



# **TIBCO Hawk®**

## Plug-in For TIBCO Administrator

Version 6.3.1 | November 2024

# Contents

---

<b>Contents</b>	<b>2</b>
<b>Introduction</b>	<b>4</b>
Overview	4
Deploying Hawk Plug-ins in TIBCO Administrator	5
Hawk Configuration	6
<b>All Alerts Console</b>	<b>8</b>
Overview	8
Security Considerations	8
All Alerts Console	9
Alerts	9
Alert Details	11
<b>Hawk Console</b>	<b>14</b>
Overview	14
Agents	15
Microagents	15
Performing Network Operations and Actions	16
Accessing TIBCO Hawk Microagent Methods	17
Agent Tab	17
Hawk Microagent Methods	18
Invoking Microagent Methods	18
Rulebases	19
<b>Monitoring Console</b>	<b>21</b>
Overview	21
Using the Monitoring Archive Utility	22
Monitoring Console	29

Creating a Monitoring Application .....	30
Deploying a Monitoring Configuration .....	31
Updating a Monitoring Application .....	35
Deleting a Monitoring Application .....	35
Using the Configure Monitoring Utility .....	36
<b>TIBCO Documentation and Support Services .....</b>	<b>40</b>
<b>Legal and Third-Party Notices .....</b>	<b>42</b>

# Introduction

---

This chapter describes the plug-ins installed by TIBCO Hawk. These plug-ins are accessed using TIBCO Administrator.

- [Overview](#)
- [Hawk Configuration](#)

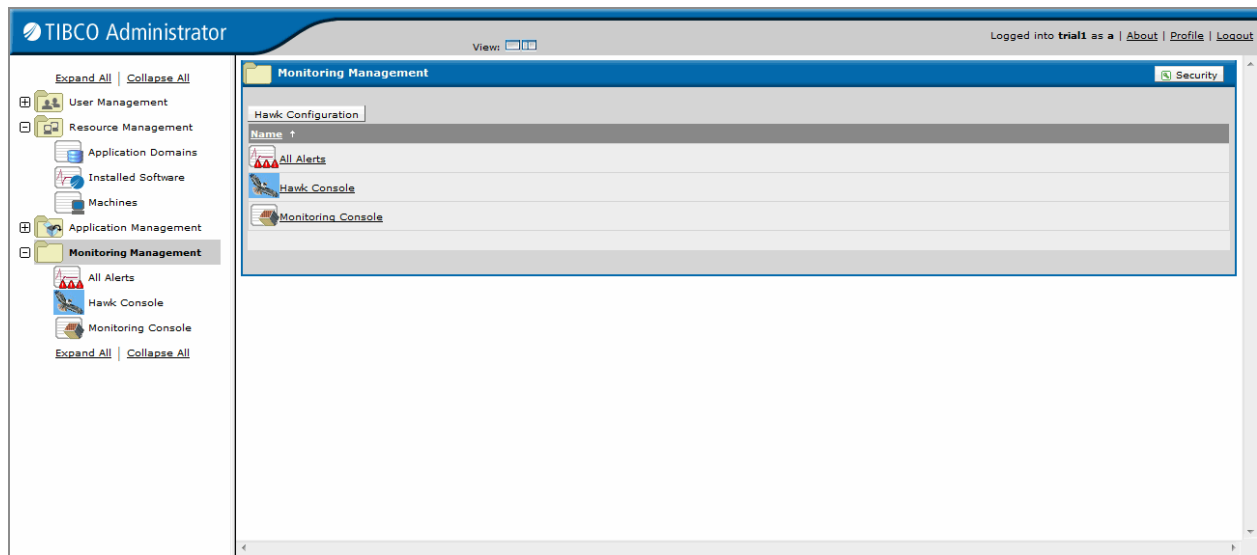
## Overview

The TIBCO Hawk installation process installs the following plug-ins:

- All Alerts  
This plug-in provides visibility for all the alerts generated in your TIBCO Administrator domain as well as any additional domains that you are monitoring.
- Hawk Console  
This plug-in provides access to the machines in your TIBCO Administrator domain as well as any additional domains that you are monitoring.
- Monitoring Console  
This plug-in provides a mechanism for you to import and configure applications to monitor other TIBCO applications in your TIBCO Administrator domain as well as any additional domains that you are monitoring

These plug-ins are contained in the Monitoring Management Folder and are accessed via TIBCO Administrator.

The following figure shows the Monitoring Management folder which in turns contains the plug-ins mentioned above.



## Deploying Hawk Plug-ins in TIBCO Administrator

TIBCO Hawk Admin Plugins for TIBCO Administrator are not available as built-in components with the TIBCO Runtime Agent/Administrator installation. To get the TIBCO Hawk Admin Plugins for TIBCO Administrator, install a licensed copy of TIBCO Hawk independently. This copy of Hawk could be installed either in the same *TIBCO\_HOME* or its own *TIBCO\_HOME*.

After the complete installation of the standalone Hawk, the Hawk Admin plug-in web applications are available at the *HAWK\_HOME/adminplugins* folder.

Now, deploy the Hawk Admin plug-ins in TIBCO Administrator using either of the following methods:

- Copy all available web application archives from the *HAWK\_HOME/admin-plugins* folder to the *ADMINISTRATOR\_HOME/administratorplugins* folder. These plug-ins are then deployed automatically on next restart of TIBCO Administrator.
- Restart the TIBCO Administrator. In the TIBCO Administrator, navigate to **Application Management > All Service Instances > View Service Instance: TIBCO Administrator > Plug-Ins**, and click **Add** to add the plug-ins manually.

# Hawk Configuration

By default, all machines that belong to your TIBCO Administrator domain are monitored by the installed plug-ins. If you wish to monitor additional domains, they have to be explicitly configured.

To configure additional domains:

1. Select **Monitoring Management** folder from the left-hand pane of TIBCO Administrator.
2. Click **Hawk Configuration**.
3. Specify the parameters for the domain. See [Adding Hawk Domains](#) for more information.

## Adding Hawk Domains

Click **Add** to configure a Hawk domain and specify the following parameters:

- Hawk Domain Transport — Network transport used by the TIBCO Hawk domain. Possible choices are RV Transport or EMS Transport.

If you choose RV Transport, values for the following fields should be specified:

- Hawk Domain Name — The name of the TIBCO Hawk domain.
- RV Service, RV Network, and RV Daemon — These attributes together configure the TIBCO Rendezvous parameters for communicating with TIBCO Hawk agent.
- Hawk Security Impl (Optional) — The name of the class implementing the security policy.

If you choose EMS Transport, values for the following fields should be specified:

- EMS Server URL — The location of the EMS server.
- EMS User and EMS Password — The login credentials to access the EMS server. Click **change . .** to change the password.
- Hawk Security Impl (Optional) — The name of the class implementing the security policy.
- Use SSL — Select this checkbox if using SSL to connect to the EMS server. If this checkbox is selected, the **Configure SSL** button is displayed. Click the **Configure SSL** button to configure the SSL parameters.

The following SSL parameters should be specified:

- Vendor — The name of the SSL implementation.
- Ciphers — When specifying this option to specify the cipher suites that can be used, use the ^ qualifier instead of a - qualifier. For more information on specifying cipher suites, refer to the *TIBCO Enterprise Message Service* documentation.

## Settings for Hawk components to verify EMS server

- Authenticate EMS server — Select this checkbox if the Hawk components should verify the EMS server.
- Server Name — The name of the EMS server.
- Trusted — The option specifies the file name of the server certificates.

## Settings for EMS server to verify Hawk components

- Identity — The digital certificate of the TIBCO Hawk components.
- Private Key — The private key of the TIBCO Hawk component.
- Password — The password to decrypt the identity file of the Hawk component.  
Click **change...** to change the password.



### Note

If using EMS transport, make sure you specify `<EMS_HOME>/client/java` in the classpath of the TIBCO Administrator `.tra` file for the corresponding TIBCO Administrator domain.

---

## Deleting Hawk Domain

If you no longer wish to monitor a Hawk domain, select it from the list of Hawk Domain names and click **Delete**.

If using TIBCO Enterprise Management Advisor to monitor additional Hawk domains (along with the TIBCO Administrator domain), make sure you remove those domains from the TIBCO Enterprise Management Advisor configuration and re-deploy your TIBCO Enterprise Management Advisor applications before deleting those Hawk domains.

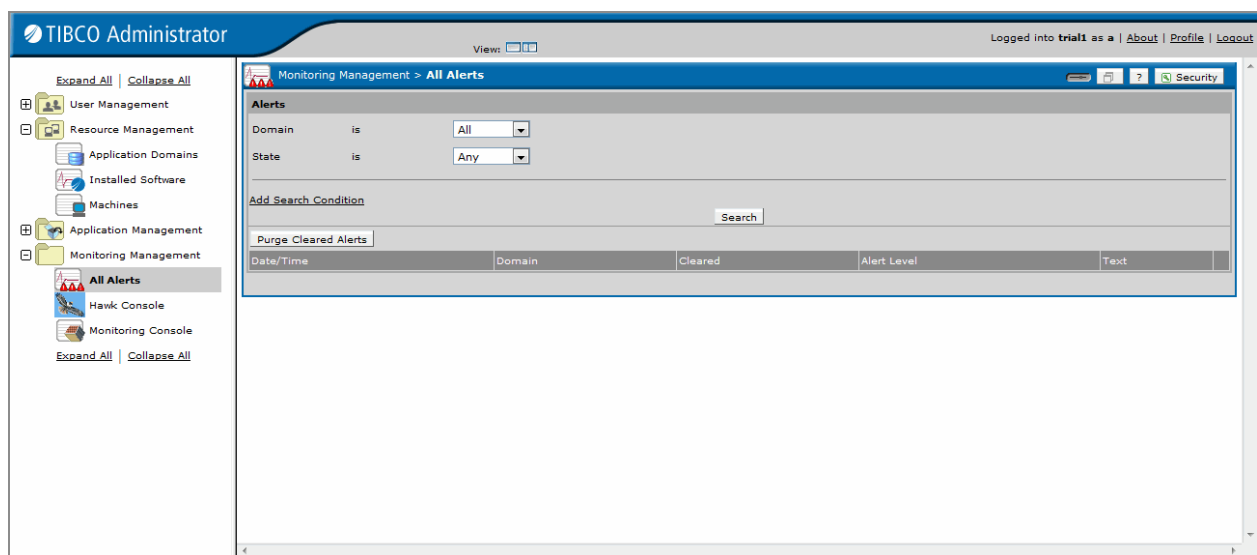
# All Alerts Console

This chapter describes the All Alerts plug-in.

- [Overview](#)
- [All Alerts Console](#)

## Overview

The All Alerts plug-in provides functionality which lets you view all TIBCO Hawk alerts generated in your TIBCO Administrator domain as well as any additional domains that you are monitoring.



## Security Considerations

Security access determines whether a user can perform an operation on a machine in your domain. TIBCO Administrator users that have Administer access can access all the functionality provided by the Hawk plug-ins.



It is strongly recommended that only administrators have access to the All Alerts console.

Users with read access can view alerts on the All Alerts console, only those users that have write access can suspend alerts.

## Security between TIBCO Administrator and TIBCO Hawk

Security is enabled between TIBCO Administrator and TIBCO Hawk by specifying a Java class that implements your security policy. This security policy is specified by the `-security_policy` option in the `hawkagent.cfg` configuration file. This configuration file is located in `CONFIG_FOLDER\hawk\bin` or domain-specific folder, when generated by TIBCO Administrator. For more information on TIBCO Hawk security see the *TIBCO Hawk Installation and Configuration Guide*.

When invoking or subscribing to TIBCO Hawk microagent methods, the security that is enforced is based on the user that started the TIBCO Administrator server and not the user accessing TIBCO Hawk microagent methods.

## All Alerts Console

You can view all TIBCO Hawk alerts generated in your domain from this console. Here you can specify search conditions to filter the alerts that are displayed. This console is accessed by clicking **Monitoring Management>All Alerts** from the left-hand pane of TIBCO Administrator.



### Note

It is strongly recommended that only administrators have access to the All Alerts console.

---

## Alerts

This console contains the following fields:

**Domain** — Choose the Hawk domain from the drop-down list which contains the TIBCO Administrator domain and any additional Hawk domains that you have configured. If you wish to view alerts from all domain, choose All.

**State** — Choose between Any, Active, Cleared, or Custom.

**Add Search Condition** — The following options are available:

- **Date/Time** — Specify the date and time before or after which you want to filter the alerts.
- **Level** — Lowest level of the alert. Possible choices are High, Medium, Low, Notification or Custom.

This level indicates the lowest alert level that you want to search for.

For example, if you choose medium, both medium and high alerts will be displayed and if you choose low, all alerts will be displayed.

- **Agent** — Name of the agent.
- **Rulebase** — Name of the rulebase that generated the alert.
- **Deployment** — Name of the deployment.
- **Component Instance** — Name of the component.

When more than one selection condition can be specified, one of the following options must also be chosen:

- Show entries where ALL conditions are true
- Show entries where ANY conditions are true

**Remove** — Click this button to remove the corresponding search condition.

**Search** — Click this button to apply the chosen search conditions to the list of generated alerts.

**Purge Cleared Alerts** — Used to purge alerts that have been cleared.



**Note**

Alerts that are cleared will stay in the list for 30 minutes if user does not click the purge alert button.

---

## List of Alerts

For each alert, the following information is displayed:

Date/ Time — Date and Time of the alert.

Domain — The domain where this alert originated.

Cleared — Whether this alert has been cleared. If the alert is cleared a x is displayed in this column.

Alert Level — Level of the alert represented by the alert icons. See [Alert Icons](#) for a description of the alert icons.

Text — Text belonging to the alert.

details — Click on this field to view details about the generated alert.

## Alert Details

This dialog lists details of the chosen alert.

### Details

Date/ Time — Date and Time of the alert.

Alert Level — Level of the alert represented by the alert icons. [Alert Icons](#) for a description of the alert icons.

Text — Text belonging to the alert.

### Properties

Domain — The domain where this alert originated.

Agent — The TIBCO Hawk Agent which generated this alert.

DNS — The DNS of the agent.

IP Address — The IP address of the agent.

Rulebase — The TIBCO Hawk rulebase which generated this alert.

DataIndex — If the alert was generated from a rule with composite data sources, this value is '\_'. If the alert was generated from a rule with a tabular data source, this value is \_  
<indexField>:<indexValue>. Where <indexField> and <indexValue> refer to values in the tabular data source.

Action — The number corresponding to its position in the action list for the test as defined in the rulebase.

Rule — The rule which uses the specified datasource to test for certain conditions.

DataSource — The datasource for the rulebase.

Test — The test performed on the datasource.

The following properties are displayed if a rulebase is configured for a service instance through TIBCO Administrator.

Action.Deployment — The deployment name of the service instance.

Action.ComponentInstance — The name of the service instance.

Action.ComponentInstanceID — The ID of the service instance.

## Suspend

Reason — The reason for suspending the alert.

Suspend Interval — The duration in seconds for which the alert should be suspended.

Suspend — Click this button to suspend the alert.

For more information on suspending alerts, refer to *TIBCO Hawk Concepts* guide.



### Note

Users with read access can view alerts on the **All Alerts** console, only those users that have write access can suspend alerts.

---






## Alert Icons

The alert icons represent the level of the alert generated by the TIBCO Hawk agent. Alert icons are yellow, amber, or red representing low, medium, or high alerts respectively. The following table describes each alert icon.

### Alert Icons

Icon	Description
	There are no alerts generated.

---

Icon	Description
	
	Low alert.
	
	Medium alert.
	
	High alert.
	
	Unable to communicate with the TIBCO Hawk Agent.

# Hawk Console

---

This chapter describes the Hawk Console.

- [Overview](#)
- [Agents](#)
- [Microagents](#)
- [Rulebases](#)

## Overview

The Hawk Console is used for viewing and managing the Hawk agents within the configured Hawk domains. Using the Hawk Console you can view each agents' microagents and the associated methods. You can also invoke the microagents methods and examine the results.

The Hawk Console adds a tab to the **View Machine** dialog for each machine in your domain. For more information on Hawk microagent methods, see *TIBCO Hawk Microagent Reference*.

The Hawk Console can also be used for viewing the rulebases that are loaded by each agent in the domain.

## Security Considerations

Security access determines whether a user can perform an operation on a managed object in your domain.

It is strongly recommended that only administrators have access to the Hawk Console.

When accessing TIBCO Hawk methods using the **Machines** console, if a user has read access to the **Machines** console, only methods of type IMPACT\_INFO are listed. If the users have read-write access to the **Machines** console, all TIBCO Hawk methods for the microagent are listed. When a method is listed, the user can invoke or subscribe to that method.

## Agents

This tab lists all machines that belong to the chosen domain.

The following information is available for each machine:

- **Agent**  
The name of the TIBCO Hawk agent. The default name for the TIBCO Hawk agent is the host name of the computer on which it is installed.  
Click the agent name for the list of available microagent methods. See [Hawk Microagent Methods](#) for more information on invoking microagent methods.
- **Cluster**  
The cluster to which the agent belongs.
- **Uptime**  
The number of days and hours this machine has been running.
- **OS/ Version**  
The operating system and version.
- **IP Address**  
The IP address of this machine.
- **Status**  
The status of the machine is indicated by both an alert icon and the corresponding alert level. This alert status corresponds to the highest alert generated by the Hawk agent.  
Clicking the status displays all alerts for that agent.  
See [Alert Icons](#) for the description of the alert icons.

## Microagents

This tab lists all microagents that belong to the domain.

The following information is displayed for each microagent:

- **Microagent**

The name of the microagent.

- Agent

The name of the TIBCO Hawk agent. The default name for the TIBCO Hawk agent is the host name of the computer on which it is installed.

- Cluster

The cluster to which the agent belongs.

- OS/ Version

The operating system and version.

You can sort this list by any listed column.

Click on a microagent name for the list of available microagent methods. See [Hawk Microagent Methods](#) for more information on invoking microagent methods.

## Performing Network Operations and Actions

Network Operations and Actions are used to communicate with multiple Hawk agents at one time.

### Network Operation

Using a network operation you can invoke a microagent method, of type IMPACT\_INFO that returns information but does not perform any action, on multiple Hawk agents at the same time.

1. Select one or more microagent and click the **Network Operation** button. This takes you to the Network Operation pane which lists the available methods.
2. Select a method and provide any necessary input parameters and click **Perform Operation**.

The results are displayed in the **Success** tab and are sorted by the microagent name. The **Timeout** tab lists any agent that did not respond, usually due to a network problem.

### Network Action

Using a network action, you can invoke a microagent method, of type IMPACT\_ACTION or IMPACT\_ACTION\_INFO, that performs an action, on multiple Hawk agents at the same time.



The procedure of invoking a network action is similar to invoking a network operation.

## Accessing TIBCO Hawk Microagent Methods

You can access the microagent methods in the following ways:

- Using the Hawk Console

The Microagents tab lists the microagents belonging to all the agents in the chosen domain. See [Invoking Microagent Methods](#) for more information.

- Using the Agent tab

TIBCO Hawk adds a tab **Agent** to the View Machine dialog for the machines in your domain. The View Machine tab is accessed by clicking **Resource Management> Machines** from the left-hand pane of TIBCO Administrator and then selecting a machine from the displayed list.

See [Security Considerations](#) for the permissions required to access the Agent tab.

## Agent Tab

This dialog lists the available microagents and the rulebases defined for the agent.

### Microagents

Displays the available microagents and for each microagent the following information is displayed:

- Name — Name of the microagent.
- Instance — Number to identify the running instance
- Description — Description of the microagent.

Click on a microagent name for the list of associated microagent methods.

### Rulebases

A list of the loaded rulebases is displayed.

Rulebases — The name of the rulebase. Click on this field to sort the rulebase names.

Click on a rulebase name to view details of the rulebase.

## Hawk Microagent Methods

This dialog lists the available microagent methods.

### Methods

The following fields are displayed for the microagent methods:

- Name — Name of the microagent methods.
- Instance — Instance number of the agent.
- Description — Description of the microagent method.

To invoke a microagent method click on the method name. See [Invoking Microagent Methods](#) for details.

## Invoking Microagent Methods

This dialog displays information about the microagent method and provides fields you can specify input parameters when either invoking or subscribing to the method.

### Method

Displays general information about the microagent method:

- Name — The name of the microagent method.
- Description — Description of the microagent method.
- Type — Type of the microagent method, either Synchronous or Asynchronous.
- Impact — The function performed by the method and can be one of the following types:
  - IMPACT\_INFO returns information.
  - IMPACT\_ACTION performs an action on the TIBCO Hawk system.

- `IMPACT_ACTION_INFO` both returns information and performs an action based on it.
- Time Out — The method invocation timeout value in milliseconds.

## Invocation

Parameters — Displays the following elements for the parameters:

- Name — Name of the input argument.
- Value — Value of the input argument.
- Type — Data type of the argument.

Description — Description of the argument.

Subscribe — Available for methods of type `IMPACT_INFO` and `IMPACT_ACTION_INFO`. You cannot subscribe to methods of type `IMPACT_ACTION`. Information is returned by the method either synchronously or asynchronously.

If the Subscribe checkbox is selected, the following fields are displayed along with the default values:

- Data Interval — The time interval for collection data points. Available when subscribing to synchronous methods.
- History — The number of data points you want to see for the historical data set.

Even though a method may return data asynchronously, the result will not be updated until the page is refreshed.

## Rulebases

This pane lists all the rulebases loaded for the chosen domain.

The following information for each rulebase is displayed:

- Rulebase

The name of the rulebase.

If the rulebase was loaded using a monitoring configuration, the name of the MAR file is the prefix for the rulebase name.

For example, if the rulebase

- Agent

The name of the TIBCO Hawk agent. The default name for the TIBCO Hawk agent is the host name of the computer on which it is installed.

- Cluster

The cluster to which the agent belongs.

- OS/ Version

The operating system and version.

- Status

The status of the machine is indicated by both an alert icon and the corresponding alert level. This alert status corresponds to the highest alert generated by the Hawk agent.

See [Alert Icons](#) for the description of the alert icons.

Click on a rulebase name to view details.

# Monitoring Console

---

This chapter describes the Monitoring Console.

- [Overview](#)
- [Using the Monitoring Archive Utility](#)
- [Monitoring Console](#)
- [Using the Configure Monitoring Utility](#)

## Overview

The Monitoring Console provides functionality to import and configure applications to monitor other TIBCO applications in your TIBCO Administrator domain.

The console uses a Monitoring Archive (MAR) file to create a monitoring application. A MAR file is a collection of one or more monitoring configurations. A monitoring configuration is a TIBCO Hawk rulebase template. The MAR file is created using the command-line Monitoring Archive utility (MAR utility). For details, see [Using the Monitoring Archive Utility](#).

You add a MAR file to your domain using the Monitoring Console to create a monitoring application that can be deployed to any *target* in your domain. Within the context of this console, a target is either a machine or a deployed application (such as TIBCO BusinessWorks or TIBCO Adapters), or a Hawk Repository within your domain.

## Installation Considerations

If you delete the Application Domain for the console using the Resource Management > Application Domains dialog, you would need to re-start TIBCO Administrator.

If you update the console by first removing it and then adding it, log out of TIBCO Administrator and log back in before using the plug-in.

**Note**

If using a TIBCO Administrator domain with a database backend, make sure you set the value for **Maximum Connections** in the **Database Configuration** tab of the **DomainUtility** to be at least 10. Refer to the *TIBCO Runtime Agent DomainUtility User's Guide* for details.

## Security Considerations

Security access determines whether a user can perform an operation on a managed object in your domain.

Users with read-only access will not be able to Add, Deploy (and Undeploy), or Update monitoring configurations.

Users with read-write access to the Monitoring Management folder get access to all contained consoles.

Only users with read-write access can use the ConfigureMonitoring command-line utility.

If your TIBCO Administrator domain or if the Application domain used for the Monitoring Management Console uses a file based repository, then read-write permissions have to be assigned to the Data Access folder.

The Data Access folder is accessed by selecting (using TIBCO Administrator)

**User Management> Security> TIBCO Administrator> Permissions**

Within this folder, assign read-write access to the Sys--<domainName> repository file.

## Using the Monitoring Archive Utility

The monitoring archive, MAR file, contains one or more monitoring configurations. A monitoring configuration is a TIBCO Hawk rulebase template.

The MAR utility converts TIBCO Hawk rulebases into templates so that they can be deployed to any target within any TIBCO Administrator domain. A rulebase template, in a MAR file, has the extension .hrt.

The rulebases can contain two types of rules:

- Application-specific

These rules use the data source of the microagents belonging to TIBCO applications, such as TIBCO BusinessWorks or TIBCO Adapters. Each of these applications have a unique type.

- Agent-specific or non-application specific.

These rules do not use the data source of the microagents belonging to TIBCO applications.

If a rulebase contains multiple application-specific rules, the MAR utility splits a single rulebase into multiple rulebases where each rulebase contains rules with the data source from the same adapter type. The name of the templated rulebase will be suffixed the type of the TIBCO application. For example, if the rulebase `myRulebase.hrb` contains rules using the microagents belonging to TIBCO ActiveMatrix BusinessWorks (of type `bwengine`) and TIBCO Adapter for Active Database (of type `adb`), then the resulting rulebases will be `myRulebase-bwengine.hrt` and `myRulebase-adb.hrt`.

If a rulebase contains only agent-specific rules, the rulebase is not split into separate rulebases and neither is the rulebase name suffixed with any type. If you want the name of such a rulebase to be assigned a specific type, use the `-Xtype` option when creating the monitoring archive file.

If the rulebase contains one or more agent-specific rules and one or more application-specific rules, the rulebases are split into agent-specific and application-specific rulebases. For example, if the rulebase `myMixedRulebases.hrb` contains rules using the Logfile microagent and microagents belonging to TIBCO ActiveMatrix BusinessWorks (of type `bwengine`) and TIBCO Adapter for Active Database (of type `adb`). The resulting rulebases will be `myMixedRulebases.hrt`, `myMixedRulebases-bwengine.hrt`, and `myMixedRulebases-adb.hrt`.

The MAR utility will convert any six part data source to a seven part data source in the input rulebases.

For Example, if the data source in a rulebase is: `COM.TIBCO.ADAPTER.<NAME>.<TIBCO_DEPLOYMENT>.<TIBCO_COMPONENT_INSTANCE>`,

the MAR utility will convert this data source to the following:

`COM.TIBCO.ADAPTER.<NAME>.<TIBCO_DOMAIN>.<TIBCO_DEPLOYMENT>.<TIBCO_COMPONENT_INSTANCE>`.



#### Note

If a rulebase contains a rule that contains an action that invokes a method from a TIBCO application which is different from the TIBCO

---

application used in the data source, the rulebase will not be templated and an error is generated. To allow other rules in the rulebase to be templated, separate the rule that caused the error and run the mar tool again.

Rulebases that use posted conditions will not work as expected if the posted condition is referred by rules with different adapter types in the same rulebase. This is because the referred rulebase will be split into multiple rulebases.

While creating or updating a MAR file (using the MAR utility), an incorrect rulebase type is assigned to the rulebase if the rulebase contains one application-specific and one or more agent-specific rules. This problem occurs only if agent-specific rule is created first in the rulebase and the application-specific rule created later. If this happens, the `Domain`, `Deployment`, `ComponentInstance` values are not substituted. It is recommended that when creating or updating a MAR file, the `-Xtype` option is used to specify the type of the rulebase.

The MAR utility, `mar`, is located in the `CONFIG_FOLDER/hawk/bin` directory. The MAR utility requires TIBCO Runtime Agent 5.5.4 to be installed.

Using the MAR utility you can:

- Create a MAR file

To create a MAR file, use the command

```
mar c[v]f <marfilename> <inputfiles> [-Xoptions]
```

```
mar c[v]df <description> <marfilename> <inputfiles> [-Xoptions]
```

Examples:

```
— mar cvf myMarFile.mar ./
```

This command creates a MAR file `myMarFile.mar` that contains all rulebases in the current directory.

```
— mar cdf "My test MAR file" myMarFile.mar ./
```

This command creates a MAR file `myMarFile.mar` that contains all rulebases in the current directory and includes the provided description.

```
— mar cvf myMarFile.mar bw.hrb agent.hrb -Xtype adb
```



This command creates MAR file `myMarFile.mar` of type `adb` and contains two rulebases `adb.hrb` and `agent.hrb`.

```
— mar cvf myMarFile.mar ./ -Xasis
```

This command creates a MAR file `myMarFile.mar` that contains all rulebases in the current directory but without converting into them into rulebase templates.

- Update a MAR file

To update a MAR file, use the command

```
mar u[v]f <marfilename> <inputfiles> [-Xoptions]
```

```
mar u[v]df <description> <marfilename> <inputfiles> [-Xoptions]
```

Example:

```
— mar uf myMarFile.mar newRB.hrb
```

This command add the rulebase `newRB.hrb` to the existing MAR file, `myMarFile.mar`.

- Extract MAR file

To extract a MAR file, use the command

```
mar x[v]f <marfilename> <inputfiles> [-Xoptions]
```

```
mar x[v]pf <propertiesfile> <marfilename> <inputfiles> [-Xoptions]
```

Example:

```
— mar xf myMarFile.mar testRB.hrb
```

This command extracts the rulebase `testRB.hrb` from the specified MAR file. Any other rulebase contained in the MAR file is not extracted.

```
— mar xpf myprop.properties myMarFile.mar testRB.hrb
```

This command extracts the rulebase `testRB.hrb` from the specified MAR file and substitute the variables in the rulebase using the key-value pair specified in `myprop.properties` file.

Any other rulebase contained in the MAR file is not extracted.

Following are the contents of a sample properties file used for variable substitution:

```
TIBCO_DOMAIN=MyHawkdomain
```

```
TIBCO_DEPLOYMENT=myDeployment
```

```
TIBCO_COMPONENT_INSTANCE=myComponentInstance
```

- List a MAR file

To extract a MAR file, use the command

```
mar t[v]f <marfilename>
```

Example:

```
— mar tf myMarFile.mar
```

This command lists all rulebases contained in the specified file.

The following table describes the input parameters and options for the MAR utility.

#### MAR Utility: Input parameters and Options

Input	Description and Usage
marfilename	The name of the MAR file.
inputfiles	<p>The files or directories, separated by spaces, that are combined into or extracted from the MAR file.</p> <p>All directories are processed at the top level only. Only files with .hrb extension are processed.</p>
description	<p>The description for the MAR file. If specify, the description must be placed within quotes (").</p> <p>If the d option is specified, you have to provide a description. In the command, the options d and f must appear in the same order as the description and MAR file.</p>
propertiesfile	The properties file containing the name-value pairs to be used for substituting variables in the

Input	Description and Usage
	<p>rulebase template when the rulebase is extracted.</p> <p>If the <i>p</i> option is specified, you have to specify the properties file. In the command, the options <i>p</i> and <i>f</i> must appear in the same order as the properties file and MAR file.</p>
c	Creates a new archive file.
u	<p>Updates an existing MAR file by adding to it the files and directories specified by <i>&lt;inputfiles&gt;</i> parameter.</p> <p>If the MAR file does not exist and the command results in adding a file, the MAR file will be created.</p>
x	<p>Extracts files from a MAR file. If input files is specified, only those files are extracted; otherwise, all files are extracted.</p> <p>If a properties file is specified, the values in the properties file are used for substituting variables when the rulebases are extracted. When a rulebase is extracted, the file extension changes to <i>.hrb</i> from <i>.hrt</i>.</p>
t	Lists the rulebases in the MAR file.
v	Generates verbose output to standard output.
p	Specifies the properties file that contains name-value pairs that will be used for substituting variables in the rulebase template.
f	Specifies the name of the MAR file.

Input	Description and Usage
<p><code>-Xtype &lt;type&gt;</code>, where type is the unique identifier assigned to TIBCO applications.</p>	<p>This option is only valid for rulebase that contain agent-specific rules.</p> <p>For rulebases that contain application-specific rules, this option will not apply.</p> <p>For rulebases that contain agent-specific rules and an application-specific rule, option will have no effect on this rulebase.</p> <p>This option will never override known type (where the type is determined from the data source of the rule).</p> <p>See <a href="#">Types Assigned to TIBCO Applications</a> for the list of valid types.</p>
<p><code>-Xasis</code></p>	<p>Do not templatized the rulebases.</p> <p>Normally all the rulebases are templatized before adding to the mar file. This option will add the rulebase to the MAR file as is without parsing the rulebase for the data source type.</p> <p>This option is useful for deploying rulebases created for a specific deployment or a component instance.</p>

The MAR utility recognizes the datatype of any rule in a rulebase whose datasource name is in the following format: `COM.TIBCO.ADAPTER.<NAME>.<TIBCO_DEPLOYMENT>.<TIBCO_COMPONENT_INSTANCE>` or `COM.TIBCO.ADAPTER.<NAME>.<TIBCO_DOMAIN>.<TIBCO_DEPLOYMENT>.<TIBCO_COMPONENT_INSTANCE>`.

The following table lists valid values for some TIBCO applications that you can use when assigning a type to the MAR file.

**Types Assigned to TIBCO Applications**

<b>TIBCO Application</b>	<b>Type</b>
TIBCO Businessworks	bwengine
TIBCO Adapter for Active Database	adb
TIBCO Adapter for Siebel	adsbl
TIBCO Adapter for Files	adfiles
TIBCO Adapter for Oracle Applications	adorapps
TIBCO Adapter for SWIFT	adswift
TIBCO Adapter for EJB	adejb
TIBCO Adapter for COM	adcom
TIBCO Adapter for CORBA	adcorba
TIBCO Adapter for Teradata	adtera
TIBCO Adapter for Tuxedo	adtuxedo
TIBCO Adapter for Infranet	adinfra
TIBCO Adapter for PeopleSoft8	adpsft8

## Monitoring Console

This console lists the monitoring applications that have been added to your domain.

To create a monitoring application you must first create a monitoring archive file (MAR file). This archive is created using the MAR utility and contains TIBCO Hawk rulebases that monitor your applications. See [Using the Monitoring Archive Utility](#) for details on using the MAR utility.

You can use the same MAR file to create multiple monitoring applications and deploy them separately onto different machines in your domain.

See [Security Considerations](#) for the permissions required to access the Monitoring Management Console.

## Creating a Monitoring Application

1. Click **Monitoring Management>Monitoring Console**.
2. Choose a domain and click **Add**.
3. Click Browse and select a monitoring archive file and click **OK**.

Hawk RulebaseMaps and Schedules are also similarly deployed. Only one RulebaseMap and Schedule file can be deployed per domain. The RulebaseMap file has to be named `rbmap.hrm` and the Schedules file has to be named `schedules.hsf`.

The following figure shows the new application that is ready for deployment.

Monitoring Management - Monitoring Console  
Edit Monitoring Console Hawk Domain Detail: mmdomain3

**New Monitoring Archive: mymar** ?

OK Cancel

**Monitoring Archive** Change MAR file

Name	mymar	
Version	1	
Description	Created by TIBCO Hawk monitoring archive tool.	
Creation Date	Mon Jul 10 14:34:00 PDT 2006	
Owner	pprasad	

**Monitoring Configurations**

Hawk Domain	mmdomain3	
Quick Configure	<input checked="" type="checkbox"/>	
Deploy On Save	<input type="checkbox"/>	

Monitoring Configuration	Type	Target
WinXP	hawk-agent	Enable All
HawkWindowsEventLog	hawk-agent	Enable All

Click **Change MAR File** if you want to select a different monitoring archive file.

Select the **Quick Configure** checkbox if you want to identify the targets where the monitoring configuration can be deployed. These targets are identified using the type of the rulebase (monitoring configuration) contained in the monitoring archive file. The type is determined by the data source of the microagents belonging to TIBCO application being monitored. If the Quick Configure checkbox is selected, the Deploy on Save field is enabled.

Select the **Deploy on Save** checkbox to deploy the monitoring configurations contained in the MAR file on the identified targets.

For each monitoring configuration contained in the monitoring archive, the following information is displayed:

- Monitoring Configuration name  
The name of the monitoring configuration file.
- Type  
This is the type of the TIBCO application for the monitoring configuration. Each TIBCO application has a unique type associated with it.
- Targets  
If you select Quick Configure, this field reflects the targets (within the domain) where the monitoring configuration can be deployed.  
Choose between Enable All (choose all targets within the domain), Disable All (disable deployment on all targets), or a specific target within the domain.

4. Click **Save**.

The chosen monitoring archive file is now added to the main Monitoring Management dialog and is ready to be deployed.

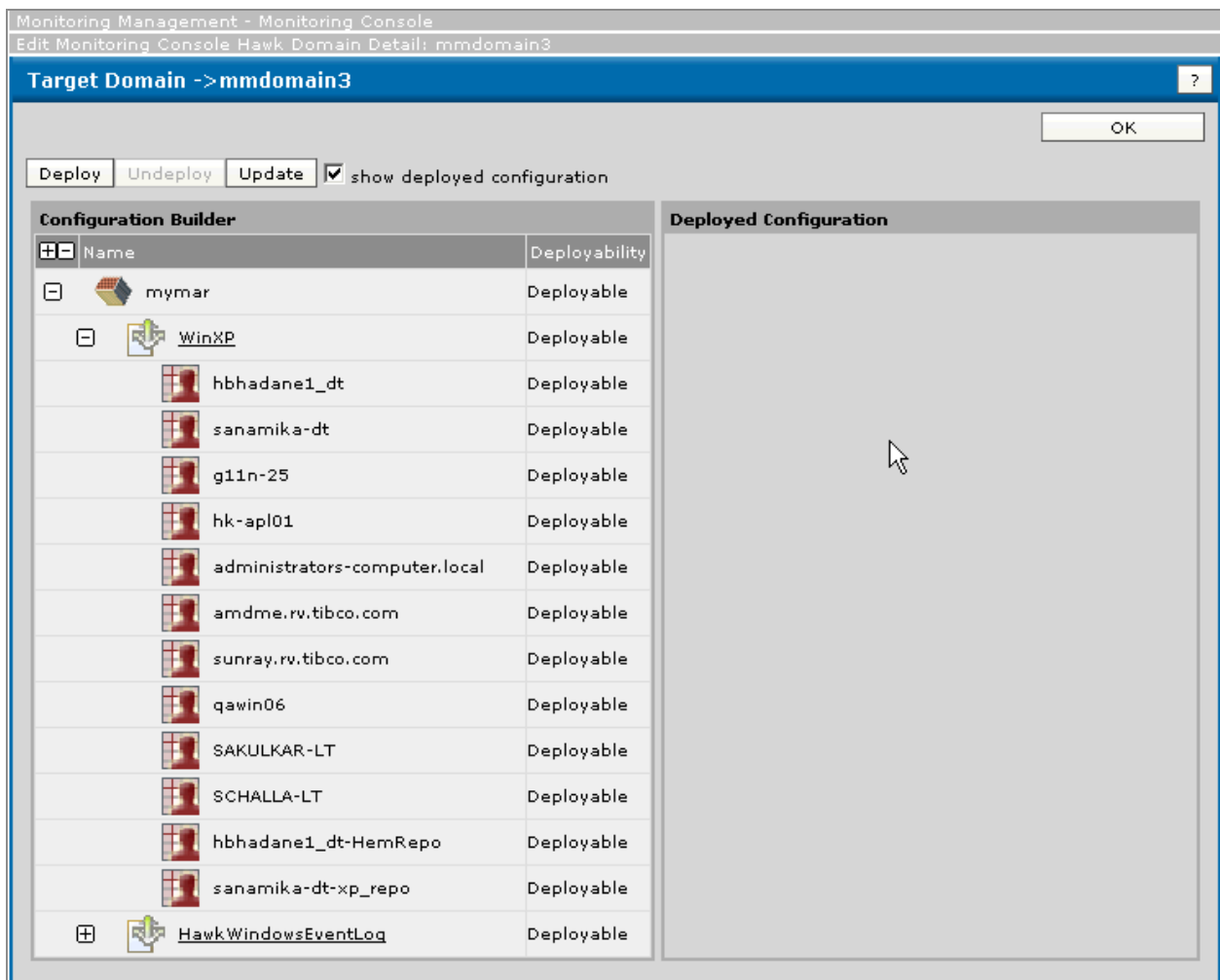
## Deploying a Monitoring Configuration

When you create a monitoring application, you can use the **Deploy on Save** option to deploy the contained monitoring configurations. Any global variables shared between the target application and the monitoring configuration are resolved at the time of deployment. If you do not use the **Deploy on Save** option, you can explicitly deploy the monitoring configuration.

To deploy an application

1. Click **Monitoring Management>Monitoring Console**
2. Choose the domain.
3. The list of monitoring archives created for this domain is displayed.
4. Click an monitoring archive to select it for deployment.
5. Choose a Monitoring Configuration by clicking on it.

If **Quick Configure** was selected when adding the monitoring application, the targets for this configuration will be listed as shown in the following figure:



If Quick Configure was not selected when adding the monitoring application, the targets have to be manually added by clicking **Add Target**. See [Adding Targets for a Monitoring Configuration](#) for more information.

6. Click **Deploy**.



If the monitoring configuration is successfully deployed, the Status changes from Deployable to Deployed (loaded).

If the target application is not running, the status is changed to Deployed (Not Loaded). When the target application starts, the status changes from Deployed (Not Loaded) to Deployed (Loaded).

For a deployed monitoring configuration, if the TIBCO Hawk agent on the target machine stops running, the status changes to Deployed (not available).

In order to successfully deploy a monitoring configuration, the TIBCO Hawk Agent on the target machine must be running.

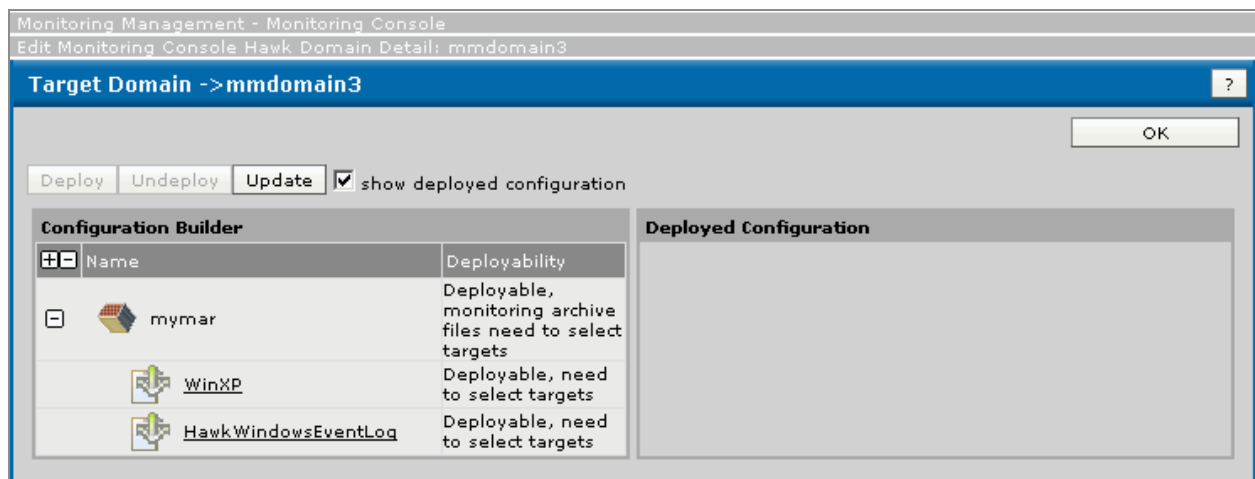
7. Click **OK**.

## Adding Targets for a Monitoring Configuration

If the Quick Configure checkbox was not selected when adding the monitoring application to the domain, you have to manually choose the machines (targets) to deploy each monitoring configuration contained within the monitoring application.

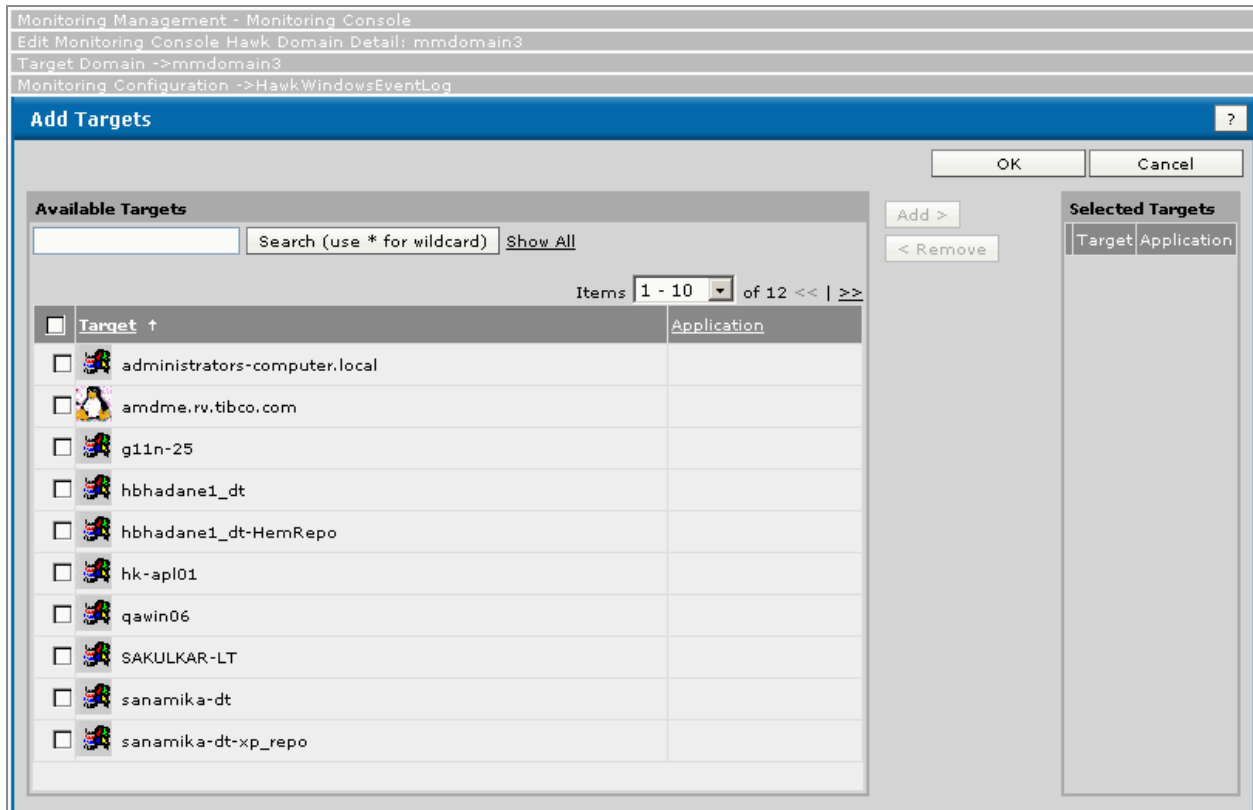
To add targets for a monitoring configuration:

1. Click **Monitoring Management> Monitoring Console**.
2. Choose the domain and select the Monitoring Archive that you want to deploy. The following Configuration Builder screen is displayed, where the list of targets is empty:



3. Choose a monitoring configuration and click **Add Target**.

The Add Targets dialog is displayed as shown in the following screen. The Available Targets pane lists the potential targets (within the domain) where the monitoring configuration can be deployed.



4. Select the checkbox for the target(s) and click **Add**.

The selected targets are moved to the Selected Targets pane.

To remove a target from the Selected Targets pane, select the checkbox for the target and click Remove.

5. Click **OK** twice to return to the Configuration Builder.
6. Click **Deploy**.



#### Note

If you deploy a monitoring configuration to any targets newly added to your domain, the configuration will be deployed only on the newly added targets and will not be re-deployed on the existing targets.

## Updating a Monitoring Application

A monitoring application contains one or more monitoring configurations. If you want to delete an existing configuration or add a new one, you must update the monitoring application for the changes to take effect. Before you proceed to update a monitoring application, make sure all its constituent monitoring configurations are in the Deployable state.

To update a monitoring application:

1. Click **Application Management > Monitoring Management**.
2. Choose the domain where the monitoring application is deployed.
3. Click the application that you want to update.  
The details of the monitoring application (MAR file) are displayed.
4. Click **Update**.
5. Click Browse and select the updated monitoring archive file and click **OK**.

The updated monitoring archive file and its monitoring configurations are now available for deployment.

## Deleting a Monitoring Application

Before a monitoring application can be deleted, each of its constituent monitoring configurations have to be undeployed from each target where it was deployed. See [To Undeploy a Monitoring Configuration](#) for details.

To delete a monitoring application:

1. Click **Monitoring Management > Monitoring Console**.
2. Choose a domain.
3. Select the monitoring application that you want to delete and click **Remove**.

The selected monitoring application is now removed from your domain.

## To Undeploy a Monitoring Configuration

4. Click **Monitoring Management > Monitoring Console**.
5. Choose a domain.

6. Select the Monitoring Application that you want to undeploy.
7. Select a monitoring configuration
8. Select the check box for each target listed whose status is Deployed (Loaded) and click **Undeploy**.
9. Perform [Select a monitoring configuration](#) and [Select the check box for each target listed whose status is Deployed \(Loaded\) and click Undeploy](#). for each monitoring configuration included in the application.
10. Click **Done**.

## Variable Substitution

The following variables, if used, will be substituted when the monitoring configuration is deployed:

- TIBCO\_DOMAIN
- TIBCO\_DEPLOYMENT
- TIBCO\_COMPONENT\_INSTANCE
- TIBCO\_COMPONENT\_TYPE
- TIBCO\_DOMAIN\_HOME
- TIBCO\_COMPONENT\_INSTANCE\_TRACE\_FILE

## Using the Configure Monitoring Utility

The command-line utility, ConfigureMonitoring, provides an alternative mechanism for deploying and undeploying monitoring configurations. This utility is located in the *CONFIG\_FOLDER/hawk/bin* directory. The log file for this utility is *hawkconsole.log*, and is created in the directory from which this command is invoked.

See [Security Considerations](#) for the permissions required to use the ConfigureMonitoring utility.

Using the ConfigureMonitoring utility you can:

- Upload a single MAR file into TIBCO Administrator

The `-upload` command uploads a single MAR file into TIBCO Administrator. If this is a new MAR file, a new monitoring application is created with the same name as the MAR file. If it already exists and if the contained monitoring configuration are in the Deployable state, the existing data is overwritten. It cannot update if any of the monitoring configurations in the deployed state.

Example: `ConfigureMonitoring.exe -upload -mar myMarFile.mar -domain myHawkDomain -user admin -pw adminpw`

Hawk RulebaseMaps and Schedules are also similarly deployed. Only one RulebaseMap and Schedule file can be deployed per domain. The RulebaseMap file has to be named `rbmap.hrm` and the Schedules file has to be named `schedules.hsf`.

Example: `ConfigureMonitoring.exe -upload -mar rbmap.hrm -domain myHawkDomain -user admin -pw adminpw`

- Retrieve all potential targets for all monitoring configurations within the specified monitoring application.

The `-getTargets` command retrieves all potential targets for a given monitoring application in the TIBCO Administrator domain. An XML file containing the targets is created in the current directory. The name of the XML file has the format `<MAR_file_name>-targets.xml`, where `<MAR_file_name>` is the MAR file for which the targets are retrieved.

Example: `ConfigureMonitoring.exe -getTargets -monitoringAppName myMarFile -domain myHawkDomain -user admin -pw adminpw`

This command creates the XML file `myMarFile-targets.xml`.



#### Note

You can edit the XML file created by the `-getTargets` options to delete a target, effectively choosing to not deploy the monitoring configuration on that target.

---

- Deploy monitoring configurations

The `-deploy` command configures and deploys the monitoring configurations on the targets specified in the target file. The status of deploying each monitoring configuration on each identified target is displayed.

Example: `ConfigureMonitoring.exe -deploy -targets myMarFile-targets.xml -monitoringAppName myMarFile -domain myHawkDomain -user admin -pw adminpw`

- Undeploy monitoring configurations

The `-undeploy` command undeploys the monitoring configurations from the targets specified in the target file. The status of undeploying each monitoring configuration from each identified target is displayed.

Example: `ConfigureMonitoring.exe -undeploy -targets myMarFile-targets.xml -monitoringAppName myMarFile -domain myHawkDomain -user admin -pw adminpw`

- Delete monitoring applications (MAR file)

The `-delete` command deletes the specified monitoring application from the TIBCO Administrator domain. To remove a monitoring application, none of its monitoring configurations and its targets should be in the deployed state.

Example: `ConfigureMonitoring.exe -delete -monitoringAppName myMarFile -domain myHawkDomain -user admin -pw adminpw`

The following table describes the input parameters for the `ConfigureMonitoring` utility.

#### ConfigureMonitoring Utility: Input parameters

Input	Description
<code>-domain</code>	The TIBCO Administrator domain name.
<code>-targetDomains</code>	<p>(Optional) The domains where you want to deploy the specified monitoring configurations.</p> <p>If this option is not specified, the monitoring configuration is deployed in the TIBCO Administrator domain.</p> <p>The domains are specified within double-quotes (").</p> <p>Specify multiple domains using a comma separated list.</p> <p>For example, <code>-targetDomains "domain1, domain2"</code></p>
<code>-mar</code>	The MAR file name. If the MAR file is not located in the current directory, specify the complete path name.

Input	Description
-user	An authenticated TIBCO Administrator user having Read-Write permissions.
-pw	<p>The password for the TIBCO Administrator user specified by the <code>-user</code> option. The password could be either plain text or encrypted. Passwords can be encrypted using password encryption tool. On Microsoft Windows platforms, the tool is <code>&lt;HAWK_ROOT&gt;\bin\tibhawkpassword.exe</code> and on UNIX platforms, it is <code>&lt;HAWK_ROOT&gt;/bin/tibhawkpassword</code>.</p>
-targets	The file containing targets for a MAR file.
-monitoringAppName	The monitoring application name.
-initTime	<p>(optional) The default time, in seconds, to wait for the Hawk components to initialize before executing the <code>ConfigureMonitoring</code> command.</p> <p>The default value is 60.</p>
-cred	<p>The credential file containing user credentials (user and pw) specified as properties. The password can be specified either in plain text or encrypted form.</p> <p>Passwords can be encrypted using password encryption tool. On Microsoft Windows platforms, the tool is <code>&lt;HAWK_ROOT&gt;\bin\tibhawkpassword.exe</code> and on UNIX platforms, it is <code>&lt;HAWK_ROOT&gt;/bin/tibhawkpassword</code>.</p>

# TIBCO Documentation and Support Services

---

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

## How to Access TIBCO Documentation

Documentation for TIBCO products is available on the [Product Documentation website](#), mainly in HTML and PDF formats.

The [Product Documentation website](#) is updated frequently and is more current than any other documentation included with the product.

## Product-Specific Documentation

The documentation for this product is available on the [TIBCO Hawk® Documentation](#) page.

## How to Contact Support for TIBCO Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our [product Support website](#).
- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the [product Support website](#). If you do not have a username, 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 [TIBCO Community](#).

# Legal and Third-Party Notices

---

SOME CLOUD SOFTWARE GROUP, INC. (“CLOUD SG”) SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, “INCLUDED SOFTWARE”). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

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

This document 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 Cloud Software Group, Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, Hawk, LogLogic, Rendezvous, Administrator, and BusinessWorks are either registered trademarks or trademarks of Cloud Software Group, 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. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG’s Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

Cloud SG 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 a specific version of Cloud SG software 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. CLOUD SG MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), THE PROGRAM(S), AND/OR THE SERVICES DESCRIBED IN THIS DOCUMENT AT ANY TIME WITHOUT NOTICE.

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 "README" FILES.

This and other products of Cloud SG may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>.

Copyright © 1996-2024. Cloud Software Group, Inc. All Rights Reserved.