



NetExpert[®] 10

Advanced Fault Manager

Configuration Guide

Revision Record

The following log shows revision history (Table 1). Refer to the *NetExpert Release Notes* for a detailed list of enhancements.

Table 1 Revision History Log

Date	Version	Description
Jul. 11, 2017	10.2.1	Added CBR LOD policy template changes.
May 19, 2015	10.1.0	Added the Dynamically Update Correlation Alert Severity option.
Jul. 9, 2014	10.1.0	Added DMPAlarmClearTime attribute.
Sep. 4, 2013	10.1.0	Remove regular expression from the Correlate by Pattern, Correlation Alert panel object name description. Added that the correlation options are available for Correlate by Relationship – Load on Demand uncorrelate policies.
Jun. 5, 2013	10.1.0	Added Correlation by Naming Convention. Added correlation options to the Policy Actions panel. Added client/server mismatch information. Noted that you can configure database reconnect attempts. Added a note about the use of object attribute filtering. Remove attribute references from the Correlation Alert panel.
Jul. 30, 2012	10.0.0	Initial release.

Technical Support Center

If you need product assistance or if you have suggestions, contact the Objective Systems Integrators (OSI) technical support site in your area listed at: <http://tac.osi.com/>

Support representatives are available between 6:00 AM and 5:00 PM, Monday through Friday, Pacific Standard Time, or between 9:00 AM and 6:00 PM Singapore and London, England time zones.

Before you contact the support center, record the actions you took before you experienced the problem. Then describe those actions and the problem to the technical support engineer.

Note that support staff located in the USA are English-speaking only. If you need help communicating with our staff in a language other than English, please contact your local OSI sales or support representative.

While the support staff will assist you with questions relating to NetExpert products and their interfaces with the required Oracle relational database management software, support for any such Oracle software that you have acquired directly from Oracle or an Oracle reseller must be obtained from Oracle.

Find a Documentation Mistake?

We encourage comments about this document. Contact OSI technical support. A representative passes your comments to the Technical Publications Department.

NOTE

OSI continually strives to provide its customers with current, accurate, and complete information to assist them in the use of our products. The OSI documents available from the technical support website contain up-to-the minute changes that occurred after the preparation of this guide.

You must log on to <http://tac.osi.com> before you can access these documents.

Important Information

This notice discusses the following important information about OSI products and guides:

- [Conventions Used](#)
- [NetExpert Default Date Displays](#)
- [Avoid These Special Characters](#)
- [Entering Field Values](#)

Conventions Used

NetExpert guides use the following conventions (Table 2).

Table 2 Documentation Conventions Used (Sheet 1 of 2)

Conventions	Description
<i>Italic</i>	Italic indicates document titles and variables, such as <i>filename</i> , in computer input and output. It also indicates links to glossary terms.
Bold	Bold identifies important words.

Table 2 Documentation Conventions Used (Sheet 2 of 2)

Conventions	Description
Sans serif	Sans serif shows call outs, file names, UNIX paths, and environment variables.
Courier	Courier denotes computer input and output.
[abc]	Square brackets enclose optional syntax for computer input.
<TAB>	Angle brackets indicate actual keyboard keys, such as <ENTER> or <SPACE>.
File Save	A vertical bar separates menu options.
Ctrl+X Alt+Y	Ctrl+X means to press and hold the <CTRL> key while you press the <X> key. Alt+Y means to press and hold the <ALT> key while you press the <Y> key.
NOTE	A note gives readers special information about the product or procedure that is apart from the general discussion.

NetExpert Default Date Displays

Date displays and time formats in NetExpert systems default to a four-digit year. When a two-digit date is received as input, the NetExpert system computes years 00–68 as 2000–2068, and years 69–99 as 1969–1999.

When building NetExpert rules, events, and alerts, specify four-digit years using the @TimeFmt intrinsic. For more information about this subject, refer to the *NetExpert Rule Language Reference Guide* or *NetExpert Rule Builder User Guide*.

Avoid These Special Characters

Avoid using these special characters when creating managed object names or creating other names, such as templates, instances, events, KPIs, and so on.

```
# @ $ ' " / \ ! & * ( ) + | [ ] ? < > . ; : { } <TAB> <CR>
<SPACE> ` (back tick)
```

CAUTION

Although the NetExpert Object Editor allows you to name managed objects using special characters, these characters can cause conflicts.

When NetExpert processes special characters in the following ways, they can be misinterpreted:

- Passing these characters to the UNIX operating system
- Passing these characters as parameters
- Interpreting or parsing the characters (delimiters)
- Creating managed objects during runtime using these characters (can place special characters into your NetExpert MIB [Management Information Base])

Contents

Introduction	13
In This Guide	14
Intended Audience	14
Advanced Fault Manager Overview	15
Features and Benefits	15
Alarm Processing	16
Alert Property List	19
Attribute List	22
Constructed Attribute Lists	23
Relationship to DMP	24
DMP Policy Templates	24
Cross-Template Policy Processing	25
Co-Existing with FM eXEL	27
Prerequisites	28
Related Documents	28
Preparing to Configure AFM	29
Verifying Your Installation	30
Starting Policy Builder	32
Starting from the Launch Pad	33
Starting from a Script	34
Starting from the Windows Desktop	35
Exiting Policy Builder	36
Creating AFM Policies	37
Creating Fault Management Policies	38
Delaying Alarm Processing	40
Defining Delay Policies	43
Defining Delay All Alarms	46
Defining Delay Clear/Non-Clear Alarms	48
Planning Outages	51
Processing Planned Outages	51
Defining Planned Outages	53
Setting Alert Severity Thresholds	55
Processing Thresholds	56
Defining Threshold Policies	57
Setting Threshold – Perform Actions Parameters	61
Escalating Alerts	66
Throttling Event Storms	73

Contents

Correlating Alerts by Naming Convention	77
Using Attribute References	78
Defining the Correlated Alert List	78
Defining the Correlation Alert	82
Correlating Actions	84
Uncorrelating Actions	86
Specifying Incoming Alarm Processing	88
Correlating Alerts by Pattern	90
Using Attribute References	90
Defining the Correlated Alert List	91
Defining the Correlation Alert	94
Correlating Actions	97
Uncorrelating Actions	99
Specifying Incoming Alarm Processing	101
Suppressing Alerts by Pattern	103
Defining the Correlated Alert List	103
Defining the Suppression Alert List	107
Specifying Incoming Alarm Processing	110
Correlating Alerts by Relationship	112
Defining the Relationship Tree	112
Defining the Correlation Tree Level	113
Including Child Relationships	115
Defining Correlation Processing	117
Defining the Correlation Alert	118
Defining Correlation Actions	120
Defining Uncorrelation Actions	122
Specifying Incoming Alarm Processing	124
Correlating Large Numbers of MO Trees	126
Defining the Relationship Tree	126
Defining the Correlation Tree Level	127
Including Child Relationships	129
Defining Correlation Processing	132
Defining the Correlation Alert	133
Defining Correlation Actions	135
Defining Uncorrelation Actions	137
Specifying Incoming Alarm Processing	139
Correlating Sub-Trees by Relationship	141
Defining the Sub-Tree Relationship	141
Defining the Correlation	143
Including Child Relationships	145
Defining Correlation Processing	148
Defining Correlation Alerts	148
Defining Correlation Actions	151
Defining Uncorrelation Actions	153
Specifying Incoming Alarm Processing	155

Throttle Policy Panel	271
Pattern List Entry Window	274
Object Identification Panel	275
Alert Identification Panel	278
Attribute Filter Window	279
Property Name and Value Window	281
Policy Action Window	283
Event Action Window	286
Message Attribute Window	290
Property Designation	292
AFM and FMeXEL Feature Comparison	295
Introduction	296
Scenario Features	298
Policy Features	301
New Features	304
Co-Existing Notes	307
Glossary	309
Index	323



NetExpert® 10
Advanced Fault Manager
Configuration Guide

Introduction

- In This Guide [14](#)
- Intended Audience [14](#)
- Advanced Fault Manager Overview [15](#)
- Prerequisites [28](#)
- Related Documents [28](#)

Related Topics

- [Preparing to Configure AFM](#)
- [Creating AFM Policies](#)

The Advanced Fault Manager (AFM) application is a flexible tool for monitoring and managing faults that occur on your network elements.

The AFM application is built on the NetExpert Distributed Management Policies (*DMP*) architecture and uses *policies* to perform network fault management functions.

Correlating Sub-Trees by Relationship

Define **correlation sub-trees by relationship** policies to correlate alerts based on the count or percentage sub-trees that contain objects in an alert state.

Correlating sub-trees by relationship is similar to correlating alerts by relationship. The only difference is when correlating sub-trees by relationship:

- You specify one and only one level in the relationship tree as the sub-tree level. This must be below the correlate level in the relationship tree.
- A correlation occurs when the specified count or percentage of sub-trees with root at the sub-tree level contains at least one managed object that is in an alert state.
- The Root panel contains an option to define the sub-tree level as the current level.

From the Correlate Sub-Tree by Relationship panel, you can set the policy control parameters by:

- [Defining the Sub-Tree Relationship](#)
- [Defining Correlation Processing](#)
- [Defining Correlation Alerts](#)
- [Defining Correlation Actions](#)
- [Defining Uncorrelation Actions](#)
- [Specifying Incoming Alarm Processing](#)

Defining the Sub-Tree Relationship

The sub-tree relationship definition contains object (*MO*) and alert specifications for each level at which a relationship exists. When a correlation occurs, a **correlation alert** is generated.

By defining a sub-tree relationship, you identify the objects to consider when establishing the correlation and generating the correlation alert.

A correlation occurs when the specified count or percentage of sub-trees with root at the sub-tree level contains at least one managed object that is in an alert state.

When defining the sub-tree relationship, you must do the following:

- Define two or more levels.
- Generate the correlation alert at **one and only one** level.
- Define at least one relationship at each level that specifies a child level. You need not define a relationship at the last (bottom) level.
- Define a class name or object name for at least one level of the tree.
- Specify **one and only one** level in the relationship tree as the sub-tree level.

If you defined the following sub-tree relationship (Figure 7) and defined the correlation threshold with a count of two, a correlation does not occur involving the A managed object because only one of its sub-trees contains objects in an alert state. However, a correlation does occur involving the B managed object because two of its sub-trees contain objects in an alert state.

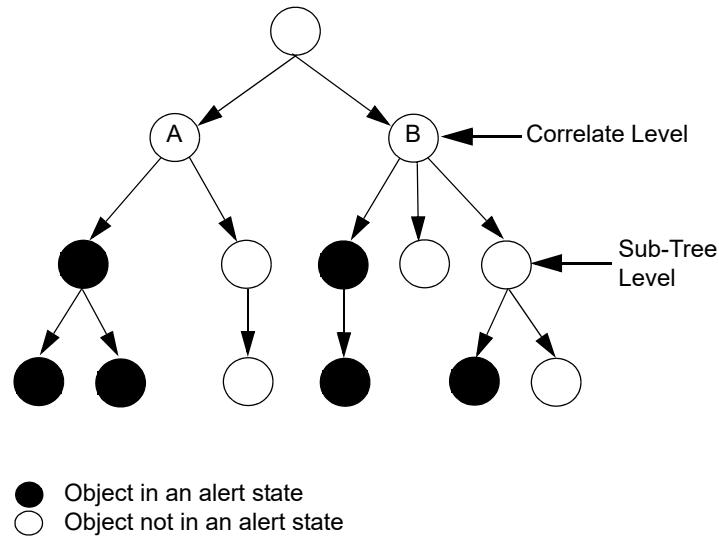


Figure 7 Correlation Relationship Sub-Trees

NOTE

Correlation by relationship policies recognize **all** MO relationship trees described by the policy, regardless of whether an alarm was directed to the policy.

Access the Root panel by selecting the Correlation Tree tab (Figure 8). Define the relationship tree, starting at the root level panel by:

- [Defining the Correlation](#)
- [Including Child Relationships](#)

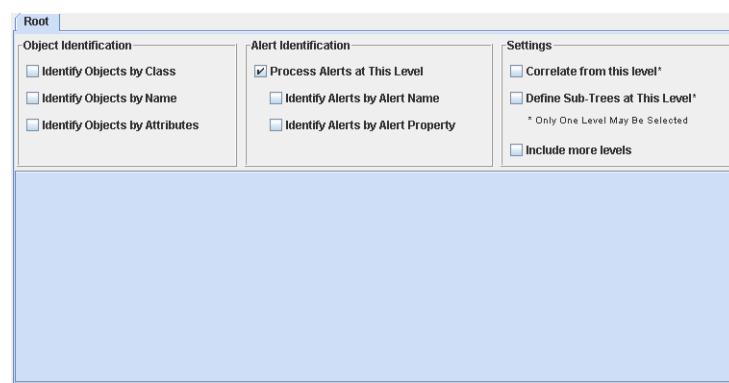


Figure 8 Root Panel

Object Identification Panel

Use the Object Identification panel (Figure 75) to define patterns that identify objects. The object class and name parameters are different for the naming convention policies than for the other policies by pattern.

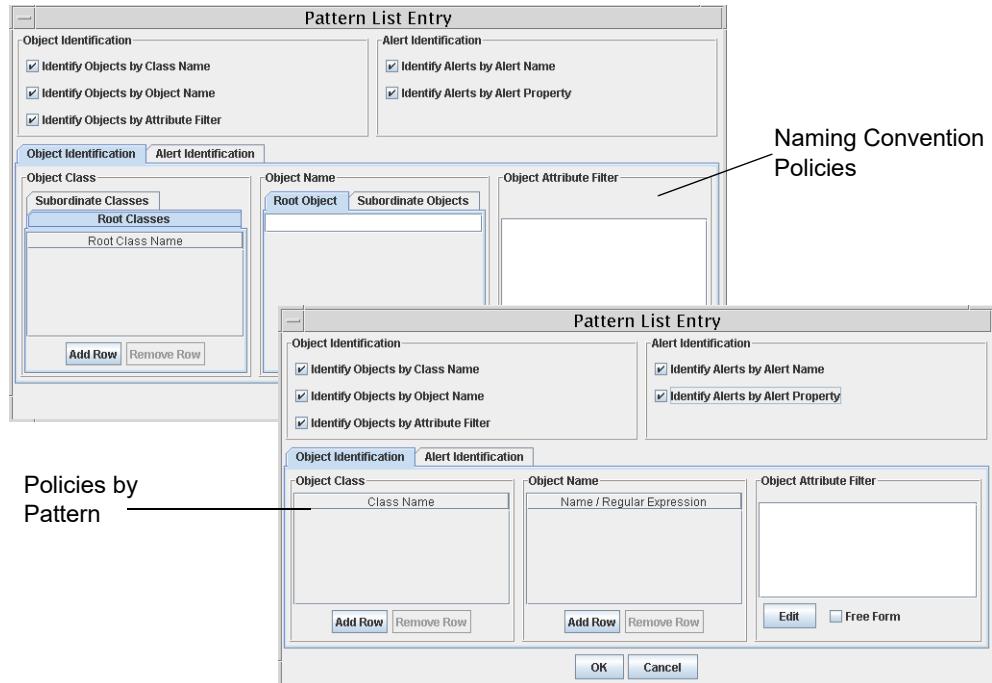


Figure 75 Object Identification Panel

Property Designation

Use the Property Designation window (Figure 83) to define alert properties and values used to identify or filter alerts properly. The property value parameters available depend on the identification type selected. Access the Property Designation window from the following policies by selecting the Identify Alerts by Alert Property option, selecting the Alert Identification tab, and then clicking the alert properties Add Row button.

- Correlate by Relationship
- Correlate Sub-Trees by Relationship

If you specify a property filter, the filter is applied only to active alerts.

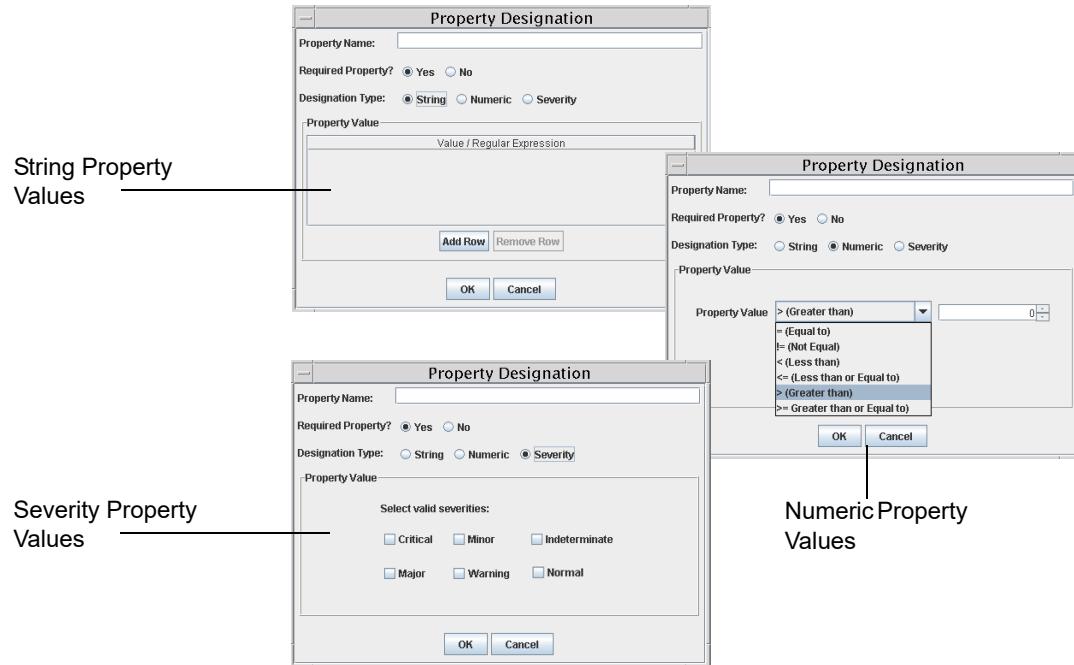


Figure 83 Property Identifier Window

The Property Designation window has the following alert property identifier control parameters (Table 86).

Table 86 Alert Property Identifier Parameters (Sheet 1 of 2)

Parameter	Description
Property Name	Specifies the name for the property. Type the property name. Right-clicking the field displays a list of properties to choose from.
Required Property	Indicates whether the alert must have this property with the appropriate value for the alert to be included in the correlation.



Glossary

This glossary defines the terms used to describe the policy-based applications, such as DMP, AFM, IPM, AD, APM, and Trouble Ticket Adapter.

Action	The final processing that a policy performs. One or more actions initiates trigger responses, or responses based on the result of a condition, such as generating an alert, updating an MO, or sending an email.
Admin Agent	A process that manages policy servers running on the agent's host. Admin agents are responsible for starting and stopping, identifying policies, performing heartbeat and health checks, and other administrative functions on policy servers. Admin agents use a centralized admin manager to report policy server failures and locate policies running on remote hosts.
Admin Manager	A process that supports admin agents in managing policy servers. While there are multiple admin agents, there is only one centralized admin manager. This process stores policy server configuration information, provides an interface to the DMP Administration Tool, coordinates the system-wide start up and shut down of policy servers with the admin agents, and performs other centralized functions for the admin agents.
Admin Repository	A set of database tables for storing DMP runtime configuration information accessed from the admin manager. You can also store the repository in the local file system where the AdminMgr process is running. The configuration information includes the number of policy servers and the policies running on a specific host.
Administration Tool	The DMP tool used to configure the system, deploy policies, administer and monitor the runtime system, and perform troubleshooting tasks.
Administrator	A person responsible for installing, configuring, and maintaining the NetExpert system. The administrator is often a NetExpert developer.

Index

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

tables (continued)
correlation alert parameters, 180, 189, 203, 215, 228
correlation parameters, 178, 187, 255
correlation processing, 201, 214
correlation processing parameters, 227
database parameters, 250
delay alarm message attributes, 43
delay all alarms behavior, 236
delay all alarms policy parameters, 237
delay clear/hon-clear alarms behavior, 240
delay non-clear alarms policy parameters, 241
delay policy parameters, 234
differences between the delay policies, 40
documentation conventions used, 4
effect of attributes in setting alert properties, 22
escalate actions parameters, 247
escalate alarm message attributes, 66
escalate parameters, 244
event action parameters, 288
event actions policies, 286
generate NetExpert event parameters, 268
incoming alarm parameters, 184, 193
invoke DMP policy parameters, 267
message attribute parameters, 290
new features AFM provides, 304
object identification parameters, 198, 211, 224, 276
planned outage incoming alarms parameters, 252
policy action parameters, 285
policy actions policies, 283
policy features, 301
polling parameters, 251
property name and value parameters, 282
root parameters, 196, 210, 222
saved state information path components, 26
scenario features, 299
suppress by pattern incoming alarms parameters, 257

threshold action designation parameters, 266
threshold incoming alarms parameters, 260
threshold parameters, 259
threshold-perform actions parameters, 262
threshold-perform actions processing parameters, 263
throttle parameters, 271
uncorrelate actions parameters, 183, 192, 205, 218, 230
technical assistance center (TAC), 4
templates defined, 320 provided, 24
Threshold Action Designation window, 265
Threshold panel, 258, 262
threshold policy alert severity example, 56 control parameter summary, 258 creating, 61 defining, 57 incoming alarms, 260 setting severity, 55 threshold panel, 258
thresholding, 320 performing actions, 61
threshold-perform actions policy actions, 264 description, 262 generate events, 268 invoke DMP policy, 266 processing, 263 threshold, 262
Throttle Policy panel, 271
throttle policy, defining, 73
throttling event storms, 73
TicketId alert property, 21
TicketStatus alert property, 21
Timeout alert property, 21
translating alarm names, 157
traps, 320
triggers, 321
Trouble Ticket Adapter (TTA)
Alert Property List, 20 defined, 321

U
Uncorrelate Actions panel, 153, 182, 191, 205, 218, 230
uncorrelation actions alerts by naming convention, 86 alerts by pattern, 99 alerts by relationship, 122, 137 sub-tree by relationship, 153
UpdateTime alert property, 21 user-defined data type (UDAT), 321 user-defined operators (UDO), 321

V
VSA and AFM, 27

W
windows Alert, 171 Attribute Filter, 279 Attribute Filter edit, 279 Database Definition, 250 Event Action, 286 Generate NetExpert Event, 268 Invoke DMP Policy, 266 Message Attribute, 290 New Policy, 38 Pattern List Entry, 274 Policy Action, 283 Property Designation, 292 Property Name and Value, 281 Threshold Action Designation, 265