BMC FootPrints Asset Core - External Integration

Version 11.5

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC™

www.bmc.com

Legal Notices

BMC Software, Inc.

2101 CityWest Blvd, Houston TX 77042-2827, USA

713 918 8800

Customer Support: 800 537 1813 (United States and Canada) or contact your local support center

Contents

External Integration

External integration in BMC FootPrints Asset Core is set up to allow for data exchange beween Asset Core and other applications, such as BMC Remedyforce and BMC FootPrints Service Core.

Whenever a specific event is generated in Asset Core a notification is sent to the target software to create an incident ticket in the target application. This allows the adminstrators of the target application to follow up on the progress of these events.

This manual explains how to define and set up external integrations with other applications, that is BMC Remedyforce and BMC FootPrints Service Core and how to track these events in Asset Core. For information on how set up the target applications for external integration with BMC FootPrints Asset Core and how to use the information made available by Asset Core in the target applications please refer to the respective product documentation, the *BMC FootPrints* section of the BMC Remedyforce Online Help and *BMC FootPrints Service Core - Asset Core Integration Guide* for BMC FootPrints Service Core.

Formatting Conventions

Throughout this manual you will encounter elements that stand out in different ways. These elements each have a specific intention and are used consistently, so when you see such an element you immediately know what kind of information to expect.

The following table explains the different formatting conventions:

What you see (Examples)	What it means
1. Select... **2.** Click...	Ordered list of instructions. Execute the steps in the given order.
• Option 1 • Option 2	Enumeration of different options/scenarios to choose from.
Operational Rules	Item of the Graphical User Interface of the software.
Properties	Title of a dialog box/popup window
You need write access to the immediate parent, from which the device or device group is being deleted..	Before a task. Informs you about the prerequisites for the following task.
The **Properties** dialog box appears on the screen.	After a step. Informs you about the immediate result of a step.
The new status has been saved and applied to the selected group.	After a set of instructions. Informs you about the final result of the task.
`MyDevice1,MyDevice1.com,255.255.255.0,"James Kirk",...` `MyDevice2,MyDevice2.com,255.255.255.0,"First Spy",...`	Lines of code.

What you see (Examples)	What it means
 The new patch group will have the same members as the selected device group.	Additional useful information.
 To scan every day at 01:00 AM, from the **at** drop-down list select **01:00**.	Example or recommendation from BMC Software for best practice.
 **Note** You can only use ISO-Latin characters even if you are using a Japanese, Greek or Arabic localization.	Simple note or piece of advice.
 **Remember** If you manage your group through a directory server you may not manually create or add objects to this group anymore.	What you are about to do will affect the system behaviour.
 **IMPORTANT** When deleting an administrator you loose all capabilities and access rights accorded to this administrator as well.	What you are about to do will lead to loss of data or settings.
 **ATTENTION** If the original group or "OU" on the directory server was renamed, moved or deleted, the Asset Core group cannot be resynchronized with this group. An error message will be displayed instead.	What you are about to do will lead to partial or entire system failure.

Getting Started with External Integrations

This first part of the manual guides you through the necessary steps to define external integrations to other software products:

- *BMC Remedyforce*
- *BMC FootPrints Service Core*

Setting Up External Integration with BMC Remedyforce

When setting up integration between BMC FootPrints Asset Core and BMC Remedyforce you need to execute some specific configurations for both applications. This paragraph guides you through the necessary steps in Asset Core. For information on how to configure BMC Remedyforce for integration refer to section *BMC FootPrints* of the BMC Remedyforce Online Help.

- Define External Integration with BMC Remedyforce
- Define Web Service if the communication between the applications is via SSL. Otherwise you can skip this step.

Configuring the Web Service

Configuring the web service for use with the BMC Remedyforce integration consists of the following two steps:

1. *Adding an SSL Certificate*
2. *Defining the Web Service*

Adding an SSL Certificate

For the BMC Remedyforce/Asset Core integration an SSL certificate issued by a trusted authority is required.

This process is divided into the following steps:

1. *Preparing the CSR (Certificate Signing Request)*
2. *Installing the SSL Certificate*

Preparing the CSR

When purchasing an SSL certificate, the certification authority will request you to provide a Certificate Signing Request (CSR). A CSR is a block of encrypted text that is generated on the server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private 2048-bit key will also be created at the same time which you should store in a safe place.

To prepare your certificate proceed as follows:

1. Click the **Prepare Certificate Request** icon.

   The **Prepare Certificate Request** appears on the screen.
2. Enter the required information into the following fields:

Parameter	Description
Domain Name	The fully qualified domain name (FQDN) of your server. This must match exactly what you type in your web browser or you will receive a name mismatch error. For example **.google.com, mail.google.com*.
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC, for example *My Spy Company, Inc.*.
Department	The division of your organization handling the certificate.
City	The city where your organization is located.
State/Province	The state/region where your organization is located. This should not be abbreviated, for example *Califiornia*.
Country	Select the country in which your organization is located from the dropdown list.
Private Key Password	Enter the password that will encode the private key. This is not mandatory but recommended.
Private Key Password Confirmation	Reenter the password for confirmation.

3. Click the **1 Save Private Key** button.

   The private key is now saved in a text file on your computer.

4. Click the **2 Save CSR** button.

   The CSR is saved in a text file on your computer. It is this file that needs to be sent to your certificate provider.

5. Click **Close** to close the window

Your private key and all required information are now saved on your commputer. Now you need to send the saved CSR file to your certificate provider who normally will send you the final certificate in an email that should also contain download links to the root and intermediary certificates required for installing the SSL certificate on Asset Core.

Note

Be aware that it may take quite a while for you to receive the certificate and can thus continue to install it.

Installing the SSL Certificate

Once you have received the certificate you need to install it in Asset Core before it can be used for the external integration with RF:

1. Click the **Install Certificate** icon.

   The **Install Certificate** window appears on the screen.

2. Enter into this field a unique name for the new SSL certificate.
3. To enter the required data into the **Root Certificate** field click the **...** button.

   You may also enter the required data into these fields by opening the respective files in a text editor and copying their content into the respective fields.

   An **Open** window appears on the screen.
4. Select the file that contains the root certificate.
5. Click the **Root Certificate**. **Open** button.

   The content of the selected file is copied to the respective field.
6. Repeat the preceeding steps for the **Intermediate Certificates** and **Final Certificate** fields.

   The **Intermediate Certificates** is optional and may remain empty if no **Intermediate Certificates** exists.
7. To display the details of a certificate, for exampel to verify if the selected certificate is the correct one click the **Details** button.

   A **Certificate Details** window appears showing the contents of the certificate in readable format.
8. Repeat the preceeding steps for the **Private Key** field.
9. If a password was defined for the private key in the certificate request preparation you need to enter it here as well. If not password was defined this field may remain empty.
10. Once all data is filled in the **Install Certificates** button becomes available. Click it.

    A **Information** window appears on the screen, with the result of the certificate installation. This may either be *The SSL certificate was successfully installed.* or an error message is displayed detailing the problem causing the error.

The required SSL certificate is now installed and Asset Core is ready for integration with BMC Remedyforce.

Defining the Web Service

To define the web service for use with the BMC Remedyforce integration proceed as follows:

1. Go to the **Global Settings** > **External Integration** > **Configuration** node.
2. Double-click an entry in the table or click the **Properties** icon.

   The **Properties** window appears on the screen.
3. Fill the required information into the respective fields:

Parameter	Description
Enable Web Service	Check this box to enable the web service defined below.
Web Service Port	Enter the number of the port on which the web service is running.
Web Service Thread Count	Enter the number of threads that may be handled simultaneously.
Web Service SSL Certificate File	Enter the path to the location where the certificate and private key for authentication of the web service

Parameter	Description
	are stored, for example *c:tempcertificates* or *../data/HttpProtocolHandler/certs*.

4. Click **OK** to confirm the web service.

Defining Integration with BMC Remedyforce

To create a new integration with BMC Remedyforce proceed as follows:

1. Go to the **Global Settings** > **External Integration** node.
2. Select **Edit** > **Create BMC Remedyforce Integration** .

   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example Remedyforce integration for help tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one.
Application Login	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one. Be aware that the administrator must be a valid Asset Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services will be called. To verify that the entered link is correct click the **Check Connection** button to the right.
Secure Communication	Check this box to activate secured connections with the integrated product.
Language	Select the language in which the incidents will be created in the application. All Console languages are available for this choice.

4. In the list below check the boxes for all events for which an incident ticket is to be created in BMC Remedyforce.

   You will also receive an event notification by email for each incident ticket that is created.
5. Click **OK** to confirm.

BMC FootPrints Asset Core is now set up for sending alert notifications to BMC Remedyforce and creating incident ticket.

Setting Up External Integration with BMC FootPrints Service Core

When setting up integration between BMC FootPrints Asset Core and BMC FootPrints Service Core you need to execute some specific configurations for both applications. This paragraph guides you through the necessary steps in Asset Core. For information on how to ocnfigure BMC FootPrints Service Core for integration refer to chapter *Integrating the BMC FootPrints Service Core CMDB with BMC FootPrints Asset Core* in the *BMC FootPrints Service Core - Asset Core Integration Guide* guide.

- Define External Integration with BMC FootPrints Service Core

Defining Integration with BMC FootPrints Service Core

To create a new integration with BMC FootPrints Service Core proceed as follows:

1. Go to the **Global Settings** > **External Integration** node.
2. Select **Edit** > **Create BMC FootPrints Integration** .

   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example Remedyforce integration for help tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one.

4. Click **OK** to confirm.

BMC FootPrints Asset Core is now set up for exporting data to BMC FootPrints Service Core and creating incident ticket.

Tracking Shared Events

Asset Core Administrators may track all events that are shared with other software products via the **Alerts and Events** node. All events that are available for external integration are part of the **Alert & Event** event log modell.

This view provides the following selection options which may be combined for the display. When opened the table of this node is empty. To launch the display click the **Find** button:

Parameter	Description
Model Name	Select from this dropdown list the type of event log model for which to display the logged events, for this case you always need to select the **Alert & Event** option.

Parameter	Description
Status	Select in this field the status value for which the logged events are to be displayed.
Start Date	Select in this field the date from which on the logged events are to be displayed.
End Date	Select in this field the date up to which the logged events are to be displayed.

The table displays the following information for all alerts and events that may be shared and tracked with other applications.

Alert & Event

The **Alert & Event** model logs agent operation events, such as events and alerts generated by operational rules, by the inventory module, security alerts, and so on. It shows the following information for each event:

Parameter	Description
Device Name	The name of the device to which the alert is related.
Event Date	The date and time the alert occurred in the default time format.
Status	Displays the current status of the event. • **Acknowledged Alert**: The administrator received the alert notification and has already acknowledged it. • **Unacknowledged Alert**: The administrator received the alert notification but has not yet acknowledged it. • **Notified Alert**: The alert notification was sent but the alert has not yet been acknowledged. • **Unnotified Alert**: An alert occurred but its notification has not yet been sent. • **Closed**: The problem that caused the alert was resolved and the alert is now closed.
Severity	Defines the severity of the selected alert, **Error, Information** or **Warning**.
Category	Defines the type of event that is being logged.
Sub-category	The alert sub-category to which the alert/event was assigned. This value can be freely defined by the administrator.
Description	Displays the textual description of the alert/event.
Shared	Shared
Acknowledged by	The name of the administrator who acknowledged the event.
Last Modified By	Displays the name of either the last person that last modified the object or its contents, such as the administrator, or it may be the system that last executed any modifications.
Notes	This free text field may contain any additional information concerning the selected object.

Filtering Alerts and Events

This view always only shows the alerts and events logged for a specific event log model. To display the events and alerts of another model or to further limit the displayed list to those of a specific status or timeframe proceed as follows:

1. Select the desired event log model from the **Model Name** dropdown box.

   To filter for a specific status of the current model do not modify this selection.

2. You can further filter the alerts and events of the selected model according to the following criteria:

   - Select a specific status value from the **Status** dropdown box to display only alerts/events of a specific status type.
   - To filter for events of a specific timeframe select the start and end date of the desired timeframe in the respective fields.

   You may use only one criteria for filtering or you can use a combination of them.

3. Then click the **Find** button.

The table will refresh and display only those alerts/events that comply with the selected criteria.

Purging Alerts and Events

Alerts and events may be purged. Be careful when using this operation, ALL alerts and events of this event log model for the current device/devide group will be irrevocably deleted from the database.

1. Click the **Purge** button.

   A confirmation window appears on the screen.

2. Click **Yes** to confirm.

   Another confirmation window appears on the screen if one or more of the selected alerts/events has a connected incident ticket in BMC Remedyforce.

3. If the incident tickets that were created in BMC Remedyforce should be closed at the same time click **Yes** otherwise click **No**.

All alerts and events will be deleted from the database and, if requrested, the status of the connected incident ticket(s) in BMC Remedyforce will be changed to `Closed`.

Deleting Individual Alerts and Events

It is possible to delete individual alerts and events that are no longer required.

1. Select the alert(s)/event(s) to delete in the table to the right.
2. Click **Edit** > **Delete** .

   A confirmation window appears on the screen.

3. Click **Yes** to confirm.

   Another confirmation window appears on the screen if one or more of the selected alerts/events has a connected incident ticket in BMC Remedyforce.

4. If the incident tickets that were created in BMC Remedyforce should be closed at the same time click **Yes** otherwise click **No**.

All selected alerts and events will be deleted from the database and, if requrested, the status of the connected incident ticket(s) in BMC Remedyforce will be changed to `Closed`.

Creating a BMC Remedyforce Integration for a Specific Event

If in the list of all available alerts and events you find that you need integration for a specific alert, you can also set up the external integration for the alert in question directly from this node.

1. Select the event in the table for which a new external integration is to be defined.
2. Select **Edit** > **Create BMC Remedyforce Integration** .

   The **Properties** dialog box appears on the screen.
3. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example Remedyforce integration for help tickets.
Application Type	The product for which to create the integration. In this case this field is preselected and cannot be modified.
Integration Administrator	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one.
Application Login	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one. Be aware that the administrator must be a valid Asset Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services will be called. To verify that the entered link is correct click the **Check Connection** button to the right.
Secure Communication	Check this box to activate secured connections with the integrated product.
Language	Select the language in which the incidents will be created in the application. All Console languages are available for this choice.

4. In the list below the notification box for the selected event is already prechecked.

   If required you can check further events for notification for this integration.
5. Click **OK** to confirm.

The new external integration to BMC Remedyforce will immediately created and activated. This means that from now on the administrator will receive a notification whenever this type of event occurs and an incident ticket will automatically be created in BMC Remedyforce.

Knowledge Center

The instructions in the preceding chapters enable you to set up and define external integrations for other applications.

In the Knowledge Center you find information on the individual functionalities and objects connected with external integration.

External Integration

The **External Integration** node under the global settings allows you to define the integrations with other software products, such as BMC Remedyforce and BMC FootPrints Service Core.

From this view you can access the web services configuration as well as the definitions of all already defined external integrations via the respective subnode.

Web Service Required for External Integration

For the external integration with BMC Remedyforce to work a web service is required. This view allows you to define and modify the service.

It provides the following information on any defined service:

Parameter	Default Value	Description
Enable Web Service	**No**	This value indicates if the web service defined below is enabled.
Web Service Port	1619	The number of the port on which the web service is running.
Web Service Thread Count	10	The number of threads that may be handled simultaneously.
Web Service SSL Certificate File		The path to the location where the certificate and private key for authentication of the web service are stored, for example *c:tempcertificates* or *../data/HttpProtocolHandler/certs*.

Configuring the Web Service

To configure the web service for use with the BMC Remedyforce integration proceed as follows:

1. Double-click an entry in the table or click the**Properties** icon.

   The **Properties** window appears on the screen.

2. Fill the required information into the respective fields:

Parameter	Description
Enable Web Service	Check this box to enable the web service defined below.

Parameter	Description
Web Service Port	Enter the number of the port on which the web service is running.
Web Service Thread Count	Enter the number of threads that may be handled simultaneously.
Web Service SSL Certificate File	Enter the path to the location where the certificate and private key for authentication of the web service are stored, for example *c:tempcertificates* or *../data/HttpProtocolHandler/certs*.

3. Click **OK** to confirm the web service.

Creating a New External Integration to BMC FootPrints Service Core

To create a new integration with BMC FootPrints Service Core proceed as follows:

1. Select **Edit** > **Create BMC FootPrints Integration** .

   The **Properties** dialog box appears on the screen.

2. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example Remedyforce integration for help tickets.
Application Type	The product for which to create the integration.
Integration Administrator	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one.

3. Click **OK** to confirm.

Creating a New External Integration to BMC Remedyforce

To create a new integration with BMC Remedyforce proceed as follows:

1. Select **Edit** > **Create BMC Remedyforce Integration** .

   The **Properties** dialog box appears on the screen.

2. Fill the required data into the following fields:

Parameter	Description
Instance Name	The name of the external integration, for example Remedyforce integration for help tickets.
Application Type	The product for which to create the integration.

Parameter	Description
Integration Administrator	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one.
Application Login	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one. Be aware that the administrator must be a valid Asset Core administrator.
Application Password	Enter the corresponding password.
Application URL	Enter the URL to the web server from which the soap services will be called. To verify that the entered link is correct click the **Check Connection** button to the right.
Secure Communication	Check this box to activate secured connections with the integrated product.
Language	Select the language in which the incidents will be created in the application. All Console languages are available for this choice.

3. In the list below check the boxes for all events for which an incident ticket is to be created in BMC Remedyforce.

   You will also receive an event notification by email for each incident ticket that is created.

4. Click **OK** to confirm.

External Integration to BMC Remedyforce

Defining an integration to BMC Remedyforce allows the administrator to define a number of events for which he wants to receive notifications and for which at the same time, incident tickets are created in BMC Remedyforce, that can be followed in that software.

This view displays its information via the following two tabs:

- *General*
- *Notification Events*

Events Defined for Notification

This tab lists all events that are available for notification and their status, that is, if they are defined for notification:

Parameter	Description
Events	This column lists all alerts that are available for notification.
Enabled	This column indicates if the respective alert is selected for notification.

General Information

This tab shows the information required by the external integration:

Parameter	Description
Instance Name	The name of the external integration, for example BMC Remedyforce integration for help tickets.
Application Type	Application Type
Integration Administrator	The name of the administrator for which the integration is created.
Application Login	The login name with which Asset Core is to establish the connection with the application.
Application Password	The corresponding password.
Application URL	The URL to the web server from which the soap services will be called.
Secure Communication	This field indicates if secure connections are used for the data exchange with the integrated product.
Language	The language in which the incidents will be created in the application.

External Integration to BMC FootPrints Service Core

Defining an integration to BMC FootPrints Service Core allows the administrator to receive notifications for a number of events and for which at the same time incident tickets are created in BMC FootPrints Service Core, that can be followed in that software.

This view displays the following information for the defined integration:

Parameter	Description
Instance Name	The name of the external integration, for example BMC Remedyforce integration for help tickets.
Application Type	Application Type
Integration Administrator	Enter the name of the administrator for which the integration is created, or click the **Select Administrator** icon to the right to select an existing one.

Events Available for Notification in BMC Remedyforce

Asset Core Application

The events and alerts of this section are concerned with the general workings of the Asset Core agents and licensing problems.

Parameter	An event notification is generated whenever
Error detected on Asset Core Agent	the agent on a client or relay has a problem executing correctly or has stopped working. The alert will automatically be closed once the agent is executing again properly.

Parameter	An event notification is generated whenever
Error detected on Asset Core Master	the agent on the master has a problem executing correctly or has stopped working. The alert will automatically be closed once the agent is executing again properly.
FootPrints Asset Core license expired	a BMC FootPrints Asset Core license that you have purchased passes its expiry date. The alert will automatically be closed once the respective license is valid again.
FootPrints Asset Core license exceeded	a BMC FootPrints Asset Core license that you have purchased exceeds its number of allowed objects created in the database. The alert will automatically be closed once the respective license is valid again.

Discovery and Inventory

The events and alerts of this section are concerned with the individual devices in the network and their agent and connection status.

Parameter	An event notification is generated whenever
New device without agent discovered	a new device was discovered in your network on which no Asset Core agent is installed.
A computer or device lost contact	a device in your network has lost contact with its parent or is in general not reachable. The alert will automatically be closed once the device is contactable again.

Applications and Application Licensing

The events and alerts of this section are concerned with application license monitoring and prohibited managed applications.

Parameter	An event notification is generated whenever
Software license count maximum exceeded	an application is newly installed on a device but there are no more licenses for it available. The alert will automatically be closed once the respective application license is valid again, that is, additional licenses were purchased or the application was removed from the device.
Software license expiration date exceeded	an application with a time license is found on at least one device in your network of which the final license date has expired. The alert will automatically be closed once the respective application license is valid again.
Underinstalled licensed software	an application is found for which there are still licenses available, that is it can still be installed on more devices. The alert will automatically be closed once all available licenses of the application are installed.

Parameter	An event notification is generated whenever
Software license count threshold exceeded	the installed application base appproaches the specified threshold from which on notification is required. For example, if 100 licenses are available and the threshold is set to 80%, an alert will be generated when the application is installed for the 80th time. This may be the time to consider purchasing additional licenses. The alert will automatically be closed once the installed application base falls below respective application license threshold again, that is, additional licenses were purchased or the applications were uninstalled, for example, from devices on which they are no longer required.
A prohibited application was started	an application is started on a device on which its execution is prohibited.

Compliance

The events and alerts of this section are concerned with

Parameter	An event notification is generated whenever
All defined compliance alerts	an alert that was defined for device compliance is generated. Many of these alerts may be closed automatically once the criterion that caused the alert on the device matches its requirements. For more information on the available alerts and how to define them refer to the *BMC Compliance Manager* manual.

Agent-based Monitoring

In this section you can select which operations rule steps are to send event notifications when they are generating alerts.

Parameter	An event notification is generated whenever
Check URL Availability	the step finds that the URL that it verified is not reachable. Once the step finds the URL reachable again the alert is closed automatically. If the URL in the step is changed, the first alert is closed automatically and a new alert is generated if the new URl is not reachable either.
Check Windows Events	the step finds a Windows event entry that contains either the specified string or has the specified event ID.
Check Running Process	the step either does not find the specified process or could not terminate it, if this was requested. The alert will automatically be closed once the process can be found (and terminated).
Advanced Process Execution Check	the step does not find the specified process. The alert will automatically be closed once the process can be found.
Generate Custom Alert	a custom alert is generated by the step.
File Analysis via Regular Expression	the step finds a match for the specified regular expression in the listed files.

Parameter	An event notification is generated whenever
Check Installed Software	the step does not find the specified software installed on the target. The alert will automatically be closed once the specified softwrae is found intalled on the target.
Advanced Installed Software Check	the step does not find the specified software installed on the target. The alert will automatically be closed once the specified software is found intalled on the target.
Service Execution Check	the step finds that a process that it has verified is not running. The alert will automatically be closed once the specified service is found executing.
Low Disk Space	the step finds that the free disk space has fallen under the defined percentage limit on the target device. The alert will automatically be closed once the step finds enough free disk space.
Check Disk Space	the step finds that there is less free disk space on the target device than defined in the step. The alert will automatically be closed once the step finds enough free disk space.
The total size of the memory has changed	the total size of the memory on a specified device has changed.