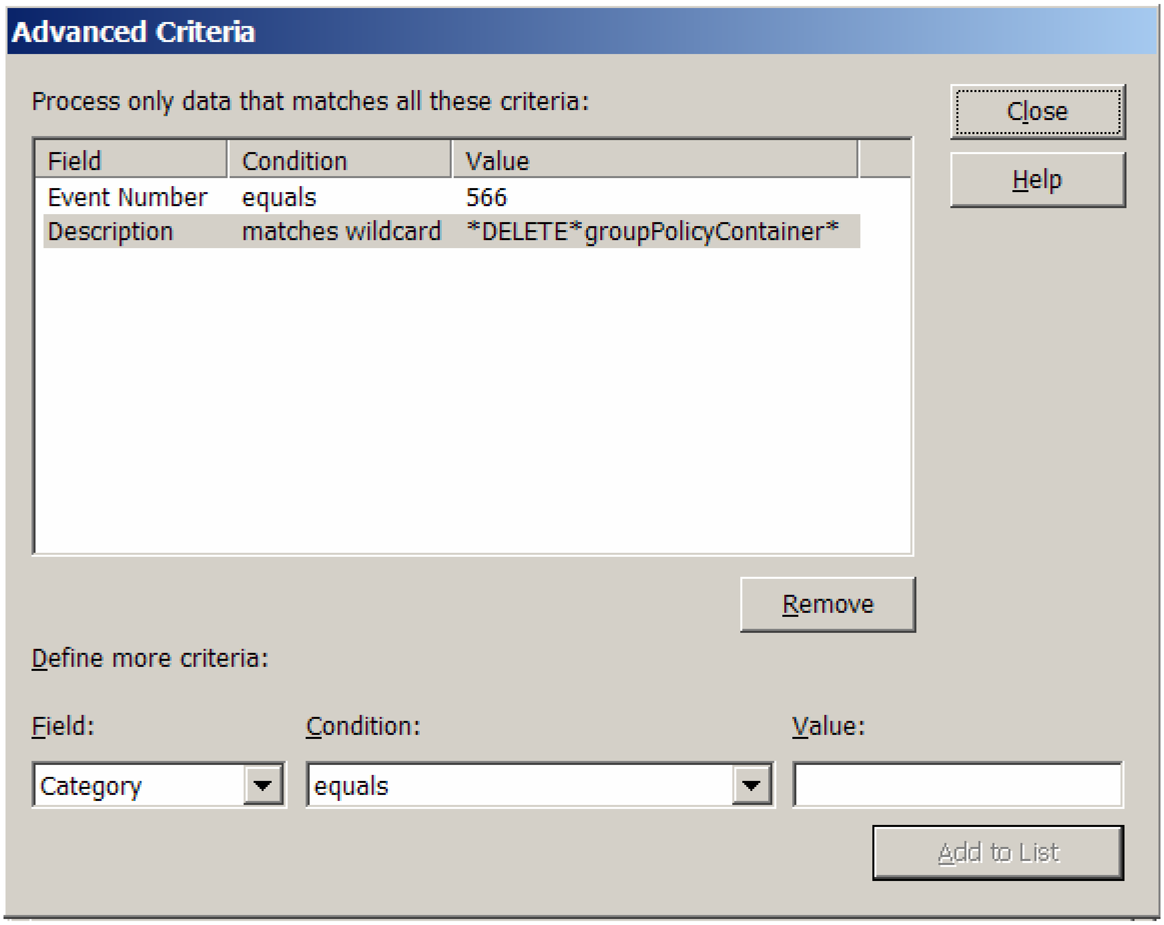
Condition: equals

Value: 566

Field: Description

Condition: matches wildcard

Value: *DELETE*groupPolicyContainer*



Process only data that matches all these criteria:

Field	Condition	Value
Event Number	equals	566
Description	matches wildcard	*DELETE*groupPolicyContainer*

Define more criteria:

Field: Category

Condition: equals

Value:

Figure C-12. Severity condition for the GPO Deletion alert

3. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked. On the Alert tab, configure the Alert Severity as a Security Issue.

Creating an Alert for a GPO Being Linked

GPOs can be linked to OUs so that the settings that are contained in that GPO are applied to the objects in that OU that match any of the security filtering that may be applied to the GPO. It is therefore important that when GPOs are linked to OUs, an alert is created so that changes can be verified to ensure that they are correct and that the change was authorized. To configure MOM to alert on any GPOs that are linked, the following steps need to be carried out:

1. Under the Active Directory Security rule group, create a new Alert on or Respond to Event rule called Alert on GPO being linked. In the description field, state that it will alert when a GPO is linked.
2. On the Criteria tab of the alert, configure the following advanced criteria. An example is shown in Figure C-13.

Field: Event Number

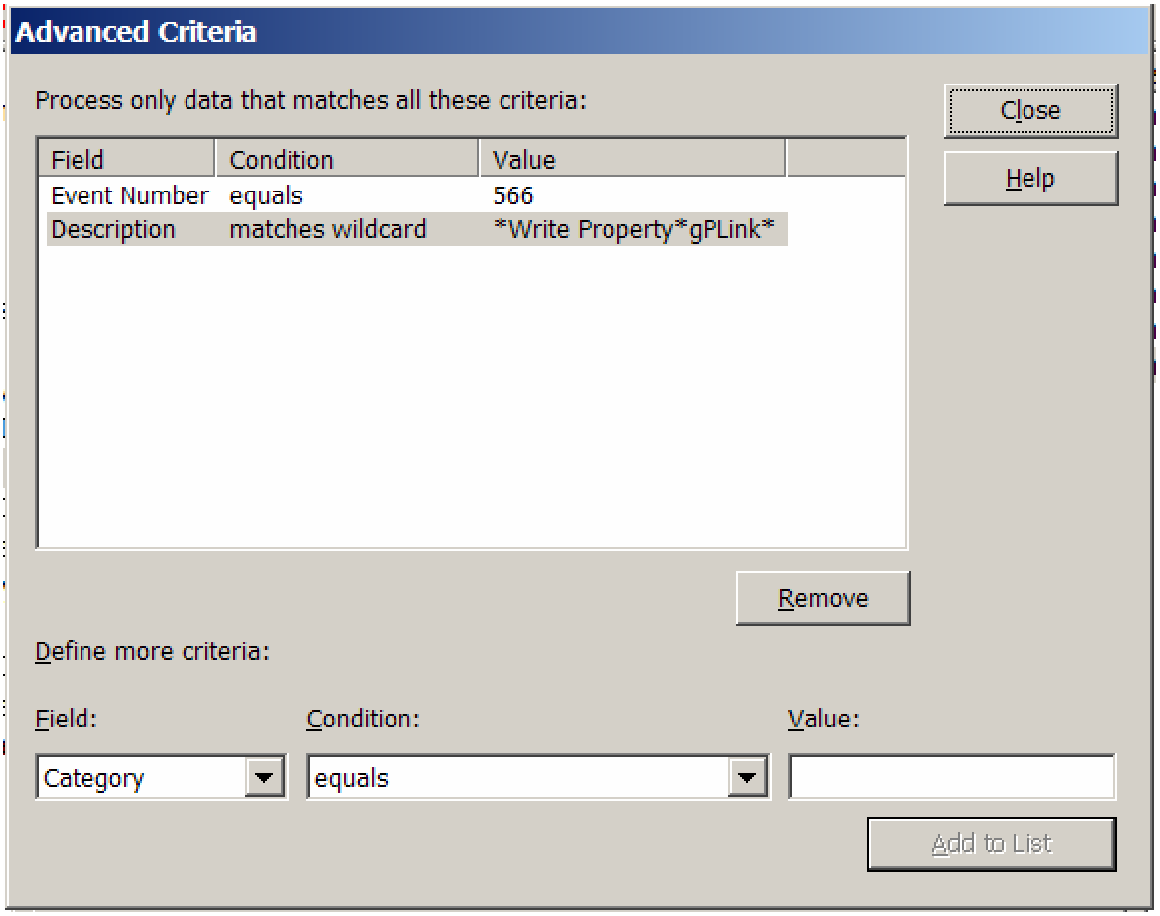
Condition: equals

Value: 566

Field: Description

Condition: matches wildcard

Value: *Write Property*gPLink*



Process only data that matches all these criteria:

Field	Condition	Value
Event Number	equals	566
Description	matches wildcard	*Write Property*gPLink*

Define more criteria:

Field: Category

Condition: equals

Value:

Figure C-13. Severity condition for the GPO Link alert

3. On the Alert Suppression tab, ensure that Computer, Domain, and Description are checked. On the Alert tab, configure the Alert Severity as a Security Issue.

Understanding GPO Alerts

When a GPO is created, the common name is recorded in the event log. Here’s an example:

```
Event Type: Success Audit
Event Source:Security
Event Category: Directory Service Access
Event ID:566
Date:7/22/2006
Time:7:43:14 PM
User:ACME\Administrator
Computer:DCONE
Description:
Object Operation:
 Object Server:DS
 Operation Type:Object Access
 Object Type:groupPolicyContainer
 Object Name:CN={5AA06240-9A9C-4AC6-
ADC6E7983C11758A},CN=Policies,CN=System,DC=ACME,DC=com
```

The friendly name can be found by using a script that is included with the Group Policy Management Console. The script `DumpGPOInfo.wsf` is located by default in `C:\Program Files\GPMC\Scripts\`, and can be run by passing the common name of the GPO to the script. Following is an example:

```
Cscript DumpGPOInfo.wsf {3120-016D-11D2-945F-0C0F9} /domain:acme.com
```

This command will return information such as the following:

```
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

==============================================
Name:Default Domain Policy
ID:{31B2F340-016D-11D2-945F-00C04FB984F9}

-- Details --
Created:5/8/2006 8:55:58 PM
Changed:5/8/2006 9:04:54 PM
Owner:ACME\Domain Admins

User Enabled:True
Mach Enabled:True

-- Version Numbers --
User DS:1
User Sysvol:1
Mach DS:3
Mach Sysvol:3

-- Who this GPO applies to --
Authenticated Users
```

```
s
-- Who can edit this GPO --

-- Who can edit settings, modify security, and delete this GPO --
Domain Admins
Enterprise Admins
SYSTEM

-- Who only has read access --
ENTERPRISE DOMAIN CONTROLLERS

-- Who has custom permissions –

-- Where this GPO is linked (Sites,Domain,OU) --
ACME.com (Domain)

==============================================
```

The output of the `DumpGPOInfo.wsf` script will allow you to easily see which GPO has changed so that you can investigate what has been altered. The GPO alert will tell you who made the change—therefore, the first point of call should be the administrator who made the change so that you can verify that the change was authorized.