

**Mule**

**Management**

**Console**

August 30, 2016

**Document Control Information**

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | Date | Description | Author |
| 1.0 | 08/30/2016 | Initial Version | Abhay Singh |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Support / SME Resources**

|  |  |  |  |
| --- | --- | --- | --- |
| **Team** | Name | Role | Contact (Email / Phone) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[1. Overview 4](#_Toc460343998)

[2. Purpose 4](#_Toc460343999)

[3. Benefits 4](#_Toc460344000)

[4. Key Features 5](#_Toc460344001)

[5. Requirements 6](#_Toc460344002)

[6. Architecture of the MMC 6](#_Toc460344003)

[7. Registration of MMC with Mule Instances 7](#_Toc460344004)

[8. Installing MMC 8](#_Toc460344005)

[9. Installation and Deployment Checklist 8](#_Toc460344006)

[10. Starting the Management Console 8](#_Toc460344007)

[11. Orientation to the Console 9](#_Toc460344008)

[12. The Quick Start Panel 9](#_Toc460344009)

[The Dashboard 10](#_Toc460344010)

[Layout of the Console 10](#_Toc460344011)

[Using the Console 11](#_Toc460344012)

[Servers Tab 12](#_Toc460344013)

[Deployments Tab 12](#_Toc460344014)

[Applications Tab 13](#_Toc460344015)

[Flows Tab 13](#_Toc460344016)

[Flow Analyzer Tab 14](#_Toc460344017)

[Business Events Tab 15](#_Toc460344018)

[Alerts Tab 15](#_Toc460344019)

[Administration Tab 15](#_Toc460344020)

[13. Managing MMC Users and Roles 16](#_Toc460344021)

[14. User Management System 16](#_Toc460344022)

[15. Automating Tasks Using Scripts 20](#_Toc460344023)

[**Saving a New Script** 21](#_Toc460344024)

[Create a Scheduled Job 22](#_Toc460344025)

[Delete a Scheduled Job 22](#_Toc460344026)

[16. Some Definitions 23](#_Toc460344027)

1. Overview

After software developer teams create Mule applications using Anypoint Studio or another IDE,

they typically pass the Mule application to another team who deploys the application in a

simulated environment for more rigorous testing. Afterwards, the application is run in production

with strict requirements to be constantly available, performing at a certain rate, and continually

working as expected. Moreover, additional Mule instances and applications may be introduced

into the infrastructure, increasing the level of complexity inherent to managing and monitoring

all systems.

This is where MMC comes in. MMC is an enterprise management and monitoring tool

designed specifically for Mule ESB instances. MMC provides a comprehensive set of functionality

for managing and monitoring running Mule instances, Mule clusters, applications within Mule

instances, and the flows within those applications. It also provides ways of looking at specific

transactions through pre-defined business events, as well as transactions in flight.

MMC provides a

centralized, convenient, and intuitive web-based interface to monitor, manage, and administer

the run-time aspects of Mule ESB. With MMC, you can save time and reduce errors by quickly

identifying, diagnosing, and appropriately addressing problems across development, testing, UAT

and production environments, all within a single interface.

1. Purpose

The purpose of this document is to provide information about the Mule Management Console

(MMC), and how it is beneficial in centralized management of on premise Mule ESB Enterprise

deployments, whether they are running as standalone instances, as a cluster, or embedded in

application servers.

1. Benefits

MMC provides the following benefits:

* Simplified troubleshooting through quick access to the most relevant information
* Enhanced availability, scalability, and performance through clustering
* Improved visibility and understanding by analyzing real-time metrics that highlight significant changes
* Increased application uptime and performance through intelligent, proactive alerting and remediation tools
* Reduced downtime and time-to-resolution with deep diagnostics and auditing capabilities
* Minimal impact on the runtime performance of your ESB infrastructure
* Improved collaboration between operations and development through controlled access to runtime diagnostic information
* Lower management cost with group-based management and control
* Insight into key business-related events

1. Key Features

**Centralized Management and Monitoring**

* Check the health of ESB resources via an easy-to-navigate visual interface.
* Access intuitive charts that reveal system performance and resource consumption.
* Manage multiple runtime environments, grouped by location, business function, or other criteria.
* Define and subscribe to Mule alerts.

**Fine-Grained ESB Control**

* Start, stop, and restart ESB resources.
* Remotely access, update, or replace any file or configuration on a Mule ESB server.
* View resource consumption and dynamically tune flows in real time.
* Dynamically configure thread pools.

**Enterprise-Level Security**

* Support for enterprise authentication (LDAP).
* Set up fine-grained role-based access control.
* Secure your runtime communications using certificates and HTTPS.

**Deep Diagnostics and Auditing**

* View detailed information on memory utilization, threads, system resources, and server configuration.
* Audit message traffic and associated properties for both the inbound and outbound sides of flows.
* Turn flow level auditing on or off to capture just enough data to diagnose an issue without impacting performance.

**Intelligent Alerting**

* Receive notifications when critical metrics cross thresholds.
* Monitor events at the individual server level or system level.
* Escalate alerts to administrators or an external monitoring system.
* Customize alerts using alert scripts.

**Flexible Cluster Management**

* Create, disband, or add nodes to clusters as conditions dictate.
* Monitor cluster status – get detailed information about cluster-based flows and memory usage.
* Deploy apps to a cluster for enhanced availability, scalability, and performance.

**In-Depth Event Visualization**

* Track key events in the flow of business transactions.
* Analyze the flow and disposition of particular messages within a business transaction.
* Drill into event data to identify failure points or bottlenecks.
* Test flows for compliance with business procedures and standards

1. Requirements

To take MMC for a test drive, there are no special technical requirements. Just download the trial version.

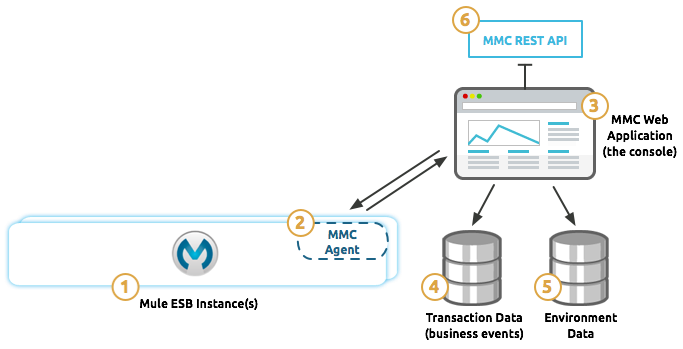
To successfully run MMC in production, you need:

* A Mule ESB Enterprise instance with a valid enterprise license
* The MMC console application file (mmc.war) deployed in a supported web application server
* The MMC agent .jar file, which is bundled with the Mule ESB Enterprise instance in versions 3.7.0 and newer. Previous versions of Mule ESB require the agent to be installed separately.

Finally, here are a few important notes to keep in mind before deploying MMC:

* MMC is compatible only with Mule ESB Enterprise
* MMC is backward compatible with previous versions of Mule ESB.

1. Architecture of the MMC



* + 1. The Mule ESB instances monitored by MMC. These can be standalone or embedded instances, or clusters.
    2. The MMC agent contained in the Mule instance, which is responsible for
* facilitating data transfer between the Mule instance and the MMC
* applying changes (i.e. thread pools, and configuration file changes) to the Mule applications
  + 1. The MMC instance, the Web-based interface that interacts with Mule through:
       - the MMC agent
* JMX functionality exposed by Mule. The MMC instance is a Web application packaged as a WAR file that executes from within your Web servlet container (i.e. Tomcat, JBoss, etc.).
  + 1. The transactional database that stores business event transactional data collected by the MMC agent within the Mule instance. This database by default is an H2 database, but you can configure MMC to use other relational databases.
    2. The environment database, that stores state information about the various Mule instances and applications managed by MMC, including alerts, deployments, configurations, etc. The database is by default Apache Jackrabbit, but you can configure MMC to use other relational databases.
    3. MMC’s REST interface, which exposes MMC functionality through a REST API. MMC users can invoke this API to programmatically Mule instances paired with MMC.

1. Registration of MMC with Mule Instances

Once Mule and its embedded MMC agent have started, within the Mule folder structure, you will

notice a new folder called  .mule that contains several subfolders and files, including keystore.jks.

To pair the MMC with a Mule instance, you provide the complete address, port and location of the

listening Mule agent, in the form http://<hostname>:<port>/mmc-support,

i.e. http://localhost:7777/mmc-support. MMC will attempt to pair with the Mule agent in the

specified URL, then report success or failure.

Additionally, in the. mule folder in the paired Mule

instance, you will notice that an additional file called truststore.jks is created. At this point, a secure

connection over HTTPS will have been created between MMC and the Mule instance.

Each Mule instance can only be registered with one MMC instance, but each MMC instance can

manage several Mule instances. There is no logical limit to the number of Mule instances that can

be paired with a single MMC instance.

You can unregister Mule instances from MMC with via

the **Servers** tab in MMC. After you unregister a Mule instance, the truststore.jks file is deleted from

the. mule directory.

1. Installing MMC

The Mule Management Console is a Web app designed to run in an application server, such

as Tomcat Server or Apache Tomcat, and usually packaged in a .war file.

This document describes where to download the required files and how to install or deploy these

files for different application servers.

Please <https://www.mulesoft.com/support-and-services/mule-esb-support-license-subscription>

[contact the Mule Soft Support team] with any questions about downloading and deploying Mule

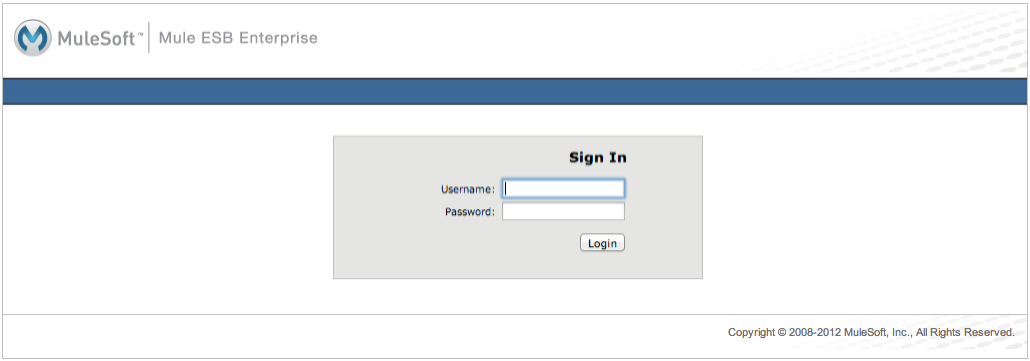
Management Console.

1. Installation and Deployment Checklist

To install the management console:

1. Download the Mule Management Console application (.war file) from the MuleSoft customer portal. (Note that the management console agent, formerly a separate download and installation, is now embedded in the Mule Enterprise distribution.)
2. Rename your .war file to mmc.war.
3. If your Mule ESB instance is packaged as a Web app (not recommended), please contact support for special instructions.
4. Adjust the configuration on your web application server so that it gives precedence to MMC’s classloader, instead of your Web application server’s own native classloader.
5. Deploy your mmc.war file to your application server. See specific instructions for each supported app server in the following section.
6. Starting the Management Console

To run the Management Console, make sure your application server is running and the Management Console Web app has been deployed correctly. Then, navigate to the URL where the Management Console Web application is hosted. If you see the login screen (see below), you have installed everything correctly and are now running the console.



1. Orientation to the Console

This page introduces the Mule Management Console’s user interface. It covers basic information

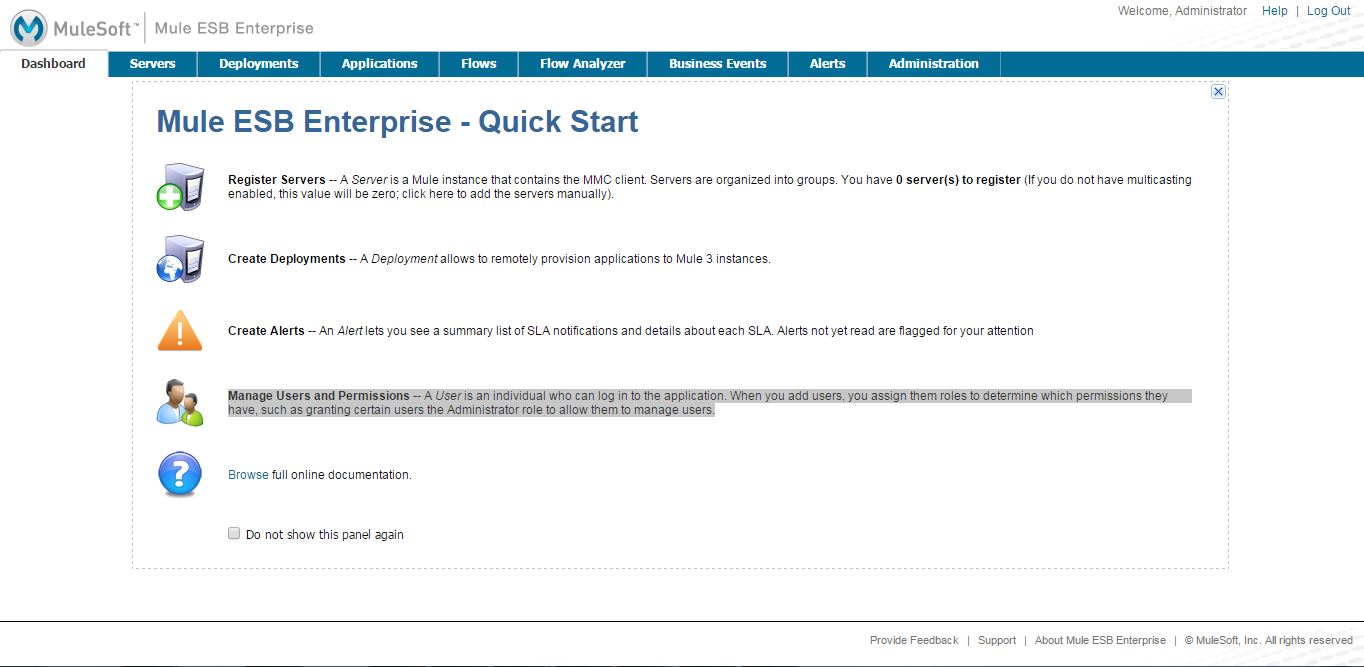
about how to customize your dashboard and interact with the functionality available on the

various tabs.

1. The Quick Start Panel

When you first start the console and log in, you are presented with the Quick Start panel, giving you

immediate access to the common tasks you might wish to perform.



The icons on the left side provide quick links to screens for registering servers, deploying

applications, creating alerts, and managing users and permissions. If you hover your mouse over

the individual tabs, pop-up tips display.

Keep in mind that if you have just installed a Mule ESB server, the server must be registered with

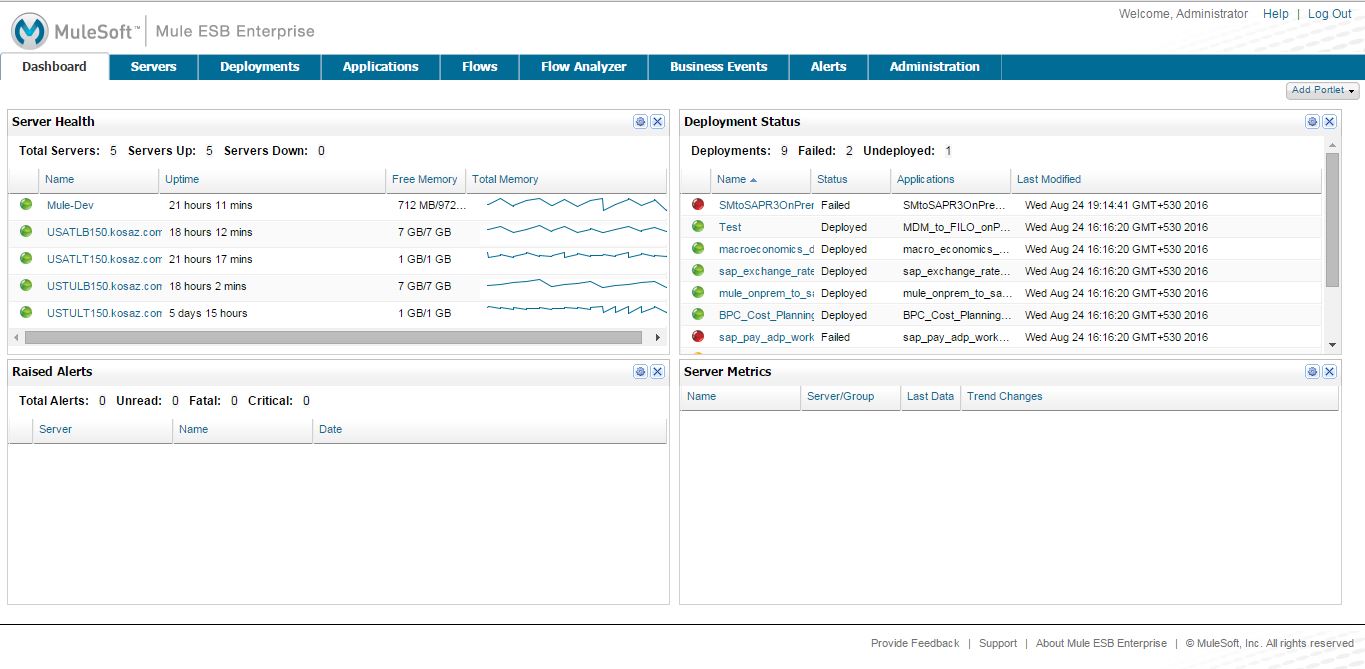
the console and you may need to connect the console to that server before using any of the other

console features. To register servers, click the icon to the left of **Register Servers** or the **Servers** tab

at the top.

## The Dashboard

By default, the Dashboard displays four portlets: Server Health, Raised Alerts, Deployment Status, and Server Metrics. A **portlet** is a customized view of information about your servers or applications. To display additional portlets, click the **Add Portlet** button, then click those portlets you want displayed.



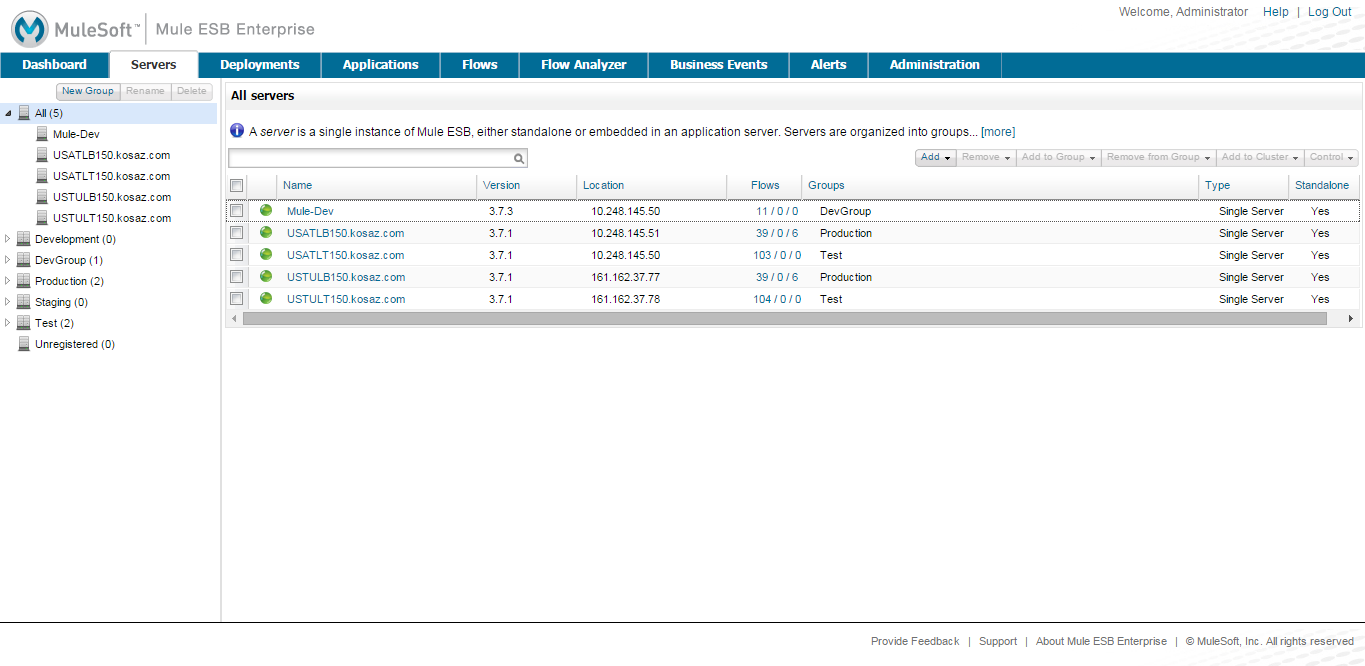
## Layout of the Console

For many of the console tabs, the Management Console screen is divided into two sections:

* A context-sensitive navigation pane on the left
* A details pane on the right that reflects the particular tab you have selected

For example, the figure below shows how the **Servers** tab might appear when you first log in. When you select the Servers tab, the navigation pane displays the organization or grouping of the servers, while the details pane shows summary information in columnar form about each server instance. Notice that when you hover the mouse over a column, a pull-down menu icon appears, allowing you to sort by that column’s data or configure which columns to display or hide.

The function buttons for the navigation pane let you add a new server group, rename a group, or delete a group. Similarly, the buttons available for the details pane provide functions for operating on individual servers. Notice that these buttons, except for **Add**, are grayed out. When you select a particular server, by clicking the box to the left of that server, the buttons become operational and you can click the function you want to apply, such as adding the server to a group.



## Using the Console

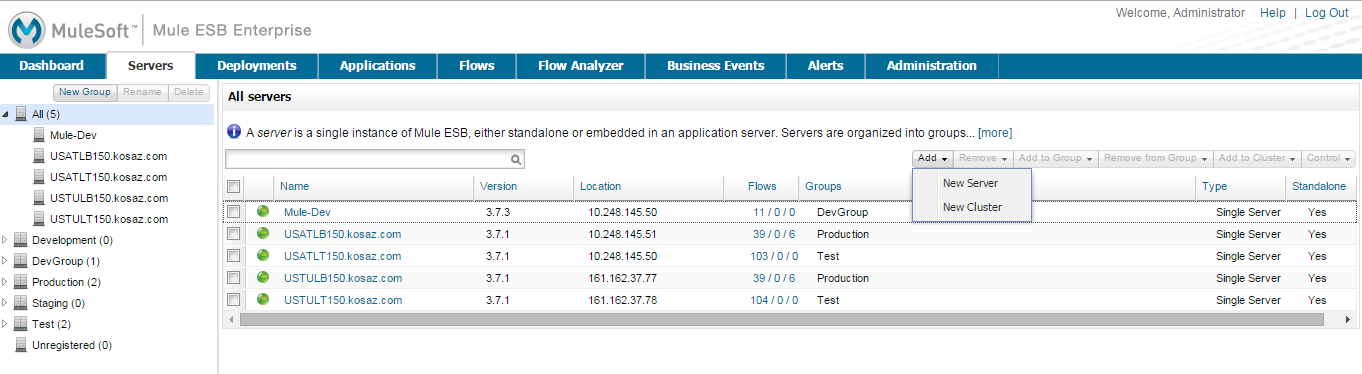
Use the tabs across the top of the console to view and manage your servers, applications, and flows, along with other administrative tasks.

* To manage the application repository and deployments, use the Deployments Tab tab
* To monitor a server or cluster, such as to check if the server/cluster is up or down, see how much memory it is using, or generally keep an eye on the server profile, use the Servers Tab tab
* To define or view alerts about server or cluster health, memory usage, etc, use the Alerts Tab tab
* To check on performance bottlenecks so that you can alert developers, look at the Flows Tab tab as well as the Flow Analyzer tab.
* To diagnose problems, such as memory and performance bottlenecks, use the Flows Tab and Flow Analyzer Tab tabs. The Flow Analyzer tab is particularly helpful because it lets you audit a flow so that you can debug the flow performance and verify payload content along with message properties.
* If you need to manage deployments or the application repository, use the Deployments Tab tab.
* If you need to create scripts to automate tasks, use the Administration Tab tab

The Administration Tab tab is intended for Management Console **administrators**. They can use these screens to manage users and roles, handle licensing issues, and schedule automated tasks.

### Servers Tab

Click the **Servers** tab to add and remove Mule ESB server instances, register servers, create your own groups to organize servers, add servers to one or more groups, start or stop servers, or move them between groups. You can also use the Servers tab to create a new cluster, add nodes to a cluster, or disband a cluster.

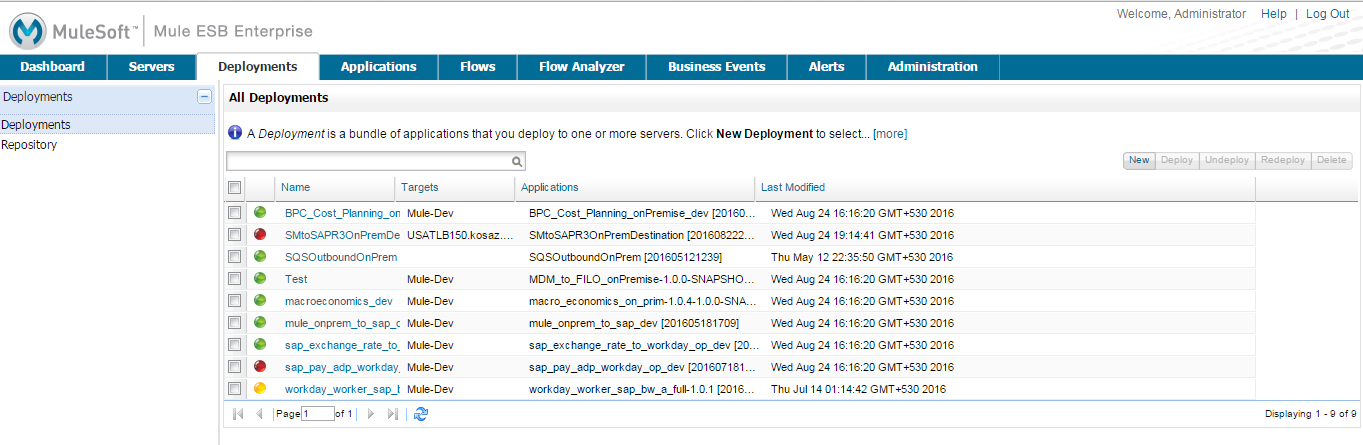


Use the **Add** button in the details pane to add a new server or a new cluster. Use the **Remove** button to unregister a server or disband a cluster and return its nodes to the pool of standalone instances.

### Deployments Tab

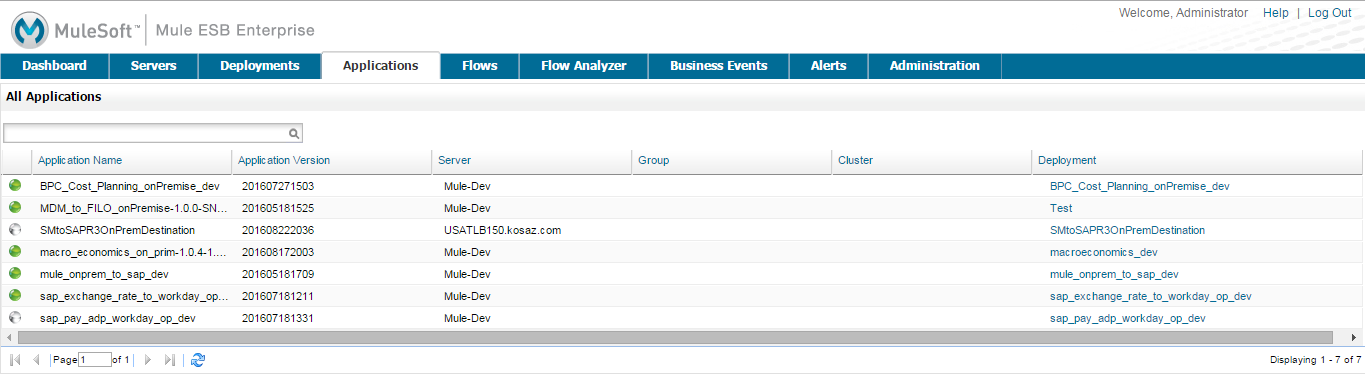
Use the **Deployments** tab to view and manage deployments, which are groups of applications deployed to the server. You can also use the Deployments tab to view and manage applications deployed to a cluster.

From this tab, you can deploy, redeploy, and undeploy groups of applications. You can also maintain the applications stored in the repository.



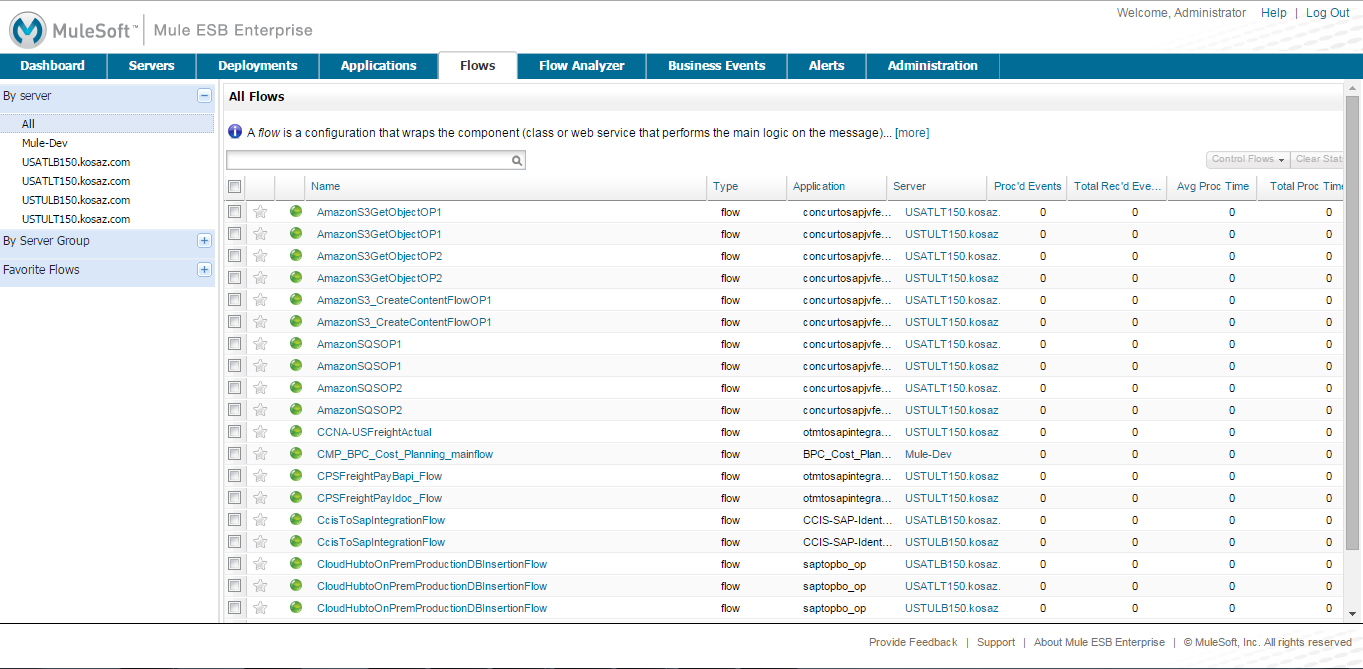
### Applications Tab

Use the Applications tab to browse or search for applications currently deployed on a server or a cluster. The table on this tab displays useful summary information about each application, such as the version, the server, group, or cluster on which it is deployed, and the name of the deployment in which this application is deployed. To manage the application, click the name of the deployment to navigate directly to the relevant deployment details.



### Flows Tab

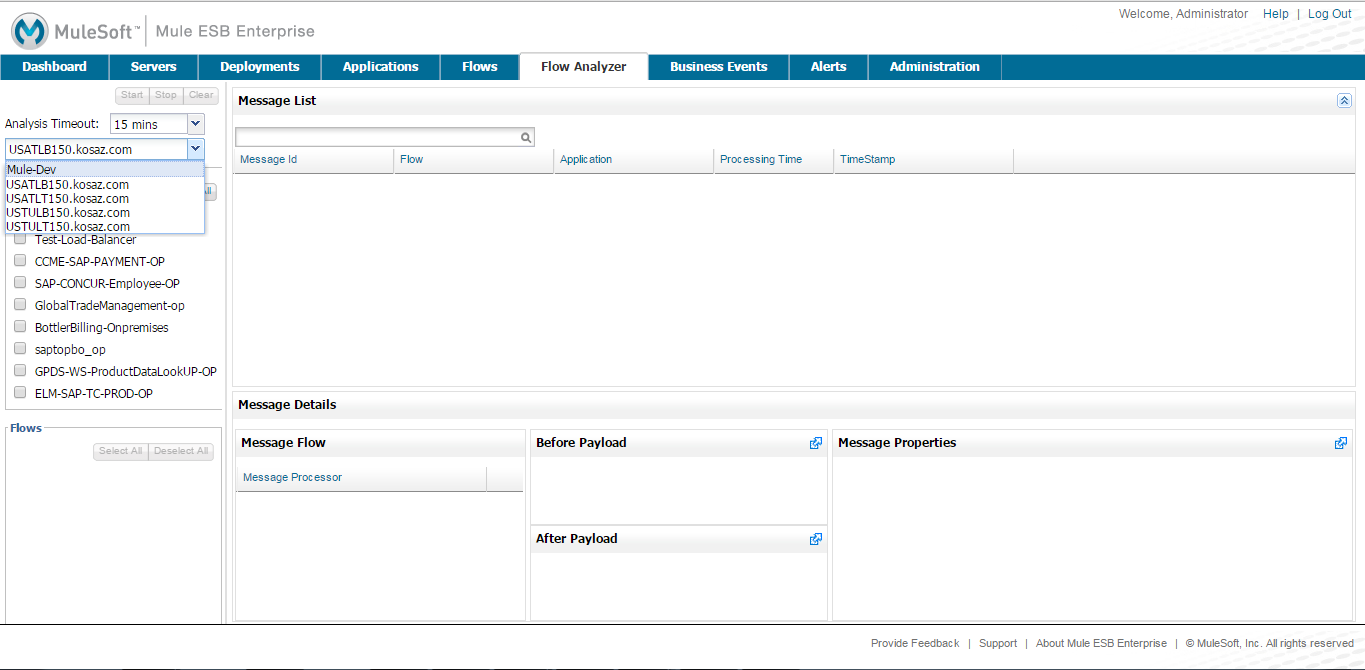
Flows are Mule configurations that include all the different components or message processors – including transformers, controllers, routers, filters, the main application class or Web component, along with the message source or endpoint itself – for processing an application’s message. Similar to the Servers tab, you click the **Flows** tab to get information about and to manage specific flows.



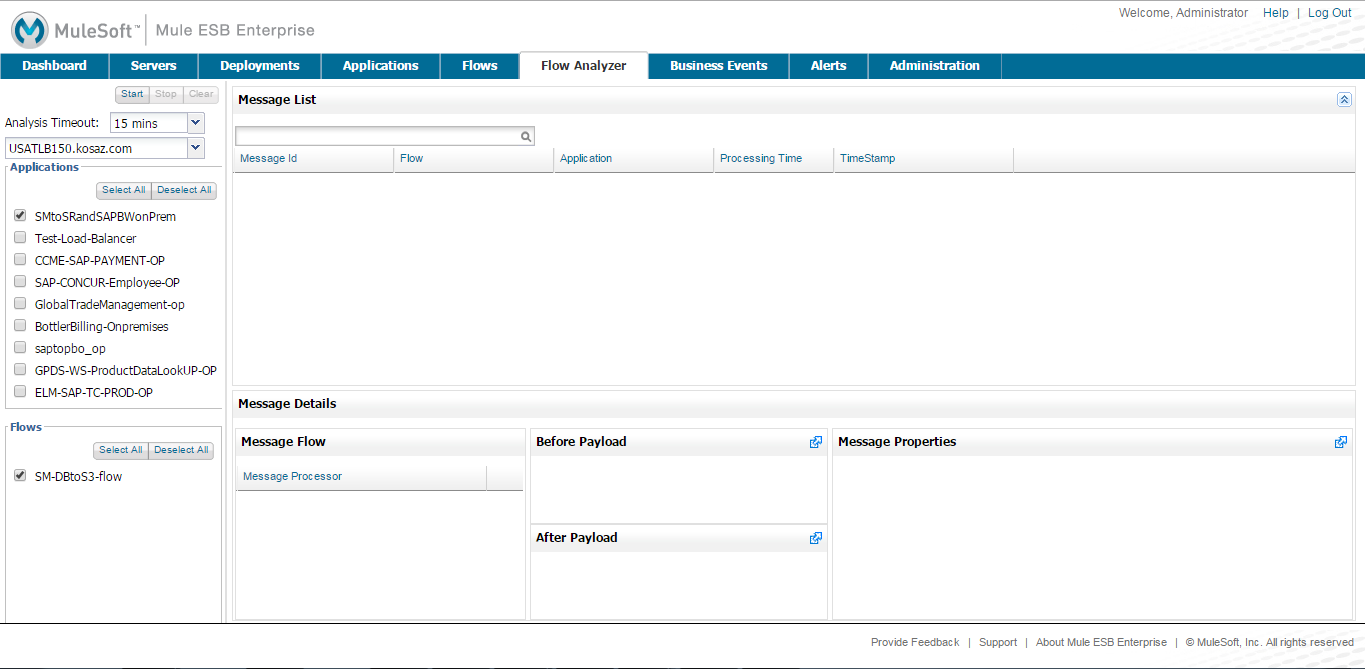
### Flow Analyzer Tab

Use the **Flow Analyzer** tab to see detailed information about your flows that the console captures for you. To view information for a flow:

1. Select a **server** from the drop-down menu in the navigation pane.



1. Select one or more **applications** deployed on that server, then select one or more **flows**.



1. Click **Start**.

Once you have started the flow analyzer, MMC audits and records details about each message that passes through the flow. You can click into messages, message processors, and properties to view granular information about your flow activity.

### Business Events Tab

Use the Business Events tab to retrieve information, such as processing time and errors, for business transactions and events on your Mule servers. You can set up queries to select and view subsets of business transactions handled by your servers. You specify various criteria for selecting transactions, search for particular values, and apply filters to the results.

### Alerts Tab

Use the Alerts tab to view and manage alerts or SLAs.

### Administration Tab

The Administration tab lets you manage users and user groups, as well as set up and schedule utility scripts.

1. Managing MMC Users and Roles

Here we’ll talk about the two ways to manage users in MMC – via the console itself or via LDAP – and defines the concepts of users, groups, server group permissions, and global permissions, as these terms are used in MMC. This document also describes how to set up user groups and assign permissions in the MMC console, which you need to do regardless of whether you manage users via the console or via LDAP.

1. User Management System

**Choosing a User Management System**

Mule Management Console offers two options for managing users, roles, and permissions:

-You can set up and manage users via the Administration tab in the Management Console.

-You can set up and manage users using LDAP.

Note that regardless of which method you choose for user management, you will need to use the Management Console to define user groups and assign permissions to them. Group permissions can be managed only via the console.

Once you have set up users, you can define User Groups, each with a set of appropriate permissions, and then add users to those groups.

**Managing User Groups**

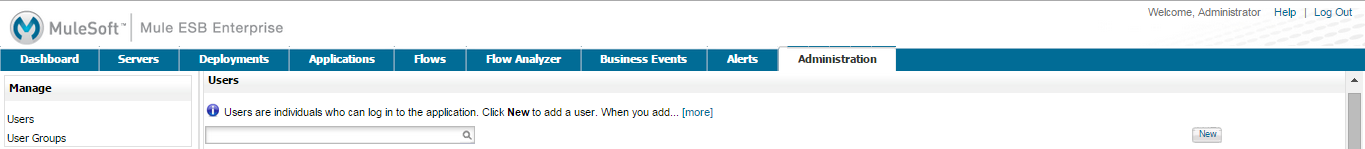
This section describes how to add, manage, and delete a user group, also referred to as a role, in the management console. Note that you cannot delete the Administrators group. The other three groups (Monitors, Deployers, and Server Administrators) model typical roles for console users and have been set up for your convenience.

Adding a new user group, or editing an existing group, entails setting server group permissions and global permissions. Server group permissions define the server groups that the user role or group can manage. The default console server groups are listed, including All servers, plus any server groups you may have created. There is also a set of permissions that apply specifically to servers, including permissions for file access, thread management, and server management.

The global permissions define the permissions that this group has regarding deployment, applications, alerts, flows, and so forth

**Adding a User Group**

1. In the Administration tab, click User Groups in the left navigation panel to see the existing user groups. Click New to create a new group.



2. Enter the Name of the new group, and optionally, a Description.

3. Select the Global Permissions from the list in the left column. Use the Select All button at the bottom of the list to give this user group all global permissions. Or, check only those permissions you want the user group to have.

4. To set Server Group Permissions, first select one or more of the server groups from the pull-down list that this user group can act on. (You can select All, or select individual server groups one at a time and check the permissions boxes for each one.) Then, use the check boxes to set the server group permissions from the list in the right column. Use the Select All button at the bottom of the list to give this user group all server permissions for the designated server groups. Or, check only those permissions you want the user group to have.

5. Click Save

**Managing Group Permissions**

1. Click User Groups in the navigation tree to see the existing groups.

2. Click the particular user group that you want to edit.

3. Use the Edit Group screen to change the name, description, and modify the server and global permissions. Changing the server group access, server permissions, and global permissions is the same as for adding a new user group. (See the section above.)

4. Click Save to save any changes you make.

**Understanding User Groups**

Assigning individual users to user groups, equivalent to assigning them a role, is particularly important from a security perspective, since you are granting that user all the privileges and rights granted to the entire user group. Likewise, setting up the permissions for a user group is extremely important.

Whether you are modifying the permissions for the default user groups or setting up your own user groups, you need to consider the "actors" who will be in each user group and the use cases that these actors will be performing. In conjunction with these use cases, you can further fine-tune these permissions via server groups. By grouping servers into logical categories (Testing, Production, Development, Staging and so forth), you can give some groups more permissions for development and testing, but keep staging and production server environments more restrictive and thus more secure.

For example, you may want to define a user group for application developers. Application developers, of course, put together the application code itself, but they also need to test and debug the code before the application is ready for a production environment. To properly test an application, developers need to deploy their applications to a test system and potentially debug the message flows. Thus, you might want to give developers permissions for all tasks related to deployment, endpoint and flow control, and monitoring abilities on test- and development-specific servers.

You might want to use the staged server environment to set up and verify specific deployment scenarios prior to using them in a production environment. You might want to allow access to these servers for only certain deployment-related user groups. You might even decide that you need two levels of deployment specialists. At the same time, you may want to restrict developer access to the staged server environment so no unintended changes are made prior to release to a production environment.

You might also want a category of support technicians to have capabilities similar to developers, but on staging and production servers. You might have a support group handling sensitive accounts to which you give virtually all permissions.

You might have other user groups whose responsibilities rest more on system administration tasks. For these groups, you may want to give them permissions to manage other users, execute scripts, and manage alerts across all server groups.

**Understanding Permissions**

Permissions give specific user groups the ability to carry out certain sets of tasks. Tasks can be server-related, such as registering or unregistering a server, or they may pertain to applications, such as deployment and flow control functions, or specific users, and so forth. Since permissions granted (or not granted) represent the security on your system, you should be particularly careful when assigning permissions to new user groups or modifying the permissions of existing groups.

Global permissions give all users in a group the ability to perform certain tasks, ranging from viewing deployments, to controlling flows and managing users.

Server permissions range from viewing and deleting files, controlling servers, and killing threads. A user group’s server permissions may apply to all servers or to only a specified server group. The server permissions also apply to the following two activities:

* creating a cluster
* disbanding a cluster

The user groups provided by default (Administrators, Deployers, Monitors, and Server Administrators) have each been given a set of global permissions and server permissions. Both Administrators and Server Administrators by default have been given all global and server permissions; that is, they function as super users. It is important that these user groups retain these permissions to keep the servers fully functional. However, you should exercise care when assigning individual users to either of these groups, since each such user would immediately have these same permissions.

By default, the Administrators and Server Administrators groups also have Clusters - Create and Cluster - Disband permissions.

The two additional default user groups (Deployers and Monitors) have a very limited set of permissions. These two user groups have been included to illustrate the sort of granularity you might employ when assigning permissions to a group. For example, for Deployers, you might only want to grant them permissions related to deployments (create, delete, deploy, modify, and view deployments).

You can modify permissions for existing user groups, such as the user groups provided by default. You can also create new user groups and then assign global permissions to that group, plus specify whether that user group can act on all servers or just a particular server group.

**Global Permissions Reference**

Global permissions encompass the following areas and may be given as noted below to a user group:

* **Applications:** A user group may be given the ability to only view applications and/or to control (start, stop, restart) applications
* **Audit flows:** A user group can have the ability to audit flows via the Flow Analyzer tab
* **Audit flows:** Admin functions: A user group can have the ability to stop any running flow analysis
* **Deployments:** A user group may be given one or more deployment-related permissions: create, delete, deploy, modify, or view deployments
* **Endpoints:** A user group may be given the ability to start and stop endpoints
* **Execute scripts:** A user group may be given the ability execute scripts
* **Flows:** A user group may be given the ability to only view flows and/or to control flows (start, stop, clear statistics)
* **Manage alert definitions:** A user group may be given the ability to manage alert definitions
* **Manage alert destinations:** A user group may be given the ability to manage alert destinations
* **Manage alert notifications:** A user group may be given the ability to manage alert notifications
* **Manage server groups:** A user group may be given the ability to manage server groups
* **Manage user groups:** A user group may be given the ability to manage user groups
* Manage users A user group may be given the ability to manage users
* Pools A user group may be given the ability to modify pools
* **Repository items:** A user group may be given the ability to delete, modify, and/or read a repository item
* **View activity:** A user group may be given the ability to view activity
* **View alerts:** A user group may be given the ability to view alerts

**Server Permissions Reference**

Server permissions include the following and apply to the specified server group or all servers:

**Clusters:** A user group may be given the ability to create or disband a cluster.

**Files:** A user group may be given the ability to manage delete, modify, and/or view files.

**Servers:** A user group may be given the ability to modify, register, restart, unregister, and/or view servers.

**Threads:** A user group may be given the ability to view and/or kill threads.

1. Automating Tasks Using Scripts

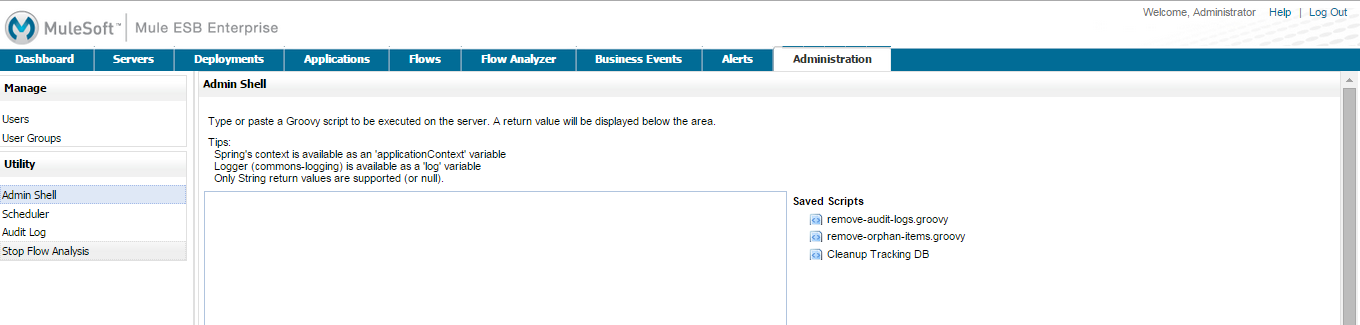
* Creating a Script
* Saving a New Script
* Installing a Script to Run on Startup
* Modifying and Deleting a Script
* Testing a Script
* Scheduling a Script
* Cron Command Syntax

Using the Admin shell to write scripts you can easily build and install your own extensions for the management console. Once written, you can install scripts (that is, set up the scripts to run on startup) or schedule them using a cron-like scheduling mechanism. Scripts are written using the Groovy scripting language.

The pane displays any saved scripts to the right of the editing box. By default, the management console includes a script that pings all your servers looking for unregistered Mule ESB instances. You should see this script in the Saved Scripts area. You should not need to modify this script. Any additional scripts you create and save appear in this area.

**Creating a Script**

To create a script, click the Administration tab, then click Utility to expand its options. Click the Utility option Admin Shell. You enter your script in the blank box in the middle of the pane. (See the figure below.) Depending on the size of your screen, you may need to scroll down to see the function buttons (such as Evaluate, Reset, Save As, and so forth) at the bottom of the script editing box.



**Saving a New Script**

To save a new script, check the Save As box and enter a unique name for the script. Once you check the Save As box, the console does not let you save the script until you enter a name for it. (See the figure below.) Then, click Save.

**Installing a Script to Run on Startup**

To have a script run whenever the management console starts, select the script if it has been saved previously or enter the new script into the edit box. Then, check the Run on startup box. Click Save to save and install the script.

**Modifying and Deleting a Script**

You can use an existing script as a template for a new script. Click the existing script on the right side of the screen, make your modifications, and then check Save As. Enter a new name for the script, then click Save. This is identical to saving a new script.

You can also modify an existing script and save it with the same name. Click the existing script from the Saved Scripts list. Make your modifications. When you’re done, click Save. Your changes to the script are saved with the same name. Be sure that you do NOT click Save As when you want your changes to overwrite the existing script.

At any time, you can click Reset to return to the last saved version of the script.

To delete a script, select it from the Saved Scripts list on the right side of the screen, and then click Delete.

**Testing a Script**

Click the Evaluate button to run a test of a new or modified script. If the script runs without errors, you can save it and, if you want, schedule it to run as a scheduled job or install it to run at startup. If the script evaluation fails, an error message pops up at the top of the page.

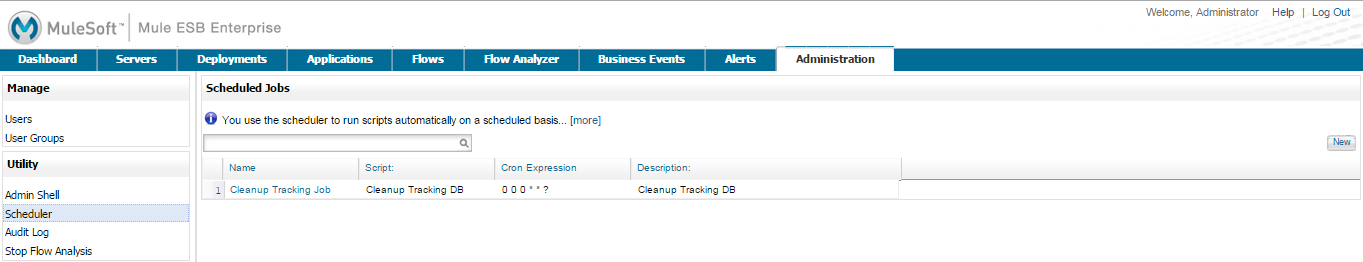
Note that using the Evaluate function does not save, schedule, or install the script. It merely tests the correctness of the script code.

**Scheduling a Script**

You can use the scheduler to periodically run your script, which is useful for jobs such as replication.

### Create a Scheduled Job

1. On the Administration tab, click Utility, then **Scheduler**. You should see a pane listing all scheduled scripts.



2. Click **New** to open the Add Scheduled Item pane to set up a new schedule for a script.

3. Select the script to run from the Script pull-down list. (See below.)

4. Enter a unique name and description for this scheduled job.

5. Enter a [Cron Command Syntax](https://docs.mulesoft.com/mule-management-console/v/3.7/automating-tasks-using-scripts#cron-command-syntax) to specify when the script should be run.

6. To allow this script to be run even if the last execution of the script is still running, click **Allow Concurrent Execution**.

7. Click **Save**.

### Delete a Scheduled Job

1. Click **Scheduler** on the Administration tab.
2. Click the scheduled job you want to delete.
3. Click **Delete**, and then click **OK** to confirm you want to delete this job.
4. Some Definitions

**Register Servers** -- A *Server* is a Mule instance that contains the MMC client. Servers are organized into groups. You have 0 server(s) to register (If you do not have multicasting enabled, this value will be zero; click here to add the servers manually).

**Create Deployments** -- A *Deployment* allows to remotely provision applications to Mule 3 instances.

**Create Alerts** -- An *Alert* lets you see a summary list of SLA notifications and details about each SLA. Alerts not yet read are flagged for your attention.

**Manage Users and Permissions** -- A *User* is an individual who can log in to the application. When you add users, you assign them roles to determine which permissions they have, such as granting certain users the Administrator role to allow them to manage users

**Users** are individuals who can log in to the console.

**User Groups** allow you to assign permissions collectively to a group of users, effectively defining user roles.

**Server Permissions** specify which actions members of a user group may perform on a specified set of servers or server groups. These actions include viewing and deleting files, controlling servers, killing threads, and creating and disbanding clusters.

**Global Permissions** specify which tasks members of a user group may perform in the Management Console, such as viewing deployments, controlling flows, and managing users.