Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

ANY SOFTWARE ITEM IDENTIFIED AS THIRD PARTY LIBRARY IS AVAILABLE UNDER SEPARATE SOFTWARE LICENSE TERMS AND IS NOT PART OF A TIBCO PRODUCT. AS SUCH, THESE SOFTWARE ITEMS ARE NOT COVERED BY THE TERMS OF YOUR AGREEMENT WITH TIBCO, INCLUDING ANY TERMS CONcernING SUPPORT, MAINTENANCE, WARRANTIES, AND INDEMNITIES. DOWNLOAD AND USE THESE ITEMS IS SOLELY AT YOUR OWN DISCRETION AND SUBJECT TO THE LICENSE TERMS APPLICABLE TO THEM. BY PROCEEDING TO DOWNLOAD, INSTALL OR USE ANY OF THESE ITEMS, YOU ACKNOWLEDGE THE FOREGOING DISTINCTIONS BETWEEN THESE ITEMS AND TIBCO PRODUCTS.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO, the TIBCO logo, Two-Second Advantage, TIB, Information Bus, Rendezvous, and TIBCO Rendezvous are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND ”READ ME” FILES.

Copyright © 2002-2018 TIBCO Software Inc. All rights reserved.
Device Group Service Operations .......................................................... 47
createDeviceGroup Operation .............................................................. 48
createDeviceGroupRemote Operation .................................................. 48
addDevices Operation ...................................................................... 49
addDevicesRemote Operation .............................................................. 49
removeDevices Operation .................................................................. 49
removeDevicesRemote Operation ........................................................ 49
readDeviceGroup Operation ............................................................... 50
readDeviceGroupRemote Operation .................................................... 50
updateDeviceGroup Operation ........................................................... 51
updateDeviceGroupRemote Operation ............................................... 51
deleteDeviceGroup Operation ............................................................. 51
deleteDeviceGroupRemote Operation .................................................. 51
gList Operation .................................................................................. 52
gListGroupRemote Operation .............................................................. 52
deviceGroupResponse Type ............................................................... 53
Common Request Parameters ........................................................... 53

Message Routing Service Operations ................................................. 55
createMsgRouting Operation .............................................................. 56
createMsgRoutingRemote Operation .................................................. 56
readMsgRouting Operation ............................................................... 57
readMsgRoutingRemote Operation .................................................... 57
updateMsgRouting Operation ............................................................ 57
updateMsgRoutingRemote Operation ............................................... 57
deleteMsgRouting Operation ............................................................. 58
deleteMsgRoutingRemote Operation .................................................. 58
gList Operation .................................................................................. 59
gListGroupRemote Operation .............................................................. 59
msgRoutingResponse Type ............................................................... 59
Common Request Parameters ........................................................... 60
Search Filter Service Operations ................................................................. 63
  createSearchFilter Operation ........................................................................... 64
  createSearchFilterRemote Operation .................................................................. 64
  readSearchFilter Operation ................................................................................ 65
  readSearchFilterRemote Operation ..................................................................... 65
  updateSearchFilter Operation ........................................................................... 65
  updateSearchFilterRemote Operation ............................................................... 65
  deleteSearchFilter Operation ........................................................................... 66
  deleteSearchFilterRemote Operation .................................................................. 66
  getList Operation .................................................................................................. 67
  getListRemote Operation .................................................................................... 67
  searchFilterResponse Type .................................................................................. 67
  Common Request Parameters ............................................................................. 68

User Administration Service Operations ......................................................... 70
  createUser Operation .......................................................................................... 71
  createUserRemote Operation .............................................................................. 71
  readUser Operation .............................................................................................. 72
  readUserRemote Operation .................................................................................. 72
  updateUser Operation .......................................................................................... 72
  updateUserRemote Operation .............................................................................. 73
  deleteUser Operation .......................................................................................... 73
  deleteUserRemote Operation .............................................................................. 73
  getList Operation .................................................................................................. 74
  getListRemote Operation .................................................................................... 74
  userResponse Type .............................................................................................. 74
  Common Request Parameters ............................................................................. 75

System Service ................................................................................................. 78
  Get Appliance System Info Operation .................................................................. 78

Report and Search Service ............................................................................... 80
  Get Report Operation ............................................................................................ 80
    Get Report Request Parameters ........................................................................ 80
    Specifying Filters for Index Searches .............................................................. 84
    Date/Time Formats for getReport ..................................................................... 84
    Get Report Response Attributes ..................................................................... 85
  Get Template Report List Operation .................................................................. 86
  Get Custom Report List Operation ...................................................................... 86
  Get Report Meta Info Operation .......................................................................... 87
  Get Detail Report Meta Info Operation .................................................................. 88

Authentication Service API ............................................................................... 90
GetAuthenticationToken Operation ................................................................. 90

Reference Lists ....................................................................................... 91
Alert Types ............................................................................................... 91
Message Areas ........................................................................................ 92
User Administration Privileges .............................................................. 92
TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

Product-Specific Documentation

The following documents for this product can be found on the TIBCO Documentation site on the TIBCO LogLogic® documentation page:

- TIBCO LogLogic® Log Management Intelligence Release Notes
- TIBCO LogLogic® Log Management Intelligence Administration Guide
- TIBCO LogLogic® Log Management Intelligence Configuration and Upgrade Guide
- TIBCO LogLogic® Log Management Intelligence Enterprise Virtual Appliance Quick Start Guide
- TIBCO LogLogic® Log Management Intelligence Hardware Installation Guide
- TIBCO LogLogic® Log Management Intelligence Log Source Report Mapping Guide
- TIBCO LogLogic® Log Management Intelligence SSD Hardware Field Installation Guide
- TIBCO LogLogic® Log Management Intelligence Syslog Alert Message Format Quick Reference Guide
- TIBCO LogLogic® Log Management Intelligence User Guide
- TIBCO LogLogic® Log Management Intelligence Web Services API Implementation Guide
- TIBCO LogLogic® Log Management Intelligence XML Import/Export Entities Reference Guide

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.
Overview of the Web Services API

The TIBCO LogLogic Web Services API is used to develop programs, or use Web Services tools, to interface with the TIBCO LogLogic appliances. You can use the Web Services API to run reports and searches, manage alert rules, manage user accounts, manage forwarding rules, and manage search filters.

The API is XML Web Services-based to provide a standardize API transport.

TIBCO LogLogic provides two main Services:

- Administration Service - for managing administrative tasks
- Report and Search Service - for accessing report and search capabilities

Administration Service

You can use the TIBCO LogLogic Administration Service API to manage TIBCO LogLogic Appliances via the following operations:

- Alert Service Operations
- Device Service Operations
- Device Group Service Operations
- Message Routing Service Operations
- Search Filter Service Operations
- User Administration Service Operations
- System Service

Report and Search Service

Using TIBCO LogLogic Search Service API you can manage reports and search queries on TIBCO LogLogic Appliances. Managing report and search queues includes running reports, viewing reports, and searching reports to return specific data.

- Report and Search Service

Requirements

To use the TIBCO LogLogic Web Services API, you need:

- A software tool to integrate your applications with the TIBCO LogLogic Web Services API (such as Apache Axis (for Java and C++ clients) or SOAP::Lite (for Perl clients).
- A software tool to create the client side API code (such as wsdl2java or wsdl2perl).
- LogLogic WSDL
- A software tool to generate client stubs
- TIBCO LogLogic appliance user name with “access web services” enabled

Port 443 is the required port on the TIBCO LogLogic appliance for accessing the Web Services API calls.
Alert Service Operations

You can use Alert Service operations to manage alerts in the TIBCO LogLogic® appliance.

Overview

You can use Alert Service operations to create, read, update, and delete alerts as well as view all alerts in the TIBCO LogLogic® appliance.

Using the CreateAlert and UpdateAlert operations, you can define and update rules to detect unusual traffic on your network or detect appliance system anomalies. Alerts can be configured to generate SNMP events and/or send an email notification when the alert rule is triggered for a specific type of alert.

The alert types are Adaptive Baseline, Cisco PIX/ASA Messages, Message Volume, Network Policy, Pre-defined Search Filter, Ratio Based, System, VPN Connections, VPN Messages, and VPN Statistics. For more information on supported alerts, see Alert Types or the online help for each specific alert. In the TIBCO LogLogic® appliance, to view the user interface implementation navigate to Alerts.

When creating (CreateAlert) or updating (UpdateAlert) an alert, you must specify a value for the alertRules Common Request Parameter. The alertRules value is used to define alert rules for a specific alert.

The following diagram provides a graphical view of the Common and Alert-Specific Parameters. The example displays an implementation of the createAlert operation specifying the VPN Messages alert type for the alertRules.

Common and Alert-Specific Request Parameters, with VPN Messages for alertRules

Implementation Guidelines

The general implementation guidelines for the Alert Service operations:

- A set of Common Request Parameters are required for each Alert Service operation. The createAlert Operation, createAlertRemote Operation, updateAlert Operation, and updateAlertRemote Operation require that you specify Common and Alert-Specific Request Parameters. Alert-Specific Request Parameters are specified using the alertRules Common Request Parameter.
- Alert Rules, defined in the alertRules Common Request Parameter, are specified as a string in the format:

  "/parameter1/valueA//parameter2/valueD/valueE/"
For example, a rule for the Network Policy alert is:

```
"FewerThan/100//MoreThan/10//alertFilter/False//policyAction/Accept//srcIPMin/10.1.2.3//srcIPMax/255.255.255.255//srcPortMin/0//srcPortMax/100//destIPMin/10.1.1.123//destIPMax/255.255.255.255//destPortMin/0//destPortMax/100//protocol/all"
```

For specific usage rules, see Common Request Parameters and Alert-Specific Request Parameters.

### Status Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Server success</td>
</tr>
<tr>
<td>4000</td>
<td>Unauthorized request</td>
</tr>
<tr>
<td>5000</td>
<td>Invalid parameter, getStatusMessage() contains detail information about the error</td>
</tr>
</tbody>
</table>

### Alert Service Operation Definitions

There are two kinds of operations:

- **local** - operation is performed on the local appliance itself
- **remote** - operations (names ending with Remote) performed on a specified remote appliance

The Alert Service Operations are as follows:

- `createAlert Operation`
- `createAlertRemote Operation`
- `readAlert Operation`
- `readAlertRemote Operation`
- `updateAlert Operation`
- `updateAlertRemote Operation`
- `deleteAlert Operation`
- `deleteAlertRemote Operation`
- `getList Operation`
- `getListRemote Operation`
- `alertResponse Type`
- `getAlertHistory Operation`
- `acknowledgeAlertHistoryByKey Operation`
- `removeAlertHistoryByKey Operation`
- `removeAlertHistory Operation`
- `alertHistoryResponse Type`

### createAlert Operation

The `createAlert` operation is used to create new alert rules in the TIBCO LogLogic® Appliance.

When using `createAlert`, you must specify:

- **Common Request Parameters**
- **Alert-Specific Request Parameters** (includes alertRules format description)

**Request Parameters**

- authToken, alertType, name, desc, priorityName, enabled, deviceNames, usernames, trapIds, resetTime, trackIndividualDevice, alertRules, snmpOid

For more information on each Common Request Parameter, see Common Request Parameters.

**Response**

- alertResponse (see alertResponse Type)

The Alert-Specific Request parameters specified in the alertRules parameter are also returned. The response depends on the alert type used.

**Example**

To create a VPN Connection Alert named MyAlertName:

```plaintext
createAlert authstr "VPN Connection Alert" "MyAlertName" "VPN Connection Alert Description" "low" "10.1.2.3_04" "admin" " " "400" "yes" "VPNUser/LogLogicUser//VPNGroup/LogLogicGroup//disconnectReason/is denied access" ""
```

**createAlertRemote Operation**

The createAlertRemote operation is used to create new alert rules on a managed TIBCO LogLogic® Appliance from a Management Station.

When using createAlertRemote, you must specify:

- **Common Request Parameters**
- **Alert-Specific Request Parameters**

**Request Parameters**

- authToken, applianceIP, alertType, name, desc, priorityName, enabled, deviceNames, usernames, trapIds, resetTime, trackIndividualDevice, alertRules, snmpOid

For more information on each Common Request Parameter, see Common Request Parameters.

**Response**

- alertResponse (see alertResponse Type)

The Alert-Specific Request parameters specified in the alertRules parameter are also returned. The response depends on the alert type used.

**Example**

To create a VPN Connection Alert named MyAlertName on remote Appliance 1.2.20.100:

```plaintext
createAlertRemote authstr 1.2.20.100 "VPN Connection Alert" "MyAlertName" "VPN Connection Alert Description" "low" "10.1.2.3_04" "admin" " " "400" "yes" "VPNUser/LogLogicUser//VPNGroup/LogLogicGroup//disconnectReason/is denied access" ""
```

**readAlert Operation**

Using readAlert operation you can view the details of existing alerts in the TIBCO LogLogic Appliance.

**Request Parameters**

- authToken, alertName
Response
alertResponse (see alertResponse Type)

Example
To view the details of the MyAlertName alert:
readAlert authstr "MyAlertName"

readAlertRemote Operation
Using readAlertRemote operation you can view the details of existing alerts on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters
authToken, applianceIP, alertName

Response
alertResponse (see alertResponse Type)

Example
To view the details of the MyAlertName alert on remote Appliance 1.2.20.100:
readAlertRemote authstr 1.2.20.100 "MyAlertName"

updateAlert Operation
With updateAlert operation you can update existing alerts in the TIBCO LogLogic Appliance. When using updateAlert, you must specify:

- Common Request Parameters
- Alert-Specific Request Parameters

Request Parameters
authToken, alertType, name, desc, priorityName, enabled, deviceNames, usernames, trapIds, resetTime, trackIndividualDevice, alertRules, snmpOId, changeNameTo

Response
alertResponse (see alertResponse Type)

The Alert-Specific Request parameters specified in the alertRules parameter are also returned. The response depends on the alert type used.

Example
To update a VPN Connection Alert named MyAlertName to be named NewAlertName with the priority set at high:
updateAlert authstr "VPN Connection Alert" "MyAlertName" "VPN Connection Alert Description" "low" "10.1.2.3_04" "admin" " " "400" "yes" "VPNUser/LogLogicUser//VPNGroup/LogLogicGroup//disconnectReason/is denied access" "NewAlertName"
updateAlertRemote Operation

Using updateAlertRemote operation you can update existing alerts on a managed TIBCO LogLogic Appliance from a Management Station.

When using updateAlertRemote, you must specify:

- Common Request Parameters
- Alert-Specific Request Parameters

Request Parameters

authToken, applianceIP, alertType, name, desc, priorityName, enabled, deviceNames, usernames, trapIds, resetTime, trackIndividualDevice, alertRules, snmpOId, changeNameTo

Response

alertResponse (see alertResponse Type)

The Alert-Specific Request parameters specified in the alertRules parameter are also returned. The response depends on the alert type used.

Example

To update a VPN Connection Alert named MyAlertName to be named NewAlertName with the priority set at high, on remote Appliance 1.2.20.100:

```
updateAlert authstr 1.2.20.100 "VPN Connection Alert" "MyAlertName" "VPN Connection Alert Description" "low" "10.1.2.3_04" "admin" " " "400" "yes" "VPNUser/LogLogicUser//VPNGroup/LogLogicGroup//disconnectReason/is denied access" "NewAlertName"
```

deleteAlert Operation

With deleteAlert operation you can delete existing alerts in the TIBCO LogLogic Appliance.

Request Parameters

authToken, alertName

Response

alertResponse (see alertResponse Type)

Example

To delete the alert named MyAlertName:

deleteAlert authstr "MyAlertName"

deleteAlertRemote Operation

Using deleteAlertRemote operation you can delete existing alerts on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, alertName

Response

alertResponse (see alertResponse Type)
Example
To delete the alert named MyAlertName on remote Appliance 1.2.20.100:
deleteAlertRemote authstr 1.2.20.100 “MyAlertName”

ggetList Operation
With getList operation you can retrieve the complete list of all alerts currently defined in the TIBCO LogLogic Appliance.

Request Parameter
authToken

Response
If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all alerts (total number indicated by resultCount) currently configured in the remote TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

Example
To retrieve a list of all alerts defined in the Appliance:
ggetList authstr

ggetListRemote Operation
Using getListRemote operation you can retrieve the complete list of all alerts currently defined on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameter
authToken, applianceIP

Response
If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all alerts (total number indicated by resultCount) currently configured in the remote TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

Example
To retrieve a list of all alerts defined in remote Appliance 1.2.20.100:
ggetListRemote authstr 1.2.20.100

alertResponse Type
alertResponse is returned for all alert operations except getList and getListRemote.
alertResponse always contains the following common elements:

- authToken
- resultCount
- statusCode
If resultCount is 1 and statusCode is 2000 (successful), the resultSet element is included after resultCount listing the following Alert details:

- alertType
- name
- desc
- priorityName
- enabled
- deviceNames
- usernames
- trapIds
- resetTime
- trackIndividualDevice
- alertRules
- snmpOId (createAlert and createAlertRemote only)
- changeNameTo (updateAlert and updateAlertRemote only)

The Alert-Specific Request parameters specified in the alertRules parameter are also returned. The response depends on the alert type used.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

getAlertHistory Operation

With getAlertHistory operation you can retrieve all alert logs currently on the TIBCO LogLogic Appliance. You may also use the filters to narrow down the result list.

Request Parameter

authToken, applianceIP, filters

Response

alertHistoryResponse (see alertHistoryResponse Type)

If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of alert logs (total number indicated by resultCount) currently on the remote TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

If the appliance is a management station, you may get the aggregated alert logs by specifying “All” in applianceIP.

Example

To retrieve the list of all high priority alert logs on Appliance 1.2.20.100:

getAlertHistory authstr 1.2.20.100 /Priority=/=High/

To retrieve all alert logs on Appliance 1.2.20.100 with empty filters:

getAlertHistory authstr 1.2.20.100 ""

To retrieve all new alert logs on Appliance 1.2.20.100:

getAlertHistory authstr 1.2.20.100 /Type=/=Unacknowledged/
acknowledgeAlertHistoryByKey Operation

With acknowledgeAlertHistoryByKey operation you can acknowledge a list of alert logs currently on the TIBCO LogLogic® TIBCO LogLogic appliance. You have to obtain the key list from getAlertHistory operation.

If you have obtained a list from the aggregated alert logs, you must specify “All” in applianceIP. Otherwise, it will be processed in single appliance mode and only alert logs on current appliance will be affected.

If resultCount is not 0, it means there are invalid keys in your key list. You can browse the returned resultSet for these keys.

Request Parameter

authToken, applianceIP, keyList

Response

alertHistoryResponse (see alertHistoryResponse Type)

Example

To acknowledge one or more alert logs on the appliance 1.2.20.100:

acknowledgeAlertHistoryByKey authstr 1.2.20.100 keyList

removeAlertHistoryByKey Operation

Using removeAlertHistoryByKey operation you can remove a list of alert logs currently on the LogLogic Appliance. You have to obtain the key list from getAlertHistory operation.

If you have obtained a list from the aggregated alert logs, you must specify “All” in applianceIP. Otherwise, it will be processed in single Appliance mode and only alert logs on the current Appliance will be affected.

If resultCount is not 0, it means there are invalid keys in your key list. You can browse the returned resultSet for these keys.

Request Parameter

authToken, applianceIP, keyList

Response

alertHistoryResponse (see alertHistoryResponse Type)

Example

To remove one or more alert logs on the Appliance 1.2.20.100:

removeAlertHistoryByKey authstr 1.2.20.100 keyList

removeAlertHistory Operation

Using removeAlertHistory operation you can remove all alert logs currently on the TIBCO LogLogic Appliance. You may also use the filters to narrow down the list.

Request Parameter

authToken, applianceIP, filters
Response

alertHistoryResponse (see alertHistoryResponse Type)

Example

To remove all medium priority alert logs on Appliance 1.2.20.100:
removeAlertHistory authstr 1.2.20.100 /Priority=/Medium/

To remove all alert logs on Appliance 1.2.20.100 with empty filters:
removeAlertHistory authstr 1.2.20.100 ""

To remove all acknowledged alert logs on Appliance 1.2.20.100:
removeAlertHistoryRemote authstr 1.2.20.100 /Type=/Acknowledged/

alertHistoryResponse Type

alertHistoryResponse is returned for all alert history operations.

alertHistoryResponse always contains the following common elements:

- authToken
- resultCount
- statusCode
- statusMessage
- summaryOnly

In getAlertHistory operation, if resultCount is greater then 0 and statusCode is 2000 (successful), the resultSet element that holds alert logs is included after resultCount.

The attributes of an alert log are:

Alert log attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Used to identify a unique log. It can be used in acknowledgeAlertHistoryByKey or removeAlertHistoryByKey operations. The user can obtain this by calling getAlertHistory.</td>
<td>string</td>
</tr>
<tr>
<td>time</td>
<td>Corresponds to the “Time” field on Alert Viewer page.</td>
<td>date</td>
</tr>
<tr>
<td>sourceIp</td>
<td>Corresponds to the “Source IP” field on Alert Viewer page.</td>
<td>string</td>
</tr>
<tr>
<td>msgType</td>
<td>Corresponds to the “Type” field on Alert Viewer page.</td>
<td>string</td>
</tr>
<tr>
<td>notifyType</td>
<td>Possible values are 1, 2, 3 for email alert, snmp alert, and no notification, respectively.</td>
<td>number</td>
</tr>
<tr>
<td>emailRcpt</td>
<td>Corresponds to the “Alert Destination” field on Alert Viewer page when email alert is used.</td>
<td>string</td>
</tr>
</tbody>
</table>
Attributes | Description | Type
--- | --- | ---
trapReceiver | Corresponds to the “Alert Destination” field on Alert Viewer page when snmp alert is used. | string
message | The alert message body. | string
priority | Possible values are 0, 1, 2 for priority low, medium, and high, respectively. | number
ArchiveFlag | Possible values are 0, 1 for unacknowledged alert logs and acknowledged alert logs, respectively. | number
ApplianceIp | Corresponds to the “Appliance” field on Alert Viewer page. This will be visible on Alert Viewer page when you view alert logs from a Management Station. | string

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Common Request Parameters**

A set of Common Request Parameters are required for each of the Alert Service operations. When using the CreateAlert or UpdateAlert operations, you must specify the alertRules parameter.

Common Request Parameters usage must follow several rules:

- You must specify a value for all Required Common Request Parameters.
- All Common Request parameters must be implemented in the order in which they appear in the Request Parameters section for each of the Alert Service operations.
- For Common Request Parameters, you must specify the value of the parameter only. Note that LogLogic expects the values in the order defined in this document.
- All values for Common Request Parameters must be enclosed by double quotation marks (“value”).

**Alert Service Common Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Token string returned from the authentication service or the “username/password”.</td>
<td></td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The managed Appliance on which you perform the operation.</td>
<td>IP address of a managed Appliance. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>If the value is blank, it retrieves the Appliance IP address from the local Appliance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This parameter is available only for Management Station Appliances using operations with Remote in the name.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>alertType</td>
<td>Type of alert, such as Network Policy Alert or System Alert.</td>
<td>For a list of alert types, see Alert Types.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>name</td>
<td>Name of the alert.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>desc</td>
<td>Description for the remote device.</td>
<td>Any text up to 64 characters in length.</td>
<td>optional</td>
<td>string</td>
</tr>
<tr>
<td>priorityName</td>
<td>Priority level of the alert.</td>
<td>Possible values: low, medium, and, high</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>enabled</td>
<td>Determines if the alert is enabled or disabled.</td>
<td>Possible values: yes — enabled, no — disabled. The default is no.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>deviceNames</td>
<td>List of devices. Valid entries contain one or more devices and/or device groups.</td>
<td>List of valid devices and/or groups. Use a forward slash (/) as a delimiter for multiple entries. For example: 10.1.1.1/10.1.1.7 If a device has a forward slash (/) in the name, such as HP/UX or IBM i5/OS, you must replace the forward slash with %2F. (The F is case-sensitive.) For example: HP%2FUX</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>usernames</td>
<td>User names for the alerts. Specify a single user or a user group.</td>
<td>Use a forward slash (/) as a delimiter for multiple entries. For example: user1/usergroup7</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>trapIds</td>
<td>Trap name or IP Address to send the SNMP messages when the alert is triggered.</td>
<td>Use a forward slash (/) as a delimiter for multiple entries. For example: trap1/trap2/trap3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>resetTime</td>
<td>Time to wait between alerts that are generated.</td>
<td>Any positive integer. The value is in seconds. For example, the value 120 represents two minutes.</td>
<td>yes</td>
<td>number</td>
</tr>
<tr>
<td>trackIndividualDevice</td>
<td>Enables or disables individual device tracking.</td>
<td>Possible values: yes — enabled, no — disabled. The default is no.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>alertRules</td>
<td>Alert rule specific to the alert type.</td>
<td>See Alert-Specific Request Parameters for a list of specific alert rules for each alert type.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>snmpOId</td>
<td>Specifies an SNMP OID to identify the originator of this alert.</td>
<td>Any valid SNMP OID</td>
<td>no</td>
<td>string</td>
</tr>
<tr>
<td>change NameTo</td>
<td>New name of the alert. If empty, the object name is unchanged.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>filters</td>
<td>List of expressions applied to narrow down affected alert logs. Filters are used only in getAlertHistory and removeAlertHistory operations. The priority and type filters work the same way as the drop-down boxes in alert viewer. For example, /Priority=/All_System/ returns all system alerts. The New_Entry, Offset and Count filters are used only in getAlertHistory operation. When New_Entry is set to true. It will return only new logs since the last call to getAlertHistory with New_Entry turned on. If this is the first time, then all alert logs will be returned. Count allows you to specify how many alert logs will be returned. The maximum count is 10,000. Offset allows you to specify the start offset. It is zero-based. Because you cannot return all alert logs at once if the total amount exceeds the maximum value. You have to use offset to get remaining alert logs. Values must use the format: /filtername=/Value/ The valid filter names are &quot;Type&quot;, &quot;Priority&quot;, &quot;Offset&quot;, &quot;Count&quot; and &quot;New_Entry&quot;. &quot;Type&quot; supports &quot;Unacknowledged&quot;, &quot;Acknowledged&quot; and &quot;All&quot;. &quot;Priority&quot; supports &quot;High&quot;, &quot;Medium&quot;, &quot;Low&quot;, &quot;All_System&quot; and &quot;All&quot;. &quot;Count&quot; and &quot;Offset&quot; can not be negative. &quot;New_Entry&quot; supports &quot;True&quot; or &quot;False&quot;. If the filters are not present, the default is all types, all priorities, 0, 1000 and New_Entry set to false.</td>
<td>no</td>
<td>Array of string</td>
<td></td>
</tr>
<tr>
<td>keyList</td>
<td>A list consists of keys returned from getAlertHistory operation. With getAlertHistory operation, you will retrieve a list of alert logs. The key value can be obtained from the key attribute of an alert log.</td>
<td>yes</td>
<td>Array of string</td>
<td></td>
</tr>
</tbody>
</table>

### Alert-Specific Request Parameters

You must specify the alert rules for each specific alert type you are managing.

Alert Rules are defined using the alertRules Common Request Parameter. The following section contains alert-specific parameters for each of the alert types. The alert types are Adaptive Baseline, Cisco PIX/ASA Messages, Message Volume, Network Policy, Pre-defined Search Filter, Ratio Based, System, VPN Connections, VPN Messages, and VPN Statistics.

Alert-Specific Request Parameters usage must follow several rules:

- All Alert-Specific Parameters can be implemented in any order. LogLogic recommends that you implement the alert rules in a consistent order and format to make managing the alert rules easier.
• Alert-Specific parameter values must include double quotation marks around the entire alert rule. For example:

“param1/valueA//param2/valueC”

• If the name of a device or the parameter value includes a forward slash (/), such as HP/UX, IBM i5/OS, or Accept/Total, you must replace the forward slash with %2F. (The F is case-sensitive.) Examples: HP%2FUX, IBM i5%2FOS, or Accept%2FTotal

• Use forward slash marks as delimiters when specifying alert rules. Use a single forward slash mark (/) as a delimiter to define multiple values for a parameter. Use double forward slash marks (//) as delimiters for parameters. For example:

param1/valueA//param2/valueC/valueD//param3/valueE

where param1, param2, and param3 are parameters and valueA, valueC, valueD, and valueE are values for param1, param2, and param3, respectively.

The example assigns the following name/value pairs:

- param1 = valueA
- param2 = valueC, valueD
- param3 = valueE

Adaptive Baseline Alert

With Adaptive Baseline Alert you would be notified if message rates fall above or below your average baseline range for a specified day and time of the week.

Request Parameters

FewerThan, MoreThan

Example

“FewerThan/10//MoreThan/100”

The following table lists the Adaptive Baseline Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.

Adaptive Baseline Alert-specific parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FewerThan</td>
<td>Minimum percentage of messages that must be received within a time period (TimeSpan parameter) before an alert is generated. If the number of messages drops below the FewerThan value, an alert is generated. The FewerThan and MoreThan parameters make up the alert range.</td>
<td>Any positive integer between 0 and 100. The FewerThan value must be greater than the MoreThan value.</td>
<td>yes</td>
<td>int</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MoreThan</td>
<td>Maximum percentage of messages that must be received within a time period (TimeSpan parameter) before an alert is generated. If the number of messages exceeds the MoreThan value, an alert is generated. The FewerThan and MoreThan parameters make up the alert range.</td>
<td>Any positive integer between 1 and 100. The MoreThan value must be less than the FewerThan value.</td>
<td>yes</td>
<td>int</td>
</tr>
</tbody>
</table>

### Cisco PIX/ASA Message Alert

The Cisco PIX/ASA Messages alert allows for triggering on PIX message criticality, code, and message rate. Since this alert is specific to Cisco PIX messages, the alert device selection is limited to Cisco PIX devices.

#### Request Parameters

criticality, FewerThan, MoreThan, MessageCode, TimeSpan

#### Example

```
criticality/1//MoreThan/10//MessageCode/1-709006//TimeSpan/40
```

The following table lists the Cisco PIX Message Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.

#### Cisco PIX/ASA message Alert-specific parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criticality</td>
<td>Criticality for the alert. See your firewall documentation for details about the values in the list.</td>
<td>Enter a numeric value from the following list: 0: emergency 1: alert 2: critical 3: error 4: warning 5: notice 6: informational 7: debug The default is 1.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>FewerThan</td>
<td>Minimum number of messages that must be received within a time period (TimeSpan parameter) before an alert is generated. If the number of messages drops below the FewerThan value, an alert is generated. The FewerThan and MoreThan parameters make up the alert range. You do not have to specify both FewerThan and MoreThan.</td>
<td>Any positive integer between 1 and 100.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>MoreThan</td>
<td>Maximum number of messages that can be received within a time period (TimeSpan parameter) before an alert is generated. If the number of messages exceeds the MoreThan value, an alert is generated. The FewerThan and MoreThan parameters make up the alert range. You do not have to specify both FewerThan and MoreThan.</td>
<td>Any positive integer between 1 and 100.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>MessageCode</td>
<td>Message code for which an alert is generated. For more information on Cisco PIX Message Codes, see your Cisco PIX documentation. The message code selections are limited to codes applicable to the selected criticality.</td>
<td>Valid Cisco PIX message code. Message codes must match the criticality parameter. For example, if criticality is set to 3, you can specify any message code that starts with 3-. The default is 1-709006.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>TimeSpan</td>
<td>Period of time that must be exceeded by the FewerThan and MoreThan thresholds before an alert is triggered. If the FewerThan and MoreThan thresholds are met for the specified TimeSpan, an alert is generated.</td>
<td>Any positive integer. The value is in seconds. For example, the value 120 represents two minutes. The default is 60.</td>
<td>yes</td>
<td>int</td>
</tr>
</tbody>
</table>

**Message Volume Alert**

The Message Volume-based alert allows alerting when message volume falls below, or is above, preset messages-per-second thresholds. The alert applies to all devices.

The Message Volume-based alert also supports Zero Message Alert by using the TimeSpan parameter. The time granularity of Zero Message Alert is in minutes, so the TimeSpan has to be 60 seconds or greater. When TimeSpan is present, you do not have to provide FewerThan and MoreThan parameters as they will be ignored.

**Request Parameters**

FewerThan, MoreThan
Example

“FewerThan/10//MoreThan/100”

Table 5 lists the Message Volume Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.

Message Volume Alert-specific parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FewerThan</td>
<td>Minimum message rate (messages per second) that can be reached before an alert is generated.</td>
<td>Any positive integer. The value is in messages per second.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>The FewerThan and MoreThan parameters make up the alert range.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MoreThan</td>
<td>Maximum message rate (messages per second) that can be reached before an alert is generated.</td>
<td>Any positive integer. The value is in messages per second.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>The FewerThan and MoreThan parameters make up the alert range.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeSpan</td>
<td>Period of time that the message rate remains to at zero.</td>
<td>The value is in seconds.</td>
<td></td>
<td>int</td>
</tr>
</tbody>
</table>

Network Policy Alert

Deprecated – This API may not be available for future releases.


Request Parameters

FewerThan, MoreThan, alertFilter, policyAction, srcIPMin, srcIPMax, srcPortMin, srcPortMax, destIPMin, destIPMax, destPortMin, destPortMax, protocol

Example

“FewerThan/100//MoreThan/10//alertFilter/False//policyAction/Accept//srcIPMin/10.1.2.3//srcIPMax/255.255.255.255//srcPortMin/0”
//srcPortMax/100//destIPMin/10.1.1.123//destIPMax/255.255.255.255
//destPortMin/0//destPortMax/100//protocol/all”

The following table lists the Network Policy Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.
## Network Policy Alert-specific parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlertFilter</td>
<td>Alert filter used for the alert.</td>
<td>Possible values:</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>None, False Acceptance, False Rejection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>None — Report on both False Rejection and False Acceptance traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>False Acceptance — Report only the traffic that passed the firewall,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>but should have been rejected according to this policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>False Rejection — Report only the traffic that the firewall denied,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>but should have been accepted according to this policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PolicyAction</td>
<td>Type of policy rules.</td>
<td>Possible values:</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accept, Deny</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accept - policy rules that define network traffic that the firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>should accept.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deny — policy rules that define network traffic that the firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>should reject.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srcIPMin</td>
<td>The minimum limit for your Source IP addresses. This is for incoming and</td>
<td>Standard IP address format. For example: 0.0.0.0</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>outgoing traffic that accesses your firewall.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The srcIPMin and srcIPMax parameters make up the source IP range.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srcIPMax</td>
<td>The maximum limit for your Source IP addresses. This is for incoming and</td>
<td>Standard IP address format. For example: 255.255.255.255</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>outgoing traffic that accesses your firewall.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The srcIPMin and srcIPMax parameters make up the source IP range.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>srcPortMin</td>
<td>The lower limit range for your source ports. This is for incoming and outgoing traffic that accesses your firewall.</td>
<td>Valid ports are ports 0 through 65,535.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>srcPortMax</td>
<td>The upper limit range for your source ports. This is for incoming and outgoing traffic that accesses your firewall.</td>
<td>Valid ports are ports 0 through 65,535.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>destIPMin</td>
<td>The minimum limit for your destination IP addresses. This is for incoming and outgoing traffic that accesses your firewall.</td>
<td>Standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>destIPMax</td>
<td>The maximum limit for your destination IP addresses. This is for incoming and outgoing traffic that accesses your firewall.</td>
<td>Standard IP address format. For example: 255.255.255.255</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>destPortMin</td>
<td>The lower limit range for your destination ports. This is for incoming and outgoing traffic that accesses your firewall.</td>
<td>Valid ports are ports 0 through 65,535.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>destPortMax</td>
<td>The upper limit range for your destination ports. This is for incoming and outgoing traffic that accesses your firewall.</td>
<td>Valid ports are ports 0 through 65,535.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol associated with the specified IP address</td>
<td>Possible values: tcp; udp; icmp; tcp, udp; tcp, icmp; udp, icmp; tcp, udp, icmp; all</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>TIBCO LogLogic Appliances support ICMP, TCP, and UDP protocols.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Pre-Defined Search Filter Alert**

The Pre-Defined Search Filter Alert allows for alert notification when a text search match occurs within the received log message. This alert leverages the Log Appliance search filters for the text search match definitions.

**Request Parameters**

searchFilterName, FewerThan, MoreThan, TimeSpan

**Example**

```
"searchFilterName/MySearchFilter//FewerThan/100//TimeSpan/60"
```

The following table lists the Pre-Defined Search Filter Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.

**Pre-Defined Search Filter Alert-specific parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchFilterName</td>
<td>Name of the search filter.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>FewerThan</td>
<td>Minimum number of messages that must be received within a time period (TimeSpan parameter) before an alert is generated. If the number of messages drops below FewerThan, an alert is generated. The FewerThan and MoreThan parameters make up the alert range. You do not have to specify both FewerThan and MoreThan.</td>
<td>Any positive integer between 1 and 100.</td>
<td>yes</td>
<td>string</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MoreThan</td>
<td>Maximum number of messages that can be received within a time period (TimeSpan parameter) before an alert is generated. If the number of messages exceeds MoreThan, an alert is generated. The FewerThan and MoreThan parameters make up the alert range. You do not have to specify both FewerThan and MoreThan.</td>
<td>Any positive integer between 1 and 100.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>TimeSpan</td>
<td>Period of time that must be exceeded by the FewerThan and MoreThan thresholds before an alert is triggered. If the FewerThan and MoreThan thresholds are met for the specified TimeSpan, an alert is generated.</td>
<td>Any positive integer. The value is in seconds. For example, the value 120 represents two minutes. The default is 60.</td>
<td>yes</td>
<td>int</td>
</tr>
</tbody>
</table>

### Ratio Based Alert

The Ratio Based Alert triggers when the percentage of a specified message type exceeds or falls below specified percentages. For example, the Denied/(Accept+Denied) Alert Ratio can be used to trigger an alert when the number of Denied messages exceeds 90% of the Accept and Denied message count.

### Request Parameters

FewerThan, MoreThan, ratio

### Example

“FewerThan/100//MoreThan/10//ratio/Accept/Total”

The following table lists the Ratio Based Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.

### Ratio Based Alert-specific rules

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FewerThan</td>
<td>Minimum percentage of messages (by ratio specified by ratio parameter) that must be received before an alert is generated. If the number of messages drops below the FewerThan value, then an alert is generated. The FewerThan and MoreThan parameters make up the alert range for the value specified by the ratio parameter.</td>
<td>Any positive integer between 1 and 100.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>MoreThan</td>
<td>Maximum percentage of messages (by ratio specified by ratio parameter)) that must be received before an alert is generated. If the number of messages drops below the FewerThan value, then an alert is generated. The FewerThan and MoreThan parameters make up the alert range for the value specified by the ratio parameter.</td>
<td>Any positive integer between 1 and 100.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Ratio</td>
<td>Message count ratio for the specified alert.</td>
<td>Possible values: Accept/Total, Deny/Total, Login Success/Total, Login Failure/Total, Accept/(Accept + Denied), Denied/(Accept + Denied), Login Success/(Success+Failure), Login Failure/(Success+Failure)</td>
<td>yes</td>
<td>string</td>
</tr>
</tbody>
</table>

**System Alert**

The System Alert allows for notification when system health and status criteria exceed acceptable bounds.

**Request Parameters**

alertCriteria, lowThreshold, highThreshold, drive, peerIP

**Example**

“alertCriteria/CPU Temperature/highThreshold/65”

The following table lists the System Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.
## System Alert-specific Rules

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>alertCriteria</td>
<td>The criteria used to generate an alert.</td>
<td>Possible values: CPU Temperature, Disk Usage, Dropped Messages, Failover, Network Connection Speed, Network Interface, Synchronization Failure, TCP Forward Connection Status, Data Migration complete, RAID Disk Failure, Resource Exhaustion, TCP Forward Falling Behind</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>• CPU Temperature — CPU temperature, in Celsius degrees, under which the CPU temperature must remain.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disk Usage — Drive and percentage under which the disk usage must remain.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped Messages — Maximum dropped message rate (messages per second).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fail-over — Identifies when failover is enacted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Network Connection Speed — Minimum throughput threshold for the network connection.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Network Interface — Identifies that a network interface (for example, eth0 or eth1) fails to function.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Synchronization Failure — Identifies if the data synchronization process fails after failover occurs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TCP Forward Connection Status — Downstream device IP address. Forwarding Rules are required for this alert criteria. Use the Message Routing Service Operations or specify the message routing rules in the LogLogic User interface (Administration &gt; Message Routing).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>Specify the interfaces that the system should alert on.</td>
<td>Possible values: eth0, eth1 or eth1</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>(Network Interface only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lowThreshold</td>
<td>Minimum connection speed.</td>
<td>Possible values: 10-half, 100-half, 100-full, 1000-full. The default is 10-half.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>highThreshold</td>
<td>CPU temperature, in Celsius degrees, under which the CPU temperature must remain. Specify a value if implementing the CPU Temperature alert criteria (AlertCriteria parameter)</td>
<td>Any positive integer between 1 and 100. The value is in Celsius degrees. The default is 80 degrees Celsius.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>highThreshold</td>
<td>The percentage of allowable disk space usage on the specified disk drive. Use in conjunction with the drive parameter. Specify only if the alertCriteria value is Disk Usage.</td>
<td>Any positive integer between 1 and 100. The default is 90 (90%).</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>highThreshold</td>
<td>Maximum dropped message rate (messages per second). Specify only if the alertCriteria value is Dropped Messages.</td>
<td>Any positive integer. The value is in seconds. The default is 100 messages per second.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>drive</td>
<td>The disk drive under which usage must remain below the value specified in the highThreshold (Disk Usage) parameter. Use in conjunction with the highThreshold (Disk Usage) parameter. Specify only if the alertCriteria value is Disk Usage.</td>
<td>Possible values: /, /failsafe, /tmp, /loglogic, /dev, /loglogic/data/dbi</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>peerIP</td>
<td>Downstream device IP address. The IP address is created using the destinationIP parameter in Message Routing Service Operations or by specifying the Destination IP in the LogLogic User interface (Administration &gt; Message Routing). Specify only if the alertCriteria value is TCP Forward Connection Status.</td>
<td>Valid IP address associated with a message routing rule.</td>
<td>yes</td>
<td>string</td>
</tr>
</tbody>
</table>

**VPN Connections Alert**

The VPN Connection Alert triggers when a VPN connection is denied access and/or disconnected. The VPN Connection alert is only applicable to Cisco VPN, Radius, and Nortel Contivity devices.

**Request Parameters**

VPNUser, VPNGroup, VPNIP, DisconnectReason
Example

"VPNUser/User1//VPNGroup/Group1//VPNIP/null//disconnectReason/both"

or

"VPNUser/null//VPNGroup/null//VPNIP/10.1.2.3//disconnectReason/is disconnected"

or

"VPNUser/null//VPNGroup/null//VPNIP/10.1.2.3//disconnectReason/is denied access"

The following table lists the VPN Connections Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.

VPN Connections Alert-specific rules

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPNUser</td>
<td>Defines the VPN user from where the connection originates.</td>
<td>optional string</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you specify a value for the VPNUser parameter, you must also specify a value for the VPNGroup parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can specify a value for the VPNIP parameter instead of the VPNUser and VPNGroup parameters together.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPNGroup</td>
<td>Defines the VPN Group from where the connection originates.</td>
<td>optional string</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must specify a value for the VPNGroup parameter if you specify a value for the VPNUser parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can specify a value for the VPNIP parameter instead of the VPNUser and VPNGroup parameters together.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPNIP</td>
<td>Defines the VPN IP address from where the connection originates.</td>
<td>Standard IP address format. For example: 10.1.2.3</td>
<td>optional string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can use the VPNIP parameter as an additional filter instead of using the VPNUser and VPNGroup parameters.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>disconnectReason</td>
<td>Identifies the reason for sending an alert. An alert is generated if a</td>
<td>Possible values:</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>connection is disconnected and/or if a connection is denied access.</td>
<td>is disconnected, is denied access, both</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>is disconnected — alert when a connection is disconnected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>is denied access — alert when a connection is denied access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>both — both is disconnected and is denied access.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VPN Messages Alert

The VPN Message Alert triggers on combinations of specific VPN message area, severity, and code. This alert is applicable to Cisco VPN devices.

Request Parameters

MessageArea, MessageCode, SeverityFrom, SeverityTo

Example

“messageArea/ANY//MessageCode/0//severityFrom/2//severityTo/6”

The following table lists the VPN Messages Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.

VPN Message Alert-specific rules

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>messageArea</td>
<td>Identifies the message area for the alert. The message area defines the</td>
<td>For a list of possible values, see the Message Areas, or view the list</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>general area from where the alert is sent. For example, alerts that are</td>
<td>in the User Interface. Examples: ANY, AUTH, DNS, SMTP, and WAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>related to HTTP, AUTH, IKE, or IPSEC.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A combination of the messageArea and MessageCode uniquely identifies the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>alert.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>MessageCode</td>
<td>Identifies the alert code. The range can vary from 1 to the maximum value for the Area you select. A combination of the messageArea and MessageCode uniquely identifies the alert.</td>
<td>Any positive integer. In addition you can leave the field blank or type a zero (0). If you leave this field blank or type zero, this equals Any to the application.</td>
<td>yes</td>
<td>int</td>
</tr>
<tr>
<td>severityFrom</td>
<td>Minimum value for the severity level range as it relates to the value specified by the messageArea parameter. The severityFrom parameter and the severityTo parameter define the numeric range</td>
<td>Any positive integer between 0 and 13. The value zero (0) equals all severity levels.</td>
<td>yes</td>
<td>int</td>
</tr>
<tr>
<td>severityTo</td>
<td>Maximum value for the severity level range as it relates to the value specified by the messageArea parameter. The severityFrom parameter and the severityTo parameter define the numeric range</td>
<td>Any positive integer between 0 and 13. The value zero (0) equals all severity levels.</td>
<td>yes</td>
<td>int</td>
</tr>
</tbody>
</table>

**VPN Statistics Alert**

The VPN Statistics Alert triggers when recorded statistics on VPN or Radius messages match relative or absolute criteria. For example, an alert can be configured to trigger when the Number of Bytes Received per day for a specific user exceeds, say, 1 Mb per day, which is an absolute value. The alert rule could also be configured as a relative rule, for example “grows by 10%.”

**Request Parameters**

VPNUser, VPNGroup, VPNIP, Statistic, MatchCount, PerTimeUnit, MeasureBy, ChangeAs, ChangeValue

**Example**

“VPNUser/null//VPNGroup/null//VPNIP/null/Statistic/bytes sent/PerTimeUnit/minute//ChangeAs/equals//ChangeValue/3.0//MeasureBy/0//MatchCount/55”

The following table lists the VPN Statistics Alert-specific parameters. You must include the parameters as inputs for the alertRules parameter.
### VPN Statistics Alert-specific rules

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPNUser</td>
<td>Defines the VPN user from where the connection originates. If you specify a value for the VPNUser parameter, you must also specify a value for the VPNGroup parameter. You can specify a value for the VPNIP parameter instead of the VPNUser and VPNGroup parameters together.</td>
<td>optional</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>VPNGroup</td>
<td>Defines the VPN Group from where the connection originates. You must specify a value for the VPNGroup parameter if you specify a value for the VPNUser parameter. You can specify a value for the VPNIP parameter instead of the VPNUser and VPNGroup parameters together.</td>
<td>optional</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>VPNIP</td>
<td>Defines the VPN IP address from where the connection originates. You can use the VPNIP parameter as an additional filter instead of using the VPNUser and VPNGroup parameters.</td>
<td>Standard IP address format. For example: 10.1.2.3</td>
<td>optional</td>
<td>string</td>
</tr>
<tr>
<td>statistic</td>
<td>Identifies the type of statistic. Specify the perTimeUnit parameter with the statistic parameter. If you specify the value as Connection Duration, the perTimeUnit parameter is not necessary as the value defaults to seconds.</td>
<td>Possible values: Number of Connections, Number of Denies, Bytes Sent, Bytes Received, Connection Duration.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>matchCount</td>
<td>In the Threshold field, enter the number of times a match must occur before an alert is sent. The match is determined by the combination of the fields you define for this type of alert.</td>
<td>yes</td>
<td>int</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>perTimeUnit</td>
<td>Rate at which the statistic type (statistic parameter) is sampled. This field is not applicable if the value of the statistic parameter is Connection Duration.</td>
<td>Possible values: second, minute, hour, day, week, none. If you specify none, statistics are measured regardless of rate.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>measureBy</td>
<td>Select whether to use a relative or absolute measurement to trigger the alert.</td>
<td>0 or 1.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>changeAs</td>
<td>Defines the percentage of increase or decrease of the alert type (statistic parameter). For example, to be alerted when a number of Denied Connections per second grows by 400% from the average, enter the value “grows by 400”. The average is taken from the previous time period and varies depending on the type of information you view.</td>
<td>Possible values: grows by ##%, drops by ##% Where ## is a positive integer. The ## value is a percentage. For example: grows by 400 or drops by 200</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>changeValue</td>
<td>Defines the absolute number of denied connections per second that an alert type (statistic parameter) must change by for an alert to be generated. For example, to be alerted when a number of Denied Connections per second increases by 400 from the average, enter the value “increases by 400”.</td>
<td>Possible values:</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exceeds ##</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>falls below ##</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>equals ##</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>increase by ##</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>decrease by ##</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Where ## is a positive integer. The ## value is the number of denied connections per second. For example: exceeds 400 or TIBCO LogLogic LMI Web Services API Implementation Guide</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Device Service Operations

The Device Service operations enable you to manage devices in your TIBCO LogLogic® appliance.

Overview

Using Device Service operations you can create, read, update, and delete devices as well as view all devices in the TIBCO LogLogic® appliance.

Devices are any source of log data that you want captured by a TIBCO LogLogic® appliance. In the TIBCO LogLogic® appliance, to view the user interface implementation navigate to Management > Devices.

Implementation Guidelines

Some general implementation guidelines for Device Service operations:

- A set of Common Request Parameters are required for each operation. You must specify a value for all Required parameters.
- You must specify the value of the Common Request Parameters only.
- All parameters must be implemented in the order in which they appear in the Request Parameters section for each of the operations.
- All values for Common Request Parameters must be enclosed by double quotation marks (“value”). If the name of a device or a parameter value includes a forward slash (/), such as HP/UX, or IBM i5/OS, you must replace the forward slash with %2F. (The F is case-sensitive.)
  
  Examples: HP%2FUX or IBM i5%2F0S
- When using the Device Operation, Device Remote Operation, Device Operation, or Device Remote Operation, if the Refresh Enabled parameter is enabled, the value for the deviceName parameter can be overwritten by the value on your DNS server. If this occurs, use the DNS name of the device as the value for the deviceName parameter. You can retrieve the DNS name by looking up the IP address of the device.

Status Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Server success</td>
</tr>
<tr>
<td>4000</td>
<td>Unauthorized request</td>
</tr>
<tr>
<td>5000</td>
<td>Invalid parameter, getStatusMessage() contains detail information about the error</td>
</tr>
</tbody>
</table>

Device Service Operation Descriptions

There are two kinds of operations:

- local - operation is performed on the local Appliance itself
- remote - operations (names ending with Remote) performed on a specified remote Appliance

The Device Service operations are as follows:

- createDevice Operation
- createDeviceRemote Operation
- readDevice Operation
- readDeviceRemote Operation
- updateDevice Operation
- updateDeviceRemote Operation
- deleteDevice Operation
- deleteDeviceRemote Operation
- getList Operation
- getListRemote Operation

**createDevice Operation**

Using `createDevice` operation you can add a new device to be supported by the TIBCO LogLogic® Appliance.

Managing File Transfer Rules is not supported through the Web Services API. You must use the LogLogic user interface to manage File Transfer Rules for each device.

**Request Parameters**

- `authToken`, `deviceName`, `deviceType`, `description`, `enabled`, `dnsRefreshEnabled`, `deviceIp`

For more information on each Common Request Parameter, see Common Request Parameters.

**Response**

deviceResponse (see deviceResponse Type)

**Example**

To add a Cisco ACS device named Cisco ACS Sample Device, with a description of Cisco ACS Description, having IP address 10.1.2.3, and enabling the Appliance to retrieve log messages from the device but not enabling DNS name refresh:

```
createDevice authstr "Cisco ACS Sample Device" "Cisco ACS" "Cisco ACS Description" "yes" "no" "10.1.2.3"
```

**createDeviceRemote Operation**

Using `createDeviceRemote` operation you can add a new device to be supported by a managed TIBCO LogLogic® Appliance from a Management Station.

Managing File Transfer Rules is not supported through the Web Services API. You must use the LogLogic user interface to manage File Transfer Rules for each device.

**Request Parameters**

- `authToken`, `applianceIP`, `deviceName`, `deviceType`, `description`, `enabled`, `dnsRefreshEnabled`, `deviceIp`

For more information on each Common Request Parameter, see CommonRequest Parameters.

**Response**

deviceResponse (see deviceResponse Type)

**Example**

To add (on remote Appliance 1.2.20.100) a Cisco ACS device named Cisco ACS Sample Device, with a description of Cisco ACS Description, having IP address 10.1.2.3, and enabling the Appliance to retrieve log messages from the device but not enabling DNS name refresh:

```
createDeviceRemote authstr 1.2.20.100 "Cisco ACS Sample Device" "Cisco ACS" "Cisco ACS Description" "yes" "no" "10.1.2.3"
```
readDevice Operation

Using readDevice operation you can view the configuration of an existing TIBCO LogLogic supported device based on the deviceName.

Request Parameters

authToken, deviceName

Response

deviceResponse (see deviceResponse Type)

Example

readDevice authstr “MyOracleDBName”

readDeviceRemote Operation

Using readDeviceRemote operation you can view the configuration of an existing LogLogic supported device based on the deviceName on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, deviceName

Response

deviceResponse (see deviceResponse Type)

Example

readDeviceRemote authstr 1.2.20.100 “MyOracleDBName”

updateDevice Operation

Using updateDevice operation you can update the configuration of an existing device.

Request Parameters

authToken, deviceName, deviceType, description, enabled, dnsRefreshEnabled, deviceIp, changeNameTo

Response

deviceResponse (see deviceResponse Type)

Example

To update the CiscoACSName device name to NewCiscoACSName:

updateDevice authstr “CiscoACSName” “Cisco ACS” “CiscoACSDescription” “yes” “no” “10.1.2.9” “NewCiscoACSName”
updateDeviceRemote Operation

With updateDeviceRemote operation you can update the configuration of an existing device on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, deviceName, deviceType, description, enabled, dnsRefreshEnabled, deviceIp, changeNameTo

Response

deviceResponse (see deviceResponse Type)

Example

To update the CiscoACSName device name to NewCiscoACSName:
updateDeviceRemote authstr 1.2.20.100 "CiscoACSName" "Cisco ACS" "CiscoACSDescription" "yes" "no" "10.1.2.9" "NewCiscoACSName"

deleteDevice Operation

With deleteDevice operation you can delete an existing device.

Request Parameters

authToken, deviceName

Response

deviceResponse (see deviceResponse Type)

Example

To delete the device MyDeviceName from the Appliance:
deleteDevice authstr "MyDeviceName"

deleteDeviceRemote Operation

With deleteDeviceRemote operation you can delete an existing device on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, deviceName

Response

deviceResponse (see deviceResponse Type)

Example

To delete the device MyDeviceName from remote Appliance 1.2.20.100:
deleteDeviceRemote authstr 1.2.20.100 "MyDeviceName"
**getList Operation**

With getList operation you can retrieve a list of all devices currently configured for the TIBCO LogLogic Appliance. This returns all devices, not just enabled devices.

**Request Parameter**

authToken

**Response**

If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all devices (total number indicated by resultCount) currently configured for the TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Example**

To list all devices currently configured for the Appliance:

```plaintext
getch
```

**getListRemote Operation**

Using getListRemote operation you can retrieve a list of all devices currently configured for a managed TIBCO LogLogic Appliance from a Management Station. This returns all devices, not just enabled devices.

**Request Parameter**

authToken, applianceIP

**Response**

If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all devices (total number indicated by resultCount) currently configured for the remote TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Example**

To list all devices currently configured for remote Appliance 1.2.20.100:

```plaintext
getchRemote authstr 1.2.20.100
```

**deviceResponse Type**

deviceResponse is returned for all device operations except getList and getListRemote.

deviceResponse always contains the following common elements:

- authToken
- resultCount
- statusCode
- statusMessage
- summaryOnly

If resultCount is 1 and statusCode is 2000 (successful), the resultSet element is included after resultCount listing the following device details:
- `applianceIp`
- `applianceName`
- `description`
- `deviceId`
- `deviceIp`
- `deviceName`
- `deviceType`
- `dnsRefreshEnabled`
- `enabled`

If `resultCount` is 0 and `statusCode` is not 2000 (successful), an error is returned in `statusMessage`.

**Common Request Parameters**

A set of Common Request Parameters are required for each Device Service operation. Table lists all of the Common Request parameters for the Device Service operations. For more information on the parameters, view the TIBCO LogLogic® Appliance user interface for managing devices as well as the online help.

*Device Service Operation Common Request Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The managed Appliance on which you perform the operation.</td>
<td>IP address of a managed Appliance. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>If the value is blank, it retrieves the Appliance IP address from the local Appliance. This parameter is available only for Management Station Appliances using operations with Remote in the name. (for xxxxRemote operations only)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deviceName</td>
<td>Name of the device from which you intend to transfer log data.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>deviceType</td>
<td>Type of device or application generating the logs to be transferred.</td>
<td>For example “Cisco Pix” See the Management &gt; Devices user interface for a list of available device type values.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>description</td>
<td>Description for the remote device. If you do not provide a description, you must at least specify the value as an empty string.</td>
<td>Any text up to 64 characters in length. Type double quotation marks (&quot;&quot;&quot;) to specify an empty string or no description text.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| dnsRefreshEnabled   | Enables the Device Name to be refreshed through DNS lookups. The DNS name might override any name you assign in the deviceName. | Possible values:  
yes — enable  
no — disable | yes      | string |
| deviceIp            | IP address of the device from which you want to transfer files.             | Standard IP address format. For example:  
10.1.2.3                                                             | yes      | string |
| changeNameTo        | New name of the device. If empty, the object name is unchanged.            | Any text up to 64 characters in length.  
(for updateDevice and updateDevice Remote only)                     | yes      | string |
Device Group Service Operations

The Device Group Service operations enable you to manage device groups in your TIBCO LogLogic® appliance.

Overview

Using Device Group Service operations you can create, read, update, and delete device groups as well as view all device groups in the TIBCO LogLogic® appliance.

Device groups are groups configured on the TIBCO LogLogic® appliance of any source of log data that you want captured by the appliance. In the TIBCO LogLogic® appliance, to view the user interface implementation navigate to Management > Devices > Device Groups.

Implementation Guidelines

These are some general implementation guidelines for Device Group Service operations:

- A set of Common Request Parameters are required for each operation. You must specify a value for all Required parameters.
- You must specify the value of the Common Request Parameters only.
- All parameters must be implemented in the order in which they appear in the Request Parameters section for each of the operations.
- All values for Common Request Parameters must be enclosed by double quotation marks ("value"). If the name of a device or a parameter value includes a forward slash (/), such as HP/UX, or IBM i5/OS, you must replace the forward slash with %2F. (The F is case-sensitive.)

Examples: HP%2FUX or IBM i5%2FOS

Status Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Server success</td>
</tr>
<tr>
<td>4000</td>
<td>Unauthorized request</td>
</tr>
<tr>
<td>5000</td>
<td>Invalid parameter, getStatusMessage() contains detail information about the error</td>
</tr>
</tbody>
</table>

Device Group Service Operation Descriptions

There are two kinds of operations:

- local - operation is performed on the local Appliance itself
- remote - operations (names ending with Remote) performed on a specified remote Appliance

There are two kinds of device groups:

- local - a group of log sources on the local Appliance (that is, the Appliance you are logged into)
- global - a group of log sources on multiple Appliances. Global groups are created and managed only from Management Station Appliances.

The Device Group Service operations are as follows:

- createDeviceGroup Operation
- createDeviceGroupRemote Operation
createDeviceGroup Operation

Using createDeviceGroup operation you can add a new device group to the TIBCO LogLogic® Appliance.

Request Parameters

- authToken, deviceGroupName, description, groupType, enabled, deviceNames

For more information on each Common Request Parameter, see Common Request Parameters.

Response

deviceGroupResponse (see deviceGroupResponse Type)

Example

To add a local device group named Cisco ACS Devices, with a description of Cisco ACS Description, including log sources 10.1.2.3 and CiscoACS1, and enabling the group:

```
createDeviceGroup authstr 1.2.20.100 "Cisco ACS Devices" "Cisco ACS Description" "local" "yes" "10.1.2.3,CiscoACS1"
```

createDeviceGroupRemote Operation

Using createDeviceGroupRemote operation you can add a new device group to a managed TIBCO LogLogic® Appliance from a Management Station.

Request Parameters

- authToken, applianceIP, deviceGroupName, description, groupType, enabled, deviceNames

For more information on each Common Request Parameter, see Common Request Parameters.

Response

deviceGroupResponse (see deviceGroupResponse Type)
**Example**

To add (on remote Appliance 1.2.20.100) a global device group named Cisco ACS Devices, with a description of Cisco ACS Description, including log sources 10.1.2.3 and CiscoACS1, and enabling the group:

```
createDeviceGroupRemote authstr 1.2.20.100 "Cisco ACS Devices" "Cisco ACS Description" "global" "yes" "10.1.2.3,CiscoACS1"
```

### addDevices Operation

With addDevices operation you can add one or more devices to a device group on a TIBCO LogLogic® appliance.

**Request Parameters**

- authToken, deviceGroupName, deviceNames

For more information on each Common Request Parameter, see [Common Request Parameters](#).

**Response**

- deviceGroupResponse (see [deviceGroupResponse Type](#))

**Example**

To add devices CiscoACS2 and 10.1.4.6 to the device group Cisco ACS Devices:

```
addDevices authstr "Cisco ACS Devices" "CiscoACS2,10.1.4.6"
```

### addDevicesRemote Operation

With addDevicesRemote operation you can add one or more devices to a device group on a managed TIBCO LogLogic® appliance from a Management Station.

**Request Parameters**

- authToken, applianceIP, deviceGroupName, deviceNames

For more information on each Common Request Parameter, see [Common Request Parameters](#).

**Response**

- deviceGroupResponse (see [deviceGroupResponse Type](#))

**Example**

To add (on remote appliance 1.2.20.100) devices CiscoACS2 and 10.1.4.6 to the device group Cisco ACS Devices:

```
addDevicesRemote authstr 1.2.20.100 "Cisco ACS Devices" "CiscoACS2,10.1.4.6"
```

### removeDevices Operation

Using removeDevices operation you can remove one or more devices from a device group on a TIBCO LogLogic Appliance.

**Request Parameters**

- authToken, deviceGroupName, deviceNames

For more information on each Common Request Parameter, see [Common Request Parameters](#).
removeDevicesRemote Operation

Using removeDevicesRemote operation you can remove one or more devices from a device group on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**

- authToken, applianceIP, deviceGroupName, deviceNames

For more information on each Common Request Parameter, see [Common Request Parameters](#).

**Response**

deviceGroupResponse (see deviceGroupResponse Type)

**Example**

To remove (on remote Appliance 1.2.20.100) devices CiscoACS2 and 10.1.4.6 from the device group Cisco ACS Devices:

```
removeDevicesRemote authstr 1.2.20.100 "Cisco ACS Devices" "CiscoACS2,10.1.4.6"
```

readDeviceGroupRemote Operation

Using readDeviceGroupRemote operation you can view the configuration of an existing device group based on the deviceGroupName on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**

- authToken, applianceIP, deviceGroupName

**Response**

deviceResponse (see deviceGroupResponse Type)

**Example**

readDeviceGroup authstr “MyOracleDBGroup”

readDeviceGroupRemote Operation

Using readDeviceGroupRemote operation you can view the configuration of an existing device group based on the deviceGroupName on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**

- authToken, applianceIP, deviceGroupName

**Response**

deviceResponse (see deviceGroupResponse Type)
Example
readDeviceGroupRemote authstr 1.2.20.100 “MyOracleDBGroup”

updateDeviceGroup Operation
With updateDeviceGroup operation you can update the configuration of an existing device group.

Request Parameters
authToken, deviceGroupName, description, groupType, enabled, deviceNames, changeNameTo
If deviceNames is empty, the group’s devices are unchanged. If deviceNames are specified, the group is updated to include the listed devices.

Response
deviceResponse (see deviceGroupResponse Type)

Example
To update the global CiscoACSGroup device group name to NewCiscoACSGroup:
updateDeviceGroup authstr “CiscoACSGroup” “CiscoACSDescription” “global” “yes” “” “NewCiscoACSGroup”

updateDeviceGroupRemote Operation
With updateDeviceGroupRemote operation you can update the configuration of an existing device group on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters
authToken, applianceIP, deviceGroupName, description, groupType, enabled, deviceNames, changeNameTo
If deviceNames is empty, the group’s devices are unchanged. If deviceNames are specified, the group is updated to include the listed devices.

Response
deviceResponse (see deviceGroupResponse Type)

Example
To update the global CiscoACSGroup device group name on TIBCO LogLogic Appliance 10.1.20.200 to NewCiscoACSGroup:
updateDeviceGroupRemote authstr 10.1.20.200 “CiscoACSGroup” “CiscoACSDescription” “global” “yes” “” “NewCiscoACSGroup”

deleteDeviceGroup Operation
With deleteDeviceGroup operation you can delete an existing device group.

Request Parameters
authToken, deviceGroupName

Response
deviceResponse (see deviceGroupResponse Type)
Example
To delete the device group MyDeviceGroup from the Appliance:
`deleteDevice authstr "MyDeviceGroup"

**deleteDeviceGroupRemote Operation**
With deleteDeviceGroupRemote operation you can delete an existing device group on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**
authToken, applianceIP, deviceGroupName

**Response**
deviceResponse (see deviceGroupResponse Type)

Example
To delete the device group MyDeviceGroup from remote Appliance 1.2.20.100:
`deleteDeviceGroupRemote authstr 1.2.20.100 "MyDeviceGroup"

**getList Operation**
With getList operation you can retrieve a list of all device groups currently configured for the TIBCO LogLogic Appliance. This returns all device groups, not just enabled device groups.

**Request Parameter**
authToken

**Response**
If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all device groups (total number indicated by resultCount) currently configured for the TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

Example
To list all device groups currently configured for the Appliance:
`getList authstr

**getListRemote Operation**
With getListRemote operation you can retrieve a list of all device groups currently configured for a managed TIBCO LogLogic Appliance from a Management Station. This returns all device groups, not just enabled device groups.

**Request Parameter**
authToken, applianceIP

**Response**
If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all device groups (total number indicated by resultCount) currently configured for the remote TIBCO LogLogic Appliance.
If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

Example

To list all device groups currently configured for remote Appliance 1.2.20.100:

ggetListRemote authstr 1.2.20.100

**deviceGroupResponse Type**

deviceGroupResponse is returned for all deviceGroup operations except getList and getListRemote.
deviceGroupResponse always contains the following common elements:

- authToken
- resultCount
- statusCode
- statusMessage
- summaryOnly

If resultCount is 1 and statusCode is 2000 (successful), the resultSet element is included after resultCount listing the following device group details:

- deviceGroupName
- description
- groupType
- enabled
- devices

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Common Request Parameters**

A set of Common Request Parameters are required for each Device Group Service operation. The following table lists all of the Common Request parameters for the Device Group Service operations. For more information on the parameters, view the TIBCO LogLogic® appliance user interface for managing device groups as well as the online help.

**Device Group Service Operation Common Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The managed Appliance on which you perform the operation.</td>
<td>IP address of a managed Appliance. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>If the value is blank, it retrieves the Appliance IP address from the local Appliance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This parameter is available only for Management Station Appliances using operations with Remote in the name.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>deviceGroupName</td>
<td>Name of the device group on the TIBCO LogLogic® Appliance.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>description</td>
<td>Description for the device group. If you do not provide a description, you must at least specify the value as an empty string.</td>
<td>Any text up to 64 characters in length. Possible values: double quotation marks (&quot;&quot;&quot;) to specify an empty string or no description text.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>groupType</td>
<td>Type of device group, either local or global. The groupType value cannot be changed once the device profile is added.</td>
<td>local or global</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>enabled</td>
<td>Indicates whether retrieval of log files from this device is enabled. (Appears as enabled or disabled in returned value.)</td>
<td>Possible values: yes — enable, no — disable</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>deviceNames</td>
<td>Names or IP addresses (comma-separated) of devices in the group.</td>
<td>Standard IP address format or device name. For example: 10.1.2.3 or CiscoACS2</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>changeNameTo</td>
<td>New name of the device group. If empty, the object name is unchanged.</td>
<td>Any text up to 64 characters in length. (for TIBCO LogLogic LMI Web Services API Implementa tion Guide and updateDeviceGroup Remote only)</td>
<td>yes</td>
<td>string</td>
</tr>
</tbody>
</table>
The Message Routing Service operations enable you to manage message routing rules for your TIBCO LogLogic® appliance.

**Overview**

The Message Routing Service operations enable you to create, read, update, and delete message routing rules as well as view all message routing rules in your TIBCO LogLogic® appliance.

Using Message Routing Rules you can forward a copy of incoming log data from one TIBCO LogLogic® appliance to another TIBCO LogLogic® appliance or 3rd party device. In the TIBCO LogLogic® appliance you can view the user interface implementation by navigating to Administration > Message Routing.

**Implementation Guidelines**

The following are general implementation guidelines for the Message Routing Service operations:

- A set of **Common Request Parameters** are required for each operation. You must specify a value for all Required parameters.
- You must specify the value of the Common Request Parameters only.
- All parameters must be implemented in the order in which they appear in the Request Parameters section for each of the operations.
- All values for Common Request Parameters must be enclosed by double quotation marks (“value”). If the name of a device or a parameter value includes a forward slash (/), such as HP/UX, or IBM i5/OS, you must replace the forward slash with %2F. (The F is case-sensitive.)

**Examples**: HP%2FUX or IBM i5%2FOS

**Status Codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Server success</td>
</tr>
<tr>
<td>4000</td>
<td>Unauthorized request</td>
</tr>
<tr>
<td>5000</td>
<td>Invalid parameter, getStatusMessage() contains detail information about the error</td>
</tr>
</tbody>
</table>

**Message Routing Service Operation Descriptions**

There are two kinds of operations:

- **local** - operation is performed on the local Appliance itself
- **remote** - operations (names ending with Remote) performed on a specified remote Appliance

The Message Routing Service contains the following operations:

- createMsgRouting Operation
- createMsgRoutingRemote Operation
- readMsgRouting Operation
- readMsgRoutingRemote Operation
- updateMsgRouting Operation
createMsgRouting Operation

With createMsgRouting operation you can create message routing rules.

Request Parameters

authToken, routingName, sourceDevice, destinationIP, destinationPort, routingProtocol, enabled, severity, facility, searchFilterName, compressionEnabled, encryptionEnabled, authenticationEnabled

For more information on each Common Request Parameter, see Common Request Parameters.

Response

msgRoutingResponse (see msgRoutingResponse Type)

Example

To add a message routing rule named MyRoutingRuleName for device 10.1.2.3 to route to 10.2.3.4 port 4433 using the TIBCO LogLogic TCP protocol, for all Syslog messages using the search filter named MySearchFilter, with encryption and authentication enabled:

createMsgRouting authstr "MyRoutingRuleName" "10.1.2.3" "10.2.3.4" "4433" "LogLogic TCP" "yes" "All Syslog" "MySearchFilter" "no" "yes" "yes"

createMsgRoutingRemote Operation

With createMsgRoutingRemote operation you can create message routing rules on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, routingName, sourceDevice, destinationIP, destinationPort, routingProtocol, enabled, severity, facility, searchFilterName, compressionEnabled, encryptionEnabled, authenticationEnabled

For more information on each Common Request Parameter, see Common Request Parameters.

Response

msgRoutingResponse (see msgRoutingResponse Type)

Example

To add a message routing rule (on remote Appliance 1.2.20.100) named MyRoutingRuleName for device 10.1.2.3 to route to 10.2.3.4 port 4433 using the TIBCO LogLogic TCP protocol, for all Syslog messages using the search filter named MySearchFilter, with encryption and authentication enabled and compression disabled:

createMsgRoutingRemote authstr 1.2.20.100 "MyRoutingRuleName" "10.1.2.3" "10.2.3.4" "4433" "LogLogic TCP" "yes" "All Syslog" "MySearchFilter" "no" "yes" "yes"
readMsgRouting Operation

With readMsgRouting operation you can view the configuration of an existing message routing rule.

Request Parameters
authToken, routingName

Response
msgRoutingResponse (see msgRoutingResponse Type)

Example
To view the configuration of message routing rule MyRoutingRule:
readMsgRouting authstr “MyRoutingRule”

readMsgRoutingRemote Operation

With readMsgRoutingRemote operation you can view the configuration of an existing message routing rule on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters
authToken, applianceIP, routingName

Response
msgRoutingResponse (see msgRoutingResponse Type)

Example
To view the configuration of message routing rule MyRoutingRule on remote Appliance 1.2.20.100:
readMsgRoutingRemote authstr 1.2.20.100 “MyRoutingRule”

updateMsgRouting Operation

Using updateMsgRouting operation you can update the configuration of an existing message routing rule.

Request Parameters
authToken, routingName, sourceDevice, destinationIP, destinationPort, routingProtocol, enabled, severity, facility, searchFilterName, compressionEnabled, encryptionEnabled, authenticationEnabled, changeNameTo

Response
msgRoutingResponse (see msgRoutingResponse Type)

Example
To update MyRoutingRuleName to NewRoutingRuleName:
updateMsgRouting authstr “MyRoutingRuleName” “10.1.2.3” “10.2.3.4” “4433” “LogLogic TCP” “yes” “All Syslog” “MySearchFilter” “no” “yes” “yes” “NewRoutingRuleName”
updateMsgRoutingRemote Operation

With updateMsgRoutingRemote operation you can update the configuration of an existing message routing rule on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**

- authToken
- applianceIP
- routingName
- sourceDevice
- destinationIP
- destinationPort
- routingProtocol
- enabled
- severity
- facility
- searchFilterName
- compressionEnabled
- encryptionEnabled
- authenticationEnabled
- changeNameTo

**Response**

msgRoutingResponse (see msgRoutingResponse Type)

**Example**

To update MyRoutingRuleName to NewRoutingRuleName on remote Appliance 1.2.20.100:

```
updateMsgRoutingRemote authstr 1.2.20.100 "MyRoutingRuleName" 10.1.2.3 10.2.3.4 4433 "LogLogic TCP" yes "All Syslog" "MySearchFilter" no yes yes "NewRoutingRuleName"
```

deleteMsgRouting Operation

With deleteMsgRouting operation you can delete an existing message routing rule.

**Request Parameters**

- authToken
- routingName

**Response**

msgRoutingResponse (see msgRoutingResponse Type)

**Example**

To delete message routing rule MyRoutingRuleName from the Appliance:

```
deleteMsgRouting authstr "MyRoutingRuleName"
```

deleteMsgRoutingRemote Operation

Using deleteMsgRouting operation you can delete an existing message routing rule on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**

- authToken
- applianceIP
- routingName

**Response**

msgRoutingResponse (see msgRoutingResponse Type)

**Example**

To delete message routing rule MyRoutingRuleName from remote Appliance 1.2.20.100:

```
deleteMsgRoutingRemote authstr 1.2.20.100 "MyRoutingRuleName"
```
**getList Operation**

With getList operation you can retrieve a list of all message forwarding rules currently configured in the TIBCO LogLogic Appliance.

**Request Parameter**

authToken

**Response**

If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all message forwarding rules (total number indicated by resultCount) currently configured in the TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Example**

To list all message forwarding rules currently configured on the Appliance:

```
getList authstr
```

**getListRemote Operation**

With getListRemote operation you can retrieve a list of all message forwarding rules currently configured on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameter**

authToken, applianceIP

**Response**

If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all message forwarding rules (total number indicated by resultCount) currently configured in the remote TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Example**

To list all message forwarding rules currently configured on remote Appliance 1.2.20.100:

```
getListRemote authstr 1.2.20.100
```

**msgRoutingModule Response Type**

msgRoutingModuleResponse is returned for all msgRoutingModule operations except getList and getListRemote. msgRoutingModuleResponse always contains the following common elements:

- authToken
- resultCount
- statusCode
- statusMessage
- summaryOnly

If resultCount is 1 and statusCode is 2000 (successful), the resultSet element is included after resultCount listing the following Message Forwarding Rule details:
- routingName
- sourceDevice
- destinationIP
- destinationPort
- routingProtocol
- enabled
- severity
- facility
- searchFilterName
- compressionEnabled
- encryptionEnabled
- authenticationEnabled
- changeNameTo (updateMsgRouting and updateMsgRoutingRemote only)

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Common Request Parameters**

A set of Common Request Parameters are required for each Message Routing Service operation. The following table lists all of the Message Routing Service Common Request Parameters. For more information on the parameters, view the TIBCO LogLogic® appliance user interface for message routing as well as the online help.

**Message Routing Service Common Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The managed Appliance on which you perform the operation.</td>
<td>IP address of a managed Appliance. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>If the value is blank, it retrieves the Appliance IP address from the local Appliance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This parameter is available only for Management Station Appliances using operations with Remote in the name.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>routingName</td>
<td>Name of the routing or forwarding rule.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>sourceDevice</td>
<td>Source device from where messages are routed.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>destinationIP</td>
<td>IP address for the message forwarding.</td>
<td>Standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>destinationPort</td>
<td>Port for the message forwarding.</td>
<td>Any positive integer.</td>
<td>yes</td>
<td>number</td>
</tr>
<tr>
<td>routingProtocol</td>
<td>Protocol used for message forwarding.</td>
<td>Possible values: UDP, Syslog, Raw TCP, Syslog</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>For more information on each protocol, see the online help.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>enabled</td>
<td>Enables message routing.</td>
<td>Possible values: yes — enable, No — disable</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>(Appears as enabled or disabled in returned value.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>severity</td>
<td>Message type used to filter messages</td>
<td>Possible values: All, Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug</td>
<td>no</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>For more information on each severity level, see the online help.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>facility</td>
<td>The facility specifies the subsystem that produced the message. For example, all mail programs log with the mail facility (LOG_MAIL) if they log using syslog.</td>
<td>Possible values: auth, auth2, Clock, Clock2, FTP, Kernel, Local0, Local1, Local3, Local4, Local5, Local6, Local7, Log Alert, Log Audit, Mail, News, NTP, Printer, Syslog, System, User-Level, UUCP</td>
<td>no</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>For more information on each facility, see the online help.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>searchFilterName</td>
<td>Name of the search filter.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>compressionEnabled</td>
<td>Enables or disables compression for LogLogic TCP message routing.</td>
<td>Possible values: yes — enable, no — disable</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>For LX Appliances, LogLogic recommends enabling compression.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>encryptionEnabled</td>
<td>Enables or disables encryption of the message routing rule.</td>
<td>Possible values: yes — enable, no — disable</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>authentication</td>
<td>Enables and disables authentication of the log message.</td>
<td>Possible values:</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
<td>yes — enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>no — disable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>changeNameTo</td>
<td>New name of the routing or forwarding rule.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(for TIBCO LogLogic® Log Management Intelligence Web Services API Implementation Guide and updateMsg RoutingRemote only)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Search Filter Service Operations

The Search Filter Service operations enable you to manage search filters in your TIBCO LogLogic Appliance.

Overview

With Search Filter Service operations you can create, read, update, and delete search filters as well as view all search filters in your TIBCO LogLogic Appliance.

Using Search filters you can define search patterns to view specific data and to define alerts. In the TIBCO LogLogic Appliance you can view the user interface implementation by navigating to Search > All Search Filters.

Implementation Guidelines

These are general implementation guidelines for the Search Filter Service operations:

- A set of Common Request Parameters are required for each operation. You must specify a value for all Required parameters.
- You must specify the value of the Common Request Parameters only.
- All parameters must be implemented in the order in which they appear in the Request Parameters section for each of the operations.
- All values for Common Request Parameters must be enclosed by double quotation marks (“value”). If the name of a device or a parameter value includes a forward slash (/), such as HP/UX, or IBM i5/OS, you must replace the forward slash with %2F. (The F is case-sensitive.)

Examples: HP%2FUX or IBM i5%2FOS

To search on the expression %2F itself, replace the % with %25. The resulting expression to use is %252F.

Status Codes

The Status Codes are:

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Server success</td>
</tr>
<tr>
<td>4000</td>
<td>Unauthorized request</td>
</tr>
<tr>
<td>5000</td>
<td>Invalid parameter, getStatusMessage() contains detail information about the error</td>
</tr>
</tbody>
</table>

Search Filter Service Operation Descriptions

Using Search Filter Service operations you can create, read, update, and delete search filters in your Appliance. In the TIBCO LogLogic Appliance user interface, you can view all actions accessible through the Search Filter Service operations by navigating to Search Filter screen from the navigation tree.

There are two kinds of operations:

- **local** - operation is performed on the local Appliance itself
- **remote** - operations (names ending with Remote) performed on a specified remote Appliance

The Search Filter Service operation contains the following operations:
- createSearchFilter Operation
- createSearchFilterRemote Operation
- readSearchFilter Operation
- readSearchFilterRemote Operation
- updateSearchFilter Operation
- updateSearchFilterRemote Operation
- deleteSearchFilter Operation
- deleteSearchFilterRemote Operation
- getList Operation
- getListRemote Operation
- searchFilterResponse Type

**createSearchFilter Operation**

With createSearchFilter operation you can create search filters with associated search terms.

**Request Parameters**

- authToken
- searchFilterName
- searchFilterType
- description
- sharedWithOtherUsers
- expression1
- expression2
- expressionOperator

TIBCO LogLogic LMI Web Services API Implementation Guide

For more information on each Common Request Parameter, see Common Request Parameters.

**Response**

searchFilterResponse (see searchFilterResponse Type)

**Example**

To add a search filter named My Search Filter Name using the BooleanSearchFilter1 filter, of the Boolean Search type, described as My Search Filter Description, sharing the filter with other users, and searching on the term failed:

createSearchFilter authstr "My Search Filter Name" "BooleanSearchFilter1" "Boolean Search" "My Search Filter Description" "yes" "failed" "" ""

**createSearchFilterRemote Operation**

With createSearchFilterRemote operation you can create search filters with associated search terms on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**

- authToken
- applianceIP
- searchFilterName
- searchFilterType
- description
- sharedWithOtherUsers
- expression1
- expression2
- expressionOperator

For more information on each Common Request Parameter, see Common Request Parameters.

**Response**

searchFilterResponse (see searchFilterResponse Type)
Example
To add a search filter (to remote Appliance 1.2.20.100) named My Search Filter Name using the BooleanSearchFilter1 filter, of the Boolean Search type, described as My Search Filter Description, sharing the filter with other users, and searching on the term failed:

createSearchFilterRemote authstr 1.2.20.100 “My Search Filter Name” “BooleanSearchFilter1” “Boolean Search” “My Search Filter Description” “yes” “failed” “” “”

readSearchFilter Operation
Using readSearchFilter operation you can view the details of a specific search filter defined in your TIBCO LogLogic Appliance.

Request Parameters
authToken, searchFilterName

Response
searchFilterResponse (see searchFilterResponse Type)

Example
To view the details of the search filter named My Search Filter Name:
readSearchFilter authstr “My Search Filter Name”

readSearchFilterRemote Operation
With readSearchFilterRemote operation you can view the details of a specific search filter defined on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters
authToken, applianceIP, searchFilterName

Response
searchFilterResponse (see searchFilterResponse Type)

Example
To view the details of the search filter named My Search Filter Name on remote Appliance 1.2.20.100:
readSearchFilterRemote authstr “My Search Filter Name”

updateSearchFilter Operation
With updateSearchFilter operation you can update an existing search filter.

Request Parameters
authToken, searchFilterName, searchFilterType, description, sharedWithOtherUsers, expression1, expression2, expressionOperator, changeNameTo

Response
searchFilterResponse (see searchFilterResponse Type)
Example
To update an existing search filter named My Search Filter Name to My New Search Filter Name:
updateSearchFilter authstr "My Search Filter Name" "BooleanSearchFilter1" "Boolean Search" "My Search Filter Description" "yes" "failed" "" "" "My New Search Filter Name"

updateSearchFilterRemote Operation
Using updateSearchFilterRemote operation you can update an existing search filter on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters
authToken, applianceIP, searchFilterName, searchFilterType, description, sharedWithOtherUsers, expression1, expression2, expressionOperator, changeNameTo

Response
searchFilterResponse (see searchFilterResponse Type)

Example
To update an existing search filter named My Search Filter Name to My New Search Filter Name on remote Appliance 1.2.20.100:
updateSearchFilterRemote authstr 1.2.20.100 "My Search Filter Name" "BooleanSearchFilter1" "Boolean Search" "My Search Filter Description" "yes" "failed" "" "" "My New Search Filter Name"

deleteSearchFilter Operation
With deleteSearchFilter operation you can remove an existing search filter from your TIBCO LogLogic Appliance.

Request Parameters
authToken, searchFilterName

Response
searchFilterResponse (see searchFilterResponse Type)

Example
To remove the search filter named My Search Filter Name from the Appliance:
deleteSearchFilter authstr "My Search Filter Name"

deleteSearchFilterRemote Operation
With deleteSearchFilterRemote operation you can remove an existing search filter on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters
authToken, applianceIP, searchFilterName

Response
searchFilterResponse (see searchFilterResponse Type)
Example
To remove the search filter named My Search Filter Name from remote Appliance 1.2.20.100:
deleSearchFilterRemote authstr 1.2.20.100 "My Search Filter Name"

ggetList Operation
With getList operation you can retrieve a list of all search filters currently configured in the TIBCO LogLogic Appliance.

Request Parameters
authToken

Response
If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all search filters (total number indicated by resultCount) currently configured in the TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

Example
To view a list of all search filters on the Appliance:
getList authstr

ggetListRemote Operation
With getListRemote operation you can retrieve a list of all search filters currently configured on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters
authToken, applianceIP

Response
If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all search filters (total number indicated by resultCount) currently configured in the remote TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

Example
To view a list of all search filters on remote Appliance 1.2.20.100:
getListRemote authstr 1.2.20.100

searchFilterResponse Type
searchFilterResponse is returned for all searchFilter operations except getList and getListRemote.
searchFilterResponse always contains the following common elements:

- authToken
- resultCount
- statusCode
If `resultCount` is 1 and `statusCode` is 2000 (successful), the `resultSet` element is included after `resultCount` listing the following Search Filter details:

- `expression1`
- `expression2`
- `expressionOperator`
- `expressionType`
- `filterDescription`
- `filterName`
- `sharedWithOtherUsers`

If `resultCount` is 0 and `statusCode` is not 2000 (successful), an error is returned in `statusMessage`.

### Common Request Parameters

A set of Common Request Parameters are required for each Search Filter operation. The following table lists all of the Search Filter parameters. For more information on the parameters, view the TIBCO LogLogic® Appliance user interface for search filters as well as the online help.

**Search Filter Operation Common Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The managed Appliance on which you perform the operation. If the value is blank, it retrieves the Appliance IP address from the local Appliance. This parameter is available only for Management Station Appliances using operations with Remote in the name.</td>
<td>IP address of a managed Appliance. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>searchFilterName</td>
<td>Name of the search filter.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>searchFilterType</td>
<td>Type of search filter.</td>
<td>Use Words, Use Exact Phrase, Regular Expression, or Boolean Search</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>description</td>
<td>Description of the search filter name (searchFilterName parameter)</td>
<td>Any text up to 255 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>sharedWithOtherUsers</td>
<td>Identifies if this search filter is available to other users. If yes, it is shared with others.</td>
<td>no, Read Only, and Read Write</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>expression1</td>
<td>The actual search terms for the search filter.</td>
<td>Any valid search criteria up to 276 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>expression2</td>
<td>The actual search terms for the search filter.</td>
<td>Any valid search criteria up to 270 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>expressionOperator</td>
<td>The actual search terms for the search filter.</td>
<td></td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>changeNameTo</td>
<td>New name of the search filter. If empty, the object name is unchanged.</td>
<td>Any text up to 64 characters in length.</td>
<td>yes (for updateSearchFilter and updateSearchFilterRemote only)</td>
<td>string</td>
</tr>
</tbody>
</table>
User Administration Service Operations

The User Administration Service operations enable you to manage users in your TIBCO LogLogic Appliance.

Overview

The User Administration Service operations enable you to create, read, update, and delete users in your system. In the TIBCO LogLogic Appliance you can view the user interface implementation by navigating to Management > Users.

Implementation Guidelines

These are the general implementation guidelines for the User Administration Service operations:

- A set of Common Request Parameters are required for each of the operations. You must specify a value for all Required parameters.
- You must specify the value of the Common Request Parameters only.
- All parameters must be implemented in the order in which they appear in the Request Parameters section for each of the operations.
- Use forward slash marks as delimiters when specifying multiple values for the privileges Common Request Parameter. For example:
  "valueA/ValueB/ValueD"
- All values for Common Request Parameters must be enclosed by double quotation marks ("value"). If the name of a device or a parameter value includes a forward slash (/), such as HP/UX, or IBM i5/OS, you must replace the forward slash with %2F. (The F is case-sensitive.)

  Examples: HP%2FUX or IBM i5%2FOS

Status Codes

The status codes are:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Server success</td>
</tr>
<tr>
<td>4000</td>
<td>Unauthorized request</td>
</tr>
<tr>
<td>5000</td>
<td>Invalid parameter, getStatusMessage() contains detail information about the error</td>
</tr>
</tbody>
</table>

User Administration Service Operation Descriptions

There are two kinds of operations:

- local - operation is performed on the local Appliance itself
- remote - operations (names ending with Remote) performed on a specified remote Appliance

The User Administration Service operation contains the following operations:

- createUser Operation
- createUserRemote Operation
- readUser Operation
- readUserRemote Operation
createUser Operation

With createUser operation you can create new users in the TIBCO LogLogic Appliance.

Request Parameters

authToken, loginName, firstName, lastName, loginPassword, phone, email, enabled, privileges, devices, appliances

For more information on each Common Request Parameter, see Common Request Parameters.

Response

userResponse (see userResponse Type)

Example

To create a user named MyFirstName MyLastName with email address me@loglogic.com, phone number 1-777-7777, authenticating locally, with an initial password MyPassword, and with Report Administrator access to all general syslog devices:

createUser authstr "me" "MyFirstName" "MyLastName" "MyPassword" "1-777-7777" "me@loglogic.com" "yes" "Report Administrator" "All General Syslog"

createUserRemote Operation

Using createUserRemote operation you can create new users on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, loginName, firstName, lastName, loginPassword, phone, email, enabled, privileges, devices, appliances

For more information on each Common Request Parameter, see Common Request Parameters.

Response

userResponse (see userResponse Type)

Example

To create a user (on remote Appliance 1.2.20100) named MyFirstName MyLastName with email address me@loglogic.com, phone number 1-777-7777, authenticating locally, with an initial password MyPassword, and with Report Administrator access to all general syslog devices:

createUserRemote authstr 1.2.20100 "me" "MyFirstName" "MyLastName" "MyPassword" "1-777-7777" "me@loglogic.com" "yes" "Report Administrator" "All General Syslog"
**readUser Operation**

With readUser operation you can view the configuration of an existing user.

**Request Parameters**

- authToken, loginName

**Response**

- userResponse (see userResponse Type)

**Example**

To view the configuration of user UserName:

readMsgRouting authstr “UserName”

**readUserRemote Operation**

With readUserRemote operation you can view the configuration of an existing user on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameters**

- authToken, applianceIP, loginName

**Response**

- userResponse (see userResponse Type)

**Example**

To view the configuration of user UserName on remote Appliance 1.2.20.100:

readMsgRoutingRemote authstr 1.2.20.100 “UserName”

**updateUser Operation**

With updateUser operation you can update the configuration of an existing user.

**Request Parameters**

- authToken, loginName, firstName, lastName, loginPassword, phone, email, enabled, privileges, devices, appliances, changeLoginNameTo

**Response**

- userResponse (see userResponse Type)

**Example**

To update the createUser example, by removing the Configuration Administrator as a privilege for the user:

updateUser authstr “me” “MyFirstName” “MyLastName” “MyPassword” “1-777-7777” “me@loglogic.com” “yes” “Report Administrator” “all” “” “”
updateUserRemote Operation

With updateUserRemote operation you can update the configuration of an existing user on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, loginName, firstName, lastName, loginPassword, phone, email, enabled, privileges, devices, appliances, changeLoginNameTo

Response

userResponse (see userResponse Type)

Example

To update the createUserRemote example, by removing the Configuration Administrator as a privilege for the user on remote Appliance 1.2.20.100:

updateUserRemote authstr 1.2.20.100 “me” “MyFirstName” “MyLastName” “MyPassword” “1-777-7777” “me@loglogic.com” “yes” “Report Administrator” “all” “” “”

deleteUser Operation

Using deleteUser operation you can delete an existing user.

Request Parameters

authToken, loginName

Response

userResponse (see userResponse Type)

Example

To delete user UserName from the Appliance:

deleteUser authstr “UserName”

deleteUserRemote Operation

With deleteUser operation you can delete an existing user on a managed TIBCO LogLogic Appliance from a Management Station.

Request Parameters

authToken, applianceIP, loginName

Response

userResponse (see userResponse Type)

Example

To delete user UserName from remote Appliance 1.2.20.100:

deleteUserRemote authstr 1.2.20.100 “UserName”
**getList Operation**

Using getList operation you can retrieve a list of all users currently configured in the TIBCO LogLogic Appliance.

**Request Parameter**

authToken

**Response**

If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all users (total number indicated by resultCount) currently configured in the TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Example**

To view a list of all users configured on the Appliance:

g getList authstr

**getListRemote Operation**

With getListRemote operation you can retrieve a list of all users currently configured on a managed TIBCO LogLogic Appliance from a Management Station.

**Request Parameter**

authToken, applianceIP

**Response**

If resultCount is greater than 0 and statusCode is 2000 (successful), the response returns a list of all users (total number indicated by resultCount) currently configured in the remote TIBCO LogLogic Appliance.

If resultCount is 0 and statusCode is not 2000 (successful), an error is returned in statusMessage.

**Example**

To view a list of all users configured on remote Appliance 1.2.20.100:

g getListRemote authstr 1.2.20.100

**userResponse Type**

userResponse is returned for all user operations except getList and getListRemote.

userResponse always contains the following common elements:

- authToken
- resultCount
- statusCode
- statusMessage
- summaryOnly

If resultCount is 1 and statusCode is 2000 (successful), the resultSet element is included after resultCount listing the following User details:
- `loginName`
- `firstName`
- `lastName`
- `loginPassword`
- `phone`
- `email`
- `enabled`
- `privileges`
- `devices`
- `appliances` (createUser, createUserRemote, updateUser, and updateUserRemote only)
- `changeLoginName` (updateUser and updateUserRemote only)

If `resultCount` is 0 and `statusCode` is not 2000 (successful), an error is returned in `statusMessage`.

### Common Request Parameters

A set of Common Request Parameters are required for each User Administration Service operation. The following table lists all of the User Administration Service Common Request Parameters. For more information on the parameters, view the TIBCO LogLogic® Appliance user interface for Manage Users as well as the online help.

#### User Administration Service Operation Common request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The managed Appliance on which you perform the operation.</td>
<td>IP address of a managed Appliance. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>If the value is blank, it retrieves the Appliance IP address from the local Appliance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This parameter is available only for Management Station Appliances using operations with Remote in the name.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>loginName</td>
<td>Login name for the user you are creating.</td>
<td>Any text up to 16 characters in length.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td>firstName</td>
<td>First name of the user.</td>
<td>Any text up to 64 characters in length.</td>
<td>No</td>
<td>string</td>
</tr>
<tr>
<td>lastName</td>
<td>Last name of the user.</td>
<td>Any text up to 64 characters in length.</td>
<td>No</td>
<td>string</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>loginPassword</td>
<td>Password used for user login.</td>
<td>The password must be at least 6 characters long, contain at least one non-alphabetic character, and cannot be the same as the loginName.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>In addition, you can use the loginPassword parameter to update/change a user's password.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Active Directory (AD) users, enclose the password in single-quotes (') when it is an input parameter to a shell script. AD passwords can contain special characters (such as !, @, or *) which the shell does not properly interpret unless within single-quotes.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>phone</td>
<td>Contact phone number of user.</td>
<td>Any valid phone number up to 32 characters in length.</td>
<td>No</td>
<td>string</td>
</tr>
<tr>
<td>email</td>
<td>Email address of the user.</td>
<td>Any valid email address up to 64 characters in length.</td>
<td>Yes</td>
<td>string</td>
</tr>
<tr>
<td>enabled</td>
<td>Enable or disable the user specified with the loginName parameter.</td>
<td>Possible values:</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>(Appears as enabled or disabled in returned value.)</td>
<td>yes — enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>no — disable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>privileges</td>
<td>Identifies the access privileges for the specified user. You can specify a User Type (contains a pre-defined list of privileges) or specific privileges.</td>
<td>For a list of possible values, see User Administration Privileges.</td>
<td>yes</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>To view the user interface implementation, navigate to the Administration &gt; Manage Users &gt; Privileges tab.</td>
<td>To specify multiple values, you must separate entries with a forward slash (/). For example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Import/Export privilege contains a forward slash (/). To specify it here, replace / with %2F.</td>
<td>User Administrator/Manage Alerts/Manage Devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>------</td>
</tr>
</tbody>
</table>
| devices            | Identifies the devices that the user can access. You can specify All for provide access to all devices in the Appliance or you can identify specific devices. You can use the getList Operation to retrieve a list of device names in your LogLogic Appliance. Alternatively, you can view use the user interface to view all devices by navigating to Administration > Manage Devices. | Possible values: All - all devices  
deviceName - specify each device name as it appears in the LogLogic Appliance.  
To specify multiple values, you must separate entries with a forward slash (/). For example: “Device1/Device2/Device7/Device9” | yes      | string |
| appliances         | (Management Station only) Identifies the Appliance in the Management Station cluster that this user accesses. | Any valid IP address | yes (for createUser, createUser Remote, updateUser and updateUser Remote only) | number   |
| changeLogin Name   | New login name for a user. If empty, the login name is unchanged. | Any text up to 64 characters in length. | yes (for updateUser and TIBCO LogLogic LMI Web Services API Implementation Guide only) | string  |
System Service

The System Service provides programmatic access to the system functionality on the TIBCO LogLogic Appliance.

Overview

The System Service API provides these operations:

- Using getApplianceSystemInfo, your program retrieve the system information on an Appliance.

Status Codes

The Status Codes are:

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No error</td>
</tr>
<tr>
<td>1</td>
<td>No data available for the query parameters provided</td>
</tr>
<tr>
<td>5</td>
<td>Insufficient Privilege for requested operation</td>
</tr>
<tr>
<td>7</td>
<td>Invalid input</td>
</tr>
<tr>
<td>8</td>
<td>Persistence exception</td>
</tr>
</tbody>
</table>

Get Appliance System Info Operation

The getApplianceSystemInfo operation returns a result containing the system information on an Appliance.

Get Appliance System Info Request Parameters

The getApplianceSystemInfo operation request parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>Yes</td>
<td>String</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The Appliance from which you retrieve the system information.</td>
<td>IP address. For example: 10.1.2.3</td>
<td>Yes</td>
<td>String</td>
</tr>
</tbody>
</table>

Get Appliance System Info Response Attributes

The getApplianceSystemInfo response attributes are:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>applianceIp</td>
<td>Appliance IP. For example, &quot;10.0.80.14&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>applianceModel</td>
<td>Appliance model. For example, &quot;LX2010&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>applianceTitle</td>
<td>Appliance title. For example, &quot;LX 2010 (Management Station)&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>applianceType</td>
<td>Appliance type. For example, &quot;LX&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>applianceVersion</td>
<td>Appliance version. For example, &quot;5.0.0&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>buildNumber</td>
<td>Build number. For example, &quot;201008071649\n&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>lspVersion</td>
<td>LSP version. For example, &quot;17.1.201003171111&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>lspVersionShort</td>
<td>LSP version short string. For example, &quot;17.1&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>logLineDelimiter</td>
<td>Logline delimiter. For example, &quot;\r\n&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>runningMode</td>
<td>Values are one of: &quot;ms&quot;, &quot;non-ms&quot;, &quot;strict-non-ms&quot;.</td>
<td>String</td>
</tr>
<tr>
<td>underRemoteControl</td>
<td>Indicate the appliance is under remote control or not.</td>
<td>Boolean</td>
</tr>
<tr>
<td>applianceTimeZoneId</td>
<td>Time zone ID. For example, “UTC”.</td>
<td>String</td>
</tr>
<tr>
<td>currentApplianceTimeEpoch</td>
<td>Current appliance time Epoch. For example, 1282241419646.</td>
<td>Number</td>
</tr>
<tr>
<td>applianceTimeZoneOffsetSeconds</td>
<td>Appliance timezone offset in seconds.</td>
<td>Number</td>
</tr>
<tr>
<td>errorCause</td>
<td>Error cause code of the error.</td>
<td>Number</td>
</tr>
<tr>
<td>errorCode</td>
<td>Error code for the request number.</td>
<td>Number</td>
</tr>
</tbody>
</table>
Report and Search Service

The Report and Search Service provides programmatic access to the Reporting and Index Search functionality on the TIBCO LogLogic Appliance.

Overview

The Report and Search Service API provides these operations:

- Using getReport, your program run a:
  - Real-Time report query
  - Pre-defined Custom Report query
  - Index Search query
- With getTemplateReportList, you can list all Real-Time report templates on the Appliance.
- With getCustomReportList, you can list all Custom Reports defined on the Appliance.
- With getDetailReportMetaInfo, you can retrieve the type information for columns in a report on the Appliance via the given detail report token.

Status Codes

The Status Codes are:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No error</td>
</tr>
<tr>
<td>1</td>
<td>No data available for the query parameters provided</td>
</tr>
<tr>
<td>2</td>
<td>Invalid time range</td>
</tr>
<tr>
<td>3</td>
<td>Invalid report name</td>
</tr>
<tr>
<td>4</td>
<td>Unknown device</td>
</tr>
<tr>
<td>5</td>
<td>Insufficient Privilege for requested operation</td>
</tr>
<tr>
<td>6</td>
<td>Invalid device for report</td>
</tr>
<tr>
<td>7</td>
<td>Invalid input</td>
</tr>
<tr>
<td>8</td>
<td>Persistence exception</td>
</tr>
<tr>
<td>9</td>
<td>Invalid token reference for detail report operation</td>
</tr>
</tbody>
</table>

Get Report Operation

The getReport operation returns a result set containing the records from a Real-Time report query, custom report query, Index Search, or Index Report.

Get Report Request Parameters

The getReport operation common request parameters are:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>Yes</td>
<td>String</td>
</tr>
<tr>
<td>applianceIp</td>
<td>The Appliance from which you retrieve the report.</td>
<td>IP address of a managed Appliance or All for retrieving an aggregated report from all managed Appliances. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>No</td>
<td>String</td>
</tr>
<tr>
<td>reportType</td>
<td>Type of report.</td>
<td>Possible values:</td>
<td>Yes</td>
<td>String</td>
</tr>
<tr>
<td>reportName</td>
<td>Name of the report template or custom report.</td>
<td>For index search:</td>
<td>Yes</td>
<td>String</td>
</tr>
</tbody>
</table>

The **Get Template Report List Operation** and **Get Custom Report List Operation** operations can be used to retrieve the available template report and custom report names, respectively.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceDeviceName</td>
<td>The name of the device, device group, or IP address to use in the report query.</td>
<td>Possible values: “ALL”, “ALL Cisco PIX”, or “10.1.1.80” The default is “All” for all devices; except, for custom reports, the default is the device list stored in the custom report.</td>
<td>Yes, except for custom reports</td>
<td>String</td>
</tr>
<tr>
<td>timeRange</td>
<td>A Pre-defined time range specification, or an indication to use the time range specified by the fromTime and toTime parameters. If SpecificTime is specified, values for fromTime and toTime must be specified. Note: If you are not using the logapp wsclient.jar, you must specify the Pre-defined and SpecificTime. You cannot specify NULL value. However, you can specify the current time.</td>
<td>Possible values: Pre-defined — Last 1 Hour, Last 2 Hours, Last “n” Hours, Yesterday, Today Specific time—SpecificTime The default is “Last 1 Hour”</td>
<td>No</td>
<td>Date</td>
</tr>
<tr>
<td>fromTime</td>
<td>Start time for the time range of the report query. This parameter is required only if the value for timeRange is a SpecificTime.</td>
<td>See Date/Time Formats for getReport</td>
<td>No</td>
<td>Date</td>
</tr>
<tr>
<td>toTime</td>
<td>End time for the time range of the report query. This parameter is required only if the value for timeRange is a SpecificTime.</td>
<td>See Date/Time Formats for getReport</td>
<td>No</td>
<td>Date</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Values</td>
<td>Required</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td>filters</td>
<td>List of expressions applied to the query to receive records passing the filter criteria. For example, for the activeConnections report template, the filter “/direction=/INBOUND/” retrieves only inbound connection records. This is similar functionality as using a “where” clause in SQL. See the Advanced Options section for the report you specified using the reportName parameter. For examples of using filters for Index Search or Index Report, see Specifying Filters for Index Searches. For examples of using filters for Detail Report, see Specifying Filters for Detail Report.</td>
<td>Values must use the format: Column/Operator/Value</td>
<td>No</td>
<td>Array of String</td>
</tr>
<tr>
<td>startRow</td>
<td>Report query result row to use as the first row of the report result set. Use the startRow and numberOfRowsToRetrieve to retrieve a specific range of records. The first row of the query result is zero (0).</td>
<td>A numeric value.</td>
<td>Yes</td>
<td>Number</td>
</tr>
<tr>
<td>numberOfRowsToRetrieve</td>
<td>Maximum number of rows to return in the report result set. Use the startRow and numberOfRowsToRetrieve a specific range of records.</td>
<td>A numeric value.</td>
<td>Yes</td>
<td>Number</td>
</tr>
<tr>
<td>sortColumn</td>
<td>Column in the generated report to sort on, and the direction of the sort (up or down).</td>
<td>Values must use the format: column-name/direction where direction is up or down</td>
<td>No</td>
<td>String</td>
</tr>
</tbody>
</table>
Specifying Filters for Index Searches

The following are examples of how to use the getReport filters parameter to specify search filters for Index Search or Index Report queries.

**Index Search**

There are two ways to specify search filters with Index Search:

- **Specify a pre-defined search filter that contains a Boolean search expression:**
  
  `/predefined=/Boolean-search-filter-name/`

- **Specify a Boolean expression:**
  
  `/fullTextSrchCriteria=/Boolean-search-expression/`

  For example, in the user interface for Index Search, you might specify “admin AND login” for the search terms. To specify the query using the Web Services API, add a filter with the string:

  `/fullTextSrchCriteria=/admin AND login/`

  The Boolean expression is case-insensitive.

**Index Report**

Using Index Report you can specify multiple pre-defined Boolean search filters:

`/filter_selection=/search-filter_name1, search-filter_name2, ../`

**Specifying Filters for Detail Report**

When the target report is a summary report, an extra column, LLDetailTokenRef will be returned in the response. You can use this value to retrieve the detail report of a specified row that you want to drilldown. To do so, set the report type to 4 and provide the detail token in the filters parameter. The values in reportName and sourceDeviceName parameters are ignored in this report type. The following are examples of how to use the getReport filters parameter to specify filter for Detail Report queries:

`/LLDetailTokenRef=/Token value from previous getReport operation/`

**Date/Time Formats for getReport**

These formats must be used when specifying fromTime and toTime to designate a specific timeRange for the getReport query.

**Year:**

`YYYY`

Example: 2009

**Year and month:**

`YYYY-MM`

Example: 2009-03

**Complete date:**

`YYYY-MM-DD`

Example: 2009-03-16

**Complete date plus hours and minutes:**

`YYYY-MM-DDThh:mmTZD`

Example: 2009-03-16T19:20+01:00
Complete date plus hours, minutes, and seconds:
YYYY-MM-DDThh:mm:ssTZD
Example: 2009-03-16T19:20:30+01:00

Complete date plus hours, minutes, seconds, and a decimal fraction of a second:
YYYY-MM-DDThh:mm:ss.sTZD
Example: 2009-03-16T19:20:30.45+01:00

where:
- **YYYY** = four-digit year
- **MM** = two-digit month (01=January, etc.)
- **DD** = two-digit day of month (01 through 31)
- **T** = literal delimiter in the string, indicating the beginning of the time element
- **hh** = two digits of hour (00 through 23; am/pm are not allowed)
- **mm** = two digits of minute (00 through 59)
- **ss** = two digits of second (00 through 59)
- **s** = one or more digits representing a decimal fraction of a second
- **TZD** = time zone designator (Z or +hh:mm or -hh:mm)

### Get Report Response Attributes

The `getReport` operation returns a tabular set of rows and columns similar to the UI-based report result. When the target report is a summary report, an extra column LLDetailTokenRef is added to columnNames and extra detail tokens are added to each record in records accordingly.

The attributes of a LogLogicReport are:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorCode</td>
<td>Error code for the query failure.</td>
<td>Number</td>
</tr>
<tr>
<td>reportName</td>
<td>Name of the report.</td>
<td>String</td>
</tr>
<tr>
<td>startTime</td>
<td>Start time for the report query.</td>
<td>Date</td>
</tr>
<tr>
<td>endTime</td>
<td>End time for the report query.</td>
<td>Date</td>
</tr>
<tr>
<td>number ofColumnsPerRow</td>
<td>Number of columns in each row in the result set.</td>
<td>Number</td>
</tr>
<tr>
<td>columnNames</td>
<td>A structure containing:</td>
<td>complexType</td>
</tr>
<tr>
<td></td>
<td>columnCount—The number of columns in the report.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>columns—An array of Strings containing the name of each column in the result set.</td>
<td></td>
</tr>
</tbody>
</table>
Get Template Report List Operation

The getTemplateReportList operation returns a list of the templates reports configured in the Appliance, identical to the Real-Time Reports in the Appliance navigation menu.

Get Template Report List Request Parameter

The getTemplateReportList operation request parameter are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>Yes</td>
<td>String</td>
</tr>
</tbody>
</table>

Get Template Report List Response Attributes

The getTemplateReportList response attributes are:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorCode</td>
<td>Error code for the request number.</td>
<td>Number</td>
</tr>
<tr>
<td>recordCount</td>
<td>Number of custom report names.</td>
<td>Number</td>
</tr>
<tr>
<td>reportList</td>
<td>An array of reportTitle (string) and reportType (string). The reportType value can be used in the getReport operation's reportName parameter.</td>
<td>Array</td>
</tr>
</tbody>
</table>

Get Custom Report List Operation

The getCustomReportList operation returns a list of the custom reports configured in the Appliance.

Get Custom Report List Request Parameter

The getCustomReportList operation request parameter are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>Yes</td>
<td>String</td>
</tr>
</tbody>
</table>
### Get Custom Report List Response Attributes

The getCustomReportList response attributes are:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorCode</td>
<td>Error code for the request number.</td>
<td>Number</td>
</tr>
<tr>
<td>recordCount</td>
<td>Number of custom report names.</td>
<td>Number</td>
</tr>
<tr>
<td>reportList</td>
<td>An array of reportTitle (string) and reportType (string). The custom report's reportTitle value can be used in the getReport operation's reportName parameter.</td>
<td>Array</td>
</tr>
</tbody>
</table>

### Get Report Meta Info Operation

The getReportMetaInfo operation retrieves the report column metadata for use together with the results of a getReport call using the same parameters. When the target report is a summary report, an extra column LLDetailTokenRef is added to columnInfo to indicate that it is a summary report.

Only displayed columns in a custom report will be returned, not all columns.

### Get Report Meta Info Request Parameter

The getReportMetaInfo operation request parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>Yes</td>
<td>String</td>
</tr>
<tr>
<td>applianceIP</td>
<td>The Appliance from which you retrieve the metadata.</td>
<td>IP address of a managed Appliance or All for retrieving an aggregated report from all managed Appliances. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>Yes</td>
<td>String</td>
</tr>
</tbody>
</table>
| reportType    | Type or report to run.                                                      | 1 = Real Time report  
2 = Summary report  
3 = Custom report | Yes      | Number   |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>reportName</td>
<td>Name of the report to run.</td>
<td>Name of a report on the specified Appliance(s) that the user in authToken can access.</td>
<td>Yes</td>
<td>String</td>
</tr>
<tr>
<td>sourceDeviceName</td>
<td>Name of the log source to include in the report.</td>
<td>One of: Log source name, Log source IP address, Device Group name, An “All xxxx” devices name</td>
<td>Yes</td>
<td>String</td>
</tr>
</tbody>
</table>

**Get Report Meta Info Response Attributes**

The getReportMetaInfo response attributes are:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorCode</td>
<td>Error code for the request number.</td>
<td>Number</td>
</tr>
<tr>
<td>errorCause</td>
<td>Error cause code of the error.</td>
<td>Number</td>
</tr>
<tr>
<td>columnCount</td>
<td>Number of columns returned in the report.</td>
<td>Number</td>
</tr>
<tr>
<td>columnInfo</td>
<td>An array of reportColumnInfo (complex type). reportColumnInfo is a structure containing displayName (string), shortDisplayName (string), internalName (string), columnType (string)</td>
<td>Array</td>
</tr>
</tbody>
</table>

**Get Detail Report Meta Info Operation**

The getDetailReportMetaInfo command performs the same functionality as getReportMetaInfo. However, instead of ReportType/LogSource, it takes an LLDetailTokenRef string as input to retrieve the report column metadata.

Only displayed columns in a custom report will be returned, not all columns.

**Get Detail Report Meta Info Request Parameter**

The getDetailReportMetaInfo operation request parameters are:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>authToken</td>
<td>Unique authentication token.</td>
<td></td>
<td>Yes</td>
<td>String</td>
</tr>
<tr>
<td>applianceIP</td>
<td>The Appliance from which you retrieve the metadata.</td>
<td>IP address of a managed Appliance or All for retrieving an aggregated report from all managed Appliances. To specify an IP address, use the standard IP address format. For example: 10.1.2.3</td>
<td>Yes</td>
<td>String</td>
</tr>
<tr>
<td>LLDetailTokenRef</td>
<td>The detail report token reference.</td>
<td>The detail token string received in previous getReport operation.</td>
<td>Yes</td>
<td>String</td>
</tr>
</tbody>
</table>

**Get Detail Report Meta Info Response Attributes**

The getDetailReportMetaInfo response attributes are:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>errorCode</td>
<td>Error code for the request number.</td>
<td>Number</td>
</tr>
<tr>
<td>errorCause</td>
<td>Error cause code of the error.</td>
<td>Number</td>
</tr>
<tr>
<td>columnCount</td>
<td>Number of columns returned in the report.</td>
<td>Number</td>
</tr>
<tr>
<td>columnInfo</td>
<td>An array of reportColumnInfo (complex type). reportColumnInfo is a structure containing: displayName (string) shortDisplayName (string) internalName (string) columnType (string)</td>
<td>Array</td>
</tr>
</tbody>
</table>
Authentication Service API

The Authentication Service gives the client program the ability to log in to the Appliance. TIBCO LogLogic® Web Services methods require an authentication token to validate that the client program has access to the Appliance. Instead of using a username and password (or basic authentication) with every Web Service call, the TIBCO LogLogic® Web Services infrastructure implements a “token” based authentication scheme. Token-based authentication schemes help prevent passwords from being exposed. Only the “token” needs to be included in code, or cached in memory by the client side application. Additionally, the authentication “token” is not applicable, or usable, by the Appliance’s user interface.

GetAuthenticationToken Operation

With GetAuthenticationToken you can Web Services program authenticate and retrieve an authentication token from the Appliance.

Request Parameters

The GetAuthenticationToken request parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
<th>Required</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>A valid user account on the Appliance with “Web Service Access” enabled.</td>
<td>No</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td>The password for the user account specified by username.</td>
<td>No</td>
<td>String</td>
<td></td>
</tr>
</tbody>
</table>

Response

The attributes of a GetAuthenticationToken response is:

errorCode—An AuthenticationResult containing the authentication token string; an error code is included in the case of authentication failure. The response is number.

Status Codes

The Status Codes are:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No error</td>
</tr>
<tr>
<td>1</td>
<td>Invalid username and/or password</td>
</tr>
<tr>
<td>2</td>
<td>Invalid authorization token</td>
</tr>
</tbody>
</table>
Alert Types

The alert types are:

**Adaptive Baseline Alert**
Use the Adaptive Baseline Alert to notify you if message rates fall above or below your average baseline range for the specified day and time of the week.

**Cisco PIX/ASA Messages Alert**
The Cisco PIX Messages alert allows for triggering on PIX message criticality, code, and message rate. Since this alert is specific to Cisco PIX messages, the alert device selection is limited to Cisco PIX devices.

**Message Volume Alert**
The Message Volume-Based alert allows alerting when message volume falls below, or is above, preset messages-per-second thresholds. This alert applies to all devices.

**Network Policy Alert**

Network Policy Alert Rules (Rules Tab) are required for this alert to trigger.

**Search Filter Alert**
The Pre-Defined Search Filter Alert allows for alert notification when a text search match occurs within the received log message. This alert leverages the Log Appliance search filters for the text search match definitions. To define the text match for the alert, use Search Filters on the navigation tree.

**Ratio Based Alert**
The Ratio Based Alert triggers when the percentage of a specified message type exceeds or falls below specified percentages.

For example, the Denied/(Accept+Denied) Alert Ratio can be used to trigger an alert when the number of Denied messages exceeds 90% of the Accept and Denied message count.

**System Alert**
The System Alert allows for notification when system health and status criteria exceed acceptable bounds.

**VPN Connection Alert**
The VPN Connection Alert triggers when a VPN connection is denied access and/or disconnected. The VPN Connection alert is only applicable to Cisco VPN, Radius, and Nortel Contivity devices.

**VPN Message Alert**
The VPN Message Alert triggers on combinations of specific VPN message area, severity, and code. This alert is applicable to Cisco VPN devices.

**VPN Statistics Alert**
The VPN Statistics Alert triggers when recorded statistics on VPN or Radius messages match relative or absolute criteria.
For example, you can configure an alert to trigger when the Number of Bytes Received per day for a specific user exceeds 1Mb per day, which is an absolute value. The alert rule can also be configured as a relative rule, such as “grows by 10%.”

**Message Areas**

The following is a complete list of available message areas that you can define in the `messageArea` parameter for the VPN Messages Alert. You can also view the list in the TIBCO LogLogic Appliance user interface.

ANY, AUTH, AUTHBDG, AUTHDECODE, AUTOUPDATE, BKPLN, BMGT, BMGTDBG, BUFFER, CAPI, CERT, CIFS, CIFSDBG, CLIENT, CONFIG, DHCP, DHCPDBG, DHCPDECODE, DIAG, DM, DNS, DNSDBG, DNSDECODE, EMAILPROXY, EVENT, EVENTDBG, EVENTMIB, EXPANSIONCARD, FILTER, FILTERDBG, FIPS, FIPSDIAG, FSM, FTPD, FW, FWDBG GWDECODE, GENERAL, GRE, GREDBG, GREDECODE, H323, H323DBG, HARDWAREMON, HDLC, HTTP, HWDIAG, IKE, IKEDBG, IP, IPDBG, IPDECODE, IPSEC, IPSECDBG, IPSECDECODE, L2TP, L2TPDBG, LBSSF, MIB2TRAP, NETBIOS, OSPF, PPP, PPPDBG, PPPDECODE, PPPOE, PPPOEDBG, PPPOEDECODE, PPTP, PPTPDBG, PPTPDECODE, FSH, PSOS, QUEUE, RADIUSACCT, REBOOT, RM, SMTP, SNMP, SSH, SSL, SYSTEM, T1E1, TCP TELNET, TELNETDBG, TELNETDECODE, TIME, VRRP, WAN, WEBVPN

**User Administration Privileges**

The following table lists the User Type (User Admin, Report Admin, and Config Admin) and the associated privileges. You can specify either the `UserType` or the associated privileges, or both.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Privileges Granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>All privileges</td>
</tr>
<tr>
<td>User Admin</td>
<td>Manage Users</td>
</tr>
<tr>
<td></td>
<td>• Manage Administrators</td>
</tr>
<tr>
<td></td>
<td>• Replicate Users</td>
</tr>
<tr>
<td>Report Admin</td>
<td>Access Custom Reports</td>
</tr>
<tr>
<td></td>
<td>• Real-Time Reports</td>
</tr>
<tr>
<td></td>
<td>• Add/Modify/Delete Custom Reports</td>
</tr>
<tr>
<td></td>
<td>• Search Archived Data</td>
</tr>
<tr>
<td></td>
<td>• Run/Schedule Custom Reports</td>
</tr>
<tr>
<td></td>
<td>• Real-Time Viewer</td>
</tr>
<tr>
<td>User Type</td>
<td>Privileges Granted</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Config Admin</td>
<td>Manage Devices</td>
</tr>
<tr>
<td></td>
<td>• Port Configuration</td>
</tr>
<tr>
<td></td>
<td>• Message Routing Configuration</td>
</tr>
<tr>
<td></td>
<td>• Manage Alerts</td>
</tr>
<tr>
<td></td>
<td>• Manage Check Point Devices</td>
</tr>
<tr>
<td></td>
<td>• Manage PIX/ASA Codes</td>
</tr>
<tr>
<td></td>
<td>• System Configuration</td>
</tr>
<tr>
<td></td>
<td>• Firewall Settings</td>
</tr>
<tr>
<td></td>
<td>• Backup/Archive Configuration</td>
</tr>
<tr>
<td></td>
<td>• Access Management station</td>
</tr>
<tr>
<td></td>
<td>• Manage File Transfer Rules</td>
</tr>
<tr>
<td></td>
<td>• Import/Export</td>
</tr>
<tr>
<td></td>
<td>• Manage Suites</td>
</tr>
<tr>
<td></td>
<td>• Manage SSL Certificate</td>
</tr>
<tr>
<td></td>
<td>• Manage Device Types</td>
</tr>
<tr>
<td></td>
<td>• Manage Tag Catalog/Column Manager</td>
</tr>
<tr>
<td></td>
<td>• Manage Message Signatures</td>
</tr>
</tbody>
</table>