

## Configuring the Threat Mitigation Application

- Accessing the Local Configuration for the Threat Mitigation Application on page 1
- Configuring Connections to the Directory on page 2
- Configuring Logging on page 4
- Configuring the SRC-TMP on page 5

### Accessing the Local Configuration for the Threat Mitigation Application

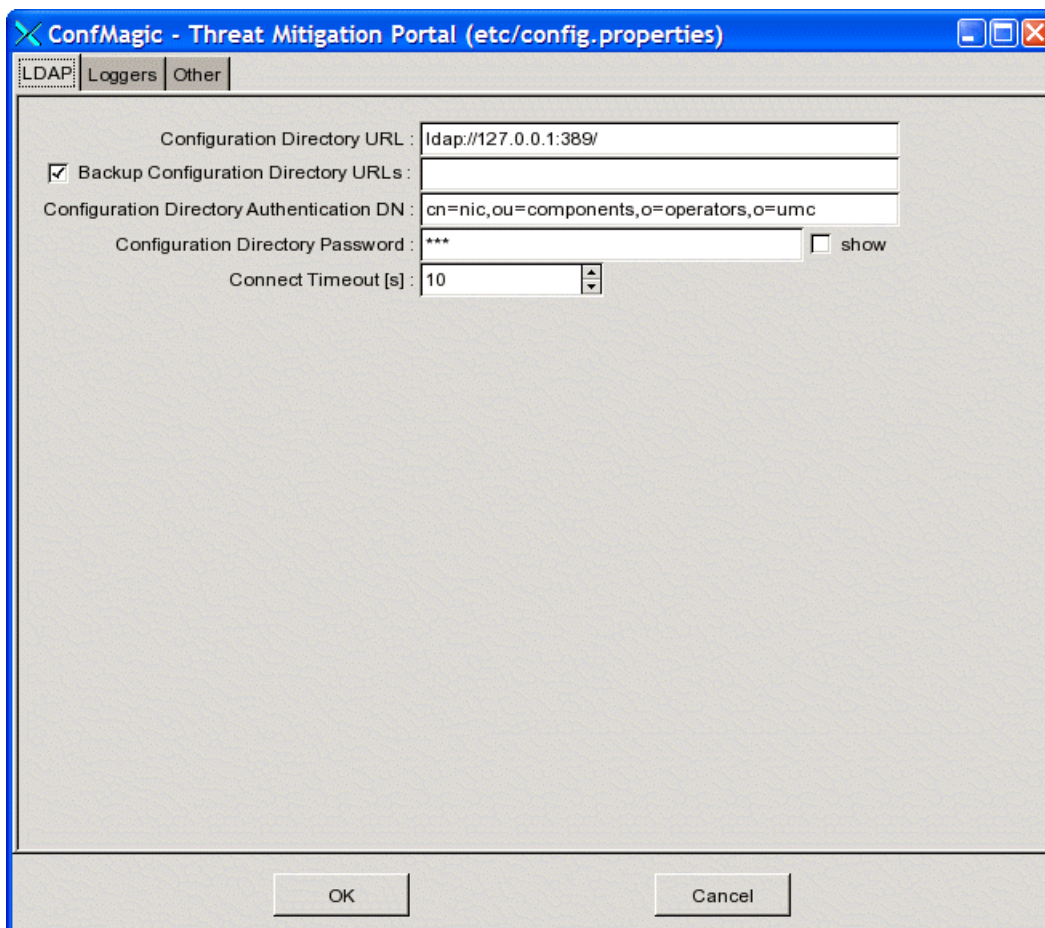
The Threat Mitigation Application configuration script updates the bootstrap configuration for the Threat Mitigation Application and configures the SRC-TMP.

To configure the Threat Mitigation Application:

1. On the host, log in as root or as another authorized administrator.
2. Launch the configuration tool.

**`/opt/UMC/conf/thma/etc/config`**

The configuration tool window appears.



3. Edit or accept the values for the fields in the appropriate tab. Click **OK**.

A file called *config.properties* appears in the */opt/UMC/conf/thma/etc* folder, and it is added to the */opt/UMC/conf/thma/webapp/thma.ear* file.

## Configuring Connections to the Directory

The Threat Mitigation Application loads configurations from the directory. If you install the directory on a different host than the J2EE application server, you must modify the bootstrap properties to specify the directory host.

To configure the connections to the directory for the Threat Mitigation Application:

- Edit or accept the default values for the fields in the LDAP tab.

The screenshot shows a Java Swing window titled "ConfMagic - Threat Mitigation Portal (etc/config.properties)". It has three tabs: "LDAP" (selected), "Loggers", and "Other". The "LDAP" tab contains the following fields and controls:

- "Configuration Directory URL" text field with the value "ldap://127.0.0.1:389/".
- A checked checkbox labeled "Backup Configuration Directory URLs" followed by an empty text field.
- "Configuration Directory Authentication DN" text field with the value "cn=nic,ou=components,o=operators,o=umc".
- "Configuration Directory Password" text field with masked characters "\*\*\*" and a "show" checkbox to its right.
- "Connect Timeout [s]" spinner field with the value "10".

At the bottom of the window are "OK" and "Cancel" buttons.

For information about values to enter in the fields, see Directory Configuration Properties for the Threat Mitigation Application.

## Directory Configuration Properties for the Threat Mitigation Application

The LDAP tab in the local configuration tool for the Threat Mitigation Application contains the following fields.

### **Configuration Directory URL**

- URL of the primary directory.
- Value—URL in the format `ldap://<host>:<port>/`
  - <host> —IP address or name of directory host
  - <port> —Port of directory host
- Default—`ldap://127.0.0.1:389/`
- Property name—`Config.java.naming.provider.url`

### **Backup Configuration Directory URLs**

- List of redundant directories.
- Value—Space-separated list of URLs; URLs have the format `ldap://<host>:<port>/`
  - <host> —IP address or name of directory host
  - <port> —Port of directory host
- Default—Unspecified
- Example—`ldap://192.0.2.1:389/ ldap://192.0.2.3:389/`
- Property name—`Config.net.juniper.smgmt.des.backup_provider_urls`

### **Configuration Directory Authentication DN**

- DN of the directory entry that defines the username with which the SRC component accesses the directory.
- Value—<DN>
- Default—`cn = nic, ou = Components, o = Operators, o = umc`
- Example—`cn = conf, o = Operators, o = umc`
- Property name—`Config.java.naming.security.principal`

### **Configuration Directory Password**

- Password with which the Threat Mitigation Application accesses the directory.
- Value—Text string
- Default—`nic`
- Example—`secret`

- Property name—Config.java.naming.security.credentials

### Connect Timeouts [s]

- Maximum time that the directory eventing system (DES) waits for the directory to respond.
- Value—Number of seconds in the range 1–2147483647
- Default—10
- Example—5
- Property name—Config.net.juniper.smgmt.des.connect.timeout

## Configuring Logging

To configure logging for the Threat Mitigation Application:

- Edit or accept the default values for the fields in the Loggers tab.

ConfMagic - Threat Mitigation Portal (etc/config.properties)

LDAP Loggers Other

☒ Error Log Filter (e.g. '/error-'): /error-

Error Log File: thma\_error.log Browse...

Error Rollover File: thma\_error.alt Browse...

☒ Error Log Rollover Size: 1000000

☒ Info Log Filter (e.g. '/info-'): /info-

Info Log File: thma\_info.log Browse...

Info Log Rollover File: thma\_info.alt Browse...

☒ Info Log Rollover Size: 1000000

☐ Debug Log Filter (e.g. '/debug-'): /debug-

Debug Log File: thma\_debug.log Browse...

Debug Log Rollover File: thma\_debug.alt Browse...

☒ Debug Log Rollover Size: 1000000

☐ Audit Log Filter (e.g. 'Audit,/info-'): Audit,/info-

Audit Log File: thma\_audit.log Browse...

Audit Rollover File: thma\_audit.alt Browse...

☒ Audit Log Rollover Size: 1000000

☐ Error Syslog Filter (e.g. '/error-'): /error-

Error Syslog Hostname: loghost

☐ Info Syslog Filter (e.g. '/info-warning'): /info-warning

Info Syslog Hostname: loghost

OK Cancel

For more information about logging, see the *SRC-PE Monitoring and Troubleshooting Guide*.

## Configuring the SRC-TMP

To configure the SRC-TMP:

- Edit or accept the default values for the fields in the Other tab.

The screenshot shows a Windows-style dialog box titled "ConfMagic - Threat Mitigation Portal (etc/config.properties)". It has three tabs: "LDAP", "Loggers", and "Other", with "Other" being the active tab. The dialog contains the following fields:

- Service Activation Interface :** A dropdown menu with "Provider Edge Interface" selected.
- Retailer Domain :** A text field containing "thma".
- Path :** A text field containing "thmp/record".
- Retry Period :** A spin box with the value "60000".
- Retry Delay :** A spin box with the value "10000".

At the bottom of the dialog are "OK" and "Cancel" buttons.

For information about values to enter in the fields, see General Configuration Properties for the Threat Mitigation Application.

### General Configuration Properties for the Threat Mitigation Application

The Other tab in the local configuration tool for the Threat Mitigation Application contains the following fields.

#### Service Activation Interface

- Type of interface on which the service would be activated.
- Value
  - Provider Edge Interface (JUNOS subscriber-facing interface)
  - Forwarding Interface (JUNOS forwarding interface)

- Subscriber Interface (JUNOS subscriber interface)
- Guidelines—If you change this property, you must reconfigure your NIC host. For more information, see Overview of Configuring and Deploying the SRC-TMP.
- Default—Provider Edge Interface

### ***Retailer Domain***

- Retailer domain for the SRC-TMP.
- Value—Text string
- Guidelines—This property must match one of the retailer domain names defined for the retailer in the target of the subscriber classification rules used for the interfaces managed by the Threat Mitigation Application. For more information about adding retailers, see Adding Retailers (SRC CLI).
- Default—thma

### ***Path***

- Pathname for the SRC-TMP and record servlet.
- Value— < pathname >
- Default—/thmp/record

### ***Retry Period***

- Time to wait between two consecutive retries of all pending service activation or deactivation tasks that were executed unsuccessfully.
- Value—Number of milliseconds in the range 0–9223372036854775807
- Guidelines—Do not specify too small a value, because the number of attempts could cause network overload.
- Default—60000

### ***Retry Delay***

- Time to wait before retrying all pending service activation or deactivation tasks that were executed unsuccessfully.
- Value—Number of milliseconds in the range 0–9223372036854775807
- Default—10000