OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Application Administration

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Application Administration

Version 6.2

Document Release Date: July 6, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
Application Administration

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

AMLIB_CAPP6.2/01

Table of Contents

PART V: ADMINISTERING THE SIEBEL SOLUTION

PART VI: ADMINISTERING THE SOA SOLUTION

PART VII: APPENDIXES

Welcome to Application Administration

This guide provides detailed instructions on how to configure and administer Mercury Business Availability Center applications.

How This Guide Is Organized

The guide contains the following parts:

Part I Dashboard Administration

Describes how to use Dashboard Administration to configure and customize the Dashboard application, and how to install and administer the Deep Transaction Tracing feature.

Part II Service Level Management Administration

Describes how to create service level agreements (SLAs) that represent the formal and informal contracts you have with your service providers and with internal business units.

Part III End User Management Administration

Describes how to configure transaction order and color settings as well as report filters.

Part IV Administering the SAP Solution

Describes how to install the SAP solution, the specific tasks involved in administering it, how the SAP discovery package discovers SAP-related CIs and general CIs (such as hosts) that are related to them, and provides information that can help troubleshooting Mercury Business Availability Center SAP solution.

Part V Administering the Siebel Solution

Describes how to administer Mercury Business Availability Center Siebel solution, the specific tasks involved in administering it, how the Siebel discovery package discovers Siebel-related CIs and general CIs that are related to them, and provide information that can help troubleshooting Mercury Business Availability Center Siebel solution.

Part VI Administering the SOA Solution

Describes the tasks to perform in Mercury Business Availability Center To monitor your Service-Oriented Architecture (SOA) enterprise environment.

Part VII Appendixes

Describes how to register Mercury Diagnostics with Mercury Business Availability Center and how to integrate Diagnostics with Mercury Business Availability Center.

Who Should Read This Guide

This guide is intended for the following users of Mercury Business Availability Center:

- Mercury Business Availability Center administrators
- Mercury Business Availability Center platform administrators
- Mercury Business Availability Center application administrators
- Mercury Business Availability Center data collector administrators

Readers of this guide should be knowledgeable about enterprise system administration and highly knowledgeable about Mercury Business Availability Center.

Getting More Information

For information on using and updating the Mercury Application Management Documentation Library, reference information on additional documentation resources, typographical conventions used in the Documentation Library, and quick reference information on deploying, administering, and using Application Management, refer to *Getting Started with Mercury Business Availability Center*.

Part I

Dashboard Administration

1

Introducing Dashboard Administration

Dashboard Administration enables you to set up Dashboard so that your users can view significant data about the entire system in the Dashboard application.

Dashboard Administration includes the following chapters:

- Chapter 2, “Configuring KPIs” describes how to edit the Key Performance Indicators (KPIs) attached to a configuration item (CI), and to attach new KPIs to CIs, in the KPIs tab.

  The KPIs you create are displayed in Dashboard to help the user monitor how well the business is achieving its objectives and assess the business impact of problems in the system.

- Chapter 3, “Configuring CI Status Alerts” describes how to create alert scheme and attach them to CIs in a view, and to edit those alert schemes, in the CIs Status Alert tab.

  When an alert occurs, send alert messages (notifications) to the recipients, and executes the actions and executable files defined for the alert scheme.

- Chapter 4, “Configuring the Custom Map” describes how to create an association between a custom image that represents a view and real-time data, in the Custom Map tab.

  The custom map you create allows the user to view real-time data on a map or diagram that represents the view.

- Chapter 5, “Configuring the Geographical Map” describes how to create an association between geographical locations and status indicators using a map applet, in the Geographical Map tab.

The geographical map you create allows the user to view real-time data at the geographical location assigned to each CI.

- Chapter 6, "General Administration for Dashboard" describes some of the settings that can be modified to customize Dashboard and logs that you can use to verify that Dashboard is running properly.
- Chapter 7, "Administering Deep Transaction Tracing" describes how to install and manage Deep Transaction Tracing.

  The Deep Transaction Tracing feature is a monitoring layer that collects more information about the behavior of Business Process Monitor transactions as they run in an external server.

2

Configuring KPIs

The **KPIs** tab in Dashboard Administration enables you to edit the KPIs attached to a CI, and to attach new KPIs or delete KPIs.

Introducing KPI Configuration

The Dashboard KPIs (Key Performance Indicators) provide quantifiable measurements that help you monitor in real-time how well your business is achieving its objectives. The KPIs provide real-time status for the CIs representing your business and processes, enabling you to assess the business impact of problems in the system.

Each KPI works with a predefined set of values, against which the incoming metrics are measured. The resulting measurement for the KPI is translated into a color-coded status indicator, displayed in the Dashboard Console, where the color represents a more desirable or less desirable condition for the KPI. You can learn more about KPI functionality in "How Dashboard KPIs Work" on page 9.

CIs can have multiple KPIs attached. KPIs can be attached to a CI as follows:

- KPIs may be attached to the CI as part of the CI creation.
  - For CIs created by the source adapters in Source Manager, all CIs are automatically assigned default KPIs, according to the nature of the CI. For example, a CI for a Business Process Monitor profile has default KPIs for availability and performance. For more information on the source adapters and how they define the default KPIs, see *Source Manager Administration*.
  - CIs that are added manually or by Discovery Manager do not have automatically assigned KPIs. For information on how Discovery Manager creates CIs, see *Discovery Manager Administration*.
- KPIs may be attached to a CI as a result of propagation from child CIs. Most KPIs propagate up through the hierarchy, so that parent CIs have the same KPIs as all their child CIs.
- KPIs may be manually attached to a CI in the Dashboard Administration KPIs tab. You may want to attach new KPIs to a CI, in addition to the default/propagated KPIs, to broaden the information derived from the monitoring measurements. For example, you can add an OT Impact KPI to assess the ongoing cost of an application that is not available.

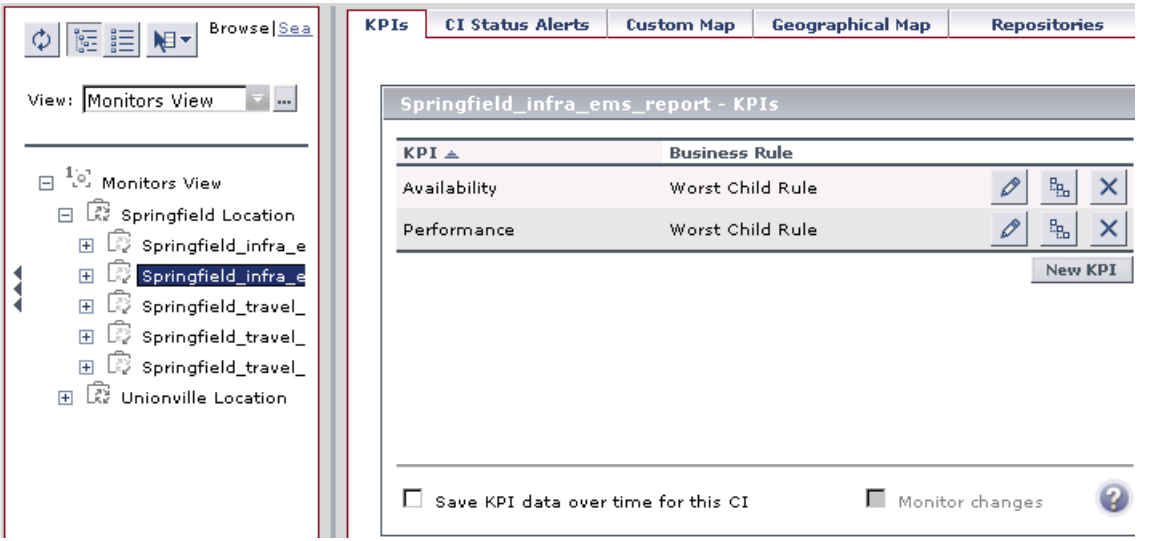
  In the KPIs tab, as well as attaching new KPIs to a CI, you can edit existing KPIs and delete attached KPIs.

Notes and Limitations

- Any change you make to the KPIs for a CI—adding new KPIs, deleting KPIs, or editing KPI properties—will change the CI in the Mercury Universal CMDB, meaning that the changes will be seen in any view that the CI appears.
- You must create at least one Mercury Business Availability Center profile database in order for Dashboard to receive data samples. For details on how to do this, see "Database Administration" in *Platform Administration*.
- There are no restrictions on the type of KPI that can be attached to a CI, or on the type of business rule that you can select from the allowed rules list for a KPI. You must ensure that you select KPIs and business rules that are appropriate for the CI type.
- The Application KPI is only applicable for CIs corresponding to Mercury Diagnostics (and is attached automatically to Mercury Diagnostics CIs when Mercury Diagnostics is supported in Mercury Business Availability Center). For more information, refer to the *Mercury Diagnostics User's Guide*.
- KPIs that are added to a CI as part of a SLA definition in Service Level Management Administration have no relevance to the Dashboard KPIs and do not appear in the KPIs tab. Conversely, KPIs added to a CI in the KPIs tab have no relevance for the CI when it is included in an SLA, and do not appear for the CI in Service Level Management.
- Deleting a KPI may impact on other KPIs that are dependant on the first KPI. For example, OT Impact is calculated based on the status of another KPI, such as Availability; in this case, deleting the Availability KPI would prevent calculation of OT Impact.
- KPIs that were created for CIs by the source adapter templates, frequently have objective values that differ from the default ones used by the business rule. However, when editing one of these KPIs, if you select a different rule and then revert to the original rule, then the original objective values are replaced with the rule default values.

Working with the KPIs Tab

The right pane of the KPIs tab contains the KPIs table, displaying a list of the KPIs and associated business rule defined for the selected CI.



To see the KPI information, you select the required view and then the required CI in the View Explorer in the left pane. (For information on using View Explorer, see "Using View Explorer" in *Working with the CMDB*.)

From the KPIs tab, you can:

- Attach new KPIs to one or more CIs, as described in "Attaching New KPIs to CIs" on page 13.
- Edit an existing KPI for a CI (or for multiple transaction CIs), as described in "Editing KPI Properties" on page 23.
- Delete a KPI attached to a CI, as described in "Deleting KPIs Attached to a CI" on page 31.
- Set Mercury Business Availability Center to save KPI data for CIs, as described in "Saving KPI Data over Time for a CI" on page 32.
- Set Dashboard to monitor (in real-time) changes made to the properties for a selected CI, or to the child CIs for the selected CI, as described in "Real-Time Monitoring of CI Property Changes" on page 36.

Tip: You can sort the information displayed in the KPIs table by clicking on the column header. You can switch the column between ascending and descending order by clicking the header again.

How Dashboard KPIs Work

Mercury Business Availability Center provides a selection of predefined KPIs to work with Dashboard. The templates for the KPIs are defined in an XML file, which contains the default parameters for creating each KPI instance.

Note: You can edit the KPI templates, or create customized KPI templates, in the KPIs Repository, as described in "Dashboard KPIs Detailed Description" in *Repositories Administration*.

Each CI has its own attached KPIs (that define what is being monitored for that specific CI). Each attached KPI generally defines:

- the business rule (for example, Performance rule) to be used with the collected metrics, to calculate a measurement for the KPI.
- the source for the metrics to be used for the KPI: either from data samples (for monitoring CIs), or from other KPIs. In the latter case, the KPI metrics may be taken from the child CIs (when using, for example, the Summary of Values rule), or from another KPI attached to the same CI (when using, for example, the Impact Over Time rule).
- the thresholds (objective values) that the KPI measurement is compared against; and the status (color) allocated to the KPI, based on the defined thresholds.
- where and how to display the status indicator for the KPI in Dashboard, and where to store the KPI measurement.

For most KPI types, the KPIs propagate up to all parent CIs (there are exceptions to this, for example, the PNR (Service Level Management) KPI). This means that if you attach a KPI, for example, Volume, to a child CI, then a Volume KPI is also added to each parent CI for that child, up to the top of the subtree.

Each KPI added by propagation has its own KPI instance definition, with its own business rule and properties. For example, the Volume KPI for a child CI may use the RUM Page Monitor Volume Rule, while the Volume KPI for the parent CI (added by propagation from the child CI) may use Worst Child Rule.

The calculations required by the KPI business rule are performed by the Business Logic Engine. When a data sample arrives on the Bus and is identified (by means of the KPI selector) as relevant for a specific monitoring CI, the required metrics are passed to the relevant KPI instance for that CI, for example, an Availability KPI. At regular intervals (default 15 seconds) the Business Logic Engine recalculates the measurement for the KPI using the metrics received for the KPI since the last calculation.

If the new measurement causes a change in the status of the KPI, the new status is passed to the parent CIs. The Business Logic Engine then recalculates the measurement for the corresponding KPI of each parent CI, using the new received status information. If the new measurement causes a change in the status for that KPI, the new status is again passed up the hierarchy to the corresponding KPI instances for the parent CIs, and so forth.

Note: You can change the default Business Logic Engine calculation time interval in the Infrastructure Settings page. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Foundations**, select **Online Business Logic Engine**, and locate the **Model calculation interval** entry in the **Calculation Related Settings** table. Edit the value as required.

About Business Rules

A KPI must always have an associated business rule that defines the logic to be performed (by the Business Logic Engine) to calculate the measurement for the KPI. The properties and objectives that are assigned to the KPI depend on the selected rule.

Mercury Business Availability Center provides predefined rules for use with the KPIs. The rules are defined in the Business Rules Repository, where you can edit the rules, or create customized rules. For information on the business rules available in Dashboard, the roles they play, and how to edit them, see "Business Rules Repository" in *Repositories Administration*.

Some business rules are specific to a particular KPI, while others can be used for a variety of KPIs. In the KPIs Repository, each KPI has a defined default rule, and a list of rules that can be used with that KPI. (If required, the default rule and the allowed rule list can be modified. For details, see Chapter 2, "Configuring KPIs.")

When a CI is created by the source adapters in Source Manager, it is assigned KPIs and business rules according to the adapter definitions. When a KPI is added manually to a CI in the KPIs tab, it is assigned the default business rule defined for the KPI (the default rule is usually a rule for groups). For example, for the **RT Impact** KPI, there are two applicable rules: **Real Time Impact Rule** and **Sum of Values Rule**. When you add a new RT Impact KPI to a CI, the default rule for the KPI, Sum of Values Rule, is automatically assigned. You can change the assigned rule when adding or editing the KPI in the KPIs tab, by selecting a new rule from the list of allowed rules for the KPI.

There are two categories of business rule, **monitor rules** and **group rules**, as described in the following sections. Most KPIs work with at least one rule from each category.

This section includes the following topics:

Monitor Rules

Monitor rules (also called leaf rules) are business rules that are applied to leaf CIs of monitor type. Monitor rules are used to calculate a measurement for the KPI based on original sample data that is caught by the KPI selector. For example, the **Availability Rule** calculates the Availability KPI for BPM Transaction from Location CIs, based on the sample data received from Business Process Monitor.

A monitoring CI is intended to receive incoming metrics, generally received via one of the data collector, such as SiteScope, Business Process Monitor, or Real User Monitor. Monitoring CIs are automatically added to the Mercury Universal CMDB by the source adapters in Source Manager, according to the monitoring definitions. These monitoring CIs have default KPIs that use a monitor rule, and predefined selector.

In general, the leaf CIs in a subtree (the CIs that form the lowest level of the hierarchy) should always be one of the monitoring CIs. When creating new subtrees in your views in IT Universe Manager, you attach monitoring CIs created by the source adapters as leaf nodes, and these CIs then pass KPI status up the hierarchy.

Group Rules

Group rules are business rules that determine KPI status based on data received from other KPIs, rather than from original sample data. The received data may come from the KPIs of child CIs, or from another KPI associated with the same CI.

Note: Even though this category are called *group* rules, some of them are also applicable for monitoring/leaf level CIs. For example, the **Impact Over Time Rule** (used with the **OT Impact KPI**) can be used with a group CI or a monitoring CI. What all rules in this category have in common is that their status calculations are contingent on data received from other KPI instances, rather than from the samples.

The group rules vary in the type of logic they use to arrive at a status result. For example:

- the rule may select a KPI status held by one of the child CIs, and apply that status to the parent, as done by the **Worst Child Rule**.
- the rule may aggregate the received data to calculate a measurement, and compare the measurement with defined objectives, as done by the **Sum of Values Rule**.
- the rule may calculate a measurement based on the status of another KPI for the CI, and compare the measurement with defined objectives, as done by the **Real Time Impact Rule** when receiving status from the **Availability** KPI.

Attaching New KPIs to CIs

You can attach new KPIs to any CI. There can be only one instance of each KPI for a CI. For each new KPI, you define the KPI type and business rule. Where relevant, you also define additional information required by the rule.

Dashboard Administration also gives you the option of attaching a KPI to multiple CIs. The KPI will be added to all CIs that do not already have that KPI attached. All instances of the KPI will have the same defined business rule and properties. The procedure for attaching to multiple CIs is defined on page 19.

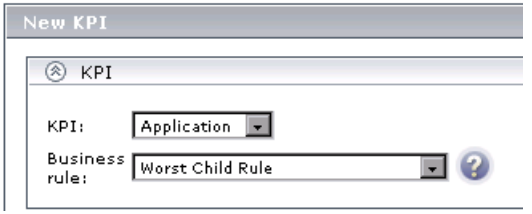
For information on KPI functionality, see "How Dashboard KPIs Work" on page 9.

The actions of attaching a new KPI to a CI, and defining the KPI properties, must be undertaken with care; these actions can result in KPIs that give an inaccurate performance assessment in Dashboard. Please read the "Notes and Limitations" on page 7 before proceeding.

To attach a new KPI to a single CI:

1. Access the **KPIs** tab and select the required CI in View Explorer.
2. Either click the **New KPI** button in the right pane, or right-click the CI in View Explorer and select **Add KPI**. The New KPI window opens, displaying the **KPI** area.

3 In the **KPI** area, select the required options:



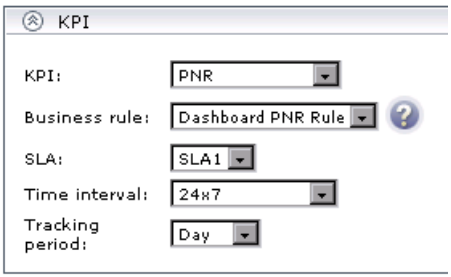
- Select a KPI from the **KPI** list. The list contains the names of all available KPIs (KPIs that are already attached to the CI are not included in the list). For an explanation of each individual KPI, see "Dashboard KPIs Detailed Description" in *Repositories Administration*.
- After selecting a KPI, the **Business rule** list is automatically updated to display all business rules that are relevant for the selected KPI. Select the required rule from the list. The rule is used to calculate the measurement and status for the KPI. For an explanation of the role of the rules, see "About Business Rules" on page 11. For information on each individual rule, see "Dashboard Business Rules Detailed Description" in *Repositories Administration*.

Hold the pointer over the question mark icon to display additional information for the rule.

Note: You should only select a monitor rule if the KPI is attached to a monitoring CI. For more information, see "Monitor Rules" on page 12.

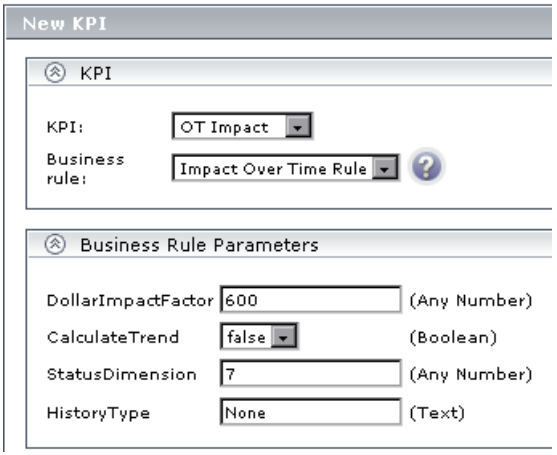
After selecting a rule, the New KPI window is automatically updated to display the areas (**Business Rule Parameters**, **Objectives**, **Selector**) that are relevant for the selected rule.

➤ If you are defining a **PNR** KPI, select the required values from the **SLA**, **Time interval**, and **Tracking period** lists.



For information on defining the PNR KPI, see "Attaching a PNR KPI to a CI" on page 20.

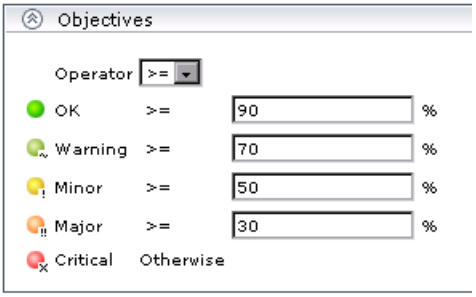
4 Expand the **Business Rule Parameters** area to view the parameters relevant for the selected rule. All parameters have default values.



If required, modify the parameter values by entering a new value in the appropriate boxes. The information after each box directs you as to the type of value that can be entered, for example, **Any Number**, **Text**, or **Boolean**.

For information on rule parameters and possible values, see the section for the relevant rule, as described in "Dashboard Business Rules Detailed Description" in *Repositories Administration*.

5 If relevant for the selected rule, the **Objectives** area is displayed in the window.



The **Objectives** area define value ranges that will be used to determine status for the KPI. The measurement for the KPI (calculated by the business rule) is compared with the objectives, and a color status assigned accordingly.

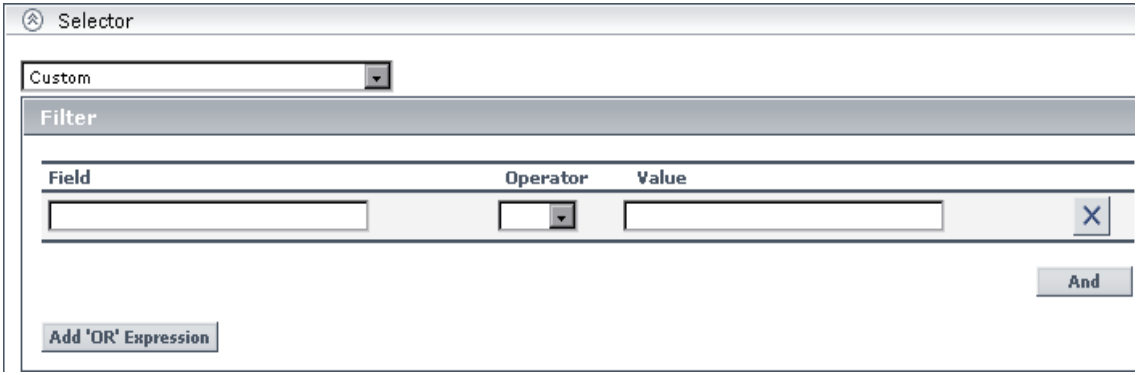
The objectives are defined in a unit of measurement appropriate to the type of data dealt with by the rule. The unit is indicated after the objective value box.

If required, you can modify the default values for the objectives:

- Select the required operator from the **Operator** list. This operator is applied for all objectives.
- Enter the required objective value for each status in the appropriate box. Make sure that the numbers you enter are logically ordered.

For more information on objectives functionality and defining objectives, see “KPI Objectives” on page 38.

6 If relevant for the rule, the **Selector** area is displayed in the window. This area is displayed only for certain monitor rules and for Dynamic Node Factory CIs.



The **Selector** area defines the filter criteria for the KPI. The selector catches data samples from the incoming data that meet the filter criteria. A selector is required for all KPIs (attached to monitoring/leaf CIs) that are intended to calculate a measurement based on original sample data; otherwise no data will be mapped to the KPI and it will remain gray in Dashboard.

Steps 7 to 9 give the basic procedure for defining a selector. For a detailed explanation of selector functionality and defining selectors, see "Selectors for KPIs" on page 46.

Note: If you do not define a selector for the KPI, then after clicking **OK** to close the New KPI window, Mercury Business Availability Center automatically assigns to the KPI the default selector (generally defined for the other KPIs attached to the monitoring CI).

---

7 Selector filters can be manually defined to create a custom filter, or defined using metadata (predefined sample types). If you want to use metadata for the filter, select a sample type from the list at the top of the **Selector** area.

Note: When the list displays **Custom**, the filter is defined manually.

For more information, see "Using Predefined Sample Data for Selectors" on page 51.

8 In the **Filter** area, define selector expressions to create a filter for the selector. Each selector expression defines a required criteria for the new KPI.

Define a single selector expression as follows:

- In the **Field** box, define the name of a reference property contained in the incoming sample.
- Select an option from the **Operator** list.
- Enter the required value for the property in the **Value** box.

For more information, see "Defining Selector Expressions" on page 48.

9 You can define additional selector expressions to build a more complex filter:

- You can attach additional selector expressions to the first selector expression using the **And** button, to create an expression block that narrows the filter.
- You can create additional expression blocks (each containing one or more selector expressions) using the **Add 'OR' Expression** button, to widen the filter.

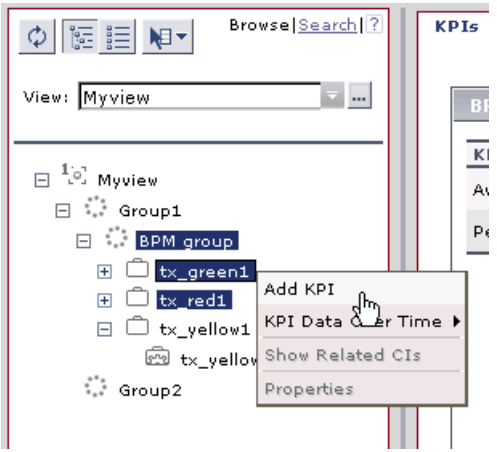
For more details, see "Building Complex Filters" on page 49.

10 Click **OK** to close the New KPI window. The new KPI is added to the KPI list for the CI. If the added KPI is one that propagates up, it is also added to all parent CIs in all subtrees for the original CI.

To attach a new KPI to multiple CIs:

1 Access the **KPIs** tab and select the required CIs in View Explorer using the keyboard CTRL key.

2 Right-click one of the selected CIs in View Explorer and select **Add KPI**.



The Add KPI to Multiple CIs window opens, displaying the **KPI** area.

3 Define KPI details, as described in the procedure for attaching a KPI to a single CI on page 13.

Note: When defining a KPI for multiple CIs, the **KPI** list contains all KPI types.

---

4 Click **OK**. The new KPI is attached to the selected CIs. (If the KPI already exists for a selected CI, the new version is not attached). If the added KPI is one that propagates up, it is also added to all parent CIs in the subtrees for the original CIs.

Attaching a PNR KPI to a CI

The PNR (Point of No Return) KPI enables you to view how well SLA objectives are being met. When the PNR KPI is defined for a CI, a bar is displayed in Dashboard indicating how much more time (in percentages) the CI can be unavailable before the SLA is in breach of contract. For an explanation of unavailability, see "How Dashboard Calculates Unavailability" in *Using Dashboard*.

Perform the following procedure to view Service Level Management data in an information bar in Dashboard.

To set up Dashboard to display Service Level Management data in Dashboard:

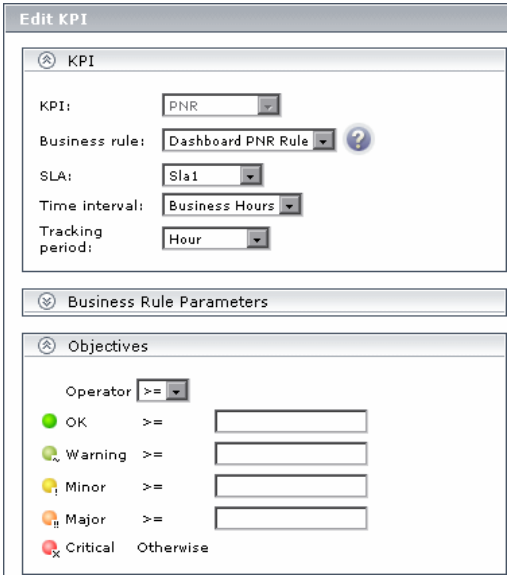
1 Create an SLA. For details, see Chapter 9, "Service Level Agreements (SLAs)." During SLA creation:

- ➤ Add a CI to the SLA.
- ➤ Attach an Availability KPI to the same CI, so that the Dashboard PNR KPI will show data in reports.

Note: An SLA must include a CI with an attached Availability KPI for the Dashboard PNR KPI to show data in reports.

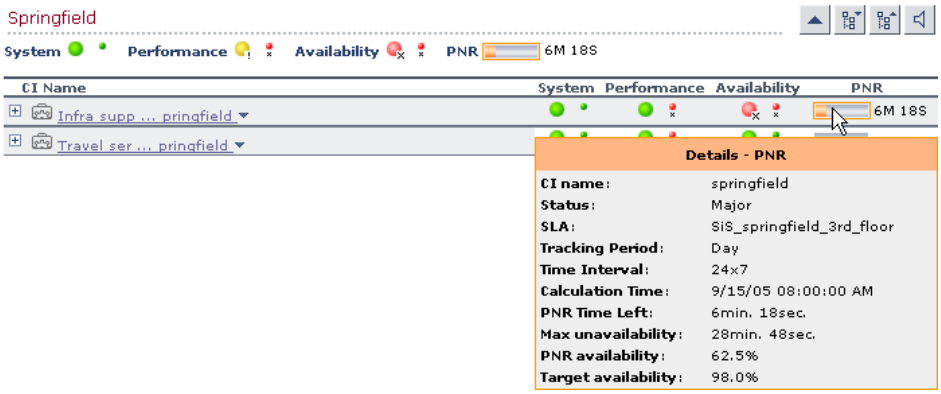
---

2 In Dashboard Administration, attach a PNR KPI to the same CI. For details on attaching a KPI, see "Attaching New KPIs to CIs" on page 13. During KPI creation:



- Choose the PNR KPI.
- Select the SLA whose data is to be displayed in Dashboard.
- Select the time interval and tracking period. These parameters are defined when creating the SLA. For details, see "Defining an SLA: Properties" on page 164.
- Add the objective's ranges that Dashboard uses to calculate when unavailability time approaches breach of contract levels.

3 View the results in Dashboard: **Applications** > **Dashboard** > **Console**. Choose the view and select the CI.



For details on the information that Dashboard displays in the Console page, see “Service Level Management Results in Dashboard” in *Using Dashboard*.

Editing KPI Properties

You edit KPI properties for individual KPIs in the Edit KPI window. You can also perform a multiple edit on certain KPI properties for transaction CIs.

Editing KPI properties must be undertaken with care; the changes can result in KPIs that give an inaccurate performance assessment in Dashboard. Please read the "Notes and Limitations" on page 7 before proceeding.

This section contains the following topics:

Editing KPI Properties for a CI

You can modify all properties for a defined KPI (apart from the KPI type), whether it is a default KPI for the CI, or a KPI attached by a user.

To edit KPI properties:

1 Access the **KPIs** tab and select the required CI in View Explorer.

2 Click the **Edit KPI** button for the KPI you want to edit.

The Edit KPI window is displayed, containing the properties defined for the KPI.

3 You can modify all properties apart from **KPI**. For details on modifying the properties, see steps 3 through 9 in the "To attach a new KPI to a single CI:" procedure on page 13.

4 Click **OK** to save your changes.

Editing KPI Properties for Multiple Transactions

The KPIs tab has a multiple edit function, enabling you to modify the Availability or Performance KPIs for all BPM Transaction from Location CIs in a group. This function enables you to define new business rule parameter values and/or objective values for all child transactions CIs that appear in a subtree of a view, in one operation.

You define the new values in the Edit KPI for Child Transactions window. Every new value you define will replace the previous value for that property, for each transaction CI in the subtree. Property boxes left blank in the Edit KPI for Child Transactions window will not affect the CIs.

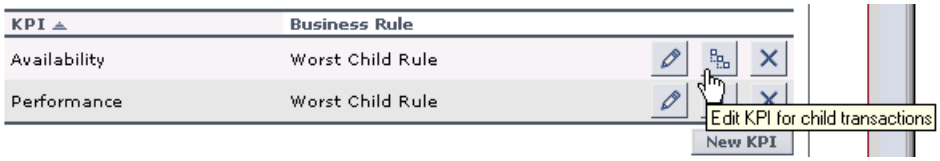
Before using the Edit KPIs for Child Transactions function, you should make sure that the planned new values are logical for all transaction CIs in the subtree. You should also review the Notes and Limitations section on page 29.

This section includes the following topics:

To edit KPI properties for multiple transactions:

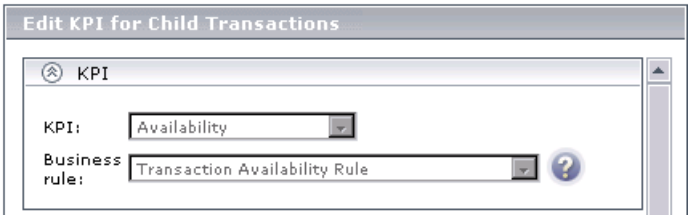
1 In the **KPIs** tab, select the required group-level CI in View Explorer.

2 Click the **Edit KPI for child transactions** button corresponding to the KPI (**Performance** or **Availability**) that you want to edit.



The Edit KPI for Child Transactions window opens.

3 The Edit KPI for Child Transactions window displays the **KPI**, **Business Rule Parameters**, and **Objectives** areas. The **KPI** area contains the names of the KPI and the default monitor business rule for the KPI (these properties are read only).



In the **Business Rule Parameters** and **Objectives** areas, the value boxes are empty. Enter the required values in the boxes, or select a different operator for the objectives. Make sure you enter values that apply logically to all transactions in the group.

For information on rule parameters and possible values, see the section for the relevant rule, as described in "Dashboard Business Rules Detailed Description" in *Repositories Administration*.

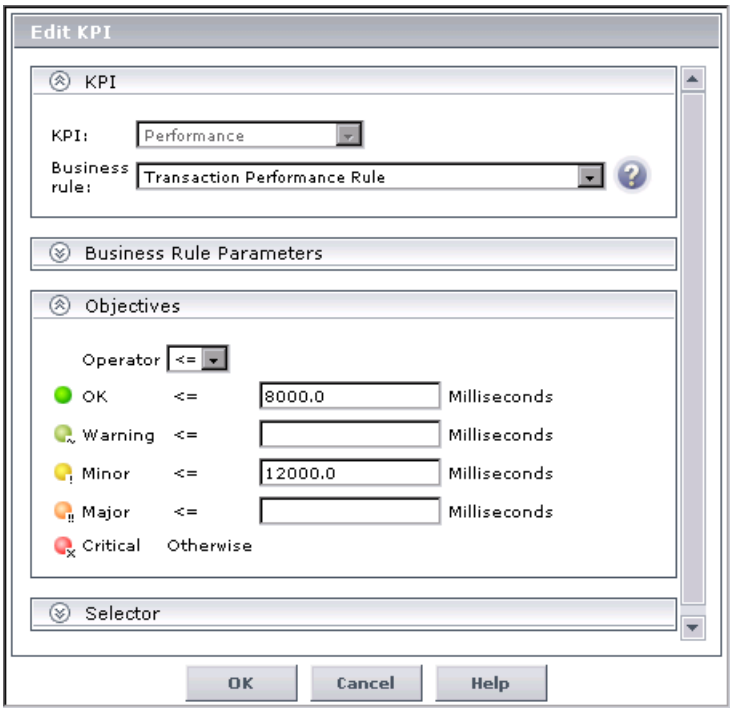
For information on defining objectives, see "KPI Objectives" on page 38.

4 Click **OK**. All transaction CIs in the group are updated with the new defined values.

Example

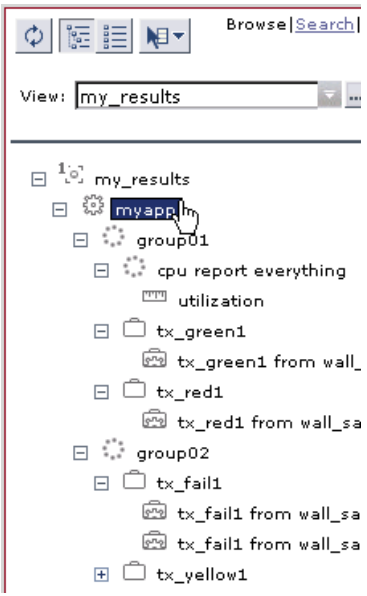
The following example describes editing the objective values for transaction CIs in a subtree.

1 In the **KPIs** tab, the Performance KPI objective values for every transaction CI in the myapp subtree are as follows (displayed by clicking the **Edit KPI** button for any of the transaction CIs):

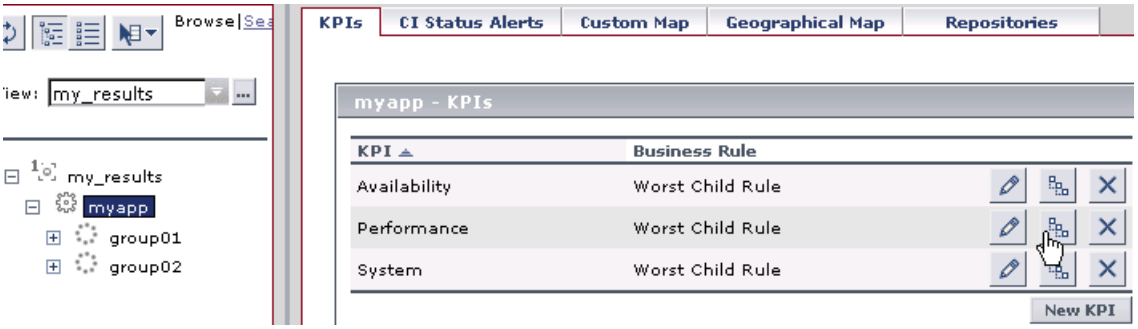


For this example, two additional objective values are added, to include **Warning** and **Major** status levels for each transaction CI, and the **Minor** objective value is modified.

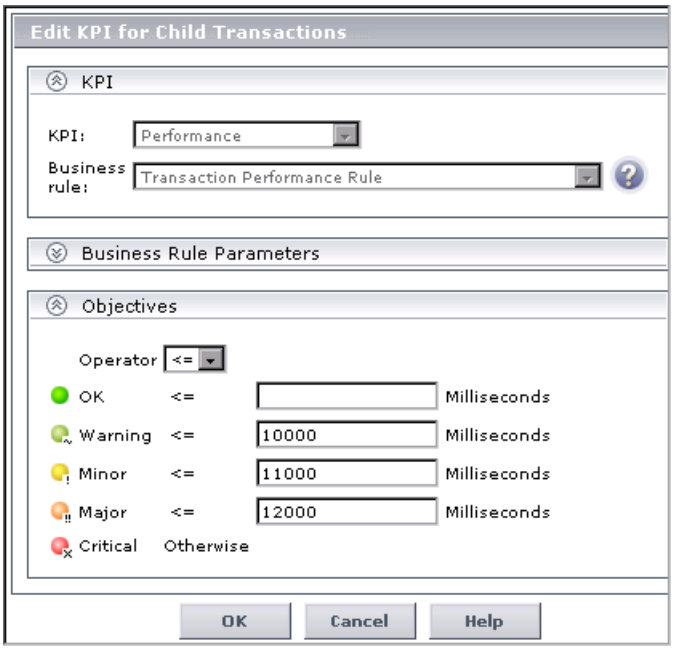
2 In View Explorer, select the parent CI for the subtree—in this case, the Application CI myapp:



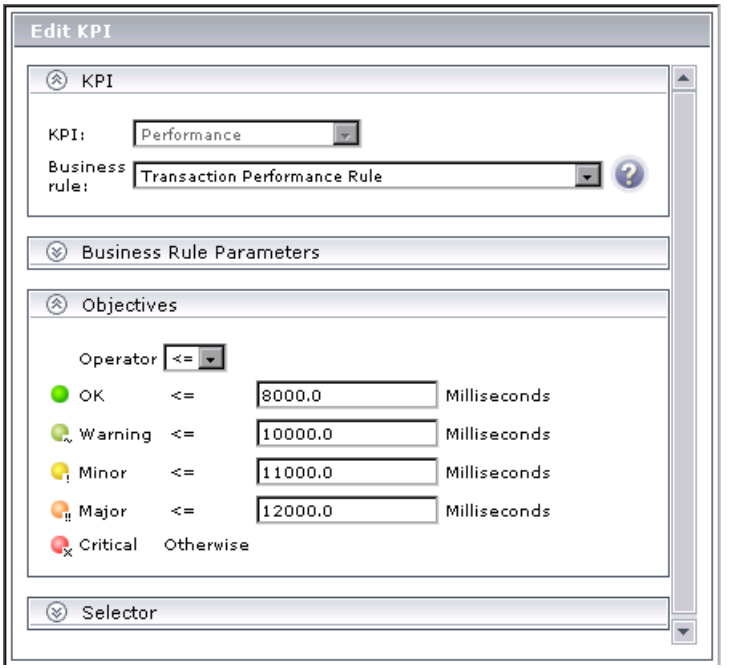
3 In the right pane, click the **Edit KPIs for child transactions** button for the required KPI—in this case, the Performance KPI.



4 In the Edit KPI for Child Transactions window, enter the required values—in this case, 10000 for **Warning** objective, 11000 for **Minor** objective, and 12000 for **Major** objective.



5 After applying the changes, all transaction CIs in the myapp subtree have the following objective values defined:



Notes and Limitations

- The **Edit KPI for child transactions** button is enabled for all KPIs, but:
  - the option is only relevant **Transaction** and **Availability** KPIs (an error message is displayed for other KPIs).
  - the option has validity only when there are Business Process Monitor transaction CIs contained in the subtree.

  Changes made in the Edit KPIs for Child Transaction window will have no effect on KPIs other than **Transaction** and **Availability**, or on CIs for which the option does not apply.
- After applying the Edit KPI for child transactions option, a **KPI was saved successfully** message is displayed in the top-right corner of the page, even if no changes were made to any CIs.

- If a transaction CI in the subtree is using a business rule other than the default monitor rule for the KPI (Transaction Availability Rule or Transaction Performance Rule), then when you apply the Edit KPI for child transactions option, the existing rule is replaced with the default rule.
- The **Objectives** area in the Edit KPIs for Child Transaction window displays the default **Operator** for the rule. When you apply your changes, the displayed default operator will be updated to all transaction CIs (regardless of which operator they were using previously).

No Data Timeout for Transaction CIs

When a KPI is using a monitor rule (for example, the Transaction Availability Rule), the **Business Rule Parameters** area includes the **No data timeout** property. This property defines the number of seconds from the time the last sample was received for the KPI, until the KPI is timed out—at which point the KPI changes to decay status (gray).

The default value for the **No data timeout** property is generally taken from the monitor rule definitions (as defined in the Business Rules Repository). However, for Business Process Monitor transaction CIs, Dashboard calculates a new **No data timeout** value, based on the schedule for running the transaction. The calculation takes the schedule interval (defined in Monitor Administration) for the Business Process profile that contains the transaction (default value = 15 minutes) and adds an additional 90 seconds. For example, for a transaction with a schedule interval of 15 minutes, the **No data timeout** value will be 990 seconds. (For details on defining the profile schedule, see "Using the Data Collectors Tab" in *End User Management Data Collector Configuration*.)

This calculation method means that the timeout value is automatically adjusted to align with changes made to the profile schedule interval in Monitor Administration, so that the KPI is not incorrectly timed out. If there is more than one scheduling scheme in effect, the following rules are used for the calculation:

- If multiple schedules are defined for a profile running on a Business Process Monitor instance, the largest schedule interval is used (all schedules are treated equally, whether they apply to the whole week or part of the week).

➤ If the profile is assigned to several locations, each with a different schedule, then smallest interval from amongst the locations is used (after first applying the rule above).

Deleting KPIs Attached to a CI

You can delete any KPI attached to a CI. When you delete a KPI, it removes the upwards propagation of the KPI to all parent CIs. This means that if you delete a KPI for a CI, and that KPI is not defined for any of the sibling CIs, then it will also be deleted from the parent CI.

Deleting KPIs must be undertaken with care; the changes can impact on the status of other KPIs. Please read the "Notes and Limitations" on page 7 before proceeding.

To delete a KPI:

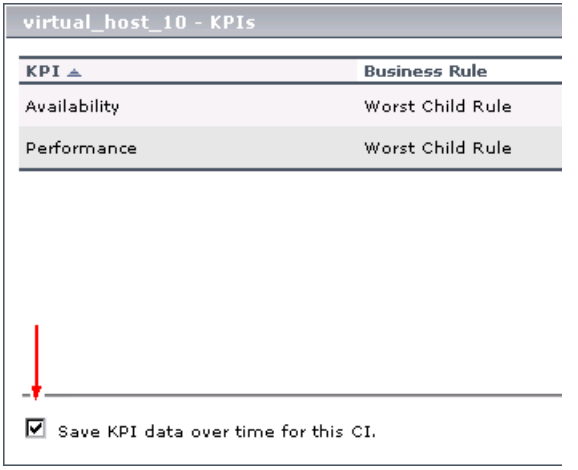
1 In the **KPIs** tab, click the **Delete KPI** button for the KPI you want to remove.

2 Click **OK** in the confirmation box. The KPI is removed from the CI, and, if applicable, from all parent CIs.

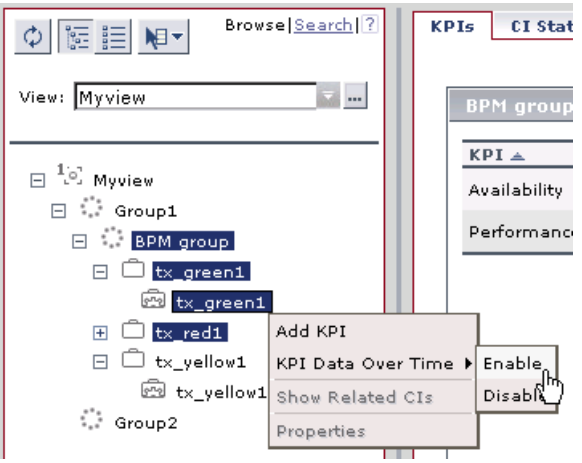
Saving KPI Data over Time for a CI

If required, data on status and measurements over time for a CI can be saved in the database. The persistent data is used to produce KPIs over time reports, as described in "KPIs Over Time Reports" in *Using Dashboard*.

To save data for a CI, the **Save KPI data over time for this CI** check box must be selected for that CI in the **KPIs** tab.



You can enable/disable this option for multiple CIs by selecting the required CIs in View Explorer (using the keyboard CTRL key) and right-clicking one of the selected CIs.



The **Save KPI data over time for this CI** option is selected by default for CIs of the following types:

- **Business Process**
- **Business Process Group**
- **Line of Business**
- **Application** (logical application)
- **End User Management Application Related Group**

The option is not available (disabled) for monitoring CIs.

When the option is selected, all status changes (for example, from red to green) for all the CI KPIs are written to the database. (If you also want to save data on the actual measurements for the KPIs, you must change the default settings for Dashboard in the Repositories, as described in "Saving Measurements Data" on page 34.)

Saving status (and measurements) data for long periods or for many CIs can occupy a lot of database memory, so this option should be used with care. When you no longer require data to be saved for a CI, deselect the **Save KPI data over time for this CI** check box.

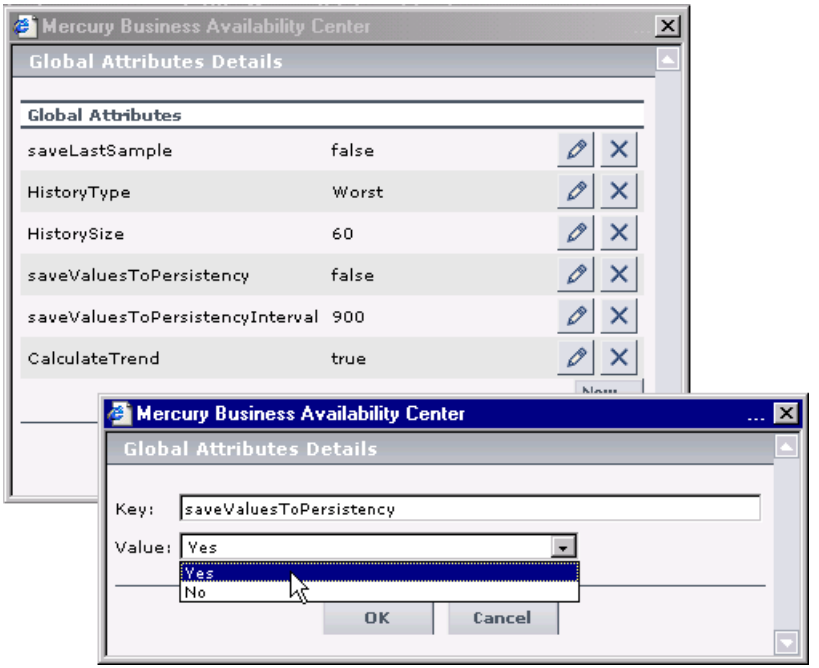
Saving Measurements Data

If required, the **Save KPI data over time for this CI** option can also be used to save the calculated measurement for each of the CI KPIs, at 15 minute intervals (default value). This is done by activating the **saveValuesToPersistency** global attribute in the Rules Repository.

To activate Dashboard to save measurements data:

1. Access the **Dashboard Administration** > **Repositories** > **Business Rules** page.
2. Click **Edit Globals** (in the **Factory Rules** area).
3. In the **Global Attributes** list, click the **Edit** button for **saveValuesToPersistency**.

4 In the displayed Global Attributes Details window, change the **Value** parameter from No to **Yes**.



Click **OK**.

5 If you want to change the default interval (900 seconds) for collecting measurements data, then in the **Global Attributes** list, click the **edit** button for the **saveValuesToPersistencyInterval**, and modify the value.

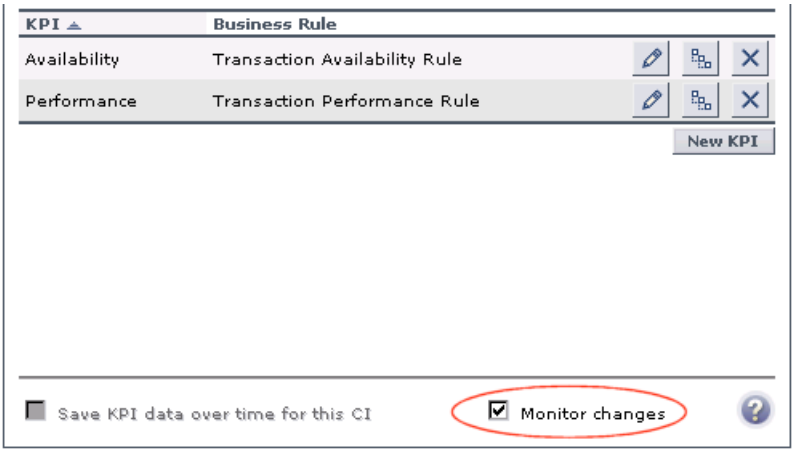
Note: To avoid overloading the database memory, it is recommended that you do not define a shorter default interval value.

Real-Time Monitoring of CI Property Changes

For a limited number of CIs, Dashboard can monitor for changes to the CI properties (or changes to the properties of the CI's child CIs) in real-time.

This information is in addition to the Dashboard Change Report, which shows a historical report on changes to properties for CIs over a period of time. (For details on the Change Report, see "Change Report" in *Using Dashboard*.)

To display real-time changes for a CI and its children, the **Monitor changes** check box must be selected for that CI in the **KPIs** tab.



Note: The **Monitor changes** option is only enabled if:

- you are working in a shared CMDB environment.
- you enable change impact monitoring by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Dashboard Application**, and locate the **Host name for MAM GUI Web server** entry in the **Change Impact Properties** table. Define the Web server name and restart Mercury Business Availability Center.

You can set the monitor changes option for up to 20 CIs. Once 20 CIs have been configured, a message is displayed when you try to set the option for another CI, stating that the limit has been reached.

If you then deselect the option for one or more of the configured CIs, the option becomes available again for all CIs, until the 20 CIs limit is again reached.

Note: To change the 20 limit, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Dashboard Application**, and locate the **Maximum monitored CIs** entry in the **Change Impact Properties** table. Modify the value as required. However, change this value with caution to avoid too much load on the system.

When the monitor changes option has been set for a CI, Dashboard continuously monitors that CI and all its child CIs, to see if a change occurs in one of the significant properties defined for the CIs.

The significant properties vary for each CIT, according to the CIT definition in **Admin** > **CMDB** > **CI Type Manager**. In CI Type Manager, in the **Attributes** tab for the CIT, the **Change Monitored** column must be selected for a property, in order for that property to be significant and therefore monitored. For more information on CIT definitions, see "Managing CITs" in *CI Type Manager Administration*.

If a change occurs in one of the significant properties for the CI or the CI children, then an icon is displayed in Dashboard beside the CI name. For more information, see "Viewing Real-Time Changes to CI Properties" in *Using Dashboard*.

After a change occurs, the change icon is displayed for 24 hours (default value). You can change the default value, as described in "Specifying the Changes Period for the Change Report" on page 132.

KPI Objectives

The KPI objectives define the standards for allocating business status to the KPI.

The following sections describe objectives and how to define them for a KPI.

➤ "About Status and Objectives" on page 38

➤ "Defining Logical Objectives" on page 41

➤ "Excluding Statuses" on page 42

➤ "Units of Measurement for Objectives" on page 44

➤ "Example of Defining Objectives" on page 45

About Status and Objectives

The status displayed for a KPI in Dashboard provides an indication of how well a business process or system is meeting your business objectives. Based on traffic light colors (with additions), the Dashboard shows you if the KPI measurement is meeting the objective requirements (green), or is critically failing (red), or is at some business risk level between the two.

Five statuses are available in Dashboard (for active status), each representing a different level of business performance:

➤ **OK** (green)

➤ **Warning** (olive)

➤ **Minor** (yellow)

➤ **Major** (orange)

➤ **Critical** (red)

Depending on the CI and KPI types, active status may be represented in Dashboard using from two to all five of these status levels. In most cases (not for SiteScope measurements), the KPI is assigned a status as follows:

➤ The business rule calculates a measurement for the KPI.

➤ The calculated measurement is compared with defined objective values.

- The KPI is assigned a status according to where the measurement falls within the objectives. For example, a KPI measurement of 50% may fall within the definition for the **Minor** objective, so the KPI is assigned Minor status (yellow).

The objective values used for each KPI can originate from various sources:

- The business rule definitions in the Business Rules Repository provide default objective values for every rule that uses objectives. The business rules generally define different objective values for each of the five statuses used in Dashboard. You can define new default objective values for a business rule, as described in "Specifying the Rule Details" in *Repositories Administration*.
- The source adapter may specify specific objective values to be used with the business rule for a KPI. These values override the values from the Business Rule Repository. You can modify the template for a source adapter to define custom objective values, as described in Chapter 5, "Working with Templates."
- The source adapter may specify reference values for the objective parameters, so that the objective values are taken from the threshold values defined in Monitor Administration. These values override the values from the Business Rule Repository.
- You can modify the objective values for an individual KPI in the Dashboard Administration KPIs tab, while adding or editing a KPI. The new values override values from the source adapter or from the business rule. For details, see "Attaching New KPIs to CIs" on page 13.

SiteScope Monitoring CIs

For SiteScope monitoring CIs, KPI status is based on the status received from SiteScope (calculated according to the thresholds defined in SiteScope). Three status levels are used in Dashboard:

- **OK** (green) in Dashboard – corresponds to **Good** or **OK** status in SiteScope
- **Minor** (yellow) in Dashboard – corresponds to **Warning** status in SiteScope
- **Critical** (red) in Dashboard – corresponds to **Error** status in SiteScope

The SiteScope status definitions cannot be changed in Dashboard, so the business rules for SiteScope KPIs do not include objective values.

End User Monitoring CIs

For end user monitoring CIs (from Business Process Monitor, Client Monitor, Real User Monitor), KPI status is calculated by comparing the KPI measurement with objective values.

- For **Business Process Monitor** and **Client Monitor** transaction CIs, the KPI objective values are either taken from Monitor Administration or the rule definition:
  - For CIs using the **Transaction Performance Rule** (ID# 13), the Business Process Monitoring source adapter references the transaction thresholds defined for the corresponding monitoring object in Monitor Administration. The threshold values map to KPI objective values for three status levels in Dashboard: **OK**, **Minor**, and **Critical**
  - For CIs using the **Transaction Availability Rule** (ID# 5), KPI objectives are taken from the default values for the rule in the Business Rules Repository. The rule defines objective values for all five status levels in Dashboard.
- For **Real User Monitor** monitoring CIs, depending on the rule used, the KPI objective values are taken from the Real User Monitor source adapter, Monitor Administration, or the rule definition. For example:
  - For RUM Application Error Monitor CIs using the **RUM Event Monitor Volume Rule** (ID# 73), the objective values are defined directly in the source adapter. The objective values defined for this rule use four of the Dashboard status levels: **OK**, **Warning**, **Minor**, and **Critical**
  - For RUM Page Monitor CIs using the **RUM Page Monitor Availability Rule** (ID# 49), the source adapter references the **Availability** threshold defined in Monitor Administration for the page. This is a single value, so two status levels are used in Dashboard: **OK** and **Critical**
  - For RUM Sessions Monitor CIs using the **RUM Session Monitor Availability Rule** (ID# 52), the source adapter does not define objective values, so KPI objectives are taken from the default values for the rule in the Business Rules Repository. The rule defines objective values for three Dashboard status levels: **OK**, **Minor**, and **Critical**

For all end user monitoring CIs, you can edit the objective values in the KPIs tab to use as many of the status levels as you require, as described in "Defining Logical Objectives" on page 41.

Warning: KPIs that were created for CIs by the source adapter templates, frequently have objective values that differ from the default ones used by the business rule. However, when editing one of these KPIs in the KPIs tab, if you select a different rule and then revert to the original rule, then the original objective values are replaced with the rule default values.

Defining Logical Objectives

The objectives values for a KPI should cover the whole spectrum of possible measurements for that KPI. (This means active measurements, the objectives do not take into consideration the values given to a KPI for no data, downtime, and so forth.)

The KPI measurement is evaluated against each objective level, starting from **OK** (green), and continuing (in order) to **Critical** (red). This process stops at the first objective level into which the KPI measurement fits.

To define where the boundaries of each objective level falls, each objective from **OK** to **Major** is associated with an **Operator**. (The **Critical** objective definition is always **Otherwise**, meaning that this status is applied to all measurements that fall beyond the **Major** objective limit.) You can select the operator that matches your requirements; the same operator is applied to all objective levels.

The available operators are:

>
>=
<
<=

You must make sure that the objectives contain logical values (according to the data type) and are correctly ordered, and that the operator is logical for the order. For example:

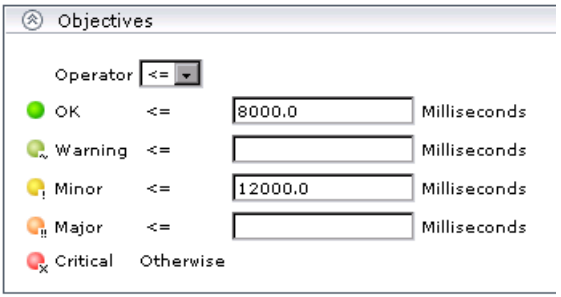
- If you enter descending objective values, such as 70, 55, 40, 20, you must use operator > or >=, so that the **OK** objective will cover all measurements greater than 70.
  For a KPI measurement of 88: **88** >= **70** is true, so assigned status is **OK**.
  For a KPI measurement of 18: evaluation of the KPI measurement against every objective is false, so status will fall into the **Otherwise** category and be assigned status **Critical**.
- If you enter ascending objective values, such as 10, 25, 35, 40, you must use operator < or <=, so that the **OK** objective will cover all measurements less than 10.
  For a KPI measurement of 7: **7** <= **10** is true, so assigned status is **OK**.
  For a KPI measurement of 50: evaluation of the KPI measurement against every objective is false, so status will fall into the **Otherwise** category and be assigned status **Critical**.

Excluding Statuses

Not all the statuses need be used for a KPI; for example, the OT Impact KPI by default uses only **OK** (green) and **Critical** (red) status. There are two methods used in Dashboard to exclude statuses, as described in the following sections.

Blank Objective Value

When the objective value for a status is left blank, Dashboard ignores that status during KPI status calculation. For example, the Performance KPI for a transaction may have the following objectives defined (taken from the threshold settings for the transaction in Monitor Administration):



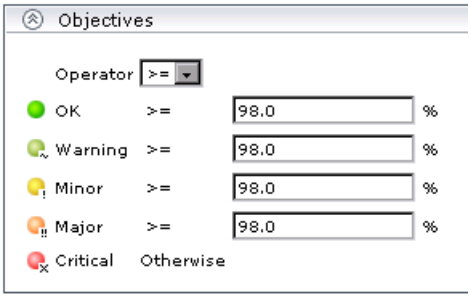
In this case, if the measurement for the KPI does not fall into the **OK** objective level, then **Warning** is skipped and the measurement is evaluated against the **Minor** objective level. If it does not fall into that level, **Major** is also skipped, and the KPI is given **Critical** status.

If you want to exclude statuses when editing the objective values for a KPI, it is recommended that you use this method.

Repeated Objective Value

Dashboard allocates status by starting at **OK** status, and evaluating the KPI measurement against each objective level until the right level is found. When an objective value is repeated for two or more statuses, the repeat occurrences are passed over and those statuses are not used.

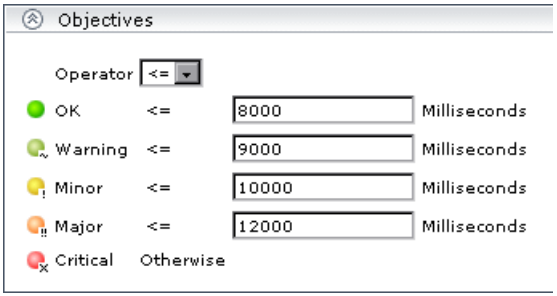
For example, the Availability KPI for a RUM page monitor may have the following objectives defined (by using the Availability threshold setting in Monitor Administration for all four defined objective values):



In this case, if the measurement for the KPI is greater or equal to 98%, then it is given **OK** status. If it is less than 98%, then evaluation against the **Warning**, **Minor**, and **Major** statuses will also not give any result and these statuses will not be used; the KPI will then be given **Critical** status.

Units of Measurement for Objectives

The objectives use a unit of measurement, shown after the objective value box in the KPI **Objectives** area:

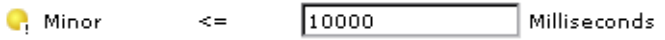


The unit is part of the business rule definition, and indicates the format of the calculated measurement. This format may reflect the units used by the incoming data (for example, **milliseconds** for performance time data), or it may be a new format applied as a result of the business rule calculations (for example, **dollars** for a financial loss calculation). If required, the default unit for a rule can be changed in the rule definition (as described in "Business Rules Repository" in *Repositories Administration*).

The following default units are used:

- **Percentage (%).** This unit is used for business rules that handle availability over time data for a transaction, for example, the Transaction Availability Rule, and for the PNR Rule, where the KPI measurement represents percentage of time remaining for CI unavailability before the SLA is in breach of contract.

- **Milliseconds** or **Seconds.** This unit is used for business rules that handle performance time data for a transaction or monitor, for example, the Transaction Performance Rule or RUM Page Monitor Performance Rule.



- **Financial ($).** This unit is used for business rules that determine financial loss for a CI, for example, the Impact Over Time Rule.

- No unit is displayed after the objective value box for business rules that handle volume, where the KPI measurement represents a simple numerical count. For example, this is the case for the RUM Transaction Monitor Volume Rule.

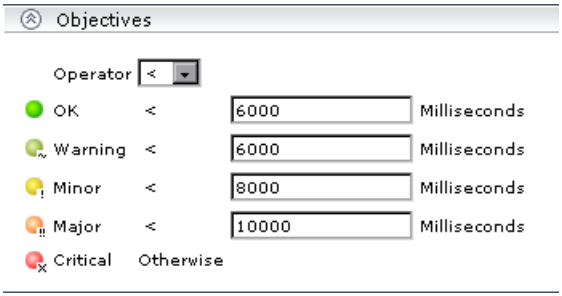
Example of Defining Objectives

A specific transaction monitor CI is using the Transaction Performance Rule. For this transaction, the required objectives are as follows:

- The objective for acceptable performance time is under 6000 milliseconds. An average performance time that reaches 6000 milliseconds is already of concern.
- Performance time of 8000 milliseconds is considered seriously problematic.
- Performance time of 10000 milliseconds is considered critical.

In addition, **Warning** status is not required for this KPI.

In the Edit KPI window for the transaction's **Performance** KPI, the objective levels and operator are modified as follows:



When a measurement is calculated for the KPI from the incoming performance data, the measurement is compared with the objectives assigned to the KPI as follows:

- For a measurement under 6000 milliseconds, status = **OK**
- For a measurement of 6000 milliseconds or more, but under 8000 milliseconds, status = **Minor**
- For a measurement of 8000 milliseconds or more, but under 10000 milliseconds, status = **Major**
- For a measurement of 10000 milliseconds or more, status = **Critical**

Selectors for KPIs

When a monitoring (leaf) CI has a KPI and associated business rule that are intended to be applied to actual data samples, the KPI properties include a **selector**. A selector is a filter definition that defines which samples are relevant for the KPI.

The following sections describe selectors and how to define them for a KPI.

- "Role of the Selector" on page 47
- "Defining Selector Expressions" on page 48
- "Using Predefined Sample Data for Selectors" on page 51

➤ "Manually Defining Custom Selectors" on page 54

➤ "Notes and Limitations" on page 55

For information on editing selector definitions in the source adapters, see "Selector Definitions" in *Source Manager Administration*.

Note: Selectors are also defined for Dynamic Rule Factory CIs, but directly as part of the CI definition, not in a KPI. The selector used by a Dynamic Node Factory can be defined and/or edited in the IT Universe Manager tab of CMDB Administration, as described in "Working with Dynamic Node Factory" in *IT Universe Manager Administration*. The functionality and definitions for a Dynamic Rule Factory selector are the same as for a KPI selector, as described in this section.

Role of the Selector

Monitoring CIs are CIs that are intended to receive real-time data from the data samples sent by the external system (purely logical CIs do not receive data samples). The data samples, containing information collected by a monitoring system (either Mercury or third-party), are supplied to Mercury Business Availability Center over the Bus.

The Business Logic Engine filters the data samples arriving on the Bus using selectors, which are set using Dashboard Administration. A selector is defined as part of the monitor rule for a KPI attached to a monitoring CI. The selector identifies and catches the data that is relevant for the CI and the KPI.

A different selector may be used by each KPI with an associated monitor rule, enabling (when required) the use of different samples for each KPI. When a monitoring CI is added to the Mercury Universal CMDB by a monitoring adapter (as described in *Source Manager Administration*), a selector is automatically defined for each of the default KPIs for the CI.

If required, you can edit the default KPI selectors in the KPIs tab. You can also attach new KPIs to a monitoring CI, assign a monitor rule and manually define the selector.

Defining Selector Expressions

In the selector **Filter** area, you define selector expressions to filter the data samples, To target only those samples that are relevant for the KPI. A selector expression requires a **Field**, an **Operator**, and a **Value**, defined in that order. (For an explanation of these expression parameters, see "Selector Expression Parameters" on page 48.)

There are two methods for defining selector expressions:

- **Using predefined sample parameters.** You define the selector expressions by selecting from metadata—predefined sample types and sample parameters in the database. For more information, see "Using Predefined Sample Data for Selectors" on page 51.
- **Manually, to build a custom selector.** You define the selector expressions by manually defining the sample type and sample parameters. You can build a custom selector using any field name, and, if required, can combine fields from two or more data types. For more information, see "Manually Defining Custom Selectors" on page 54.

Note: You can have Mercury Business Availability Center automatically assign the default selector for the monitoring CI, by leaving the selector expressions blank in the New KPI/Edit KPI window. After clicking **OK** to close the window, Mercury Business Availability Center assigns the KPI the default selector for the CI, as used by the default KPIs attached to the CI.

A selector filter may consist of a single simple expression, or you can build more complex filters containing blocks of selector expressions. For more information, see "Building Complex Filters" on page 49.

Selector Expression Parameters

Selectors use Boolean expressions to evaluate sample properties.

When the values for the Field and Value properties are defined manually, they must be entered precisely as used in the data samples from the data source, or the selector will fail. For explanations of the data samples and their fields, see "Samples" in *Reference Information*.

For each selector expression, you must define the following:

- **Field.** The reference property that the selector expression checks in the data samples sent from the data source.
- **Operator.** The relational operator that the selector expression uses when comparing the actual value for the property against the value defined in the selector. The expression gives a result of TRUE or FALSE for each data sample.

  The following operators are available:

  - ==
  - **!=**
  - >
  - >=
  - <
  - <=
  - **in**
  - **notIn**
  - **like**
- **Value.** The property value that the expression compares with the value in the data sample. Note that the value must be in numeric format if a numeric operator is selected, or must be entered between quotation marks if a text string operator is selected.

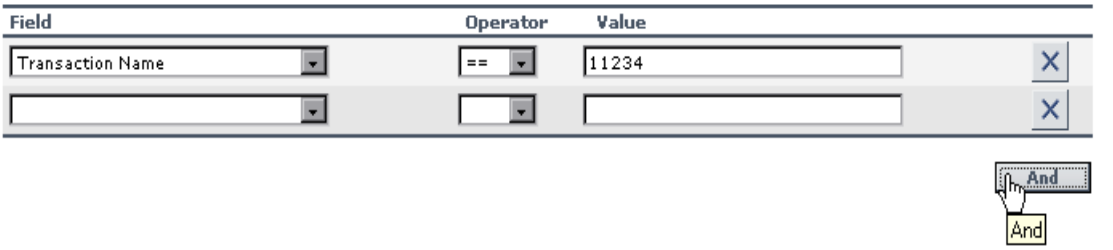
Building Complex Filters

You can build more complex filters for a KPI, by defining blocks of selector expressions that together form a complex logical expression:

- You can narrow the filter by using a logical "And" operator to attach additional selector expressions to an expression block.
- You can widen the filter by using a logical "Or" operator to add alternative expression blocks (each containing one or more selector expressions).

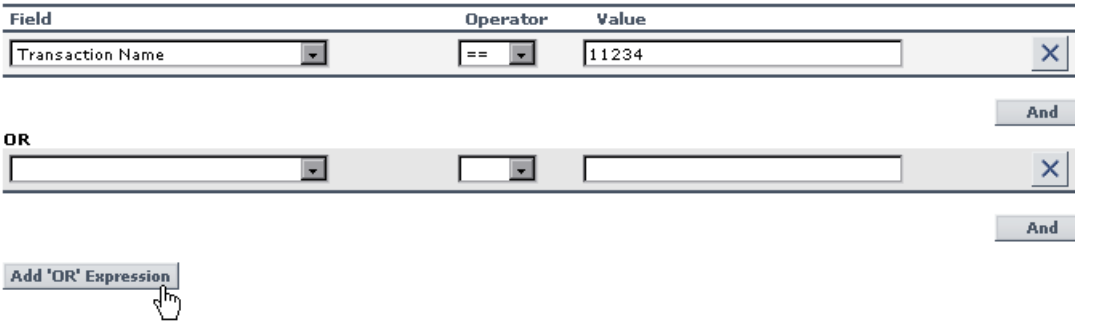
You can define as many selector expressions and blocks of selector expressions as required:

➤ To define an additional selector expression within a block, click the **And** button for that block. An additional empty selector expression row is displayed in the block.



For example, you can define a filter that looks for transaction samples that contain both profile name X *and* transaction name Y.

➤ To define an alternative expression block, click the **Add 'OR' Expression** button. A new block is created, with an empty selector expression row.

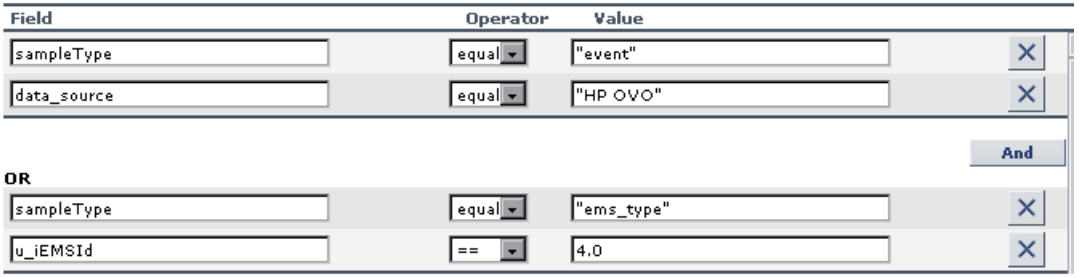


For example, you can define a filter that looks for transaction samples that contain either transaction name X *or* transaction name Y.

You can add additional selector expressions to the new block using the **And** button for the block.

A data sample qualifies for the selector if all the selector expressions in a single expression block are TRUE for the data sample. For example, either selector expressions **a** and **b** and **c** in block 1 are all TRUE, or selector expressions **d** and **e** and **f** in block 2 are all TRUE.

Example of selector with two expression blocks.



Using Predefined Sample Data for Selectors

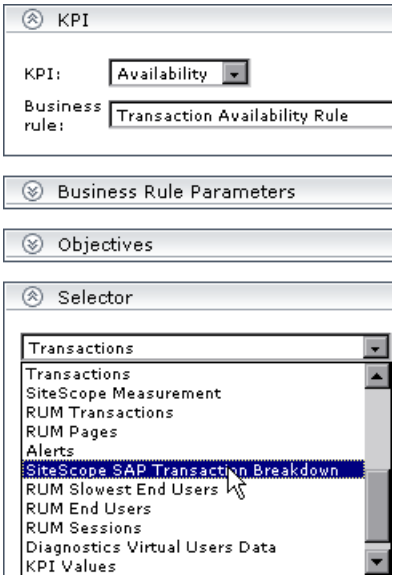
When defining or editing a selector using predefined sample data, you have the option to select **Field** and **Operator** values from predefined lists. This definition method validates the field names and operators, and prevents errors that may occur when manually entering field names. It also simplifies the process of defining a selector.

The predefined fields use metadata, information on sample types collected from data samples arriving from various data sources (including Mercury data collectors and third-party data sources) and stored in the database. For explanations of the data samples and their fields, see "Samples" in *Reference Information*.

You can use metadata to build a complex filter with multiple selector expressions, just as with manually defined filters. For more information on defining selector expressions and building complex filters, see "Defining Selector Expressions" on page 48.

To define a selector expression using metadata:

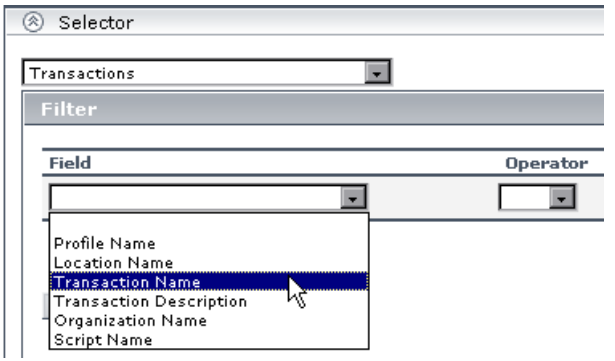
1 First define the sample type that applies for this KPI. You select the sample type from the list at the top of the **Selector** area in the New KPI or Edit KPI window. The list is based on the sample types currently in the database.



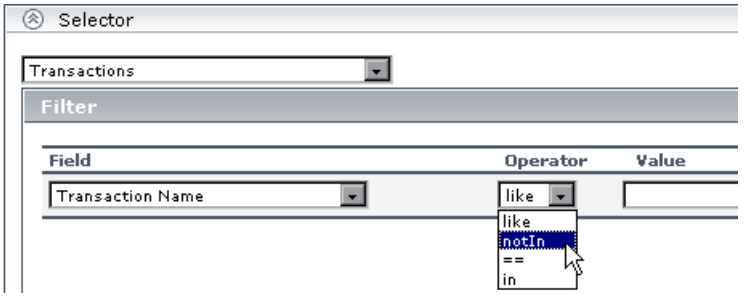
For example, for a KPI that relates to transaction measurements, you select sample type **Transactions** from the list.

When you select a sample type from the list, all previously defined expressions for the selector are overridden, so the contents of the **Filter** box are automatically deleted.

2 After selecting a sample type, the **Field** box in the first selector expression converts to a dropdown list, containing all valid options for the selected sample type. The **Field** box defines the required reference property in the data samples.



3 After selecting an option from the **Field** list, the **Operator** list is automatically updated so that it contains only those operators that are valid for the selected field. For example, if the selected field always contains a text string, then only the operators that are used with text are included in the list, such as **like**, **notIn**, ==, **in**.

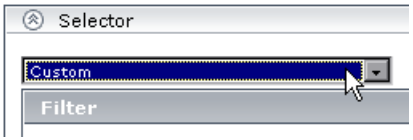


4 The required value for the selected field must be entered manually in the **Value** box.

Note: The **Value** property is case sensitive and must be entered precisely as used in the data samples from the data source, or the selector will fail. The recommended method is to take the values from the samples published on the Bus, as described in "Selector Expression Parameters" on page 48.

Manually Defining Custom Selectors

When defining or editing a selector, you can build a custom selector by manually defining all information for the selector. To do this, you must make sure that no sample type is defined in the list at the top of the **Selector** area in the New KPI or Edit KPI window (the box should display **Custom**).



If a sample type was previously selected in the list, and you then select **Custom**, all previously defined expressions for the selector are overridden and the contents of the **Filter** box are automatically deleted.

Every selector must include the definition of the sample type required for the KPI, so when manually defining a selector, at least one selector expression must contain this information. For example, for a KPI that relates to transaction measurements, the selector must "catch" transaction samples, which are defined by the sample type **"trans_t"** in the selector.

Note: The **Field** and **Value** properties are case sensitive and must be entered precisely as used in the data samples from the data source, or the selector will fail. The recommended method is to take the values from the samples published on the Bus, as described in "Selector Expression Parameters" on page 48.

To define a custom selector expression:

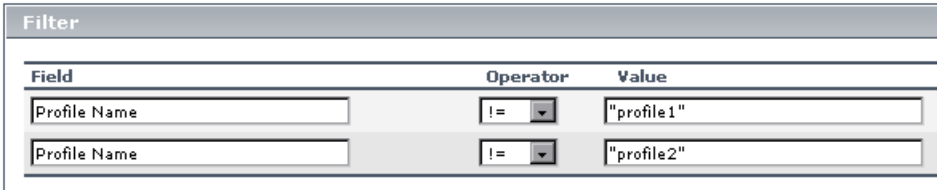
1. Enter the required reference property directly in the **Field** box.
2. Select an operator from the **Operator** list. You can select from any of the operators used in Dashboard.
3. Enter the required value for the property directly in the **Value** box.

Notes and Limitations

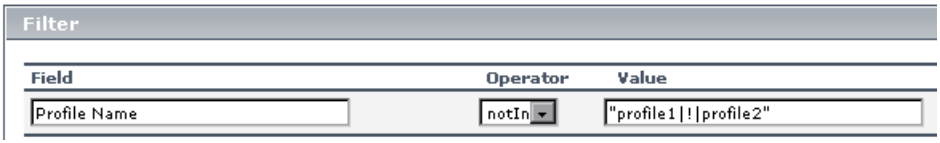
- The sample type must be appropriate for the rule you selected for the KPI. For example, samples of type "**ss_monitor_t**" (**SiteScope Measurement** in the predefined sample type list) have no relevance for the **Transaction Performance Rule** defined for a **Performance** KPI.
- If you define *only* a sample type (either as part of a custom selector expression, or by selecting one of the predefined sample types) and do not define anything else for the filter, the KPI will receive *all* samples for that sample type category.
- You should define the selector parameters in the order **Field**->**Operator**->**Value**.
- When manually defining the properties for a custom selector with multiple blocks of selector expressions, every block must contain a **sample type** selector to identify the relevant data source, for example, sampleType == "trans_t" for a Business Process Monitor transaction. A different sample type can be defined for each expression block.

  When using metadata for a selector, only one sample type can be selected for the whole selector.

➤ Do not repeat the same key and operator combination within a logical expression block; otherwise, the KPI will not receive samples. For example, do not use the following combination:



Instead of this format, use, for example, the **notIn** operator in place of **!=**. You can use this method to avoid almost any repeated key/operator scenario.



KPIs for User Modes

Mercury Business Availability Center provides the option to define Dashboard KPIs for two different user types (modes): **operations** and **business**. This option enables the creation of two versions of a single KPI, where each KPI version is geared towards the particular viewing requirements of one of the user types.

For example: You might want to create two versions of the Availability KPI, so that the Availability KPI for an operations user shows Critical status (red) when transaction availability is below 30%, and the Availability KPI for a business user shows Critical status when transaction availability is below 20%.

Each user type sees the appropriate version of the KPI in the Dashboard views.

This section includes the following topics:

Setting Up User Mode Functionality

You set up user mode functionality in Mercury Business Availability Center by defining the mode for users, defining the KPI versions for each mode, and attaching the KPI versions to the CIs.

This section includes the following topics:

Assigning a User Mode

There are two ways to assign a user mode to a user:

- The system administrator, when defining new users in the **Admin** > **Platform** > **Users and Permissions** > **User Management** page, can set **User Mode** to **Undefined**, **Operations User**, or **Business User**. By default, all new/existing users are set as **Unspecified** (meaning that they see KPIs for both modes in Dashboard).
- Users can change their own user mode in the **Admin** > **Personal Settings** > **General Settings** page. In the **User Mode** area, select the required mode from the **Select user mode** list.

  After changing the mode in the General Settings page, you must log out of Mercury Business Availability Center and log in again to see the mode filtering work.

Defining KPI Versions for the User Modes

The following steps describe how to define different versions of a KPI to use with each user mode. You can assign user modes to a new KPI that you define, or to an existing KPI by cloning or overriding the KPI. For more information, see "KPIs Repository" in *Repositories Administration*.

If you want one of the KPI versions for a user mode to automatically replace an existing KPI, then you must override the existing KPI and edit the new version.

It is recommended that you give a name to each KPI that is assigned a user mode that will easily identify the KPI with the appropriate user version. For example, you can add an appropriate suffix.

To define KPI versions for user modes:

1. Access the **Admin** > **Dashboard** > **Repositories** > **KPIs** page.
2. Define the business user version of the KPI:
   - Add the required KPI to the Custom KPIs area by cloning or overriding a KPI, or creating a new KPI. Open the KPI for editing.
   - In the displayed KPI Details window, give the new KPI/copied KPI an appropriate name. For example, add the suffix "**_biz**" (as in Availability_biz).

➤ Select **Business** in the **Applicable for User Mode** list.

3 Define the operations user version of the KPI:

➤ Add the required KPI to the Custom KPIs area by cloning or overriding a KPI, or creating a new KPI. Open the KPI for editing.

➤ In the displayed KPI Details window, give the new KPI/copied KPI an appropriate name. For example, add the suffix "**_ops**" (as in Availability_ops).

➤ Select **Operations** in the **Applicable for User Mode** list.

Note: If you override a KPI, the overridden version of the KPI replaces the original KPI throughout Dashboard, so all CIs that are assigned the original CI (for example, Availability) are automatically updated to the new version (for example, Availability_ops).

---

4 Edit the details for each KPI version, according to your requirements. For example, you may want different business rules to apply to each version. For more information, see "Specifying KPI Details" in *Repositories Administration*.

5 If you want to use a different version of a business rule with each KPI version, then you must define the rule versions in the Business Rules Repository. For example, for two versions of the Availability KPI, you may require two versions of the Transaction Availability Rule, each with different default objective values.

For details on defining business rules, see "Business Rules Repository" in *Repositories Administration*.

Attach KPI Versions to CIs

You manually attach the KPI versions to the CIs to which you want them to apply.

➤ If the original KPI was already attached to CIs (for example, the Availability KPI is automatically attached to transaction CIs), then the KPI version that overrode the original (for example, Availability_ops) is automatically attached to the CIs instead. You then manually attach the second KPI version (for example, Availability_biz).

➤ If there are two new KPI versions, one for business and one for operations then for every applicable CI you manually attach the two versions (and delete the original KPI if it is not required).

To attach the KPI versions to CIs:

1 In the **Admin** > **Dashboard** > **KPIs** page, add the KPI versions to each CI where they are required, so that the CIs have both versions of the KPI. You can add the KPI to multiple CIs in one operation. For more information, see "Attaching New KPIs to CIs" on page 13.

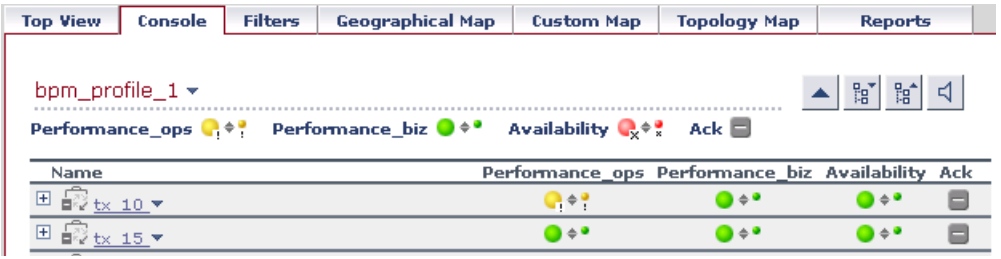
2 Edit the KPI properties as required in the New KPI/Add KPI to Multiple CIs window. For example, you may want to define different objective values for the KPI.

3 For KPIs that require selectors: Do not define anything in the **Selector** area, leave the selector expressions empty. After you click **OK** to add the KPI to the CI(s), Mercury Business Availability Center automatically replaces each blank selector with the default selector defined for the other KPIs attached to each CI.

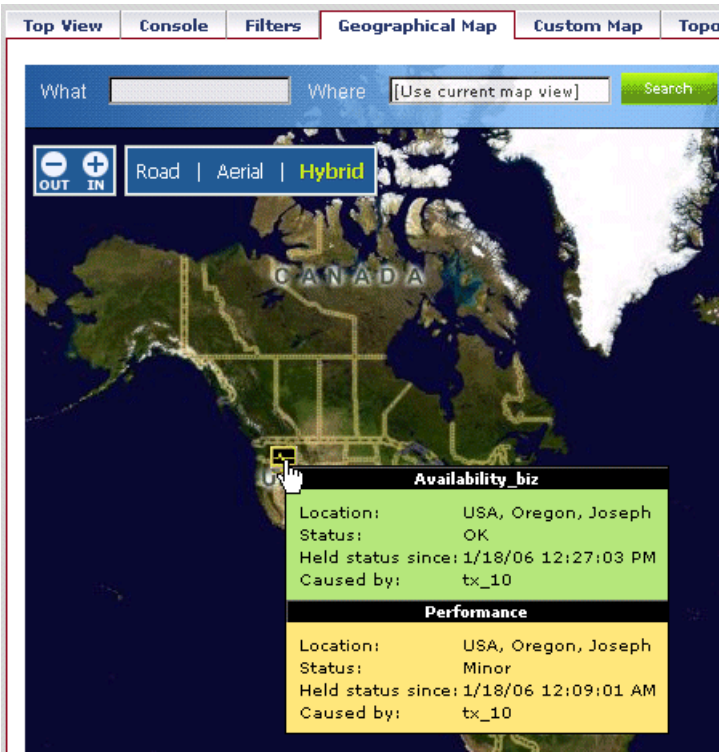
4 Click **OK** to save the KPI details. The KPI version is added to each selected CI, and propagates up the hierarchy to the parent CIs.

Result in Dashboard

Each user type sees in Dashboard the appropriate KPI version for their assigned user mode (operations or business user), for all KPIs that are defined as specific to a user mode. Users who are not assigned a user mode (undefined) see KPIs for both modes, as do system administrators:



In the Geographical Map and Custom Map tabs, status at a location is based on whichever KPI versions the user sees in Dashboard:



Notes and Limitations

- If you define different versions of a KPI, and another KPI is dependant on that KPI, then you must also define versions for the dependant KPI.

  For example, a CI has attached Availability and OT Impact KPIs, where OT Impact is based on Availability status. If you change Availability to **Availability_biz** and **Availability_ops**, then To have OT Impact function for both user modes, you must have two versions of the OT Impact KPI defined in the KPI Repository: **OT Impact_biz** and **OT Impact_ops**.

- In the **Admin** > **Dashboard** > **KPIs** page, both Availability KPI versions and both OT Impact KPI versions must be attached to each applicable CI. Each OT Impact version must have the appropriate KPI ID defined in the **StatusDimension** parameter.

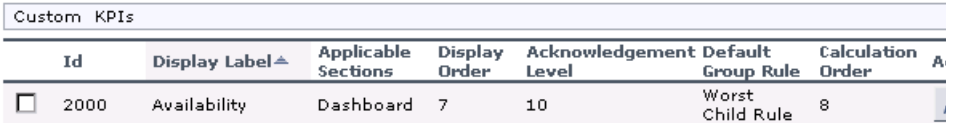
Example Scenario of KPI Versions for User Modes

In the following example scenario, two versions of the Availability KPI are set up, one for each user mode. The Availability_ops version uses the default objective values; however, when the Availability_biz version is attached to CIs, different objective values are defined.

To set up and use Availability KPI versions for user modes:

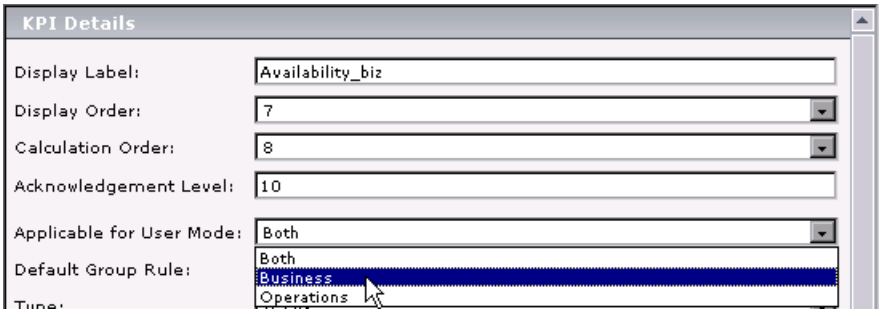
1 Access the **Admin** > **Dashboard** > **Repositories** > **KPIs** page.

2 In the **Factory KPIs** area, select the check box for the **Availability** KPI and click **Clone**. The cloned KPI is displayed in the **Custom KPIs** area.



3 Click the **Edit** button for the cloned KPI. In the displayed KPI Details window, edit the KPI properties as follows:

- In the **Display Label** box, add the suffix **_biz** to the **Availability** label.
- Select **Business** in the **Applicable for User Mode** list.



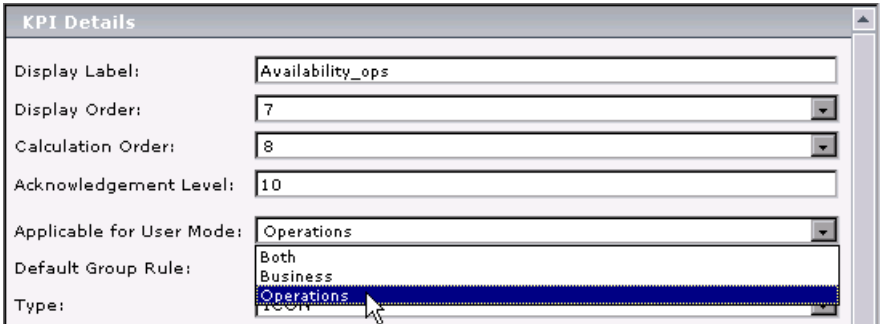
- Click **OK**.

4 In the **Factory KPIs** area, select the check box for the **Availability** KPI and click **Override**. The old Availability KPI is shown as overridden, and the new version of the KPI is displayed in the **Custom KPIs** area.

5 Click the **Edit** button for the new KPI. In the displayed KPI Details window, edit the KPI properties as follows:

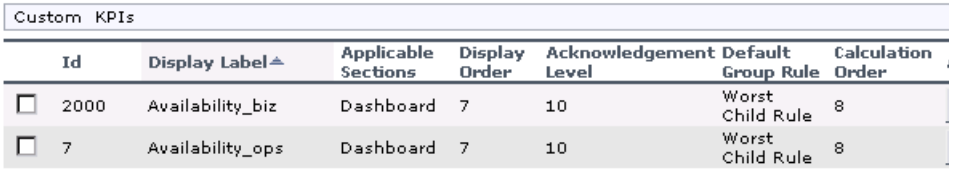
➤ In the **Display Label** box, add the suffix **_ops** to the **Availability** label.

➤ Select **Operations** in the **Applicable for User Mode** list.



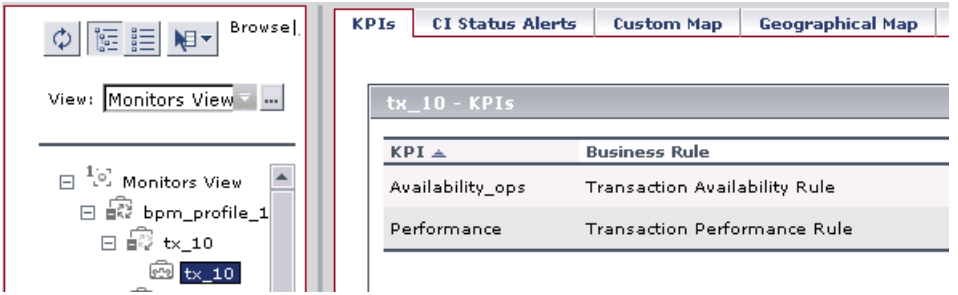
➤ Click **OK**.

The KPI names are displayed in the **Custom KPIs** area.

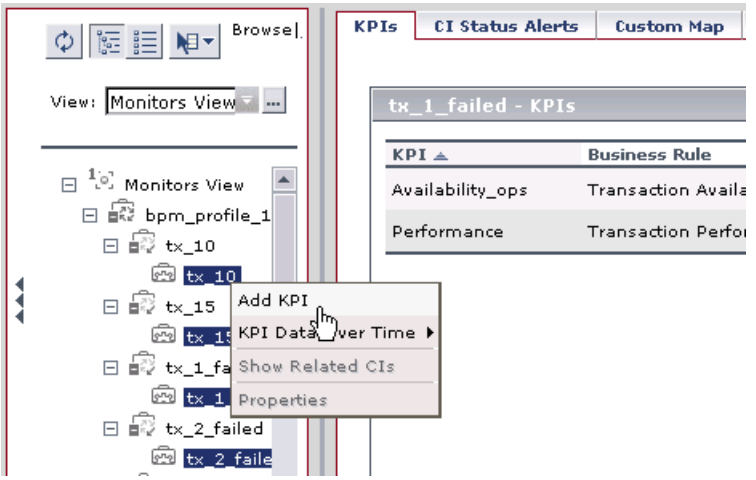


	Id	Display Label	Applicable Sections	Display Order	Acknowledgement Level	Default Group Rule	Calculation Order
☐	2000	Availability_biz	Dashboard	7	10	Worst Child Rule	8
☐	7	Availability_ops	Dashboard	7	10	Worst Child Rule	8

6 Access the **Admin** > **Dashboard** > **KPIs** page and open the **Monitors View**. For all BPM Transaction from Location CIs, the Availability KPI has been replaced with the Availability_ops KPI.



7 Add the Availability_biz KPI to all BPM Transaction from Location CIs. Use the keyboard CTRL key to select all the CIs, then right-click on one of the selected CIs and select **Add KPI**.

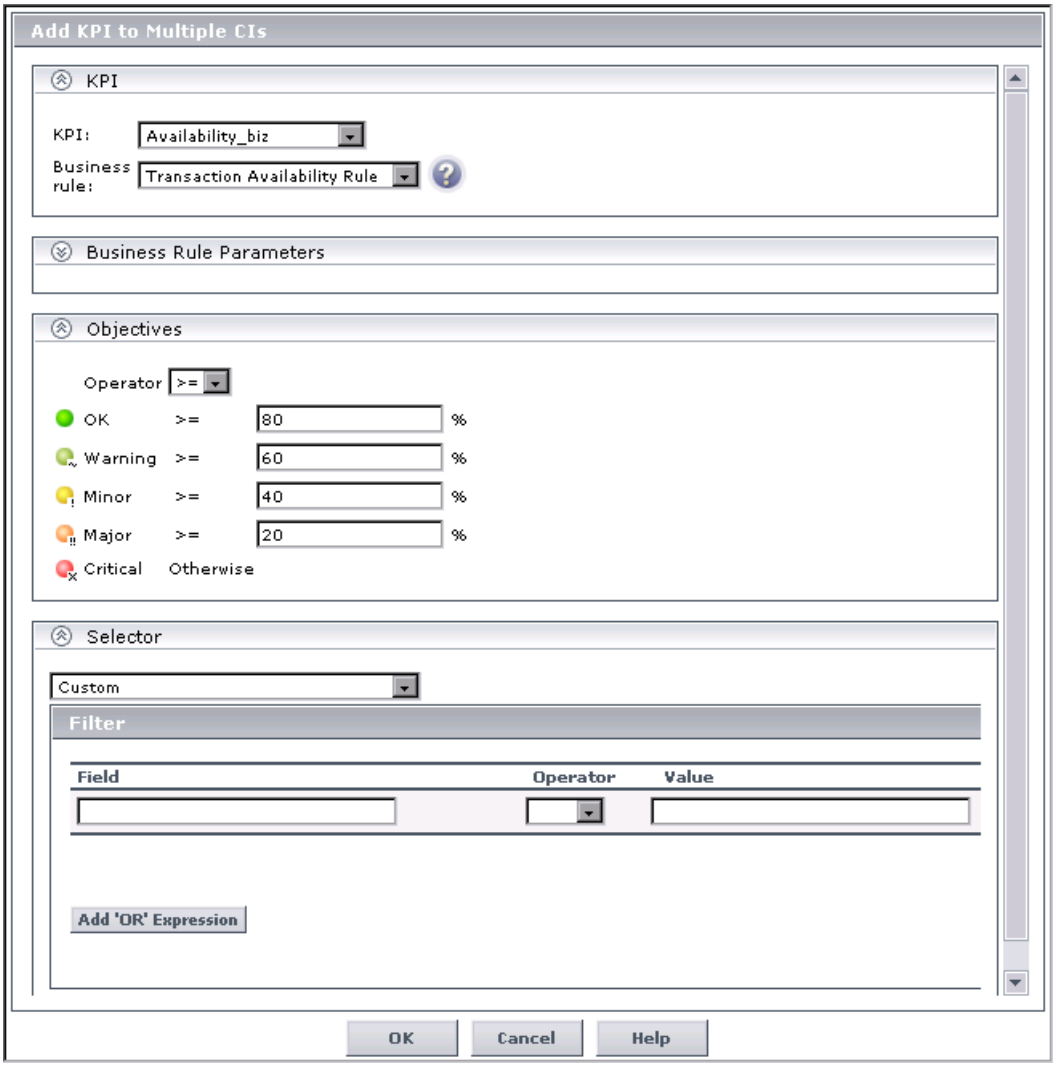


The Add KPI to Multiple CIs window opens.

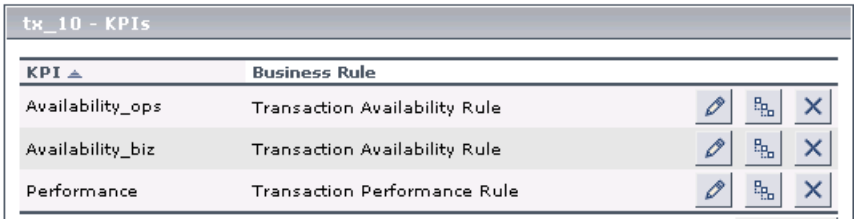
8 Edit the properties in the Add KPI to Multiple CIs Window as follows:

- Select **Availability_biz** in the **KPI** list.
- Select **Transaction Availability Rule** in the **Business rule** list.
- In the **Objectives** area, enter the objective values required for Availability KPI in business user mode: 80, 60, 40, 20.

➤ Leave the selector expressions empty.

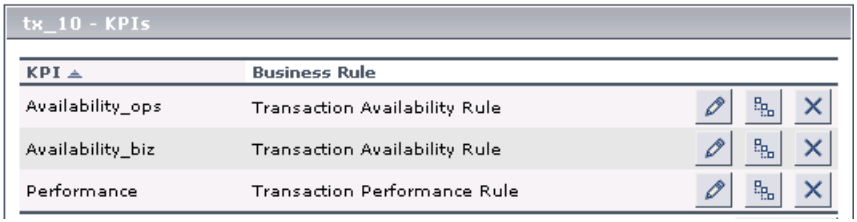


➤ Click **OK**. The Availability_biz KPI is added to the KPIs list for each selected CI.



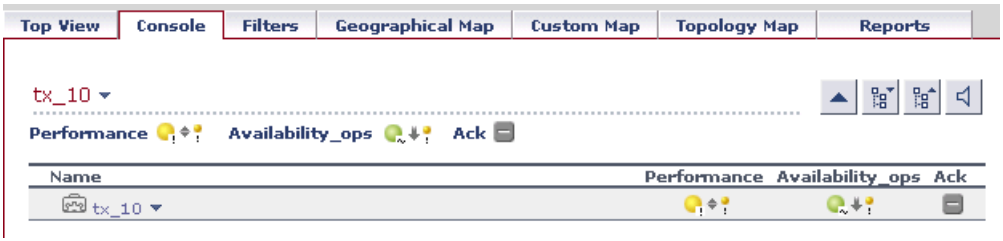
The appropriate selector is automatically defined for each new KPI, by copying the selector definitions for the other KPIs attached to the BPM Transaction from Location CI. (You can click the **Edit** button for the Availability_biz KPI to view the selector.)

The Availability_biz KPI also propagates up to the CI parents, using the default group rule for the KPI.



9 In the **Applications** > **Dashboard** > **Console** page, you can see the Availability KPI versions as follows:

➤ For users assigned **Operations** mode:



➤ For users assigned **Business** mode:

A CI may display different status for each Availability KPI version (although each KPI has the same Availability score), due to the different objective levels that are defined for each version.

3

Configuring CI Status Alerts

The CI Status Alerts tab in Dashboard Administration enables you to create alert schemes and attach them to CIs in a view, and to edit those alert schemes.

Introducing CI Status Alerts

Note: It is recommended to use the new CMDB-based alerting mechanism under **Admin** > **Dashboard** > **CI Status Alerts**, which provides greater granularity and flexibility for configuring alerts. The existing alerting mechanism under **Admin** > **Platforms** > **Alerts and Recipients** will be gradually phased out in future Mercury Business Availability Center versions.

Mercury Business Availability Center alerts proactively inform you when predefined performance limits are breached. To instruct Mercury Business Availability Center under what conditions to send alerts, you create alert schemes using a wizard.

Mercury Diagnostics – You can create CI status alerts on Diagnostics entities. For details, see this chapter and refer to *Mercury Diagnostics User's Guide*.

This section includes the following topics:

Types of Alerts

Two types of alerts are available:

- **monitor alerts.** You can create monitor alert schemes in **Admin** > **Platform** > **Alerts and Recipients.** For details, see Alerts Management in *Platform Administration*.
- **Configuration Item Status alerts.** You create CI Status alert schemes, and attach those alert schemes to KPIs or CIs in the CI Status Alerts tab accessed by selecting **Admin** > **Dashboard**. The decision to send an alert is handled by the rules. The alert engine sends alert messages (notifications) to the recipients, and executes the actions and executable files defined for the alert. The Configuration Item Status alerts are triggered by the Business Logic Engine.

Alerts Mechanism

Any changes you make to the alert schemes for a CI—adding new alert schemes, deleting alert schemes, or editing alert scheme properties—changes the CI in the Mercury Universal CMDB, so the changes are propagated to any view that includes the CI.

When an alert is triggered, it sends a pre-defined notification (via e-mail, SMS, or Pager) to a pre-defined recipient. Whenever a notification is sent, information related to the notification is logged into the CMDB. You can view the log in the Alert report. For details, see "Configuration Item Status Alerts Report" in *Using Dashboard*.

When an alert is triggered, the alert engine receives the message, gets the alert details from the CMDB, parses the alert messages, and sends the notification. The alert engine publishes the messages containing the information regarding the alert that was sent and the notifications. The Loader receives the alert and notification messages and inserts them into the CMDB database. The alert engine is persistent; if the process is restarted or crashes while an alert is being sent, it will resume as soon as the process is restarted. The messaging system supports guaranteed delivery.

Using the CI Status Alerts Tab

You can use the CI Status Alerts tab in Dashboard Administration to:

- create a CI Status alert scheme and attach it to a CI in a view. The rules attached to the CI's KPIs are used to trigger the alert(s).
- define the CI Status alert to apply to a specific KPI or to all the KPIs attached to the CI, so that any change to the status of one KPI triggers the alert. For details, see "Specifying the Alert Scheme General Information" on page 73.
- attach more than one CI Status alert to a CI.
- send the same CI Status alert notification to different recipients according to the CI status. For details, see "Administering Alert Schemes" on page 92.
- share the same CI Status alert scheme definition between several CIs. For details, see "Specifying the Related Configuration Items" on page 74.

Creating an Alert Scheme and Attaching it to a CI

You can create new alert schemes and attach them to any CI. You can attach more than one alert scheme to a CI, and you can attach the same alert scheme to more than one CI.

An alert attached to a CI in a view is attached to the CI in any view where the CI is included.

You can attach an alert scheme to a CI using a wizard that takes you through the following steps:

- "Specifying the Alert Scheme General Information" on page 73
- "Specifying the Related Configuration Items" on page 74
- "Specifying Templates and Recipients" on page 75
- "Specifying the Actions to be Triggered by the Alert" on page 77
- "Displaying the Alert Summary" on page 78

Specifying the Alert Scheme General Information

Use this step to define the alert scheme general information.

To specify the alert scheme general information:

1. Select **Admin** > **Dashboard**.
2. Click the **CI Status Alerts** tab to open the Configuration Item Status Alerts page.
3. Click **New Alert** to open the alert wizard General page.
4. In the **Name** box, enter the name of the alert scheme.
5. In the **Description** box, enter the alert scheme's description.
6. In the **Alert type** area, select:
   - **All KPIs** if you want the alert to be triggered by the specified status change in any of the KPIs attached to any of the selected CIs
   - **Selected KPIs** if you want the alert to be triggered by the specified status change in the selected KPIs attached to any of the selected CIs

     You select CIs and KPIs in the next step of the wizard. For details, see "Specifying the Related Configuration Items" on page 74.
7. In the **Condition** area, select one of the following options:
   - **Send alert once status worsens (not including "No Data" and "Downtime")** to trigger the alert when the current status of the KPI(s) is worse than the previous status. The **No Data** and **Downtime** statuses are not taken into consideration.

     For example, the alert is triggered when the status changes from Warning to Minor.
   - **Send alert once status improves (not including "No Data" and "Downtime")** to trigger the alert when the current status of the KPI(s) is better than the previous status. The **No Data** and **Downtime** statuses are not taken into consideration.

     For example, the alert is triggered when the status changes from Warning to OK.

- **Send alert if status value was changed from** to set the appropriate conditions for sending an alert. Select the appropriate status in the **from** box, and in the **to** box. The available statuses are: **critical, major, minor, warning, OK, no data, downtime, stop, and uninitialized.** For details, see "KPI Objectives" on page 38.

8 In the **Notification frequency** area, select one of the following options:

- **Send alert for every trigger occurrence** to send an alert notification every time an alert is triggered
- **Send no more than one alert per <time_period>** and specify the time period and unit to send an alert notification every time period

9 Click **Next** to open the **Related Configuration Items** page.

Specifying the Related Configuration Items

Use this step to specify the CIs and KPIs to which you want to attach to the alert scheme.

If you selected **All KPIs** in the **General** page (see step 6), then in the Related Configuration Items page, select the CIs to which you want to attach the alert scheme. The alert is triggered by the specified status change in any of the KPIs attached to any of the selected CIs.

If you selected **Selected KPIs** in the **General** page (see step 6), then in the Related Configuration Items page, select the CIs to which you want to attach the alert scheme. You must also select one or more of the KPIs that are listed in the KPIs area. The KPIs area lists all the types of KPIs that are attached to the selected CIs. The alert is triggered by the specified status change in the selected KPIs attached to any of the selected CIs.

You can share the same CI Status alert scheme definition between several CIs when you select more than one CI in the Related Configuration Items page.

To specify the related configuration items:

1 Access the Related Configuration Items page.

2 Select the CI(s) to which you want to attach the alert scheme from the View Explorer (you can expand the View Explorer if needed), and click the right arrow button to move your selection(s) to the **Selected Configuration Items** list. You can select multiple CIs using the CTRL key.

To deselect a CI, click it in the **Selected Configuration Items** list and click the left arrow button.

The alert is triggered by any change in any of the KPIs attached to the CI the alert scheme is assigned to.

3 If you selected **Selected KPIs** in the **General** page (see step 6), select the KPI(s) whose change of status will trigger the alert.

4 Click the **Properties** button to display the CI General Properties page. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.

5 Click **Next** to open the Templates and Recipients page.

Specifying Templates and Recipients

Use this step to define the alert recipients and templates. When an alert is triggered, an e-mail, SMS message, or Pager message is sent to a pre-defined recipient. The e-mail, SMS message, or Pager messages have a pre-defined templates. For details, see "E-Mail, SMS, and Pager Message Templates" on page 86.

To specify notification templates and recipients:

1 Access the Templates and Recipients page.

➤ **E-mail message template**. Choose between:

- Short HTML e-mail message, short text e-mail message – These messages include the change in status only.
- Long HTML e-mail message, long text e-mail message – These messages include a subject line and body.

➤ **SMS or pager template**. SMS and pager messages are sent via e-mail to the service provider. The pager messages use the same templates as the SMS messages.

The e-mail address is:
<SMS provider access number>@<SMS provider e-mail address>
or
<Pager provider access number>@<Pager provider e-mail address>.

Choose between:

- Long SMS/Pager message – The message includes the change in status and information about the SLA.
- Short SMS/Pager message – The message includes the change in status only.

For details on modifying the message character set, and about the structure of the e-mail, SMS, and Page message templates, see "E-Mail, SMS, and Pager Message Templates" on page 86.

2 In the **Available recipients** list, select the recipient(s) to whom you want notifications sent, and click the right arrow button to move your selection(s) to the **Selected recipient** list. You can select multiple recipients using the CTRL key. To deselect a recipient, click it in the **Selected recipient** list and use the left arrow button.

To define a new recipient, click **New Recipient.** For details, see "Configuring and Selecting Recipients" in *Platform Administration*.

The notification method that is used to notify a recipient depends of the recipient definition.

Note: You cannot use customized templates for e-mails, SMS messages, or Pager messages with the CI Status alerts.

---

3 Click **Next** to open the Actions page.

Specifying the Actions to be Triggered by the Alert

Use this step to define the user-defined alert handlers (actions) that will be triggered by the alert – for more information, see "Specifying a Notification URL" on page 78 and "Creating an Executable File" on page 80.

To specify the actions to be triggered by the alert:

1 Access the Actions page.

2 Choose from the following options:

- To open a URL when the alert is issued, click **New URL** to open the **Create New URL** page. For details, see "Specifying a Notification URL" on page 78.
- To execute an executable file when the alert is issued, click **New Executable File** to open the **Create Executable File** page. For details, see "Creating an Executable File" on page 80.
- To send an SNMP trap when the alert is issued, click **New SNMP Trap** to open the Create New SNMP Trap page. For details, see "Configuring an SNMP Trap" on page 83.

3 Click **Next** to open the Summary page.

Displaying the Alert Summary

The last step of the wizard displays a summary of the alert scheme definition.

To display the alert summary:

1. Access the Summary page to display the details of the alert scheme you created.
2. You can now:
   - ➤ click **Back** to go back to the previous wizard pages to modify the alert scheme definition
   - ➤ click **Finish** to save the new alert scheme
   - ➤ click **Cancel** to cancel the alert scheme definition
3. If you click **Finish**, the following message is displayed: **Alert was successfully saved**. Click **Close** to close the wizard and return to the Configuration Item Status Alerts page where the new alert scheme is displayed.

Specifying a Notification URL

You can create a notification URL to attach to an alert. This notification URL is used to pass alert information to external systems such as a customer Web application.

You can embed pre-defined alert parameters in the notification URL. The parameters are used as placeholders when the message is formatted.

To create a notification URL:

1. Access the **Create New URL** dialog box. For details on accessing this dialog box, see the Actions page in "Creating an Alert Scheme and Attaching it to a CI" on page 72.
2. In the **Field** list, select the name of the field and click **Insert Field**. The field appears between double angle-brackets in the **Enter URL** box.

The field values represent:

- **CI Name** – the name of the CI.
- **Alert Name** – the name of the alert scheme.
- **Trigger Time** – the time and date when the alert was triggered. The format is: dd/mm/yy hh:mm GMT[<offset>].
- **Previous Status** – the previous status of the KPI(s).
- **Current Status** – the current status of the KPI(s).

  The change from previous status to current status triggers the alert.
- **KPI Name** – the name of the KPI.
- **KPI Value** – the result of the calculation performed by the rule attached to the KPI. This is the result that triggered the alert.

3 Enter the URL in the **Enter URL** box.

4 Click **OK** to save the new URL.

Example: Creating a URL

To include the name of the CI and the current status of the CI in the URL proceed as follows:

1 Enter the following string in the **Enter URL** box:
http://dogbert.com/myjsp?entityname=

2 Select **CI Name** in the **Field** box and press **Insert Field** to insert the <<**CI Name**>> variable.

The string in the **Enter URL** box is now:
http://dogbert.com/myjsp?entityname=<<Entity Name>>

3 At the end of the string in the **Enter URL** box, enter severity=

4 Select **Current Status** in the **Field** box and press **Insert Field** to insert the <<**Current Status**>> variable.

The string in the **Enter URL** box is now:
http://dogbert.com/myjsp?entityname=<<Entity Name>> severity=
<<Current Status>>

Modifying the Default Centers Server URL

You can modify the default URL that appears in the notifications. This URL represents the URL of the Mercury Business Availability Center Centers server.

To specify the default Centers server URL:

1. Select **Admin** > **Platform**.
2. Click **Setup and Maintenance**.
3. Click **Infrastructure Settings**.
4. Select **Foundations**.
5. Select **Alerting**.
6. Scroll down to the **Alerting - Triggered alerts** area.
7.  Click the **Edit** button for the **Notification URL** parameter to open the **Notification URL** dialog box, enter the URL in the <processing_server> **Value** box, and click **Save** to save the changes. The <processing_server> is the name of the server where you are changing the Infrastructure Settings.

Creating an Executable File

Only users with administrative privileges can create an executable file to be run when the alert it is attached to is triggered. For details, see "Setting the Appropriate Administrative Privileges" on page 82. The executable file writes information in special logs or inserts information into external databases.

Note to Mercury Managed Services customers: To create an executable file, contact Mercury Managed Services Support.

This section includes the following topics:

Creating an Executable File

You can create an executable file and embed pre-defined alert parameters in the file. The parameters are used as placeholders when the message is formatted.

To create an executable file:

1 Access the **Create New Executable File** dialog box. For details on accessing this dialog box, see the Actions page in "Creating an Alert Scheme and Attaching it to a CI" on page 72.

2 In the **Field** list, select the name of the field and click **Insert Field**. The field you selected appears between double angle-brackets in the **Enter command** box. The field values represent:

- **CI Name** – the name of the CI.
- **Alert Name** – the name of the alert.
- **Trigger Time** – the time and date when the alert was triggered. The format is: dd/mm/yy hh:mm GMT[<offset>]
- **Previous Status** – the previous status of the KPI(s).
- **Current Status** – the current status of the KPI(s).

  The change from previous status to current status triggers the alert.
- **KPI Name** – the name of the KPI.
- **KPI Value** – the value of the KPI.

3 Enter the command in the **Enter command** box.

4 Click **OK** to save the new command.

Example: Creating An Executable File

To include the name of the CI in the command proceed as follows:

1. Enter the following string in the **Enter command** box:
   \\servername\myfolder\run.exe -name
2. Select **CI Name** in the **Field** box and press **Insert Field** to insert the <<**CI Name**>> variable.

   The string in the **Enter command** box is now:
   \\servername\myfolder\run.exe -name <<Entity Name>>

Setting the Appropriate Administrative Privileges

You can set the appropriate administrative privileges to create a command that can be attached to an alert scheme.

To set the appropriate administrative privileges:

1. Select **Admin** > **Platform**.
2. Click **Users and Permissions**.
3. Select **Permissions Management**.
4. Choose the **Monitors** context.
5. Click **Alerts - Run executable file**.
6. Select the **Operations** tab.
7. Set the permissions to **Change.** For details, see "Configuring User Permissions" in *Application Administration*.

Configuring an SNMP Trap

You can create an SNMP trap to attach to an alert. This SNMP trap is sent when the alert criteria is met. The alert notice can be viewed via any SNMP management console in the organization.

Note: Mercury Business Availability Center supports only SNMP V1 traps.

To enable alerts via SNMP trap, it is recommended that you configure your SNMP management console to read the Alerts MIB. For details, see "Configuring the Alerts MIB" in *Platform Administration*. This enables you to see names, rather than Object IDs (OIDs), when working in the management console.

Note: Mercury Business Availability Center uses the AM alerts MIB 5.0 by default and supports SNMPv1.

This section includes the following topics:

Creating an SNMP Trap

To create an SNMP trap, access the Create New SNMP Trap dialog box and specify the host address.

To create an SNMP trap:

1. Access the Create New SNMP Trap dialog box. For details on accessing this dialog box, see the Actions page in "Creating an Alert Scheme and Attaching it to a CI" on page 72.
2. Enter the host address in the **Enter destination host** box. You can use different formats:
   - <target_host_name|target_host_IP_address>
   - <target_host_name|target_host_IP_address>[:<port_number>]
3. Click **OK** to save the new SNMP trap.

Editing an SNMP Trap

To edit an SNMP trap, access the Create New SNMP Trap dialog box and specify the host address.

To edit an SNMP trap:

1. Access the SNMP Trap dialog box. For details on accessing this dialog box, see the Actions page in "Creating an Alert Scheme and Attaching it to a CI" on page 72.
2. Modify the host address in the **Enter destination host** box. Select one of the following options:
   - If you work with Alerts for profiles, use the following format:
     - <target_host_IP_address>
     - <target_host_IP_address>[:<port_number>]
   - If you work with CMDB, use the following format:
     - <target_host_name|target_host_IP_address>
     - <target_host_name|target_host_IP_address>[:<port_number>]
3. Click **OK** to save the new SNMP trap.

Specifying the Default SNMP Trap Host Address

You can specify a default host address: IP address, server name, and/or port number in the Alerting - Triggered Alerts area of the Infrastructure Settings. The default host address appears automatically in the **Enter host destination** box in the Create New SNMP Trap or in the Edit SNMP Trap dialog box.

If, when you create or edit an SNMP trap, you select the default host address and then modify the default host address in the Infrastructure Settings, the address in the SNMP trap you created is updated to the new default. Any alert that is sent causes the SNMP trap to be sent to the new default address.

To specify the default SNMP trap host address:

1. Select **Admin** > **Platform**.
2. Click **Setup and Maintenance**.
3. Click **Infrastructure Settings**.
4. Select **Foundations**.
5. Select **Alerting**.
6. Scroll down to the **Alerting - Triggered alerts** area.
7. If you are working with Alert for profiles (for details, see "Creating Alert Schemes" in *Platform Administration*) you can specify the default host address for all the customers as follows:

➤ Click the **Edit** button for the **Legacy SNMP Target Address** parameter to open the **Legacy SNMP Target Address** dialog box, enter the IP address in the **Value** box, and click **Save** to save the changes.

➤ Click the **Edit** button for the **Legacy SNMP Port** parameter to open the **Legacy SNMP Port** dialog box, enter the port number in the **Value** box, and click **Save** to save the changes

8 If you are working with CMDB, you can specify the default host address as follows:

➤ Click the **Edit** button for the **Default SNMP Target Address** parameter to open the **Default SNMP Target Address** dialog box, enter the IP address or the server name in the **Value** box, and click **Save** to save the changes.

➤ Click the **Edit** button for the **Default SNMP Port** – parameter to open the **Default SNMP Port** dialog box, enter the port number in the **Value** box, and click **Save** to save the changes.

E-Mail, SMS, and Pager Message Templates

Select the appropriate format for the notification(s) you want to send to the recipient(s). You can select any combination of e-mails, SMSs, or pager messages. This section details the structure of each format of e-mail, SMS, and Pager message templates.

Note: You cannot edit the e-mail, SMS, and Pager message templates.

This section includes the following topics:

Message Syntax

Select the e-mail template you want to use in the **E-mail message template** list. The message is displayed as a table or as text. The syntax can be a subset of one of the following:

➤ table format:

ci-name status has changed to *current-status*

Trigger TIme:	*trigger-time*
alert-name:	*alert-value*
KPI value:	*KPI-value*
Previous status:	*previous-status*
Alert name:	*alert-name*
Alert Description:	*alert-description*
URL:	*URL*

For more details login into Mercury Business Availability Center:
machine-address

➤ text format:

ci-name status has changed to *current-status*.
Trigger Time: *trigger-time* KPI Name: *KPI-name* KPI value: *KPI-value* Previous status: *previous-status* Alert name: *alert-name* (Long text) Alert Description:
alert-description

For more details login into Mercury Business Availability Center:
URL

where:

➤ **ci-name** – the name of the CI whose change of status triggered the alert.

➤ **current-status** – the new status of the CI.

- **trigger-time** – the time and date when the alert was triggered. The format is: dd/mm/yy hh:mm GMT[<offset>]
- **KPI-name** – the name of the KPI.
- **KPI-value** – the value of the KPI.
- **previous-status** – the previous status of the CI.
- **alert-name** – the name of the alert.
- **alert-description** – the description of the alert.
- **machine-address** – the URL of the machine where the status change occurred.
- **URL** – the URL of the Centers server. For details, see "Modifying the Default Centers Server URL" on page 80.

E-mail Message Templates

Select the e-mail template you want to use in the **E-mail message template** list.

- **Long text e-mail message**

  For example:

boston status has changed to critical.
Trigger Time: Wed, 6 Jul 2005 09:06:50 IDT Stam Test KPI Name: Availability KPI value: 90% Previous status: informational Alert name: boston failure (Long text) Alert Description:

For more details login into Mercury Business Availability Center: http://swall.mercury.co.il:80/topaz

➤ **Long HTML e-mail message**

For example:

boston status has changed to critical.

Trigger Time:	Wed, 6 Jul 2005 09:06:50 IDT
Test KPI:	Availability
KPI value:	90%
Previous status:	informational
Alert name:	boston failure
Alert Description:	

For more details login into Mercury Business Availability Center:
http://swall.mercury.co.il:80/topaz

➤ **Short HTML e-mail message**

For example:

boston status has changed to **critical**.
For more details login into Mercury Business Availability Center: http://swall.mercury.co.il:80/topaz

➤ **Short text e-mail message**

For example:

```
boston status has changed to critical.
For more details login into Mercury Business
Availability Center:
```

SMS and Pager Message Templates

Select the SMS or Pager template you want to use in the **SMS template** list.

- **Long SMS/Pager message** – Use the same template as the long text e-mail message. For details, see "E-mail Message Templates" on page 88.
- **Short SMS/Pager message** – Use the same template as the short text e-mail message. For details, see "E-mail Message Templates" on page 88.

Modifying the Message's Character Set

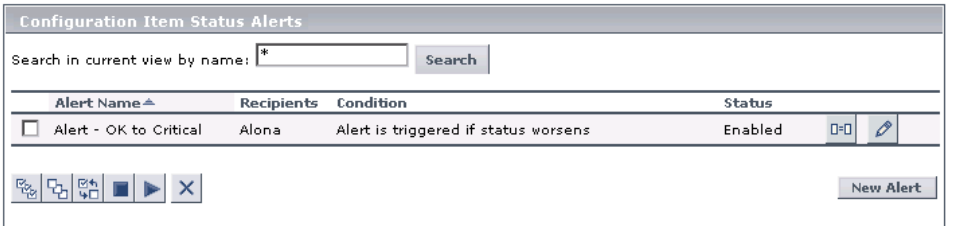
You can select one of the following character sets: **UTF-8** (default) or **ISO-2022-JP** for the e-mail, SMS, or Pager messages.

To modify the message's character set:

1. Select **Admin** > **Platform**.
2. Click **Setup and Maintenance**.
3. Click **Infrastructure Settings**.
4. Select **Foundations**.
5. Select **Alerting**.
6. Scroll down to the **Alerting - Triggered alerts** area.
7. To change the e-mail, SMS, or Pager alert character set, click the **Edit** button for the relevant parameter: **Email alerts charset**, **SMS alert charset**, or **Pager alert charset**.
8. In the page that opens, in the **Value** list, select the appropriate character set: **UTF-8** (default) or **ISO-2022-JP**.

Viewing the Alerts

After you complete defining an alert scheme, it is listed in the CI Status Alerts tab.



The Configuration Item Status Alerts page displays the following information:

Field	Description
Alert Name	The name of the alert scheme.
Recipients	The name(s) of the recipient(s).
Condition	A description of the condition.
Status	Indicates if the alert scheme is enabled or disabled.

You can perform the following actions:

- You can attach a new alert scheme to a CI. For details, see "Creating an Alert Scheme and Attaching it to a CI" on page 72.
- You can duplicate and edit an existing alert scheme. For details, see "Administering Alert Schemes" on page 92.
- You can delete an existing alert scheme. For details, see "Administering Alert Schemes" on page 92.
- You can enable or disable an alert scheme. For details, see "Administering Alert Schemes" on page 92.

Note: To make your selections, you can also use the buttons at the bottom of the page for, **Select All**, **Clear All**, and **Invert Selection**.

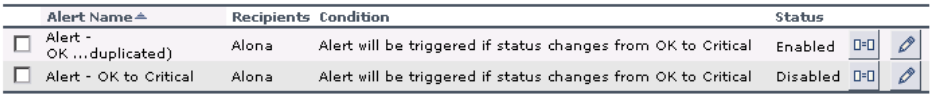
Administering Alert Schemes

You administer existing alert schemes by duplicating a scheme and customizing it, deleting a scheme that is no longer needed. You can also enable alert schemes so that they send notifications to the recipients when the appropriate KPI(s) status changes, or you can disable them. By default, alert schemes are enabled.

To duplicate alert schemes:

1 Access the Configuration Item Status Alerts page.

2 Click the **Duplicate** button next to the alert you want to duplicate. The duplicated alert scheme is listed under the first alert and the note **(Duplicated)** appears underneath the duplicated alert scheme as follows:



	Alert Name	Recipients	Condition	Status		
☐	Alert - OK ...duplicated)	Alona	Alert will be triggered if status changes from OK to Critical	Enabled		
☐	Alert - OK to Critical	Alona	Alert will be triggered if status changes from OK to Critical	Disabled		

3 Click the **Edit** button to edit the duplicated alert scheme. The Alert wizard opens. For details, see “Creating an Alert Scheme and Attaching it to a CI” on page 72.

To delete alert schemes:

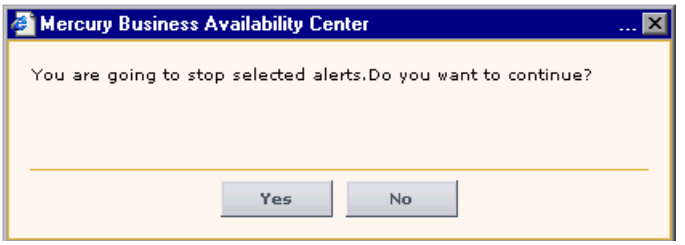
1 Access the Configuration Item Status Alerts page.

2 Select the alert scheme(s) you want to delete and click the **Delete** button to remove the alert scheme from the list.

To disable alert schemes:

1 Access the Configuration Item Status Alerts page.

2 Select the appropriate alert scheme(s) and click the **Click to disable selected alerts** button to issue a popup message.



The status of the alert scheme changes to **Disabled**. For example:

To enable alert schemes:

1 Access the Configuration Item Status Alerts page.

2 Select the appropriate alert scheme(s) and click the **Click to enable selected alerts** button to change the status of the alert scheme to **Enabled**. For example:

Searching for Specific CI Alert Schemes in the Current View

You can search for specific alert schemes assigned to a CI in the current view using the search feature. The search feature works only on alert scheme names.

You can, for example, search for all the alert schemes whose names include the string OK so that you can change their conditions.

To search for specific CI alert scheme(s):

1. Access the Configuration Item Status Alerts page.
2. In the **Search in current view by name** box, enter the string that you want to use to search for specific alert schemes.

   You can use the asterisk wildcard (*) to represent a string of characters and the question mark wildcard (?) to represent one character.
3. Click **Search** to display the alert schemes whose name correspond to the string.

4

Configuring the Custom Map

The Custom Map tab in Dashboard Administration enables you to create an association between a custom image that represents a view and real-time data.

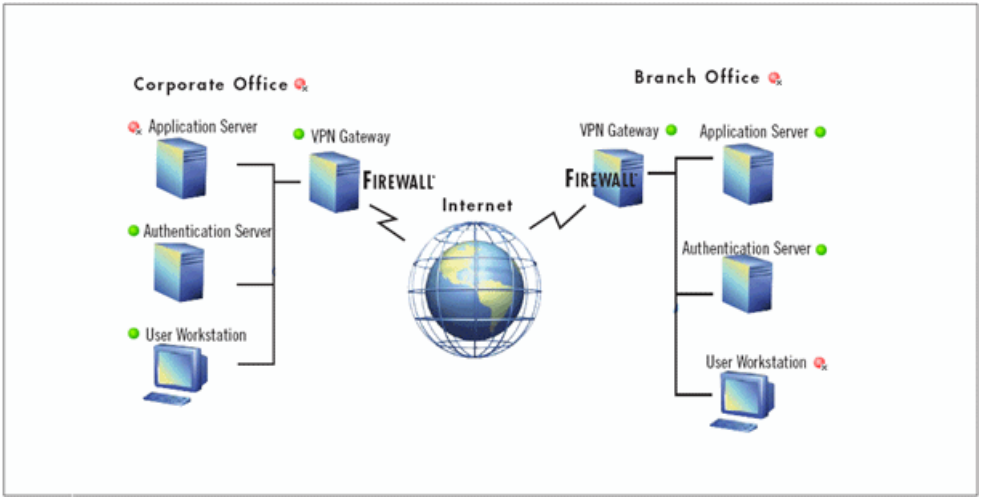
Overview of Custom Maps in Dashboard

The Custom Map feature allows you to associate a view's CIs and a custom image that describes the real world that your view represents.

You create a custom map by adding CI icons from the view and associating them with elements of the custom image.

In Dashboard, the custom map will display the CI icons as real-time status indicators – for details, see "Dashboard Custom Map" in *Using Dashboard*.

For example, you might associate a graph representing your company's network with real-time data coming from the different parts of the network.



One custom map can be defined for each view. If you do not define a custom map for a view, users accessing the Custom Maps tab, when that view is active, will see a message stating that there is no defined image.

In a custom map, you can use, as an image, any diagram or picture, created using any tool, provided that the format is supported by the Mercury Business Availability Center browser. It is recommended to use one of the following formats: **.gif**, **.jpg**, or **.png**

You can then add the view's CIs to the custom map, at the appropriate location. The status indicator shows the worst status (worst of all KPIs) for that CI.

Note: When a CI is removed from the IT universe model, the corresponding CI icon (in Dashboard Administration) and the corresponding status indicators (in Dashboard) are automatically removed from the relevant custom maps.

Configuring a Custom Map

To configure a custom map, select a view and specify the URL of the image you want to use for the view.

You can add CI icon(s) where appropriate on the image, to create an association between the image and the view.

Once you have created a custom map, you can delete CI icons from the diagram, revert to the previous custom map, delete the entire custom map, refresh the image, or move a single CI icon to a new location.

This section includes the following topics:

Creating a Custom Map for a View

You create a custom map by selecting a view and attaching the URL of the custom image to that view.

The image URL can use HTTP or HTTPS, but must be in the format:
http://*hostname*/*path_to_image*

If you would like to use a local machine as the location of the image, enter the URL with the following format:
file:///*path_to_image*

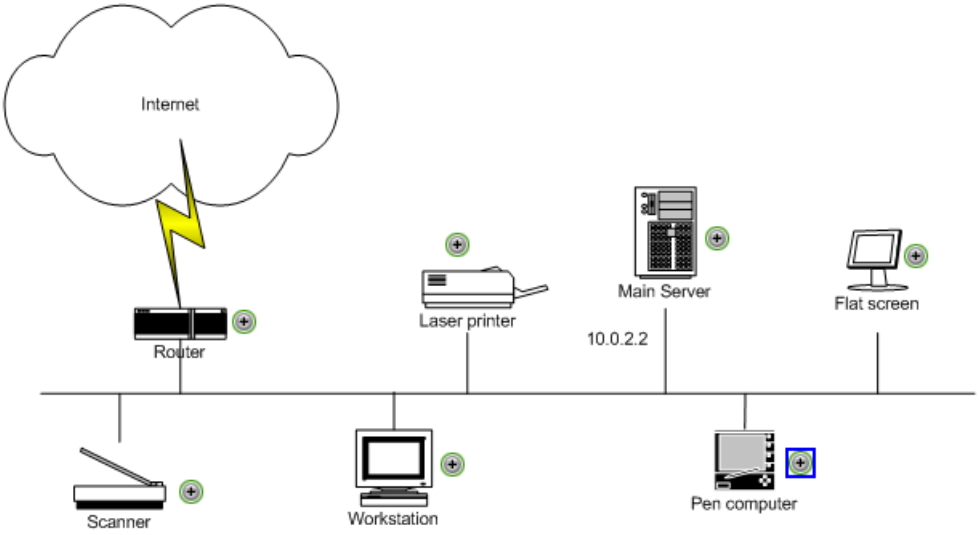
This results in an image that cannot be displayed for a user working outside the local network.

You can also use a file-sharing path as follows:
*server**path_to_image*

Any type of image that can be displayed by the browser can be loaded from any URL the user can access (including HTTP protocol and HTTP authentication). You must make sure that the URL is available at all times.

The best image depends on the customer's environment. The custom map feature does not resize the image, so in higher resolution screens it looks different from the same image in lower resolution screens. Additionally, you can view the Custom Map tab with or without View Explorer which influences the size of the image you want to display.

For example:



To create a custom map for a view:

1. Select **Admin** > **Dashboard**.
2. Click the **Custom Map** tab to open the Custom Map Administration page.
3. Select the appropriate view in the View Explorer.
4. In the **Image URL** box, enter the URL of the diagram that will be used for the view. Click the **Refresh** button to display the diagram.

Tip: You can use the **Refresh** button at any time to reload the diagram (for example, if changes have been made to the source file). Reloading the diagram will not affect the position of the item indicators.

5 For each CMDB CI that you want to associate with a location in the diagram:

- ➤ Select the CI in the View Explorer.
- ➤ Click **Add CI Icon.** The CI icon is displayed in the left top corner of the diagram. The CI icon you just added is shown with a blue outline.
- ➤ Drag the CI to the required location in the diagram.

The CI icon is set at that position.

6 When you have added the required CI icons, click **Save** to save the changes.

Removing All the CI Icons from a Custom Map

You can remove all the CI icons from a custom map.

To remove all CI icon(s) from a custom map:

1 Select **Admin** > **Dashboard**.

2 Click the **Custom Map** tab to open the Custom Map Administration page.

3 Select the appropriate view in the View Explorer.

4 Click **Clear CI Icons**. A confirmation message is issued: **You are about to clear all nodes from the view. Are you sure?**

5 Click **OK** to delete all the CI icons.

Reverting to the Previous Custom Map

If you have made changes to a custom map, you can revert to the last saved configuration before you save the changes.

To revert to the previous custom map:

1. Select **Admin** > **Dashboard**.
2. Click the **Custom Map** tab to open the Custom Map Administration page.
3. Select the appropriate view in the View Explorer.
4. Click **Revert**. The diagram reverts to the situation at the last **Save**.

Deleting the Image and the CI Icons of a View

You can delete the image and all the CI icons associated with a view.

To delete the image and the CI icons of a view:

1. Select **Admin** > **Dashboard**.
2. Click the **Custom Map** tab to open the Custom Map Administration page.
3. Select the appropriate view in the View Explorer.
4. In the **Custom Map** tab, click **Delete Image**.
5. Click **OK**. The image and CI icons are removed from the page.

Refreshing the Image

You can refresh the image after it has been modified.

To refresh the image:

1. Select **Admin** > **Dashboard**.
2. Click the **Custom Map** tab to open the Custom Map Administration page.
3. Select the appropriate view in the View Explorer.
4.  Click the **Refresh** button to refresh the image. The CI icons are not removed or moved.

Moving a CI Icon

You can move a CI icon to another location in the custom map.

To move a CI icon:

1. Select **Admin** > **Dashboard**.
2. Click the **Custom Map** tab to open the Custom Map Administration page.
3. Select the appropriate view in the View Explorer.
4. Click the appropriate CI icon. The CI icon you just added is shown with a blue outline.
5. Drag it to the new location.

Hints and Tips

CI icons should not overlap otherwise you will see only the top status indicator in the custom map.

After setting a CI icon on the diagram, you can move the cursor over it to display the CI name in a tooltip – for details about the tooltip, see "CI Status Indicator Tooltip" in *Using Dashboard*.

5

Configuring the Geographical Map

The Geographical Map tab enables you to create an association between geographical locations and status indicators using a maps applet, Google Earth, or Virtual Earth.

About Configuring the Geographical Map

In Dashboard, a geographical map is associated with a view. If you have specified locations for the view's CIs, real-time status indicators representing the CIs statuses are displayed on the map at those geographical locations.

To determine the status of a location, Dashboard takes the worst status for all KPIs relevant for each CI, for all CIs that are attached to the location.

In Dashboard Administration, in the geographical map, you can shift the map's focus and enlarge or shrink the map to fit the view it represents. This modified map will automatically be displayed when you select the view in the Geographical Map tab in Dashboard. For details, see "Dashboard Geographical Map" in *Using the Dashboard*.

Note: The Virtual Earth map is only available in English and cannot be translated. For localization purposes, use the Maps Applet. The Maps Applet does not display the names of cities or countries.

You can select one of the following technologies to display the map:

- if you have an Internet connection, use Virtual Earth. This is the default. For details, see "Working with Virtual Earth Geographical Map" on page 108.
- if you do not have an Internet connection, use the maps applet. For details, see "Working with the Maps Applet Geographical Maps" on page 113.

You can also display a map using Google Earth. For details, see "Working With Google Earth" on page 117.

For details on how to select the type of display, see below.

Selecting the Type of Display Used for Geographical Maps

By default the technology used to display geographical maps is Virtual Earth. You can change the default and select to work with the maps applet or with Google Earth.

If you want to work with Google Earth (only available for administrators) you must specify that you want to display the **Export to Google Earth** button in the Geographical Map tab in Dashboard Administration.

This section includes the following topics:

- "Selecting the Technology to Be Used to Display Geographical Maps" on page 105
- "Specifying That you Want to Display the Export to Google Earth Button" on page 106

Selecting the Technology to Be Used to Display Geographical Maps

By default the technology used to display geographical maps is Virtual Earth (the **Use Virtual Earth** parameter is set to **true**). You can change the default and select to work with the maps applet or with Google Earth (the **Use Virtual Earth** parameter is set to **false**).

To select the technology to be used to display geographical maps:

1. Select **Admin** > **Platform**, click the **Setup and Maintenance** tab, and click **Infrastructure Settings**.
2. Select the **Applications** context, and the **Dashboard Applications** in the **Applications** list.
3. Scroll down to the **Dashboard Application - Maps Management Properties** area.
4.  Click the **Edit** button for the **Use Virtual Earth** parameter to open the Use Virtual Earth page.
5. Select one of the following options:
   - **true** – to use Virtual Earth geographical map. By default, Virtual Earth is enabled. Use this option if the user has an Internet link.

     For details on Virtual Earth, see "Working with Virtual Earth Geographical Map" on page 108
   - **false** – to use the maps applet or Google Earth. Use this option if the user does not have an Internet link.

     For details on the maps applet, see "Working with the Maps Applet Geographical Maps" on page 113. For details on Google Earth, see "Working With Google Earth" on page 117.
6. Click **OK** to save the changes.

Specifying That you Want to Display the Export to Google Earth Button

You can also specify that you want to display the **Export to Google Earth** button in the Geographical Map tab in Dashboard Administration.

To specify that you want to display the Export to Google Earth button:

1. Select **Admin** > **Platform**, click **Setup and Maintenance**, click **Infrastructure Settings**.
2. Select **Dashboard Application** in the **Applications** list.
3. Scroll down to the **Dashboard Application - Maps Management Properties** area.
4. Click the **Edit** button corresponding to the **Enable Export to Google Earth button** and select one of the following:
   - **true** – to display the **Export to Google Earth** button in the Geographical Map tab in Dashboard Administration. This is the default.
   - **false –** to hide the **Export to Google Earth** button.

Note to Mercury Managed Services: The **Export to Google Earth** button is not available when working with Mercury Managed Services.

---

5. Click **OK** to save the changes.

Assigning a Geographical Map to a View

Once you have selected the technology to display the geographical map, you must assign a map to a view. You can then adjust the map focus and magnification until you have the required display.

If you assigned geographical location to a view's CIs, the corresponding status indicators are displayed on the map as soon as you assign a map to the view. For details on how to define a CI's geographical locations, see "Configuration Item Properties" in *IT Universe Manager Administration*.

To remove CI icons from the map, you must delete their geographical location.

The city names use UTF8 format. If Mercury Business Availability Center is working with MS-SQL Server, or with an Oracle Server that is not configured for UTF8 support, then when the name of a city includes non-English characters (for example, é), these characters are displayed as empty square brackets [ ].

You assign a map to a view by selecting a view in the Geographical Map and saving the map.

To assign a geographical map to a view:

1 Select **Admin** > **Dashboard**.

2 Click the **Geographical Map** tab to open the Geographical Map Administration page.

3 Select the appropriate view in the **View** list in View Explorer.

4 You can then:

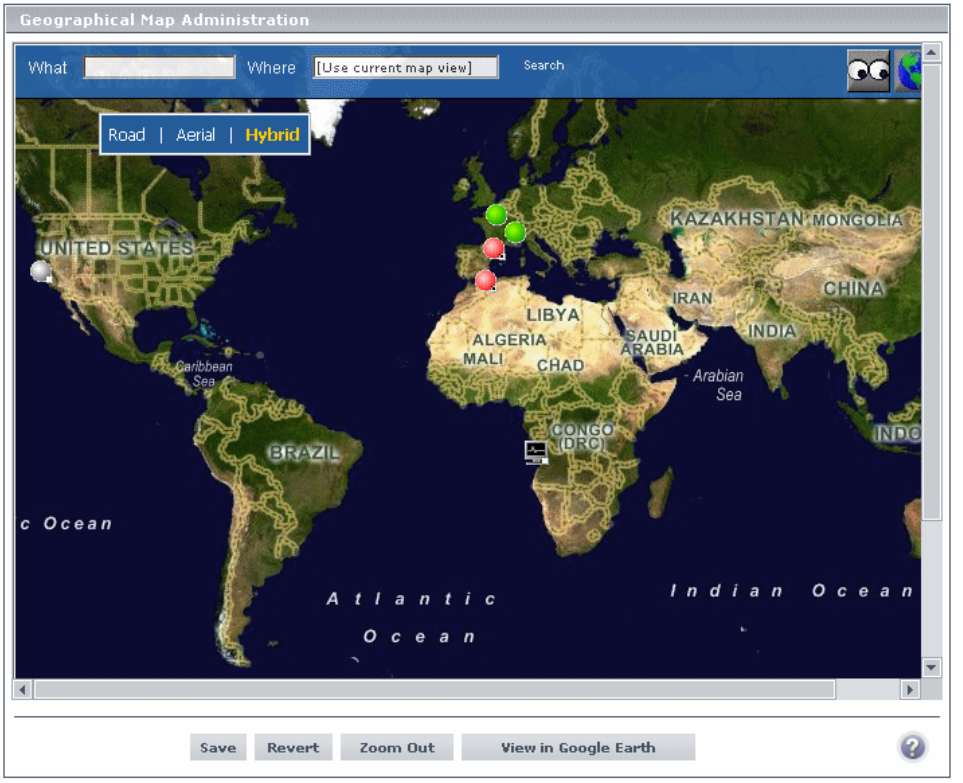
- shift the map focus and magnification to create the map display for the view – how to do that depends on the type of display you selected. You can also do that at a later time.
- click **Revert** to go back to the previously saved geographical map.
- click **Zoom Out** to go back to displaying the complete map.
- click **View in Google Earth** to display the map in 3D if you set the **Use Virtual Earth** parameter to **false**. For details, see "Working With Google Earth" on page 117.

5 Click **Save** to save your changes.

Working with Virtual Earth Geographical Map

If you have an Internet connection you can display the geographical map using Microsoft MSN Virtual Earth. Mercury Business Availability Center integrates Virtual Earth online mapping functionality, available over MSN, to enable you to use the geographical map of a view. If the view's CIs are assigned geographical locations, real-time status indicators are displayed on the map at those geographical locations.

Virtual Earth geographical maps are based on Microsoft Network (MSN) technology and use dynamic HTML.



The Virtual Earth geographical map presents a flat geopolitical view of the planet where you can display only the country borders, only the geographical features, or both.

When you magnify the view, the main cities appear for the part of the map that is displayed on the screen.

This section includes the following topics:

Viewing More Information About the CI

Double-click a status indicator to open the KPIs Over Time report for the CI. For details about the KPIs Over Time report, see "KPIs Over Time Reports" in *Using Dashboard*.

Adjusting a Virtual Earth Map

For each view, you can set a default focus area and magnification to adjust the map to the view. You can:

- click the flag button to shift center of map to the nearest CI.
- double-click on the map to zoom in.

- click the globe button to zoom out completely.
- click on map and drag to move the map in the window.

Click **Save** to save the map magnification and focus. Those settings become the default settings for the user's map.

Modifying Virtual Earth Settings

To work with Virtual Earth geographical map, you must set the **Use Virtual Earth** parameter to **true**. For details, see "Selecting the Type of Display Used for Geographical Maps" on page 104.

You can also specify the size of the indicators, whether to ignore gray statuses, and the time delay between the completion of new location download from the server and the display of the information by Virtual Earth.

This section includes the following topics:

Specifying the Size of the Indicators

You can modify the default size (19 pixels) of the indicators that are displayed on the Virtual Earth map.

To specify the size of the indicators:

1. Select **Admin** > **Platform**, click the **Setup and Maintenance** tab, and click **Infrastructure Settings**.
2. Select the **Applications** context, and the **Dashboard Applications** in the **Applications** list.
3. Scroll down to the **Dashboard Application - Maps Management Properties** area.
4. Click the **Edit** button for the **Indicator size in Virtual Earth** parameter to open the Indicator Size in Virtual Earth page.
5. Enter the size (in pixels) of the indicator in the **Value** field. The default is 19.
6. Click **OK** to save the changes.

Specifying the Statuses to Be Displayed

You can select the statuses you want to display in the Virtual Earth map.

To specify the statuses to be displayed:

1. Select **Admin** > **Platform**, click the **Setup and Maintenance** tab, and click **Infrastructure Settings**.
2. Select the **Applications** context, and the **Dashboard Applications** in the **Applications** list.
3. Scroll down to the **Dashboard Application - Maps Management Properties** area.
4. Click the **Edit** button for the **Ignore gray statuses** parameter to open the Ignore Gray Statuses page.

5 Select one of the following options:

- **ALL** – locations with gray statuses (downtime, stopped, no data and uninitialized) are not displayed on the map.
- **NO** - locations with gray status are displayed on the map.
- **UNINITIALIZED** - locations with gray statuses (downtime, stopped, and no data) are displayed on the map, locations with uninitialized status are not displayed.

6 Click **OK** to save the changes.

Specifying the Time Delay

You can modify the default time delay between the completion of new location download from the server and the display of the information by Virtual Earth (in seconds). Use larger values if user has slower connection.

To specify the time delay:

1 Select **Admin** > **Platform**, click the **Setup and Maintenance** tab, and click **Infrastructure Settings**.

2 Select the **Applications** context, and the **Dashboard Applications** in the **Applications** list.

3 Scroll down to the **Dashboard Application - Maps Management Properties** area.

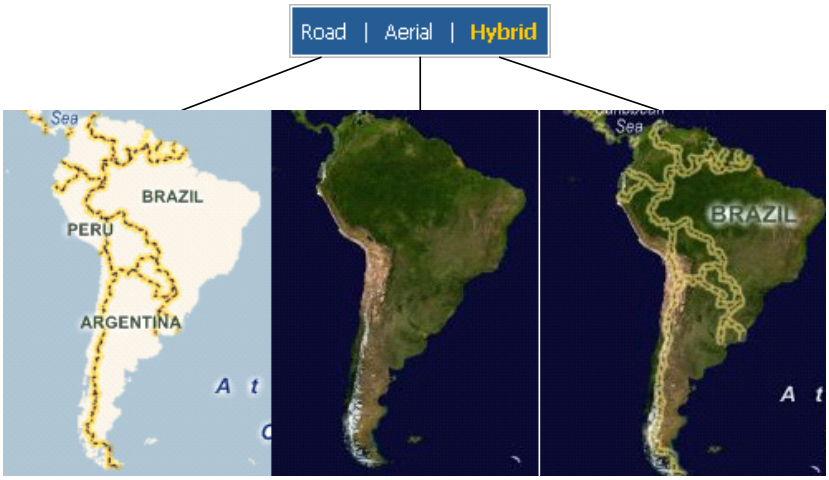
4 Click the **Edit** button for the **Wait after getting data** parameter to open the Wait After Getting Data page.

5 Enter the delay (in seconds) in the **Value** field. The default is 4.

6 Click **OK** to save the changes.

Modifying the Virtual Earth Map Display

To help you when you create a geographical map, you can select different types of display. You cannot save the selected display. The same tools are available to the user in Dashboard.

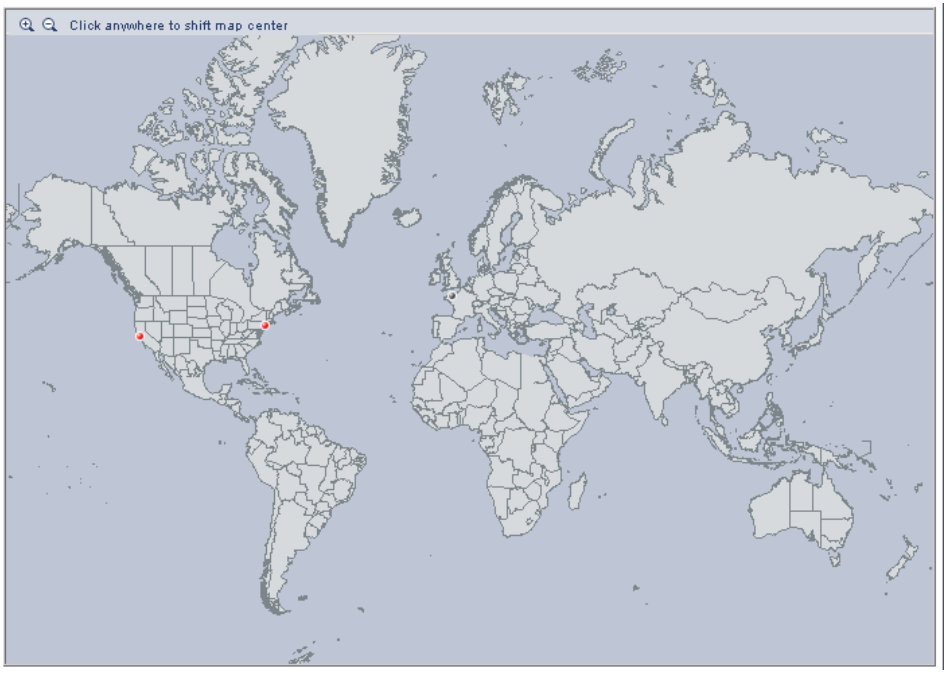


- click **Road** – to display the map with country borders
- click **Aerial** – to display the map with topographical features
- click **Hybrid** – to display the map with both country borders and topographical features

Working with the Maps Applet Geographical Maps

The map applet present a flat geopolitical view of the planet. When you magnify the view, the main cities appear for the part of the map that is displayed on the screen.

You can use the maps applet to display the geographical map of a view. The map displays the worst status at each geographical location and detailed information about the CI's KPIs.



Note: The maps applet requires that Sun JRE plug-in 1.4.2_08 or later be installed on the client machine. If an earlier version is installed, then Mercury Business Availability Center will automatically try to download JRE 1.4.2_08 when you access the maps applet.

Once you have assigned a geographical map to a view you can adjust the map and modify its settings. For details, see "Assigning a Geographical Map to a View" on page 106.

This section includes the following topics:

Viewing More Information about a CI

Tooltips provide the overall status for each KPI associated with the location, and how long the KPI has been at that status – for more details, see "Geographical Map Tooltips" on page 121.

Adjusting a Map Applet

For each view, you can set a default focus area and magnification to adjust the map to the view. You can:

- click the area that interests you. The map shifts to make the location you clicked the new center of the map.

- use the **Zoom In** and **Zoom Out** buttons in the top-left corner of the map pane to enlarge or shrink the map.

Click **Save** to save the map magnification and focus. Those settings become the default settings for the user's map.

Modifying the Map Applet Settings

To work with the map applet geographical map, you must set the **Use Virtual Earth** parameter to **false**. For details, see "Selecting the Type of Display Used for Geographical Maps" on page 104.

You can also modify the refresh rate of the geographical map, and the maximum number of tooltips per location. You can also specify whether you want to display the **Export to Google Earth** button in the geographical map.

This section includes the following topics:

Specifying the Map Refresh Rate

You can modify the default of the map refresh rate. The default is 30 seconds.

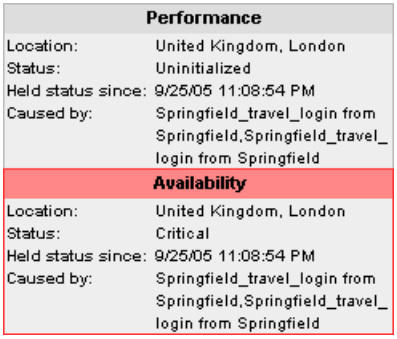
To specify the map refresh rate:

1. Select **Admin** > **Platform**, click **Setup and Maintenance**, click **Infrastructure Settings**.
2. Select **Dashboard Application** in the **Applications** list.
3. Scroll down to the **Dashboard Application - Maps Management Properties** area.
4. Click the **Edit** button corresponding to the **Maps Applet Refresh Rate** and enter the new refresh rate.
5. Click **OK** to save the changes.

Specifying the Maximum Number of CIs Displayed in a Location's Tooltip

You can specify the maximum number of CIs that can be displayed in the tooltip for a location in the Geographical Map. The default is 10.

Do not make this value too large, as it represents the number of CIs shown in the **Caused by** section of the tooltip.



To specify the maximum number of CIs displayed in a location's tooltip:

1. Select **Admin** > **Platform**, click **Setup and Maintenance**, click **Infrastructure Settings**.
2. Select **Dashboard Application** in the **Applications** list.
3. Scroll down to the **Dashboard Application - Maps Management Properties** area.
4. Click the **Edit** button corresponding to the **Maximum CIs in tooltip for location** and enter the new maximum.
5. Click **OK** to save the changes.

Working With Google Earth

Note to Mercury Managed Services: This feature is not available when working with Mercury Managed Services.

You can view the geographical map information in a three-dimensional map using the Google Earth feature. This feature is available only to the administrator.

Note: The integration of CI locations with your Google Earth installation is at the beta stage.

This section includes the following topics:

Importing Location Status into Google Earth

You can import the location status information shown in the geographical map for the current view into a local Google Earth application. After importing the information, Google Earth displays all the CI status indicators in the appropriate geographical locations.

To have all the views you created listed in the same folder, create, for example, a Mercury Business Availability Center folder in the **Places** folder in Google Earth and then add to that folder all the views you create.

You create a view in Google Earth by creating a network link using the view's URL. This creates a container folder and a sub-folder.

To import location status into Google Earth:

1. If you have not already installed Google Earth on your local computer, open the Google Earth site (http://earth.google.com/) and download the application.
2. Open the Google Earth application.
3. Click the **My Places** directory in the **Places** area.
4. Select **Add** > **Network Link**.

   The **Google Earth - New Network Link** dialog box opens.
5. Enter the view name in the **Name** box.
6. Copy the URL displayed in the **Integration with Google Earth** page to the **Location** box.

Note: This URL creates a container folder called by the name you specified in the **Name** box, and a sub-folder called by the name of the view.

---

7. If this is the first time you are creating a view in Google Earth, in the **Create In** area, click **New Folder** and enter **Mercury Business Availability Center** to create a new folder called Mercury Business Availability Center.

   If the Mercury Business Availability Center folder already exists in the **Create In** area tree: select the folder (you can also set the cursor on that folder before you select **Add** > **Network Link** in step 4).
8. Click **OK** to close the New Network Link dialog box.

The Google Earth page displays the Mercury Business Availability Center folder in the Places area.

Open that directory to list the views you have added.

Setting the Refresh Rate for the View

You set the refresh rate of the view sub-folder.

To set the refresh rate for the view:

1 Right-click the view sub-folder.

2 Select **Edit**.

3 Select **Refresh Parameters** to open the **Time-Based Refresh** area.

4 In the **Time-Based Refresh** area, select **Periodically** from the **When** list and select **1** minute.

5 Click **OK**.

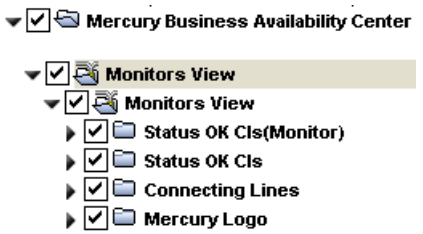
Viewing Indicators by Status

You can filter the status indicators that are displayed in Google Earth to include specific statuses.

To view the indicators by status:

1 In the **Places** area, expand the **Mercury Business Availability Center** folder.

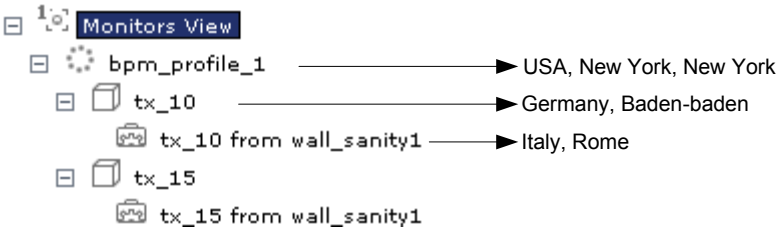
2 Select the view you want to display. The folder displays the list of statuses of the CIs in the view.



3 Select one or more of statuses to filter out the CIs that do not have the selected statuses. Only the CIs with the selected statuses will be displayed in Google Earth.

Viewing Connecting Lines

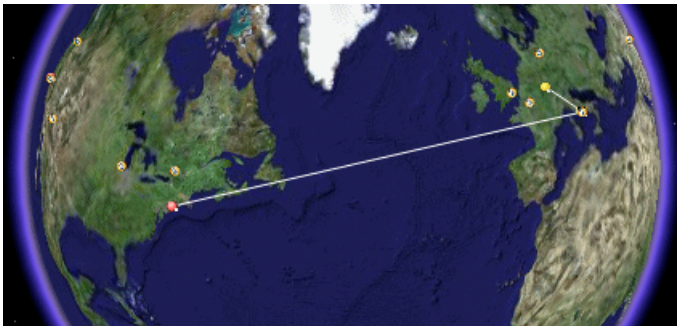
Different locations are connected with a line when you specify different geographical locations for monitor CIs and non-monitor CIs that are monitored by the monitor CI in the view. For example:



To view the connecting lines:

1 In Google Earth, select the view you want to display.

2 Select **Connecting Lines** in your view folder to display the connecting lines in Google Earth:



If you select **Connecting Lines** in more than one view, you will see all the lines of all the selected views at the same time.

6

General Administration for Dashboard

This chapter describes some of the settings that can be modified to customize Dashboard and logs that you can use to verify that Dashboard is running properly.

Note: Only the administrator or users with the appropriate permissions can modify the infrastructure settings.

About General Customization Options for Dashboard

This chapter describes some of the elements of Dashboard that you can customize to your specifications in Infrastructure Settings in Platform Administration.

You can:

- specify the URL of an external application to be opened from Top View – for details see "Accessing an External Application from Top View" on page 125
- specify the layout of the hierarchy in Top View – for details see "Customizing the Layout of the Hierarchy in Top View" on page 127
- enable the display of Chinese or Japanese characters in Top View – for details see "Enabling Chinese or Japanese Characters in Top View" on page 130
- modify the number of levels displayed in the Console tabs – for details see "Modifying the Number of Levels in the Console Tab" on page 130
- modify the sound alert for Red Status in the Console and Filter tabs – for details see "Sound Alert for Critical Status in the Console and Filter Tabs" on page 131
- hide or show the Ack column – for details see "Hiding or Showing the Ack Column" on page 131
- modify the Change History Period for the Change report – for details see "Specifying the Changes Period for the Change Report" on page 132
- specifying the number of CIs that can be monitored for change in real-time – for details see "Specifying the Number of CIs that Can Be Monitored for Change in Real-Time" on page 133

Accessing an External Application from Top View

You can configure Dashboard Top View so that a user can open an external application. You do that by specifying the URL for the external application on the Infrastructure Settings page.

Specifying a URL automatically adds the **Open in New Window** option to the right-click menus in Top View. By default, no URL is specified and the **Open in New Window** option does not appear in the right-click menus in Top View.

You can also use a dynamic URL that can be used to integrate external tools with Mercury Business Availability Center for example – for details, see "To create a Dynamic URL:" on page 126.

To specify the URL of an external application:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.

2 Select the **Applications context**, and select **Dashboard Application** in the Applications context list.

3 Scroll down to the **Top View Properties** area.

4 Click the **Edit** button to the right of the **Top View URL to Open** property to open the Top View URL to Open window.

5 Enter the URL in the **Value** box and click **Save**.

If you want to reset the URL to the default (empty), click **Default**.

Note:

- The change takes place immediately.
- The user must disable his browser's popup blockers to open a window with the external application.

To create a Dynamic URL:

You can also create a dynamic URL using the following syntax (HTTP GET format):

```
http://<URL>?nodeName=NODE.NAME&nodeId=NODE.ID
&nodeStatus=NODE.STATUS&nodeParentId=NODE.PARENTID
&nodeChildId=NODE.CHILDIDS
```

Use only the parameters you need in any combination. For example: http://<URL>?nodeName=NODE.NAME&nodeParentId=NODE.PARENTID adds the CI name and the ID of the parent CI to the URL.

When the user clicks the **Open in New Window** option, Top View calls the URL in another window and supplies it with the values of the parameters you specified in the URL. The URL page uses the values of the parameters to display what is necessary.

The following constants will be replaced by the corresponding values:

- **NODE.NAME** - the name of the CI. When the URL is executed, **NODE.NAME** is replaced by the name of the CI from which you want to open the URL The page specified in the URL opens and is filtered so that it displays only information related to the CI.
- **NODE.ID** - the ID number of the CI. When the URL is executed, **NODE.ID** is replaced by the ID number of the CI from which you want to open the URL The page specified in the URL opens and is filtered so that it displays only information related to the CI.
- **NODE.STATUS** - the status of the CI. When the URL is executed, **NODE.STATUS** is replaced by the status of the CI from which you want to open the URL The page specified in the URL opens and is filtered so that it displays only information related to the status. The available statuses are:
  - **-4** – downtime
  - **-3** – stop
  - **-2** – no data
  - **-1** – uninitialized
  - **0** – critical

- **5** – major
- **10** – minor
- **15** – warning
- **20** – OK

- **NODE.PARENTID** - the ID of the parent CI. When the URL is executed, **NODE.PARENTID** is replaced by the ID of the parent of the CI from which you want to open the URL The page specified in the URL opens and is filtered so that it displays only information related to the parent CI.
- **NODE.CHILDIDS** - the ID number of the CI's children. When the URL is executed, **NODE.CHILDIDS** is replaced by a list of the IDs of the children of the CI from which you want to open the URL. The page specified in the URL opens and is filtered so that it displays only information related to the children CI.
- **NODE.NAME** – the name of the node
- **NODE.ID** – the ID number of the node
- **NODE.STATUS** – if you want to filter by status, use NODE.STATUS.
  NODE.PARENTID – the ID of the parent CI
- **NODE.CHILDIDS** – the ID number of the CI's children

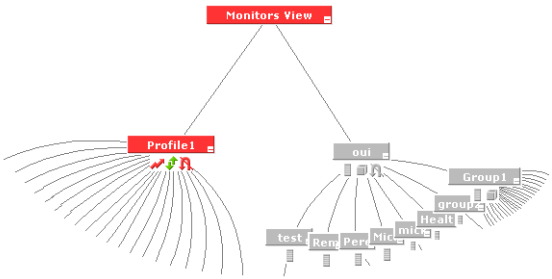
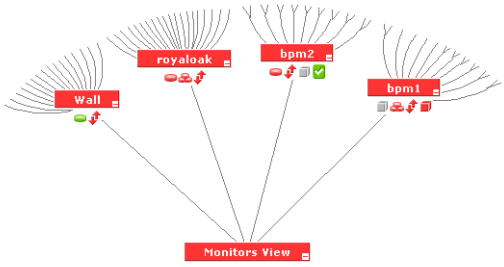
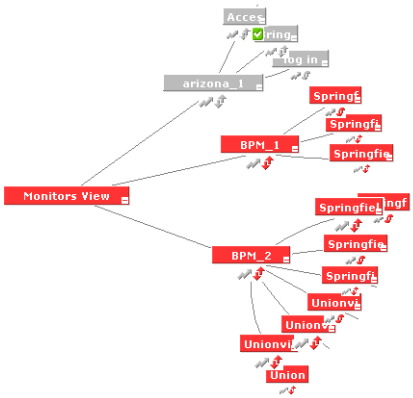
Customizing the Layout of the Hierarchy in Top View

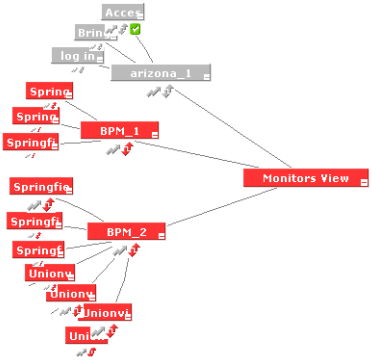
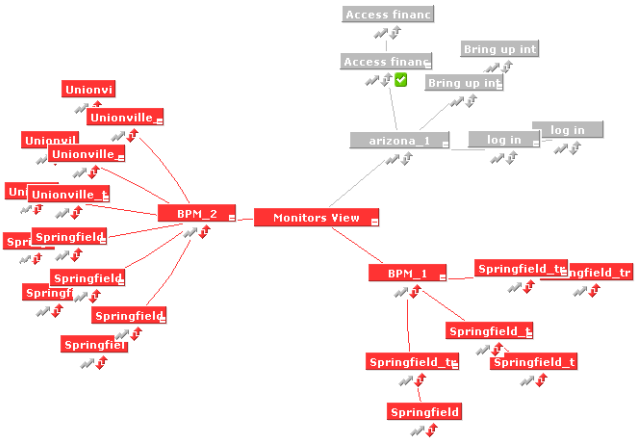
You can customize the layout of the hierarchy in the Top View page. By default, the parent CI is displayed above the child CIs and the child CIs are close to the bottom part of the Top View tab.

To set the layout of the hierarchy:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Applications context**, select **Dashboard Application**, and locate the **Top View Graph Layout** in the Top View Properties area.

3 Modify the type of layout:

Value	Resulting Display
BOTTOM – default. The parent CI is above the child CIs and is centered on the page.	
TOP – the parent CI is under the child CIs and is centered on the page.	
RIGHT – the child CIs are to the right of the parent CI and the parent CI is centered on the page.	. 

Value	Resulting Display
LEFT – the child CIs are to the left of the parent CI and the parent CI is centered on the page.	. 
RADIAL – the second level of the tree is distributed around the parent and the parent is centered on the page.	. 

4 Click **Save**.

Note: The change takes place immediately.

Enabling Chinese or Japanese Characters in Top View

The Top View tab can display Chinese or Japanese characters if you set the **Top View Font Name** setting to: Arial Unicode MS. You must also have installed the Chinese or Japanese packages – for details, see "Working in an I18N Environment" in *Working in an I18N Environment*.

To enable the display of Chinese or Japanese characters:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Applications context**, select **Dashboard Application**, and locate the **Top View Font Name** in the Top View Properties area.
3. Enter **Arial Unicode MS** in the **Value** box.
4. Click **OK** to save the change.

Modifying the Number of Levels in the Console Tab

You can modify the number of levels displayed in the Console tab under each parent. The default is 2. If you specify 1 only the parent CIs are displayed.

To modify the number of levels in the Console tab:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Applications context**, select **Dashboard Application**, and locate the **Business Console - Number of display levels** in the Dashboard Layout Properties area.
3. Enter the required number of levels in the **Value** box.
4. Click **OK** to save the change.

Sound Alert for Critical Status in the Console and Filter Tabs

Dashboard provides the option to have a sound play when a CI changes status to **Critical** (red), to provide an aural notification of the change in status. This feature appears in the Dashboard application in the Console and Filter tabs and in the Mercury Dashboard Ticker.

The Sound On/Off button is displayed in the top right corner of the Console tab. The user can click the button to toggle the sound on or off.

To modify the alert sound:

If you want to use another alert sound for Dashboard, access **<Mercury_Business_Availability_Center_server_root_directory>\AppServer\webapps\site.war\bam\pages\sounds** and replace the **ding.wav** file with your own .wav file (you must rename your file **ding.wav**).

Note: The change takes effect immediately.

Hiding or Showing the Ack Column

The acknowledge utility enables the user to track performance problems identified in the system and network infrastructure by keeping a record of when the problem was acknowledged and by which user. The user can access the utility using right-click options or by clicking the **Ack** icon that is displayed in an **Ack** column in some of the Dashboard tabs.

You can show or hide the Ack column in the Dashboard application.

To hide or show the Ack column:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Applications context**, select **Dashboard Application**, and locate the **Show CI Acknowledgment column** in the **Business Console** area.

3 Select:

- **false** in the **Value** list to hide the **Ack** column
- **true** in the **Value** list to display the **Ack** column

4 Click **Save**.

Note: The change takes effect immediately.

Enabling the Change Report

To view Change reports, you must:

- be working in a shared CMDB environment. For details, see "Sharing the Mercury Universal CMDB Environment" in *Working with the CMDB*.
- enable change impact monitoring by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Dashboard Application**, and locate the **Host name for MAM GUI Web server** entry in the **Change Impact Properties** table. Enter the Web server name and restart Mercury Business Availability Center.

  The Change Report option is disabled in the context menus if the shared CMDB feature is not installed.

Specifying the Changes Period for the Change Report

The Change report enables you to view the changes made to CI's properties for all properties that were selected to keep this information. The report shows change information for the last time period that is specified in the **Change period** parameter. You can modify the default time period (set at 1440 minutes (24 hours)).

For details about the Change report, see "Change Report" in *Using Dashboard*.

To specify the Change History period:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Applications context**, select **Dashboard Application**, and locate the **Changes period** in the **Change Impact Properties** area.
3. Enter the time period (in minutes) in the **Value** box. The recommended value is the default: 1440 minutes.
4. Click **Save**.

Note: The change takes effect after the server has been restarted.

Specifying the Number of CIs that Can Be Monitored for Change in Real-Time

A limited number (twenty by default) of CIs (and their children) can be monitored for real-time changes at any one time. This number can be customized.

For details about real-time monitoring for change, see "Viewing Real-Time Changes to CI Properties" in *Using Dashboard*.

Note: You can increase the default number of CIs that can be monitored but be aware that this might overload Mercury Business Availability Center.

To specify the number of CIs that can be monitored for change in real-time:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Applications context**, select **Dashboard Application**, and locate the **Maximum monitored CIs** in the **Change Impact Properties** area.
3. Enter the number of CIs in the **Value** box. The recommended value is 20.
4. Click **Save**.

Note: The change takes effect after the server has been restarted.

Integrating with Mercury Change Control Management

If you are working with Mercury Change Control Management, then you have the option to view in Dashboard a Related Change Requests report for a CI, showing the impact of planned IT changes which have been submitted to the service desk. For more details on the report, see "Related Change Requests Report" in *Using Dashboard*.

To view Related Change Requests reports in Dashboard, you must set up the integration environment and configure infrastructure settings, as described in the following sections.

Requirements for Integrating with Change Control Management

To set up integration with Change Control Management:

- Mercury Business Availability Center and Mercury Change Control Management should be working with the same Mercury Application Mapping server.
- Mercury Business Availability Center and Mercury Application Mapping should be installed in a shared CMDB environment. For information on setting up a shared CMDB, see "Sharing the Mercury Universal CMDB Environment" in *Working with the CMDB*.

Configuring Infrastructure Settings to Work with Change Control Management

To view change request information in Dashboard, you must configure settings on the Infrastructure Settings page in Mercury Business Availability Center.

To configure infrastructure settings:

1. Access the **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** page, click **Applications**, select **Dashboard Application**, and locate the **Change Control Management Integration Settings** table.
2. Set the **Active** property to **True**.
3. In the **CCM Web Service address** property, define the address of the server where Change Control Management is installed.
4. In the **CCM Statuses** property, define the change request statuses used in Change Control Management that you want to include in the Related Change Requests reports. By default, Mercury Business Availability Center is configured to use the **CLOSED** and **IN_PROGRESS** statuses.

   You can change the default statuses or add additional ones, as long as you use the definition defined in Change Control Management (**<Change Control Management root directory>\conf\enumeration-labels.properties**). For example, the value **StatusEnum.ASSIGNED=Assigned** should be entered in the CCM Statuses property as **ASSIGNED**.
5. In the **CCM Username** and **CCM Password** properties, enter the details of a user that exists in Change Control Management. The defaults are username **admin**, with no password.
6. Restart the Centers server for the changes to take effect.

Monitoring Usage in the System

You can monitor usage of the Dashboard application in a sessions log file. A line is added to the **<Mercury Business Availability Center server root directory>\log\EJBContainer\bam.sessions.log** file for every 6-, 12-, and 24-hour period, stating the number of Dashboard users during that time period. If a user accesses Dashboard, then closes Mercury Business Availability Center, then accesses the Dashboard application again, this counts as two user sessions in the log file.

To change the time period, open the **<MercuryAM>\conf\settings\BACAppSettings.xml** file, look for the keys: **session.log.interval.0**, **session.log.interval.1**, or **session.log.interval.2**. Change the key to match the required time period as follows:

- **session.log.interval.0** – represents a 6-hour period
- **session.log.interval.1** – represents a 12-hour period
- **session.log.interval.2** – represents a 24-hour period

Dashboard Administration Logs

To facilitate the creation of troubleshooting logs, you must enable Debug mode. For details, see "Mercury Business Availability Center Logs" in *Reference Information*. The logs are located in the **<Mercury Business Availability Center home>\log\EJBContainer** folder:

- **bam.app.rules.log** – To verify the status of a KPI, scan the log file manually or via a script for errors in the rule calculations. The log should not contain any errors such as Java exceptions.
- **TrinitySamples.log** – To verify that samples have reached the Mercury Business Availability Center Bus, scan the log file manually or via a script for samples coming from SiteScope or Business Process Monitor.

A utility called BusDiscovery can be activated to search for samples transmitted on the Bus. The utility is available under the **<Mercury Business Availability Center home folder>\tools\BusDiscovery** directory. Below is a sample command line that causes the utility to dump the arriving samples into **D:\Temp\drv.log**:
sprinter -dc_attach localhost -dc_print_format sample_per_line -drv_log_file D:\Temp\drv.log

Installing Mercury Dashboard Ticker

To use Mercury Dashboard Ticker, you must install it and then launch it to configure the various options that control its behavior. For details about Mercury Dashboard Ticker, see "Dashboard Ticker" in *Using Dashboard*.

This section includes the following topics:

Installing Mercury Dashboard Ticker

You must first install Mercury Dashboard Ticker.

To install Mercury Dashboard Ticker:

1. Select **Admin** > **Platform** > **Setup and Maintenance** to open the Downloads page.
2. Click **Mercury Dashboard Ticker** and follow the on-screen instructions.

Launching Mercury Dashboard Ticker

After Mercury Dashboard Ticker is installed, you must launch it to configure its behavior.

To launch Mercury Dashboard Ticker:

Select **Start** > **Programs** > **Mercury Dashboard Ticker** > **Mercury Dashboard Ticker** to launch the application and open the Preferences page. For details, see "Modifying Preferences" in *Using Dashboard*.

Requirements

To use the Mercury Dashboard Ticker you must have the following software installed on your computer:

- Win2000 or Windows XP
- Microsoft Internet Explorer 6.0 Service Pack 1 or later

Note: The requirements listed above are for the desktop version of Mercury Dashboard Ticker. To log on to Mercury Business Availability Center from the Message Window, you must fulfill the requirements detailed in *Preparing the Database Environment*.

Customizing View Options

You can customize some of the aspects of the user interface.

- **Modifying Tooltip Border and Header Colors.** A KPI tooltip border and header have a default color that you can modify. For details, see "Modifying the Tooltip Border and Header Colors" in *Repositories Administration*.
- **Specifying a Different Icon Set.** A different icon is used for the KPI status for each value range.

  You can replace the icons set in the Top View tab and for the KPIs in the other Dashboard. You can also replace the Trend and History icons with customized ones. For details, see "Specifying Different Status Icons" in *Repositories Administration*.

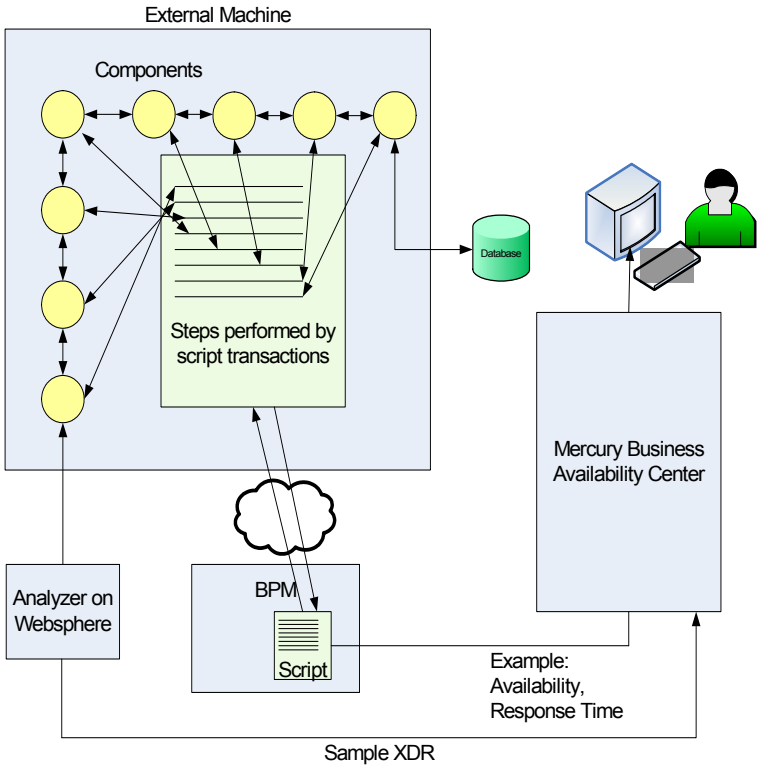
7

Administering Deep Transaction Tracing

This chapter describes the specific tasks involved in administering the Deep Transaction Tracing feature. Deep Transaction Tracing provides a monitoring layer for collecting information about the behavior of Business Process Monitor transactions within the target machine, achieved through integration with Bristol's TransactionVision application. The resulting information is displayed in the Deep Transaction Tracing view in Dashboard, as described in "Working With Deep Transaction Tracing" in *Using Dashboard*.

Deep Transaction Tracing Architecture

The following diagram illustrates the path of the Deep Transaction Tracing data.



When Business Process Monitor runs a script (transaction monitor), the transactions in the script performs specific tasks in the components of the target (external) machine. The Deep Transaction Tracing feature tracks the behavior of the transactions as they flow through the target machine via each component.

The TransactionVision sensors collect data on transaction traffic inside the target machine while the transaction is running, and pass it to the analyzer service (the logic engine), installed on a server that is running the WebSphere application. The analyzer performs calculation and analysis of the data.

A data sample containing information about the behavior of the transactions inside each component of the target machine is sent to Mercury Business Availability Center using the Extensible Data Representation (XDR) format. The samples are caught on the Mercury Business Availability Center bus by a special Dynamic Node Factory, and are used to create new Deep Transaction Tracing Monitor CIs, and to set KPI status for the CIs.

Deployment and Set Up for Deep Transaction Tracing

To view Deep Transaction Tracing data in Mercury Business Availability Center, you install Bristol TransactionVision, and deploy the Deep Transaction Tracing package.

In addition, you must configure the URL, user name, and password to open the Deep Transaction Tracing reports. The reports are opened from the Deep Transaction Tracing context menu, used with Deep Transaction Tracing Monitor CIs in Dashboard. The menu contains options to open the following dynamic reports in TransactionVision for the selected transaction:

- **Tracking Report**
- **Service Level Report**
- **Component Topology Report**

This section includes the following topics:

Deploying Deep Transaction Tracing

TransactionVision is installed on a separate machine in your environment, and the Deep Transaction Tracing package is installed on the Mercury Business Availability Center to integrate the TransactionVision data into Mercury Business Availability Center.

Installing the Deep Transaction Tracing package creates:

- the Deep Transaction Tracing view – for details, see "Working With Deep Transaction Tracing" in *Using Dashboard*.
- the Deep Transaction Tracing Monitor CIT in the CMDB.
- the Dynamic Node Factory that creates Deep Transaction Tracing CIs from the incoming samples.

To deploy the Deep Transaction Tracing package:

1. Install Bristol's TransactionVision application on a separate machine, using WebSphere as the application server. For installation instructions and system requirements, refer to the TransactionVision documentation.
2. On the Mercury Business Availability Center Data Processing Server, copy the **DeepTransactionTracing.zip** file from:

   <Mercury Business Availability Center server root directory>\mam_lib\packages_extension

   to:

   <Mercury Business Availability Center server root directory>\mam_lib\packages
3. Deploy the Deep Transaction Tracing package using the JMX console. Follow the instructions for deploying Mercury Business Availability Center packages given in "Deploying, Displaying, and Removing Deployed Packages" in *Discovery Manager Administration*.

Configuring Parameters to Open the TransactionVision Reports

To open the TransactionVision reports from Dashboard, the URL, user name, and password to access the TransactionVision machine must be configured in Mercury Business Availability Center. This is done on the Infrastructure Settings page.

For information on the reports, see "Deep Transaction Tracing Reports" in *Using Dashboard*.

To configure the TransactionVision access parameters:

1. Access the **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** page.
2. Select the radio button for context **Foundations**, then select **Third-Party Components** from the dropdown list.
3. Locate the **Bristol Environment** table in the page. Click the **Edit** button for the **Bristol Machine Base URL** parameter.
4. In the displayed dialog box, enter the URL for the TransactionVision machine. Include the full domain or host name and the port. For example: **http://<TransactionVision host name>:9080/**
5. Edit the **User name for Bristol login** parameter and enter the required user name (default is **Admin**).
6. Edit the **User password for Bristol login** parameter and enter the required password (default is **Admin**).
7. Save your changes. Restart is not required.

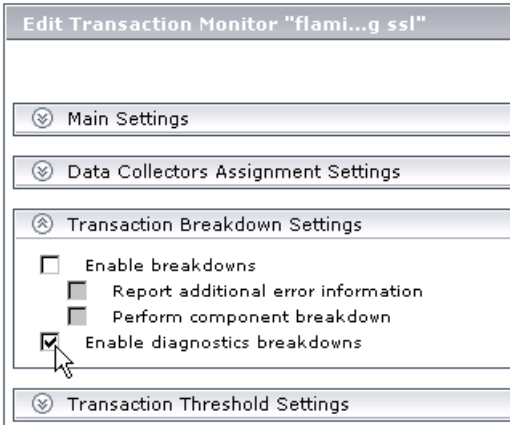
Enabling Deep Transaction Tracing for Transaction Monitors

To view Deep Transaction Tracing data correlated with Business Process transactions in Dashboard, a link must be made between the two. This is done in Monitor Administration by enabling the breakdown data flag for a transaction monitor, so creating a mapping for the transaction monitor to the TransactionVision application.

To enable Deep Transaction Tracing for a Transaction Monitor:

1. Open the **Admin** > **Monitors** page.
2. In the **Monitors** tab, right-click the required transaction monitor, and select **Edit**.
3. In the right pane, expand the **Transactions Breakdown Settings** area.

4 Select the check box for **Enable diagnostics breakdowns**.



5 Click **OK** to save the changes.

Activating Deep Transaction Tracing in TransactionVision

In the TransactionVision application, you must activate the **Mercury BAC** job by pointing to the Mercury Business Availability Center server and starting the job. You must also configure the transactions on the TransactionVision side.

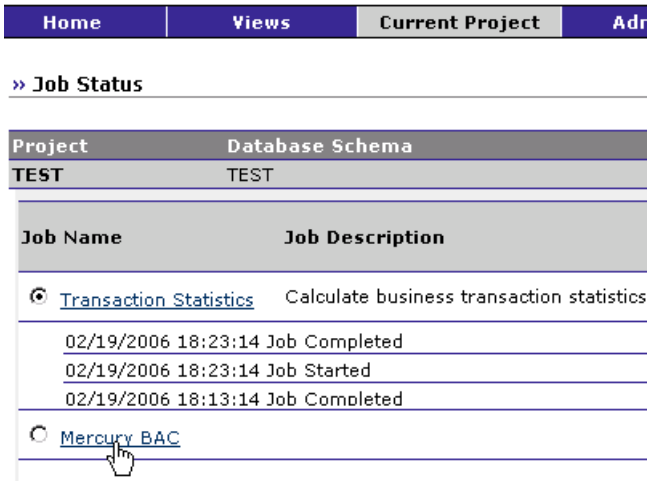
After activating the job and configuring transactions, TransactionVision sends samples for Deep Transaction Tracing to Mercury Business Availability Center.

To activate Deep Transaction Tracing in TransactionVision:

1 Log into TransactionVision.

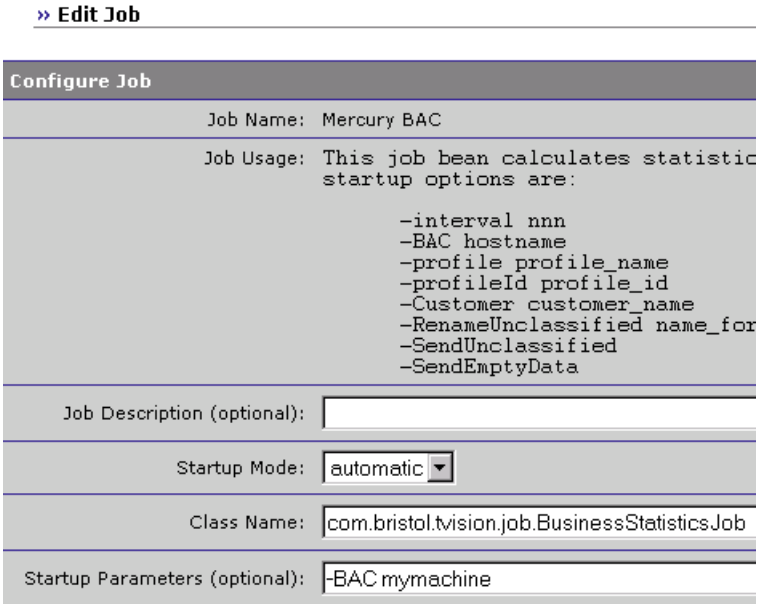
2 In the top menu, select **Current Project** > **Job Status**. The **Job Status** page opens.

3 Click the **Mercury BAC** link.



The **Edit Job** page opens.

4 In the Startup Parameters (optional) box enter **-BAC <Mercury Business Availability Center Core Server host name>**. For example:
-BAC mymachine



Click **Finish**.

5 On the **Job Status** page, click the **Start Job** button to start the Mercury BAC job.

6 For each transaction monitor set for Deep Transaction Tracing in Mercury Business Availability Center, you must configure the equivalent transaction on TransactionVision (you will need the exact name of the transaction monitor). For details, refer to the TransactionVision documentation.

Part II

Service Level Management Administration

8

Introduction to Service Level Management Administration

A Service Level Management administrator defines service level agreements (SLAs) that represent the formal and informal contracts you have with your service providers and with internal business units. This chapter describes the administrative tasks you perform to enable Service Level Management to compare the KPIs of availability percentages and performance times with service levels, and to display the results in reports.

Introducing Service Level Management

Service Level Management determines compliance with your service level agreements by measuring your business applications. The data produced by these measurements helps you determine whether the availability and performance requirements of users and infrastructure are being met.

You begin by examining performance trends and setting baselines for a variety of business processes. These baselines in turn enable you to establish realistic service level objectives for availability percentages and performance times, for the different subsidiaries, geographical locations, or organizations that you serve.

To access Service Level Management administration pages:

Select **Admin** > **Service Level Management**.

To access Service Level Management reports:

Select **Applications** > **Service Level Management**. For details on reports, see *Using Service Level Management*.

Note: Mandatory fields in the Service Level Management application are marked with an asterisk (*****).

Setting Up Service Level Management

Before defining SLAs, verify that views and KPIs have been set up:

Views – During SLA definition, you choose CIs that have been associated with Views. For details on views, see "Getting Started with IT Universe Manager" in *IT Universe Manager Administration*.

KPIs – Service Level Management includes default KPIs that are attached automatically to the SLAs you define. You can also associate further KPIs or edit existing KPIs. For details on Service Level Management KPIs, see Chapter 16, "Repositories." Note that Service Level Management uses its own KPIs, and not those of Dashboard.

Users – After you define an SLA, the Mercury Business Availability Center administrator must give users permissions to work with the SLA. Users with view permission can view or generate reports for their SLAs. For details, see "Granting and Removing Permissions" in *Platform Administration*.

The Service Level Management administration pages include the following tabs:

Service Level Agreements

In this tab, you can create a service level agreement, recalculate existing agreements and create downtime events.

- **Service Level Agreements.** You define SLAs that reflect actual agreements you have with your service providers or with internal business units. The SLAs enable you to build reports showing the level of service management. For details, see Chapter 9, "Service Level Agreements (SLAs)."

Note: By default, you can create up to ten service level agreements. To increase this number, contact Mercury Managed Services Support.

- **Recalculations.** You can run recalculations on an SLA, usually after making retroactive changes. For details, see Chapter 10, "Recalculation."
- **Downtime Events.** You can define downtime or incidents that represent actual event occurrences that may skew results and which you may want to exclude from reports. For details, see Chapter 11, "Downtime Events."

SLA Management

In this tab, you can set up services provided by your department in Mercury Business Availability Center to enable you to build and maintain services. For details, see Chapter 12, "SLA Management Administration." For details on viewing reports in SLA Management, see "SLA Management Services Reports" in *Using Service Level Management*.

SLA Status Alerts

In this tab, you can create alerts to notify you if an SLA is not reaching the target you set for it, or if its status is changing for the worse. For details, see Chapter 13, "SLA Status Alerts."

Repositories

In this tab, you can define time intervals and outage categories, and edit or create KPIs and rules.

- **Time Intervals.** Time intervals specify periods during which objectives must be checked. Service Level Management provides two default time intervals (**24x7** and **Business Hours**); you can define more time intervals if needed. For details, see Chapter 14, "Time Intervals."
- **Outage Categories.** Outage categories can be used in Service Level Management reports, to make results more meaningful. Service Level Management provides default categories (Database, Network, Undefined, and Webserver); you can define more outages categories if needed. For details, see Chapter 15, "Outage Categories."
- **KPIs.** Service Level Management includes default KPIs that you use when defining SLAs. For details, see Chapter 16, "Repositories" and "Service Level Management KPI Repository" in *Repositories Administration*.
- **Business Rules.** Service Level Management includes default business rules (also known as business logic) that you use when defining SLAs. For details, see Chapter 16, "Repositories" and "Service Level Management Business Rules Repository" in *Repositories Administration*.

Six Sigma Reporting

You can produce certain reports that show data from a Six Sigma perspective. This is on condition that you associate a Six Sigma KPI with the SLA. For details, see page 173.

Customizing Reports

You can generate reports automatically or manually and you can specify a header and a footer for a report. For details, see "Customizing Reports" in *Platform Administration*.

Editing Settings with the Infrastructure Settings Manager

Caution: Many of the settings in the Infrastructure Settings Manager should not be modified without first consulting Mercury Customer Support, Mercury Managed Services Support, or your Mercury Services representative. Modifying certain settings can adversely affect the performance of Mercury Business Availability Center.

Administrators with an advanced knowledge of Mercury Business Availability Center can customize certain Service Level Management settings, such as the first day of the week, the number of CIs that can be displayed in a tree, and the types and contents of the default KPIs that are associated with SLAs.

To access the Infrastructure Settings Manager, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the Applications context and choose **Service Level Management** from the list.

When editing XML files in the Infrastructure Settings Manager, you can comment out lines using the regular HTML comment tag: **<!-- comment out this line -->**.

For SLA Status alerts, the administrator can define a default SNMP trap destination. Select the Foundations context and choose **Alerting** > **Alerting - Triggered Alerts**.

For details on editing infrastructure settings, see "Editing Infrastructure Settings" in *Platform Administration*.

The Audit Log

You use the Audit Log to track configuration changes to the SLAs and services. The audit log displays all configuration changes that can affect reports, including changes to the SLA.

As the audit log can become very long, you can use filters to display only those SLAs and services in which you are interested.

The Audit Log tracks the following changes:

- creation or deletion of an SLA
- any changes made to an SLA
- a configuration item's (CI) addition to, or removal from, an SLA
- any changes made to a CI
- any changes to SLA Management
- any changes to downtime or event scheduling, including the creation, editing, and removal of SLM and BPM events
- any changes to the time intervals
- any changes to user permissions

For details on using the Audit Log, see "Using the Audit Log" in *Platform Administration*.

Data Purging

Note to Mercury Managed Services customers: Mercury Operations administers this functionality and the interface is hidden from your view.

Data collection tables can grow to a very large size, and thus need occasional purging. These tables include those that contain SiteScope data. For details on managing historical data and the Purging Manager, see "Purging Historical Data from Profile Databases" in *Platform Administration*.

Upgrading SLAs to Work with Mercury Business Availability Center 6.2

For details of the upgrade procedure for SLAs created in Mercury Business Availability Center version 5.x, see Chapter 17, "Upgrading Service Level Management to Mercury Business Availability Center 6.2" or refer to *Upgrading Mercury Business Availability Center* available from the **Deployment_Documentation** directory on the Mercury Business Availability Center 6.1 Setup CD-ROM.

Viewing PNR Data for Service Level Management in Dashboard

You can view PNR (point of no return) data for SLAs in Dashboard. For details on configuring the PNR KPI, see "Attaching a PNR KPI to a CI" on page 20.

Note: You view Service Level Management KPIs in Service Level Management reports only, except for the PNR KPI which you view in Dashboard.

Monitoring Events on Other Systems

Data samples are sent to Mercury Business Availability Center from other systems such as EMS applications. To monitor activity on those systems, you configure Mercury Business Availability Center to display external source data.

To display external source data in Service Level Management reports:

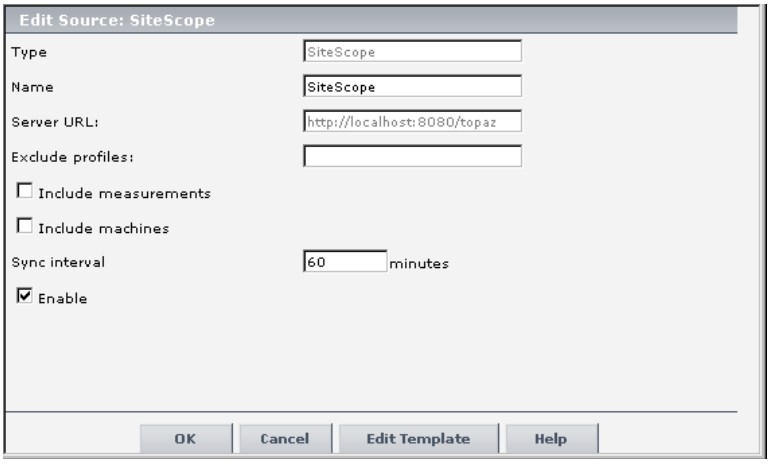
1. Create a measurement filter. For details, see "Defining Measurement Filters" in *Platform Administration*.
2. Create a view that includes a monitor configuration item type (CIT) called **UDX Measurement Filter**. For details, see "Creating and Editing Views" in *View Manager Administration*.

   Mercury Business Availability Center automatically adds the measurement filter you created in step 1 to the CIT as a configuration item (CI). For details on adding CIs to the IT Universe, see "Creating a New CI" in *IT Universe Manager Administration*.
3. Create an SLA. For details, see Chapter 9, "Service Level Agreements (SLAs)." During SLA creation, choose the view that you created in step 2, and add its CI to the SLA. For details, see "Defining an SLA: Configuration Items" on page 168.
4. View a Service Level Management report for the SLA. For details, see *Using Service Level Management*.

Importing SiteScope Data into Service Level Management

Note the following limitation when setting up SiteScope to send data to Service Level Management:

You can configure the SiteScope adapter to generate the SiteScope hierarchy with or without measurements. To display the Edit Source window, select **Admin** > **CMDB** > **Source Manager**. Locate the SiteScope source and click its **Edit** button:



For an explanation of this window, see "SiteScope" in *Source Manager Administration*.

9

Service Level Agreements (SLAs)

Before your users begin viewing Service Level Management reports, you must create service level agreements (SLAs) that represent contracts entered into by your department with service providers and internal business units.

For a checklist of all Service Level Management functionality, see "Setting Up Service Level Management" on page 150.

Note to Mercury Managed Services customers: By default, you can create up to ten SLAs. To increase this number, contact Mercury Managed Services Support.

Note: If you change a user's permissions for a specific SLA, the user must log out and log in again to view the changes.

The Service Level Agreements Page

You use this page to create SLAs or to perform actions on existing SLAs. Service Level Management displays those SLAs which you, the logged-in user, have permissions to change or delete.

Note: The Service Level Agreements page displays SLAs compatible with Mercury Business Availability Center version 6.1. For details of the upgrade procedure for SLAs created in previous versions (Topaz version 4.5 or Mercury Business Availability Center version 5.x), see Chapter 17, "Upgrading Service Level Management to Mercury Business Availability Center 6.2" or refer to *Upgrading Mercury Business Availability Center* available from the **Deployment_Documentation** directory on the Mercury Business Availability Center 6.1 Setup CD-ROM.

The page includes the following components:

Name. The name of the SLA. For a long name, hold the cursor over the name to view it in full in a tooltip.

Description. The description of the SLA. Hold the cursor over the description to view the complete text in a tooltip.

Start date. The date and time when Service Level Management begins calculating the SLA. Note that this date is not the SLA's creation date.

End date. The date and time on which the SLA should stop. You can enter an end date that is in the past, but the date cannot be earlier than the start date.

State. The state of an SLA can be:

- **Preliminary**. The SLA has not begun running. You can change any properties of the SLA. Note that you must start the SLA (that is, click the **Start** button) for Service Level Management to calculate the SLA.
- **Pending**. The SLA has been started, but its start date is in the future. You can terminate a pending SLA (click the **Stop** button).
- **Running**. The SLA begins collecting data. You cannot change the start date and time zone, but you can change the end date to any future end date. That is, the end date cannot be in the past. You can terminate a running SLA (click the **Stop** button).
- **Terminated**.The SLA finishes running and no longer collects data. A terminated SLA cannot be restarted. (However, you can clone a terminated SLA. For details, see "Cloning an SLA" on page 183.) An SLA is terminated in two ways, either by manually stopping it (that is, by clicking the **Stop** button), or when its end date has passed. The SLA terminates on the next hour after you stop it.

Creator. The user name of the person who created the SLA.

Actions. You can start/stop, edit, clone, or delete an SLA by clicking the appropriate button.

For details see "Editing an SLA" on page 182, "Cloning an SLA" on page 183, and "Deleting an SLA" on page 184.

New SLA button. To define an SLA, click this button. For details, see the next section.

You can sort the list by any column: An arrow next to a title shows by which column the SLAs are sorted, and also the direction in which the column has been sorted (that is, ascending or descending).

Start, Stop, and Delete buttons. To perform an action on more than one SLA simultaneously, select the check boxes of the SLAs you want to start, stop, or delete. Click the relevant button.

SLA Definition Workflow

You create service level agreements by extracting information from actual service agreements and duplicating the information in Service Level Management.

You perform the following steps to define an SLA:

- Use the SLA Wizard to define an SLA. For details, see "Defining an SLA: Begin" on page 163.
- Set the SLA's properties, that is, name, description, and so forth. For details, see "Defining an SLA: Properties" on page 164.
- Choose the CIs to add to the SLA. For details, see "Defining an SLA: Configuration Items" on page 168.
- Choose the KPIs to associate with the CIs. For details, see "Defining an SLA: KPIs" on page 171.
- Give a weight to each configuration item (CI). For details, see "Defining an SLA: Weights" on page 176.
- Verify that all SLA parameters are correct on the Summary page. For details, see "Defining an SLA: Finish" on page 177.
- Grant permissions to users to work with the SLA. For details, see "Defining an SLA: Grant Permissions to Users" on page 178.

Note: When defining a new SLA, you click the **Next** button on each page to proceed to the next page. You click the **Finish** button only after you have completed the SLA definition. When editing an SLA, once you have made changes, you can click the **OK** button on any page.

Mandatory fields in the Service Level Management application are marked with an asterisk (*****).

Defining an SLA: Begin

You use the SLA Wizard to define service level agreements (SLAs).

To create an SLA:

1 Select the **Service Level Agreements** tab to open the Service Level Agreement page (**Admin** > **Service Level Management**). The page shows a list of existing SLAs, organized alphabetically.

For a description of this page, see "The Service Level Agreements Page" on page 160.

Note: If no default profile database has been set, Service Level Management cannot display this page. For details on setting profile databases, see "Database Administration" in *Platform Administration*.

---

2 Click **New SLA** to open the SLA Wizard at the Welcome page.

3 Click **Next** to begin creating an SLA.

The first stage in the procedure is to name the new SLA. Continue to the next section.

Defining an SLA: Properties

The first stage in the procedure is to define the SLA's properties, such as name and description.

To define the SLA properties:

1 Fill in the following fields:

Name. The name of the SLA must be unique and must not be longer than 100 characters.

Description. Enter a description to appear in Service Level Management reports.

Agreement Details. Enter details to appear in Service Level Management reports, when SLA Description is displayed. For details, see "Adding Descriptions to Reports" in *Using Service Level Management*.

Start Date. By default, the start date is the current date and time. To change the date, click the date link to open a calendar.

End Date. By default, the end date shown is one year after the current date and time. To change the date, click the date link to open a calendar.

Time zone. Specify the time zone of the SLA. Service Level Management calculates reports according to this time zone, so that data is linked to the appropriate time interval.

Type. Choose the type of agreement:

- OLA (Operational Level Agreement): An internal agreement covering the delivery of services which support the IT organization in their delivery of services. OLA is usually used to indicate that the contract addresses system hardware (machines, routers, and so forth).
- SLA (Service Level Agreement): Written agreement between a service provider and the customer(s), that documents agreed service levels for a service. SLA is usually used to indicate that the contract addresses services (applications, services, business processes, and so forth).
- Underpinning contract: A contract with an external supplier covering delivery of services that support the IT organization in their delivery of services.

Classification. Choose between **External** and **Internal**. You would choose External when classifying an SLA for a contract with a customer and Internal when classifying an OLA for a contract with someone within your organization.

Maintainer, Customer, Provider. Use these fields to enter additional information about the SLA. They can be left empty.

Creator. Displays the user name with which you logged in.

Customer. Enter the name of a customer or click the **Select customer** button to choose the customer who is associated with the business unit service you are defining. For details on SLA Management, see "SLA Management Administration" on page 203.

Provider. Enter the name of a provider or click the **Select provider** button to choose the provider who is associated with the business unit service you are defining.

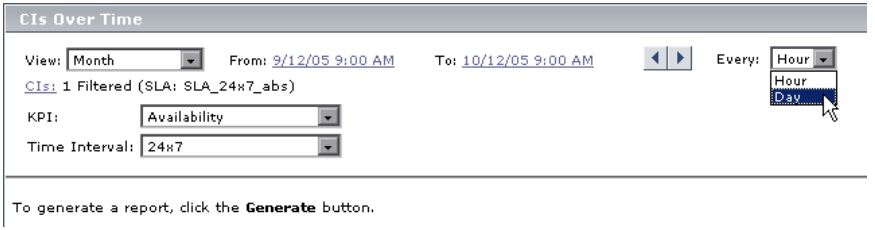
Time intervals – Click the link to choose which time intervals are to be monitored by the SLA. (A time interval is the actual period of time for which Service Level Management calculates data.) You can create time intervals (up to three per SLA) and you can edit the default time intervals (**24x7** and **Business Hours**). For details, see Chapter 14, "Time Intervals." You can add time interval descriptions to Service Level Management reports. For details, see "Adding Descriptions to Reports" in *Using Service Level Management*.

Tracking periods – Click the link to choose by which tracking periods (that is, time periods) you can view data in Service Level Management reports.

To enable users to view reports that include data from the start date of the SLA till the present, select **SLA period**.

The tracking periods that you select here for the SLA define which granularities are available in reports. For example, say you select the **Hour** and **Day** tracking periods:

A user chooses to view a report with a **Week** time period and a **Day** granularity (chosen in the **Every** box in the Over Time report). Because you did not select the **Week** tracking period, the **Week** granularity does not appear in the **Every** box:



Targets – Click the link to choose which targets are to be available when adding KPIs to the SLA. For details on defining objective targets, see page 181. Target descriptions are displayed as legends in Service Level Management reports.

Status	Color
Exceeded	Green
Met	Olive green
Minor Breached	Yellow
Breached	Orange
Failed	Red

Administrators with an advanced knowledge of Mercury Business Availability Center can change the target names in the Infrastructure Settings Manager page. For example, to change the default name of **Breached SLA** to **Contravened SLA**, change:

```
<Target Color="ff3333" Default="true" Id="0" Name="settings.slm.targets.def.target.breached.text"/>
```

to:

```
<Target Color="ff3333" Default="true" Id="0" Name="Contravened SLA"/>
```

For details, see "Editing Settings with the Infrastructure Settings Manager" on page 153 and "Infrastructure Settings" in *Platform Administration*.

2 Click **Next** to continue.

The next stage in the procedure is to select configuration items (CIs). Continue to the next section.

Defining an SLA: Configuration Items

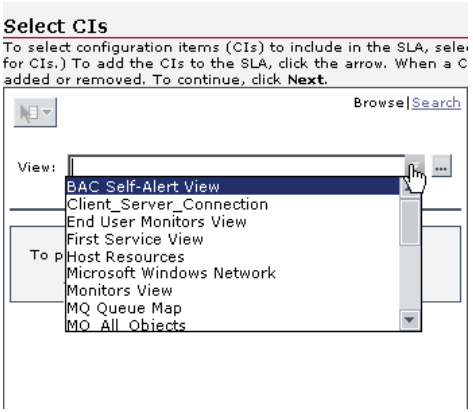
The next stage in the procedure is to select the configuration items (CIs) that are to be included in the SLA. CIs are organized into views in IT Universe. You can select CIs from more than one view to include in the same SLA.

For details on the View Explorer, where you search for CIs, see "Using View Explorer" in *Working with the CMDB*. For details on the IT universe, see *IT Universe Manager Administration*.

Note to Mercury Managed Services customers: By default, you can define up to 500 CIs. To increase this number, contact Mercury Managed Services Support.

To select CIs:

1 Display the CIs you want to include in the SLA. You do this by displaying a view that includes the CIs or by searching for the CIs (if you do not know in which view they are included).



Note: Service Level Management displays only those CIs that belong to a configuration item type (CIT) defined as persistent. Non-persistent CITs cannot be added to SLAs. You define non-persistent CITs in the Infrastructure Settings Manager page. For details, see “Editing Settings with the Infrastructure Settings Manager” on page 153 and “Infrastructure Settings” in *Platform Administration*.

Persistent data refers to data that is stored in the database. Non-persistent data, by comparison, is data that is reported only to the Bus on the Core Server.

---

2 To display a view, choose the view from the list, or click the button to open the Select View window (where views are organized in folders). Choose the view you want to display and click **OK**, or click **Cancel** to close the window without choosing a view.

The CIs are displayed below the View list.

To display all the actions you can perform on a selected CI, select the CI and click the **Menu options** button. For example, to view the properties of a CI, select the CI, click the **Menu options** button, and choose **Properties** from the menu to open the General Properties window. You can also display menu options by right-clicking a CI.

Continue to step 5.

3 To search for any CI that can be added to the SLA, click the **Search** link. For details on searching, see "Using View Explorer" in *Working with the CMDB*.

4 To add the CI to the SLA, locate and right-click the CI. Choose **Locate Element in View** from the menu to return to the Browse pane.

5 In the Browse pane, select the CIs you want to assign to the SLA. If you select a parent CI, all descendants are automatically selected. (This is known as recursive selection.)

You can select multiple CIs to assign to the SLA by holding down the CTRL key and selecting adjacent or non-adjacent CIs.

6 To move the CIs to the Selected CIs list, use the upper arrow. All descendants are automatically added to the SLA.

To remove CIs from the Selected CIs list, select the CIs and use the lower arrow.

7 **Automatically define default KPIs for new CIs** – select this check box to add KPIs to all CITs.

8 To make changes to the KPIs or weights, click **Next** to continue to the next stage in the procedure. Continue to the next section.

To save the SLA with default KPIs and weights, click **Finish**. Service Level Management displays the Summary page. For details, see "Defining an SLA: Finish" on page 177.

Defining an SLA: KPIs

This section explains how to attach a KPI to a CI in the SLA. To enable maximum flexibility in planning your SLAs, you can attach a KPI to any CI, at any level in the SLA hierarchy.

Service Level Management automatically associates default availability and performance KPIs with Business Process Monitor, SiteScope, Host, Application, and Group CITs. This is on condition that you select **Automatically define default KPIs for new CIs** in the Select CIs page (for details, see page 168).

The information on default KPIs is stored in the Infrastructure Settings Manager. For details, see "Editing Settings with the Infrastructure Settings Manager" on page 153 and "Infrastructure Settings" in *Platform Administration*.

For the list of KPIs that Service Level Management uses, see "Service Level Management KPI Repository" in *Repositories Administration*.

To add outage definitions to the SLA, see "Defining an SLA: Outages" on page 174.

To continue to the next stage of SLA definition, without changing any KPI parameters and without adding outage definitions, click **Next** in the Define KPIs page. For details on the next stage, see "Defining an SLA: Weights" on page 176.

To make changes to the KPIs associated with the SLA or to add further KPIs, see the following sections:

- filter the list of CIs – for details, see page 172
- edit KPIs or objectives associated with the SLA – for details, see page 172
- associate other KPIs with the SLA – for details, see page 173
- define a Six Sigma KPI – for details, see page 173
- remove a KPI from the SLA – for details, see page 173
- define KPIs and outages for multiple CIs in a single definition – for details, see page 174

To filter the list of CIs:

You use Search to filter the list of CIs that Service Level Management displays. This is useful if you want to locate a specific CI in a lengthy list. The list displays the CIs that are already associated with the current SLA.

1 To search for any CI in the SLA, click the **Search** link.

2 Enter the name of the CI (or part of the name) in the **Search for** field. Click the **Search** button to display the results below.

You can also search for CIs using the **Related to** or **Type** fields. **Related to** searches for CIs that are related to the selected CI, and **Type** searches for CITs. Select the check box and click the button to open the Select Configuration Item (or Select Configuration Item Type) window. In the Select Configuration Item window, choose the CI you want to display; in the Select Configuration Item Type window, choose the CIT. Click **OK**, or click **Cancel** to close the window without choosing a CI or CIT. In the Search pane, click the **Search** button to display the results below.

3 To manage the CI's KPI, locate and right-click the CI. Choose **Locate Element in View** from the menu to return to the Browse pane.

4 In the Browse pane, select the CI.

To display all the actions you can perform on a selected CI, select the CI and click the **Menu options** button. For example, to view the properties of a CI, select the CI, click the **Menu options** button, and choose **Properties** from the menu to open the General Properties window. You can also display menu options by right-clicking a CI.

To refresh the list of CIs, click the **Refresh** button.

Note: At this stage, you have not yet added the CI to the SLA, so the information in the right pane is not yet up to date. To update the SLA information, save the SLA by clicking the **Finish** or **Next** button.

---

5 Continue with the procedure. For details, see:

- "Editing and Adding KPIs and Objectives" on page 178
- "Defining an SLA: Outages" on page 174

To edit KPIs or objectives associated with the SLA:

1 Click the **Edit** button to open the KPI window.

2 Make any necessary changes to the KPI (for details, see "Editing and Adding KPIs and Objectives" on page 178) and click **Save**.

For details on setting up a PNR KPI for Service Level Management, see "Attaching a PNR KPI to a CI" on page 20.

3 Click **Next** to continue to the next stage of the procedure. For details, see "Defining an SLA: Weights" on page 176.

To associate other KPIs with the SLA:

1 Click **Add KPI** to open the KPI window. For details on adding a KPI to the CI, see "Editing and Adding KPIs and Objectives" on page 178.

2 Click **Next** to continue to the next stage of the procedure. For details, see "Defining an SLA: Weights" on page 176.

To define a Six Sigma KPI:

Service Level Management includes two Six Sigma KPIs: **Availability Six Sigma** and **Performance Six Sigma**.

1 Click **Add KPI** to open the KPI window.

2 Choose **Availability Six Sigma** or **Performance Six Sigma**. For details on Six Sigma KPIs, see page 178.

3 Click **Next** to continue to the next stage of the procedure. For details, see "Defining an SLA: Weights" on page 176.

To remove a KPI from the SLA:

To remove one KPI, click the KPI's **Delete** button.

To remove more than one KPI, select their check boxes and click the **Delete** button.

Click **Next** to continue to the next stage of the procedure. For details, see "Defining an SLA: Weights" on page 176.

To define KPIs and outages for multiple CIs in a single definition:

You can make changes to the associated KPIs or outages for multiple CIs with one procedure.

1. To display the Global Settings pane, click one CI, hold down CTRL, and click each additional CI.
2. Click the relevant button to attach or edit a KPI, to remove a KPI, or to update the outage definition.
3. Continue with the procedure. For details, see:
   - ➤ "Editing and Adding KPIs and Objectives" on page 178
   - ➤ "Defining an SLA: Outages" on page 174
4. Click **Next** to continue to the next stage of the procedure. For details, see "Defining an SLA: Weights" on page 176.

Defining an SLA: Outages

You can define outages and outage conditions and criteria. Outages are periods of time during which measurements fail. Service Level Management considers a CI to have failed if it does not meet the criteria defined in the business rule. For example, a CI can fail because the failure has a duration of at least the minimum duration defined in the outage. A CI can also fail if a minimum number of failures has been reached.

You can associate one outage only for each CI.

To define an outage:

1. Click **Add Outage** to open the Add Outage window.

   If an outage has been defined previously, click the **Edit** button to open the Add Outage dialog box.
2. Choose the business rule that you want to associate with the KPI.

   For a short explanation of the business rule and its parameters, place the cursor over the icon or over a field name.

   Only the rule (or rules) that is appropriate to the KPI is displayed.

3 Make any necessary changes to the rule parameters.

For details on the business rule and its parameters, see "Outage Business Rules" in *Repositories Administration*.

4 Choose the category that will be associated with the outage in Service Level Management outage reports.

To define a new outage, click **New Outage Category**.

If you leave the outage undefined at this stage, you can add a category to the outage in the Outage Summary report page (for details, see "Outage Summary Report" in *Using Service Level Management*). However, it is recommended to categorize outages at this stage. For details on defining categories, see "Outage Categories" on page 229.

5 Click **OK**.

6 Click **Next** to continue to the next stage of the procedure. For details, see "Defining an SLA: Weights" on page 176.

Note: Any changes made to a KPI associated with a specific SLA do not affect the KPI when it is associated with other SLAs.

You can view PNR (point of no return) data for SLAs in Dashboard. For details on configuring the PNR KPI, see "Attaching a PNR KPI to a CI" on page 20.

Defining an SLA: Weights

The next (optional) stage in the procedure is to define weights. CIs are given a default weighting of 1, but you can change the weight of each CI and of each of its descendants to reflect their relative importance in the SLA. Service Level Management takes weighting into consideration when calculating the KPIs.

For example, say you create a KPI that includes two Business Process Monitor CIs. One CI simulates a user buying a product at one location and the other CI simulates a user at a second location. You decide that availability and performance at the first location are more important than at the second, and so you give the CIs weights of 2 and 1. When Service Level Management calculates availability and performance, CI 1 is awarded two thirds of the overall score and CI 2 is awarded one third.

When weighting CIs, it may be helpful to consider the percentage weight you want to give each CI. For example, say you have two CIs and you think one should carry 40% of the weight and the other 60%, you could set their weights at 40 and 60 respectively.

To define weights:

1. Display the CIs whose weights you want to change. You can search for specific CIs. For details, see page 172.
2. Select the SLA or any of its CIs. The CI's descendants are displayed in the CI pane.
3. In the CI pane, enter a new weighting value for those CIs that have greater importance.

   Alternatively, if all CIs must have the same weight, enter the value in the **All CIs** row, and click **Apply**.
4. Click **Next** to continue.

   The last stage in the procedure is to verify that all the SLA details are correct and to save the SLA. For details, see "Defining an SLA: Finish" on page 177.

Notes and Limitations

- Weight values can be between zero and 100 inclusive, with up to three digits after the decimal point.

- The weight of a CI is calculated in the same way for all KPIs, time intervals, and tracking periods.
- If you set all weights to zero, KPIs are marked with a hyphen for all calculated reports.
- Weighting is reflected in Service Level Management reports that are dependent on the defined business logic (for example, average availability).
- By default, Six Sigma calculations do not take weighting into account.
- Versions previous to 5.1 SP1 weighted transactions according to the number of samples they received. From version 5.1 SP1 onwards, weighting is calculated for each CI.

Defining an SLA: Finish

The last stage in the procedure is to verify that the details you entered are correct, to save the SLA, and to begin running it.

You can display the information on this page in Service Level Management reports, on condition that you enable its display. For details, see "Adding Descriptions to Reports" in *Using Service Level Management*.

To verify details and save the SLA:

1. Read through the summary and verify that the details are correct.

   To make changes to SLA parameters, click **Back**.

2. **Start SLA** – Select this check box for Service Level Management to begin running the SLA immediately. If you clear this check box, Service Level Management marks the SLA's state as preliminary, and you can run the SLA at a later time. For details on SLA states, see page 161.

3. Click **OK**. You are returned to the Service Level Agreements page.

   Verify that users are granted permissions to work with the SLA. For details, see the next section.

Defining an SLA: Grant Permissions to Users

You must now ensure that users are granted permissions for the SLA you just created, otherwise they will not be able to work with the SLA. Click the link at the bottom of the Service Level Agreements page to access the Platform Administration page. Set permissions for Service Level Management and choose the user and SLA for which you want to configure permissions. For details, see "Granting and Removing Permissions" in *Platform Administration*.

Editing and Adding KPIs and Objectives

You can edit KPIs that are already associated with the CI and you can add further KPIs to a CI. Each CI may have only one KPI associated with it and each KPI must include at least one objective.

This section contains the following topics:

- Associating KPIs with an SLA
- Defining Objectives

Associating KPIs with an SLA

For the list of KPIs, business rules, and business logic parameters that Service Level Management uses, see Chapter 16, "Repositories."

To associate a KPI:

1. In the Define KPIs page, select the CI to which you want to add a KPI.

   If you selected **Automatically define default KPIs for new CIs** in the Select CIs page, the CI and its direct children already have KPIs attached to them, that is, if the CI is related to Business Process Monitor or SiteScope measurements. For other measurements, Service Level Management automatically defines KPIs if the measurement has been so configured. For details on working with the Infrastructure Settings Manager, see "Editing Settings with the Infrastructure Settings Manager" on page 153.

2. Click **Add KPI** to open the KPI and Objectives window.

3. Select a KPI from the list.

Service Level Management displays only those KPIs that have not yet been associated with the CI.

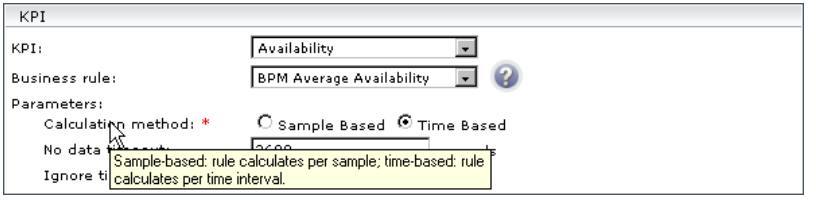
To produce reports that show data from a Six Sigma perspective, choose the **Availability Six Sigma** or **Performance Six Sigma** KPI.

You can enter a Six Sigma condition value between 0 and 6 with up to three decimal points.

- **Availability Sigma** – the sigma value against which Service Level Management measures the time that a business application or a service is up and running. For example, if you set a sigma of 4, you are expecting that for every million opportunities (CIs), not more than 6,210 will fail.
- **Performance Sigma** – the objective against which Service Level Management measures the time taken to execute a CI. For example, if you set a sigma of 3, you are expecting that for every million opportunities (CIs), less than 66,800 will **not** meet the target performance goal.

4 Select the business logic to be used when Service Level Management calculates the objectives.

For a short explanation of the business logic and its parameters, place the cursor over a field name:



5 Enter the parameter values (where these exist).

A red asterisk after a parameter signifies that the parameter is mandatory.

6 Define the objectives for the KPI. For details, see the next section.

7 Click **Save** to save the KPI details and return to the Define KPIs page.

Defining Objectives

You define CI objectives for availability percentages and performance times that reflect the terms of the SLA. For example:

- a Business Process Monitor CI that measures the time taken to add a purchase to a shopping cart
- a SiteScope CI that measures runtime for a servlet on a WebLogic 6.x application server
- a UDX (custom data) CI that monitors the accessibility of an HP OVO server

Performance objectives also measure other metrics such as percentiles, for example, that disk space must be at least 40% empty.

Extracting Objectives from a Service Level Agreement

The following is an example of clauses in a service level agreement:

> Users will be able to access the Mercury Web site within 8 seconds for 98% of the time during West Coast business hours. After business hours, they will be able to access the site within 12 seconds for 95% of the time.
> ...
> The average round-trip transmission between a UUNET-designated Hub Router in the Sunnyvale metropolitan area and a UUNET-designated Hub Router in the Chicago metropolitan area will take 120 milliseconds or less during business hours and 150 milliseconds or less after business hours.

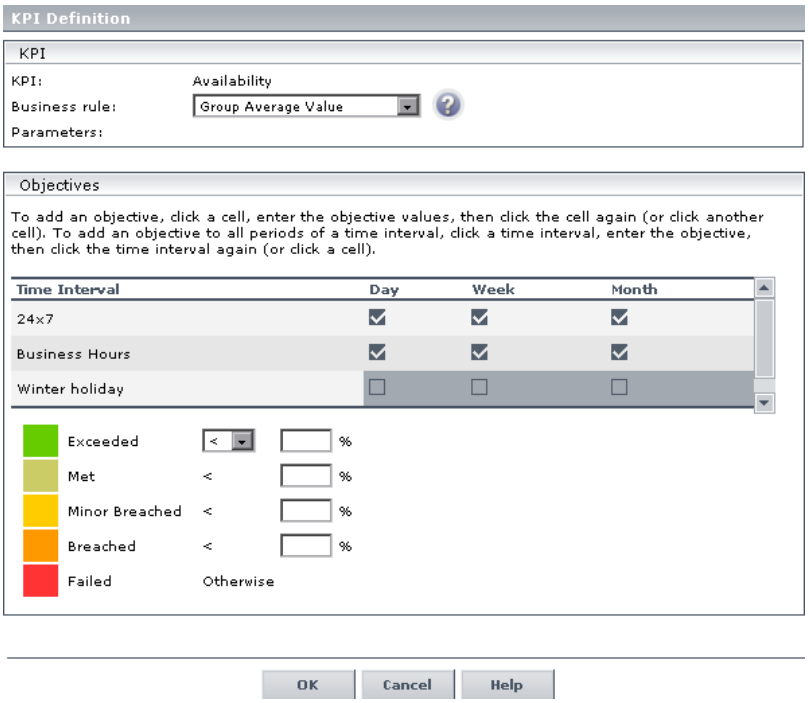
When defining objectives, you would interpret these clauses as follows (for previously created Business Process Monitor, Client Monitor, and SiteScope CIs):

Term	During Business Hours	After Business Hours
Time Interval	9 AM to 5 PM, Monday to Friday PST	5 PM to 9 AM, Monday to Friday PST 5 PM Friday to 9 AM Monday PST
CI 1 (measures availability objective)	98%	95%

Term	During Business Hours	After Business Hours
CI 2 (measures performance objective)	Home page must download within 8 seconds.	Home page must download within 12 seconds.
CI 3 (measures network performance)	120 milliseconds from hub router in Sunnyvale to hub router in Chicago	150 milliseconds from hub router in Sunnyvale to hub router in Chicago

To define objectives:

The units that appear here are defined in the Rule Detail page. (Access **Repositories** > **Rules**. Locate the business logic and click the **Edit Globals** button.)



1 To add an objective to a time interval, click a time interval cell, enter the objective value ranges in the target boxes, then click the cell again. The cell's tooltip changes to **Defined**.

   To add one objective to all periods of a time interval, click the time interval name, enter the objective values in the target boxes, then click the time interval again (or click any cell).

   The objective targets displayed here are selected in the Define SLA Properties page. For details, see "Defining an SLA: Properties" on page 164.

2 Click **Save** to save the KPI details and return to the Define KPIs page.

Note: If you do not define objectives, Service Level Management still performs calculations for the SLA and reports include data. However, reports do not show status by colors.

Editing an SLA

You can access any page in the SLA wizard directly through the left menu.

To edit an SLA:

1 In the Service Level Agreements page (**Admin** > **Service Level Management** > **Service Level Agreements**), locate the SLA that you want to edit, and click its **Edit** button to open the Edit SLA page.

2 In the left menu, click the name of the step you want to edit to display that page.

3 Make any necessary changes, as described in "SLA Definition Workflow" on page 162.

4 Click **Finish** to save the SLA.

Note:

- If the SLA to be edited is not in a preliminary state, the SLA start date and time zone cannot be changed and the SLA end date can be changed only to a future date.
- If the SLA to be edited is in a running state, historical data is not updated with the changes you make. To update historical data, you must run the recalculation process. Furthermore, if the changes you make to the SLA affect historical data, you must run the recalculation process. For details, see Chapter 10, "Recalculation."

Cloning an SLA

You can clone an existing SLA. The cloned SLA inherits all the properties of the existing SLA, including CIs, KPIs, and objectives. The creator of the new SLA is the user who cloned it.

To clone an SLA:

1 Locate the SLA in the Service Level Agreements page (**Admin** > **Service Level Management** > **Service Level Agreements**), click its **Clone** button, and answer **Yes** to the message.

Service Level Management adds a copy of the SLA to the list of SLAs, renames the clone **Copy of <name>**, and changes its start date to the present date and time.

If the start and end dates of the original SLA are no longer valid (for example, the SLA terminated a week ago or the start date falls before the allowed start date of the cloned SLA), Service Level Management sets the following default dates: the start date is the original start date or three months before the current date and the end date is the original end date.

2 To rename and edit the SLA, click the **Edit** button.

Note: You can clone an SLA on condition that you are an administrator or have been given change permissions on the SLA.

Deleting an SLA

To delete an SLA, locate the SLA in the Service Level Agreements page (**Admin** > **Service Level Management** > **Service Level Agreements**), and click its **Delete** button. Answer **Yes** to the question that is displayed.

To delete several SLAs simultaneously, select their check boxes, and click the **Delete** button. Answer **Yes** to the question that is displayed.

Note: You change an SLA's state (for example, from running to terminated) in the Service Level Agreements page. For details, see "The Service Level Agreements Page" on page 160.

10

Recalculation

Note to Mercury Managed Services customers: Mercury Operations administers these pages. For information about recalculation, contact Mercury Managed Services Support.

This chapter explains how to run the recalculation process to update the data in your SLAs, and how to cancel a recalculation task.

Recalculation Overview

You will generally use recalculation after making retroactive changes. For example:

- After defining a downtime event for the previous week, you should run the recalculation process to show the effect of the event on results.
- In the case of a connection problem with a site where data is sent after a one day delay, you should run recalculation so that this data is also included in calculations. (Service Level Management automatically supports "late arrivals," that is, data that reaches the database up to one hour after the data is recorded. However, for data reaching the database after a longer period of time, you must run the recalculation function.)
- After viewing the reports of a specific SLA, you notice that the objective definition was set too high. You edit the objective and run recalculation so that the change is reflected in the historical data.

The Recalculation Page

Caution: If you recalculate an SLA for a period when the raw data has already been purged, you will lose the recalculated data for that period. To verify the purging policy, select **Admin** > **Platform** > **Setup and Maintenance** > **Data Purging**.

You use this page to follow a recalculation task, to run new tasks, and to cancel recalculation tasks. This page includes recalculation tasks that are running and that are scheduled to run:

SLA – The name of the SLA. Service Level Management displays only those SLAs whose state is **Running or Terminated** (if their end date falls within the recalculation period—for example, an SLA that terminated a week ago can still be recalculated and will be included in this table). SLAs with a **Preliminary** state are not displayed.

Time Stamp of Latest Calculation – The last time that Service Level Management calculated the SLA data. Note that Service Level Management recalculates the SLA data once an hour for the previous hour. That is, if the time is now 07:30 AM, Service Level Management recalculated the data at 7:00 AM for data that was received between 05:00 AM and 06:00 AM.

Status – The current status of the recalculation run. When a task is running, Service Level Management displays the progress of the recalculation process in percentages.

Actions – You can run or cancel a recalculation task. For details, see the next sections.

Running Recalculation Tasks

You generally run recalculation tasks after making retroactive changes.

To run a recalculation task:

1 Select the Recalculation tab (**Admin** > **Service Level Management** > **Recalculation**).

2 Locate the SLA which you want to recalculate, and click its **Schedule** button to open the Recalculation Task dialog box.

3 To define the start of the recalculation period, click the **Recalculate from** date and time to make changes in the calendar.

The recalculation period must begin before the Last Calculation date and time.

The earliest date at which the recalculation process can begin running is set in the Infrastructure Settings Manager. By default, the recalculation period is three months. It is not recommended to lengthen this period as the recalculation task takes longer for a longer period. For example, Service Level Management takes longer to recalculate a month than to recalculate a week. For details, see “Editing Settings with the Infrastructure Settings Manager” on page 153 and “Infrastructure Settings” in *Platform Administration*.

4 To define when the recalculation must begin: click the **Schedule the task to start** date and time to make changes in the calendar.

Note: If you have just created an SLA whose start date has the current date and time, and you choose to start the SLA now, Service Level Management immediately begins calculating the first hour. However, since the first hour's raw data has not yet been sent to the database, the results are of no value. In this case, choose to start the SLA in a few hours.

---

5 Click **OK**.

Cancelling a Recalculation Task

You can cancel a recalculation task if it has been scheduled but has not yet begun running.

To cancel a task, locate the task and click its **Cancel** button.

11

Downtime Events

This chapter explains how to define events that represent actual event occurrences such as downtime, that may skew results and that you may want to exclude from reports.

The Downtime Events Page

You use this page to create events or to edit or delete existing events. The page includes existing events and the following components:

Name – The name of the event.

Start Date – The date and time when the event begins running.

End Date – The date and time when the event terminates. If there is no end date, the event is considered **unbound**.

Scheduling – The frequency of the event, either **single**, that is, a one-time event, or **recurring**, that is, daily, weekly, monthly, yearly, or compound.

Type – The type of event, either BPM event or SLA event.

Impact – The CIs that are affected by the event.

Actions – You can edit or delete an event. For details, see "Editing a Downtime or Scheduled Event" on page 194 and "Deleting a Downtime or Scheduled Event" on page 195.

New BPM Event and New SLA Event Buttons – Click this button to define an event. For details, see the next section.

Defining a BPM or SLA Event

You can define BPM and SLA events. You use BPM events when adding an event to Business Process Monitor data, and SLA events when adding an event to SLAs. You can define an event retroactively and you can define a recurring event. For examples of event definitions, see "Event Examples" on page 195.

You define an event for a specific SLA.

Note: You can create events only for existing SLAs. For details on defining an SLA, see Chapter 9, "Service Level Agreements (SLAs)."

To define an event:

1. Select the **Events** tab (**Admin** > **Service Level Management** > **Events**). Service Level Management lists events already defined.
2. Click **New BPM Event** or **New SLA Event** to open the Downtime/Event Schedule window.
   - ➤ choose **New BPM Event** when adding an event to Business Process Monitor data
   - ➤ choose **New SLA Event** when adding an event to an SLA
3. Enter the name of the new event and a description—to appear in Service Level Management reports—that describes the downtime or scheduled event.

You include the event description in reports, by selecting the **Advanced options** link in the report page. For details, see "Adding Descriptions to Reports" in *Using Service Level Management*.

4 To exclude data such as scheduled maintenance periods, select **Exclude data reported during event**.

5 Define the time periods during which data is affected. You can define a one-time event (**Once**) or a recurring event (**Daily**, **Weekly**, **Monthly**, or **Yearly**; for examples, see "Event Examples" on page 195):

Note: Dates are specified according to the user's time zone.

- **Once.** To change the start date, click the date and time to make changes in the calendar. Choose either an end date (select **End time**) or the duration of the event in days, hours, and minutes (select **Event duration**).
- **Daily.** Select how often the event is to run.

  Set the duration and recurrence range: To change the start date, click the date and time to make changes in the calendar. Choose the duration of the event in hours and minutes.

  For the event to be open-ended (unbound), select **No end date**. To limit the event, select **End time** and click the date and time to make changes in the calendar.
- **Weekly.** Choose the frequency at which the event is to occur. For example, select **3** for the event to occur every third week. Select the days of the week on which the event is to occur.

  Set the duration and recurrence range: To change the start date, click the date and time to make changes in the calendar. Choose the duration of the event in hours and minutes.

  For the event to be open-ended, select **No end date**. To limit the event, select **End time** and click the date and time to make changes in the calendar.

➤ **Monthly.** Choose the frequency at which the event is to occur. For example, you could choose the 10th day of every month, the first Sunday of every fourth month, or the last day of every sixth month.

Set the duration and recurrence range: To change the start date, click the date and time to make changes in the calendar. Choose the duration of the event in hours and minutes.

For the event to be open-ended, select **No end date**. To limit the event, select **End time** and click the date and time to make changes in the calendar.

➤ **Yearly.** Choose the frequency at which the event is to occur. For example, you could choose the 4th of every July or the last Sunday in November.

Set the duration and recurrence range: To change the start date, click the date and time to make changes in the calendar. Choose the duration of the event in hours and minutes.

For the event to be open-ended, select **No end date**. To limit the event, select **End time** and click the date and time to make changes in the calendar.

Note: This page may display incorrectly when viewed with Microsoft Internet Explorer.

---

6 In the Event Schedule Action section, select the SLA from the list.

To define a downtime event on one Business Process Monitor CI that will affect all existing SLAs and any future SLAs, select **All**. This is on condition you have edit permissions for all SLAs. Service Level Management reports will show downtime events defined for a specific SLA and for all SLAs. If the Downtime Event Description is displayed for an event defined for all SLAs, each of which has a different time zone, the event's date and time may not be relevant for all the SLAs.

Note: The SLA list includes only those SLAs that you have permissions to change.

---

7 To select specific CIs that will be affected by the event:

a Click **CI Filter** to open the CIs Selection window. Service Level Management displays a list of:

- End User monitors, if you are defining a BPM event
- the SLA tree, if you are defining an SLA event

b Locate the CIs that will be affected, select their check boxes, and click **OK**.

Note: The descendants of the selected CIs are also affected by this event.

---

c To search for CIs, click the **Search** link.

- Enter the name of the configuration item (CI), or part of the name, in the **Search for** field. Click the **Search** button to display the results below.

  You can also search for CIs using the **Related to** or **Type** fields. **Related to** searches for CIs that are related to the selected CI, and **Type** searches for CITs. Select the check box and click the button to open the Select Configuration Item (or Select Configuration Item Type) window. In the Select Configuration Item window, choose the CI you want to display; in the Select Configuration Item Type window, choose the configuration item type (CIT). Click **OK**, or click **Cancel** to close the window without choosing a CI or CIT. In the Search pane, click the **Search** button to display the results below.

- To add the CI to the event, locate and right-click the CI. Choose **Locate CI in View** from the menu to return to the Browse pane.
- For SLA events only, locate the CIs that will be affected, select their check boxes, and click **OK**.

- For BPM events only, locate the CI that will be affected, select it and click **OK**.

8 Click **OK**.

Note:

➤ From version 5.0 FP1, the maximum duration for an event (not including a one-time event) is 23 hours and 59 minutes. If you have created events in previous versions of Mercury Business Availability Center that are longer than this duration, Service Level Management shortens the event to 23 hours and 59 minutes.

➤ If an event is defined for an SLA after the SLA has started running, the event affects data received after the event is defined. To affect data retroactively, Service Level Management must recalculate the SLA. For details, see Chapter 10, "Recalculation."

Editing a Downtime or Scheduled Event

You can make changes to existing events. Changes affect reports retroactively. For example, if you change the event frequency, data may now be included in reports that was previously excluded. Once the changes are saved, any generated reports include the updated event.

Note: For events to affect reports retroactively, you must recalculate the SLA.

To edit a downtime or scheduled event:

1 Select the **Events** tab (**Admin** > **Service Level Management** > **Events**). Service Level Management lists events already defined.

2 Locate the event that you want to change and click the **Edit** button to open the Downtime/Event Schedule window.

3 Make any required changes to the event general properties and event scheduling parameters (you cannot change the SLA or the CIs). For details, see "Defining a BPM or SLA Event" on page 190.

4 Click **OK**.

Deleting a Downtime or Scheduled Event

You can delete existing events. Any reports generated from this time will reflect the deletion. Service Level Management also updates the Audit Log (for details, see "The Audit Log" in *Application Administration*).

Note: For a deleted event to affect reports retroactively, you must recalculate the SLA. For details, see Chapter 10, "Recalculation."

To delete an existing downtime or scheduled event:

1 Select the **Events** tab (**Admin** > **Service Level Management** > **Events**). Service Level Management lists events already defined.

2 Locate the event that you want to change and click its **Delete** button. Click **OK** to confirm deletion.

Event Examples

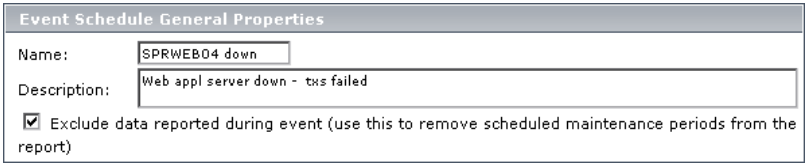
This section provides examples of events for all scheduling periods, and contains the following topics:

Once

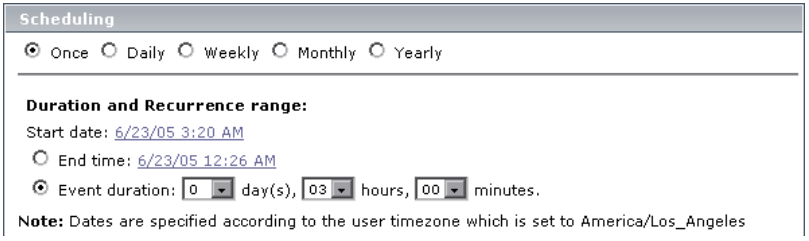
Every morning the VP of eBusiness looks through the previous day's SLAs Summary reports. One morning, she realizes that due to maintenance in the Springfield office, the Web applications server had been down for three hours and all Business Process Monitor CIs from that location have failed. She needs to define a retroactive downtime event and adjust the reports to reflect the downtime.

➤ She accesses the Events tab and creates a new Business Process Monitor event by clicking the **New BPM Event** button.

➤ She enters a name and description for the downtime. She leaves the **Exclude data reported** check box selected.



➤ In the Scheduling section, she chooses the **Once** option and enters the start date, time, and duration of the server downtime.



➤ In the Event Schedule Action section, she selects one of the SLAs that cover the Springfield office contracts (she must create an event for each SLA).

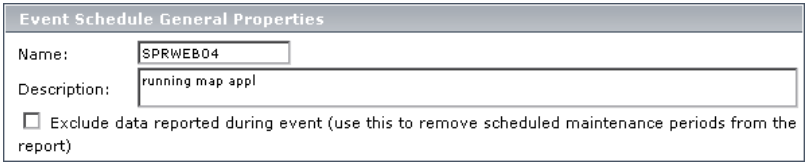
➤ She clicks **CI Filter** to select the SLA.

- She selects the relevant SLA and then clicks **CI Filter** to select the Springfield location.
- She saves the event.
- She recalculates the SLA over the relevant period of time.
- She next accesses the SLAs Summary page, generates reports for relevant KPIs, and verifies that during this time, the data is ignored and the status of the SLA is **downtime**.

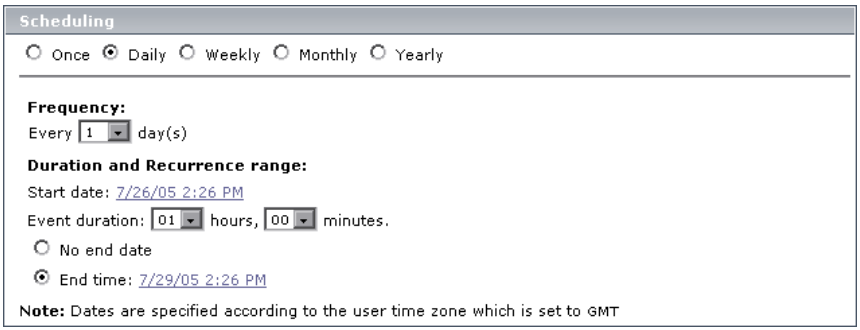
Daily

The operations support engineer is told that a server's graphics card is being upgraded for a new map application. A slowdown of the server may be expected for three days beginning today, while the R&D team tests the new application. To minimize problems, the team will be running tests for one hour each day. All SLAs that monitor this server will be affected, and he should define an event to appear in reports to explain the slowdown.

- He defines a new SLA event, and enters a name and detailed description for the downtime (each SLA needs its own event). He clears the **Exclude data reported** check box.



- In the Scheduling section, he chooses the **Daily** option and enters a frequency of 1 day (the default). In the Duration and Recurrence range, he chooses today's date and time from the calendar. He chooses a duration of 1 hour, and the end date and time for three days' hence.

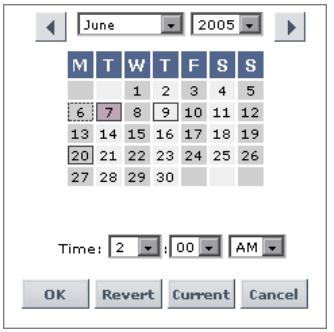


- In the Event Schedule Action section, he selects the relevant SLA, clicks **CI Filter**, and selects the server.
- He saves the event.
- He accesses the CIs Over Time report (**Applications** > **Service Level Management** > **Over Time Reports**) and clicks the Advanced Options link. He selects the **Downtime Event Description** check box.
- The next day he generates a CIs Over Time report and verifies that the event appears in the report.

Note: The operations support engineer has no need to recalculate the SLA, since the **Exclude data reported** check box was not selected.

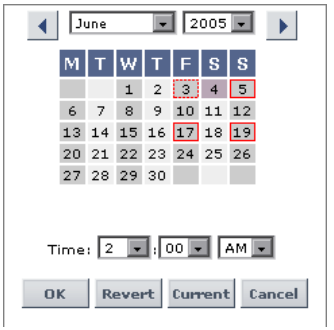
Weekly

Example 1: You define an event to occur once every two weeks (**2**) with a start date of Tuesday, 7 Jun 05. For calculation purposes, the first week runs from Monday, 6 Jun 05 till Monday, 13 Jun 05.



- If the event is to occur every second Tuesday, the first occurrence of the event will be on Tuesday, 7 Jun 05.
- If the event is to occur every second Thursday, the first occurrence of the event will be on Thursday, 9 Jun 05.
- If the event is to occur every second Monday, the first occurrence of the event will be on Monday, 20 Jun 05.

Example 2: You define a recurring event that occurs every second week on a Friday and a Sunday, to begin on a Saturday. In the first week, the event will run only on Sunday. In the second week, the event does not run. In the third week, the event runs on Friday and on Sunday, and so forth.

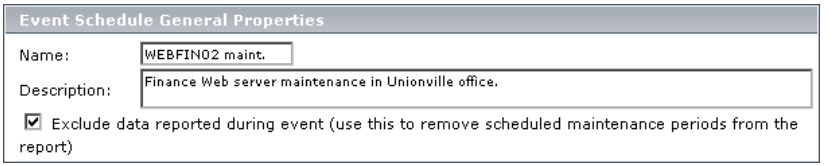


Monthly

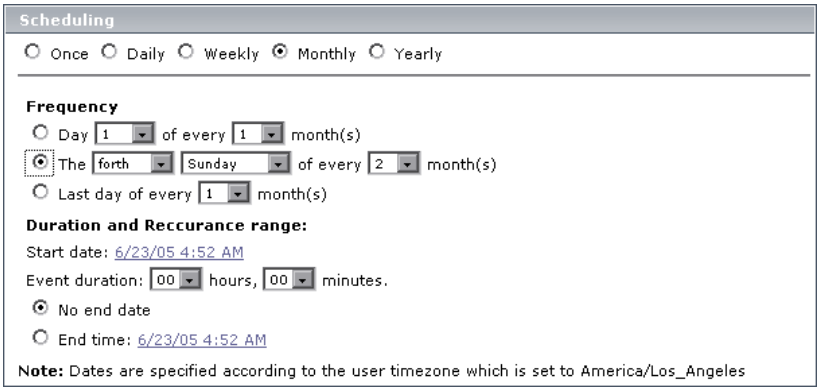
Every other month, on the forth Sunday, the Web server for the Finance department in the Unionville office is scheduled for maintenance at 1:00 AM for two hours. Therefore, the IT Ops director must define a recurring event and exclude all CIs from reports during this period.

➤ The IT Ops director accesses the Events tab and creates a new Business Process Monitor event by clicking the **New BPM Event** button.

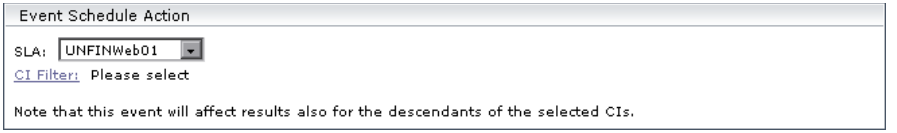
➤ He enters a name and description for the maintenance. He leaves the **Exclude data reported** check box selected.



➤ In the Scheduling section, he chooses the **Monthly** option. In the Frequency section, he selects **Fourth**, **Sunday**, and **2**. He enters the start date and time and enters **2** for the event duration. He leaves **No end date** selected.



➤ In the Event Schedule Action section, he selects one of the SLAs that cover the Unionville office contracts (each SLA needs its own event).



- He selects the SLA's CI from the CI filter, so that all descendants are also affected.
- He saves the event.

Yearly

The VP of eBusiness likes to be prepared. Each July 5th, her boss sends her an e-mail requesting network statistics for the previous day to compare to their targets. This year, on July 3rd, she prepares an SLA to measure network performance and creates an event that will run throughout the next 24 hours.

In the Scheduling section, she chooses the **Yearly** option. In the Frequency section, she selects **Every**, **July**, and **4**. She enters the start date and time of July 4th at 12:00 AM and sets an event duration of 23 hours and 59 minutes. She leaves **No end date** selected.

On July 5th she is able to reply immediately to her boss's e-mail with the network performance results compared to the target objectives.

12

SLA Management Administration

This chapter explains how to document IT services provided by your department in Mercury Business Availability Center. Examples of services include project management services, application development for departmental applications, and Web development or publishing services.

SLA Management Workflow

Use the following workflow to set up SLA Management.

1 Access SLA Management.

Admin > Service Level Management > SLA Management.

The View Explorer displays the three SLA Management views: Business Unit, SLA Management, and Service Measurements.

2 Define a business unit.

The Business Unit view enables you to manage business entities such as customers, external providers, the IT department, and so forth. This step is optional, as you can choose to add a new service to an existing business unit. For details, see "Defining a Business Unit" on page 204.

3 Define a service.

The SLA Management view enables you to view the business service topology, and to manage business services by creating services and editing existing services. For details, see "Defining a Service" on page 206.

4 Add monitors to the service.

The Service Measurements view enables you to add measurements (such as Business Process Monitor transactions, Real User Monitors or SiteScope monitors) to business services. For details, see "Defining a Service Measurement" on page 207.

For details on viewing reports that use SLA Management services, see "SLA Management Services Reports" in *Using Service Level Management*.

Defining a Business Unit

You create business units to reflect your organization's structure. That is, you create business units for customers, providers, and any other entities with which you conduct business. For each business unit, you can build a hierarchy of components.

To define a business unit:

1 In View Explorer, select **Business Units**.

2 Right-click **Business Units** and select **New CI**.

The Define General Properties page opens. For details on using this page, click the Help button or see "Creating a New CI" in *IT Universe Manager Administration*.

The new CI with a Business Unit CIT is added to the list of business units.

3 The next stage is to assign a CI to the business unit. Select the new business unit to display the Properties and Related Configuration Items tabs. For details on defining properties and CIs, see "Creating a New CI" and "Related Configuration Items Tab" in *IT Universe Manager Administration*.

4 To display a menu of actions, right-click the business unit:

- **New Related CIs.** Displays the Define General Properties window. You can create a CI that is related to the current CI. For details, see "Creating a New CI" in *IT Universe Manager Administration*.
- **Attach Related Cis.** Displays the Attach Related CIs window. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.
- **Attach Monitor CIs.** Displays the Attach Related CIs window with the Monitors View displayed. Select monitors to attach to the business unit. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.
- **Delete CI.** Displays a message. Click **OK** to delete the business unit, or **Cancel** to close the message without deleting the unit.
- **Show Related CIs**. Displays related CIs in the View Explorer search pane. For details, see "Searching for Configuration Items" in *Working with the CMDB*.
- **Properties.** Displays the General Properties window. For details, see "Configuration Item Properties" in *Working with the CMDB*.

Defining a Service

For each business unit, you can create business services. Although you can assign monitors and measurements to the services, it is recommended that you add the monitors and measurements in the Service Measurements view. For details, see "Defining a Service Measurement" on page 207.

To create a service:

1 In View Explorer, select **SLA Management**.

2 Right-click **SLA Management** and select **New CI**.

The Define General Properties page opens. For details on using this page, click the Help button or see "Creating a New CI" in *IT Universe Manager Administration*.

The new CI with a Business Service CIT is added to the list of services.

3 The next stage is to assign a CI to the business service. Select the new business service to display the Properties and Related Configuration Items tabs. For details on defining properties and CIs, see "Creating a New CI" and "Related Configuration Items Tab" in *IT Universe Manager Administration*.

4 To display a menu of actions, right-click the business unit:

- **New Related CIs.** Displays the Define General Properties window. For details, see "Creating a New CI" in *IT Universe Manager Administration*.
- **Attach Related CIs.** Displays the Attach Related CIs window. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.
- **Attach Monitor CIs.** Displays the Attach Related CIs window. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.
- **Delete CI.** Displays a message. Click **OK** to delete the business unit, or **Cancel** to close the message without deleting the unit.
- **Show Related CIs.** Displays related CIs in the View Explorer search pane. For details, see "Searching for Configuration Items" in *Working with the CMDB*.
- **Properties.** Displays the General Properties window. For details, see "Configuration Item Properties" in *Working with the CMDB*.

Defining a Service Measurement

The Service Measurements view contains all existing business services as well as the monitors (or measurements) that have been assigned to them (in the SLA Management view). In this view you can view monitors and measurements and edit the properties of the service CIs.

Note: Although you can add monitors to both SLA Management and Service Measurements views, it is recommended to add them to the Service Measurements view only.

To edit a service measurement property:

1. In View Explorer, select **Service Measurements**.
2. Locate and select the service measurement you want to view or edit.
3. To display a menu of actions, right-click the service measurement:
   - **New Related CIs.** Displays the Define General Properties window. For details, see "Creating a New CI" in *IT Universe Manager Administration*.
   - **Attach Related Cis.** Displays the Attach Related CIs window. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.
   - **Attach Monitor CIs.** Displays the Attach Related CIs window. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.
   - **Delete CI.** Displays a message. Click **OK** to delete the service measurement, or **Cancel** to close the message without deleting the service measurement.
   - **Show Related CIs.** Displays related CIs in the View Explorer search pane. For details, see "Searching for Configuration Items" in *Working with the CMDB*.
   - **Properties.** Displays the General Properties window. For details, see "Configuration Item Properties" in *Working with the CMDB*.

Configuring SLA Management

You can manage SLA Management either through Mercury Business Availability Center or through Mercury IT Governance Center.

To choose how to manage SLA Management:

Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Service Level Management**, and locate the **SLA Management managed by Service Management Lifecycle** entry in the SLM Admin table.

- **true.** SLA Management is managed by Mercury IT Governance Center.
- **false.** SLA Management is managed by Mercury Business Availability Center.

13

SLA Status Alerts

This chapter explains how to create an SLA status alert that notifies you or another user of changes to an SLA's KPI status.

The SLA Status Alerts Page

You use this page to create SLA status alerts or to perform actions on existing alerts. Service Level Management displays those alerts which you, the logged-in user, have permissions to change or delete.

The page includes the following components:

Alert Name – The name of the alert. For a long name, hold the cursor over the name to view it in full in a tooltip.

Recipients – The names of the users who are to be informed when alert conditions are met.

Condition – The conditions that trigger an alert.

Actions – You perform the following actions by clicking the appropriate button:

- **Enable** – click to run the alert (if this button is disabled, the alert is running)
- **Disable** – click to stop the alert (the alert can be enabled again)
- **Clone** – click to duplicate the alert. For details, see "Cloning SLA Status Alerts" on page 221.
- **Edit** – click to edit the alert. For details, see "Defining an Alert: General" on page 212.
- **Delete** – click to delete the alert. For details, see "Deleting SLA Status Alerts" on page 221.

New Alert button – To define an alert, click this button. For details, see the next section.

You can sort the list by any column: An arrow next to a title shows by which column the alerts are sorted, and also the direction in which the column has been sorted (that is, ascending or descending).

Select, Unselect, Invert Selection, Disable, Enable, and Delete buttons – To perform an action on more than one alert simultaneously, select the check boxes of the alerts you want to start, stop, or delete, using the **Select**, **Unselect**, and **Invert Selection** buttons. Click the relevant button.

To search for an alert in the list:

Enter the name of the alert in the **Search in current view by name** box and click **Search**.

Service Level Management displays the alert on the page.

When searching, you can type an asterisk (*) to replace characters. For example, to search for an alert named **alert on finance machine**, enter *finance*. To display all alerts, type an asterisk only.

SLA Status Alert Workflow

Perform the following steps to define an SLA status alert:

- Use the Alert Wizard to define an SLA. For details, see "Defining an Alert: Welcome" on page 212.
- Give a name to the alert, set conditions, and define the notification frequency. For details, see "Defining an Alert: General" on page 212.
- Choose the SLAs that will be monitored by the alert. For details, see "Defining an Alert: Related SLAs" on page 213.
- Choose the recipients and templates for the alert. For details, see "Defining an Alert: Templates and Recipients" on page 214.
- Select the actions that will be triggered by the alert. For details, see "Defining an Alert: Actions" on page 216.
- Verify that the alert scheme you created is correct. For details, see "Defining an Alert: Summary" on page 221.

Defining an Alert: Welcome

You use the Alert Wizard to define SLA status alerts.

To create an SLA status alert:

1 Select the **SLAs Status Alerts** tab to open the Service Level Agreement page (**Admin** > **Service Level Management**). The page shows a list of existing alerts, organized alphabetically.

For a description of this page, see "The SLA Status Alerts Page" on page 210.

2 Click **New Alert** to open the Alert Wizard at the Welcome page.

3 Click **Next** to begin creating an alert.

The first stage in the procedure is to name the new alert and set conditions. Continue to the next section.

Defining an Alert: General

The first stage in the procedure is to define the alert's name and description and to set conditions.

To define alert properties:

1 Fill out the following fields:

Name – The name of the alert must be unique and must not be longer than 100 characters.

Description – Enter a description to appear in Service Level Management reports.

Alert Type – Choose between **All Tracking Periods** (the alert monitors all tracking periods) or **Selected Tracking Periods** (you select the tracking periods in the next stage of the procedure).

Condition – Choose between:

- **Send alert once status worsens**: triggers the alert when the current status of an SLA is worse than the previous status. **No Data** is ignored. For example, if the status changes from Met to Minor Breached, the alert is triggered.
- **Send alert once status improves**: triggers the alert when the current status of the SLA is better than the previous status. **No Data** is ignored. For example, if the status changes from Breached to Minor Breached, the alert is triggered.
- **Send alert if status value was changed from**: sets the appropriate conditions for sending an alert. Select the appropriate status in the **from** and **to** boxes.

Notification Frequency – Choose between:

- **Send alert for every trigger occurrence**: send an alert each time the condition is triggered.
- **Send no more than one alert per**: send an alert once only according to the selection, even if the condition is triggered more than once.

2 Click **Next** to continue.

The next stage in the procedure is to associate SLAs with the alert. Continue to the next section.

Defining an Alert: Related SLAs

The next stage in the procedure is to select the SLAs and the tracking periods that the alert should monitor. The list of SLAs includes those which you, the logged-in user, have permissions to change or delete.

To specify related SLAs and to select tracking periods:

1 Add SLAs to the list of SLAs that the alert will monitor.

To move the SLAs to the Selected SLAs list, use the upper arrow.

To remove SLAs from the Selected SLAs list, select the SLAs and use the lower arrow.

Select multiple SLAs by holding down the CTRL key and selecting the SLAs.

2 If you chose the **Selected Tracking Periods** alert type in the previous page, the Related SLAs page includes a list of tracking periods.

Select the tracking periods to include in the alert. The tracking periods that appear here are chosen during SLA creation.

To make your selections, you can also use the buttons at the bottom of the list for **Select All**, **Clear All**, and **Invert Selection**.

Note: The list of tracking periods is displayed after you have selected the SLAs.

---

3 Click **Next** to continue.

The next stage in the procedure is to choose the alert's format and to define to whom the alert should be sent. Continue to the next section.

Defining an Alert: Templates and Recipients

The next stage in the procedure is to choose the alert's format and to define to whom the alert should be sent.

To choose formats and recipients:

1 Select the template formats that are to be used when Mercury Business Availability Center sends the alert to recipients:

➤ **E-mail message template**. Choose between:

Short HTML e-mail message, short text e-mail message – These messages include the change in status only.

Long HTML e-mail message, long text e-mail message – These messages include a subject line and body.

Mercury Business Availability Center supports secure mail. For details, see "E-mail Messages" in *Platform Administration*.

➤ **SMS or pager template**. SMS and pager messages are sent via e-mail to the service provider. The e-mail address is:
<SMS provider access number>@<SMS provider e-mail address>
or
<Pager provider access number>@<Pager provider e-mail address>.

Choose between:

Long SMS/Pager message – The message includes the change in status and information about the SLA.

Short SMS/Pager message – The message includes the change in status only.

For details on modifying the message character set, see below.

2 To define a new recipient, click **New Recipient**. For details, see "Configuring and Selecting Recipients" in *Platform Administration*.

3 Click **Next** to continue.

The next stage in the procedure is to choose the actions that should occur when the alert is triggered. Continue to the next section.

To modify a message character set:

The default character set for e-mail, SMS and pager messages is **UTF-8**. You can change this character set in the Infrastructure Settings Manager.

1 Access the Infrastructure Settings Manager: **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.

2 Select the Foundations context and choose **Alerting** from the list.

3 Scroll down to the **Alerting - Triggered alerts** table.

4 Click the **Edit** button for the relevant parameter: **E-mail alerts charset**, **SMS alert charset**, or **Pager alert charset**.

5 In the View list, select another character set, for example, **ISO-2022-JP**.

Defining an Alert: Actions

The next stage in the procedure is to choose the actions that occur when an alert is triggered.

You can embed alert parameters in a URL, set up an executable file to run when an alert is triggered, and set up an SNMP trap to run when an alert is triggered.

This section includes the following topics:

Create URL

You can embed predefined alert parameters in a URL that is accessed when an alert is triggered.

By accessing a URL, Mercury Business Availability Center can send alerts via a Web site, for example, using Active Server Pages, CGI, or Perl. The URL can activate an executable program on a Web server, report to a custom database, activate a Web-based fax service, and so forth.

When accessing a URL, Mercury Business Availability Center supports the GET method only. For details, see "Differences Between GET and POST" on page 218.

To create a URL:

1. Click **New URL** to open the Create New URL window.
2. Enter the URL in the box and embed alert parameters by choosing alert parameters and clicking **Insert Field**. The field appears between double angle-brackets in the **Enter URL** box.

When embedding alert parameters in a URL, use the following format:

```
http://<server_or_IP>?<alert parameters>
```

For example:

```
http://financesystem.com?name=<AlertName>&sla=<SLA
Name>&TriggerTime=<Trigger Time>&CurrentStatus=<Current Status>
```

The alert parameters are:

- **SLA Name** – the name of the SLA

  If an alert monitors more than one SLA, the name that appears in this field is the SLA that triggered the alert.

- **Alert Name** – the name of the alert scheme
- **Trigger Time** – the start date and time of the alert.
- **Previous Status** – the previous status of the SLA

  Service Level Management includes the following statuses: Exceeded, Met, Minor Breached, Breached, and Failed.

- **Current Status** – the current status of the SLA

  The change from previous status to current status triggers the alert.

- **Tracking Period** – the period that the alert is monitoring, chosen during SLA creation

3. Click **OK** to return to the Actions page.
4. Set up an executable file ("Create Executable File" on page 218) or an SNMP trap alert ("Create SNMP Trap" on page 220), or click **Finish** to continue.

   The last stage in the procedure is to verify that the settings you defined for the alert are correct. Continue to the next section.

Differences Between GET and POST

Mercury Business Availability Center supports the GET method only, for the following reasons:

- **Usability** – with the POST method, the HTML file must first be saved on the client computer and then sent by the administrator to the specific user. With the GET method, the URL can be copied from Mercury Business Availability Center, pasted into an e-mail, and sent to the user.
- **HTTP specifications** – for the differences between the GET and POST methods, see http://www.cs.tut.fi/~jkorpela/forms/methods.html.

Create Executable File

You can specify that you want Mercury Business Availability Center to run an executable file (for example, an **.exe** or **.bat** file) when an alert is triggered.

You can embed alert parameters in the executable file. The parameters are used as placeholders when the message is formatted.

Note: The executable file must not be interactive (no user response required) and should not have a user interface.

To create an executable file:

1. Click **New Executable File** to open the Create New Executable File window.
2. Enter the URL in the box and embed alert parameters by choosing alert parameters and clicking **Insert Field**. The field appears between double angle-brackets in the **Enter command** box.

   When using a custom command line, the command line that runs the executable file must be in the following format:

```
<full path to program from Data Processing Server machine> <program command line switches>
```

You embed the alert parameters—which are expanded before the command line is executed—in the program command line switches section of the command line statement. For example:

```
C:\Bin\MyAlertReporter.exe –title “<Alert Name> for <SLA Name>” –Text “<Current Status>”
```

Note: Because the server triggers the executable, the path to the executable must be available from the Data Processing Server machine.

The alert parameters are:

- **SLA Name** – the name of the SLA
- **Alert Name** – the name of the alert scheme
- **Trigger Time** – the start date and time of the event that triggered the alert.

  Note: Trigger time is not necessarily the time of the alert. For example, if the alert engine is down when the alert is triggered, the alert may be sent several minutes later.

- **Previous Status** – the previous status of the SLA

  Service Level Management includes the following statuses: Exceeded, Met, Minor Breached, Breached, and Failed.

- **Current Status** – the current status of the SLA

  The change from previous status to current status triggers the alert.

- **Tracking Period** – the period that the alert is monitoring, chosen during SLA creation

3. Click **OK** to return to the Actions page.
4. Set up a URL (“Create URL” on page 216) or an SNMP trap alert (“Create SNMP Trap” on page 220), or click **Finish** to continue.

   The last stage in the procedure is to verify that the settings you defined for the alert are correct. Continue to the next section.

Create SNMP Trap

You specify that you want Mercury Business Availability Center to send an SNMP trap when alert trigger criteria are met. The alert notice can be seen via any SNMP management console in the organization.

For details on configuring the Alerts MIB in your SNMP management console, see "Configuring the Alerts MIB" in *Platform Administration*. (For traps created through the SLA Status Alerts page, use the file **CIAlerts.mib**.)

Note: Mercury Business Availability Center supports only SNMP V1 traps.

To create an SNMP trap:

1. Click **New SNMP Trap** to open the Create New SNMP Trap window.
2. Enter the IP address or name of the host destination.

   If Service Level Management displays a default host destination, you can accept the default, or enter another IP address or name.

   If you do not enter a port number, Service Level Management uses a default port number.

   The SNMP default trap destination host and port are set in the Infrastructure Settings Manager. Select the Foundations context and choose **Alerting** > **Alerting – Triggered Alerts**. For details, see "Editing Settings with the Infrastructure Settings Manager" on page 153 and "Editing Infrastructure Settings" in *Platform Administration*.
3. Click **OK** to return to the Actions page.
4. Set up a URL ("Create URL" on page 216) or an executable file alert ("Create Executable File" on page 218), or click **Finish** to continue.

   The last stage in the procedure is to verify that the settings you defined for the alert are correct. Continue to the next section.

Defining an Alert: Summary

The last stage in the procedure is to verify that the settings you defined for the alert are correct.

To verify the alert settings:

1. Read through the alert summary.
2. To save the alert, click **OK**. You are returned to the SLA Status Alerts page.

   To make changes to the alert, click **Back** or click the stage in the left menu to go directly to the page you want to change.

Cloning SLA Status Alerts

You can clone an existing alert. The cloned alert inherits all the properties of the existing alert, including SLAs and recipients. The creator of the new alert is the user who cloned it.

To clone an alert:

1. Locate the alert in the SLA Status Alerts page (**Admin** > **Service Level Management** > **SLA Status Alerts**) and click its **Clone** button.

   Service Level Management adds a copy of the alert to the list of alerts, renames the clone **Copy of <name>**, and changes its start date to the present date and time.
2. To rename and edit the alert, click the **Edit** button.

Deleting SLA Status Alerts

To delete one alert or several alerts, select the alerts in the SLA Status Alerts page (**Admin** > **Service Level Management** > **SLA Status Alerts**), and click the **Delete** button. Answer **Yes** to the question that is displayed.

14

Time Intervals

This chapter explains how to define time interval schedules. The Service Level Management reports organize results according to time intervals. A time interval is the actual period of time for which Service Level Management calculates data.

Time Intervals Overview

In your organization, the same service levels are probably not required at all times of the day or night, or during all days of the week or year. For example, performance and availability are more crucial to a Web retailer during a busy shopping period before a holiday. Likewise, resource allocators in an ERP system must have 99% availability every working morning, whereas at other times 97% might be acceptable.

To monitor your business processes at these crucial times, you define time intervals that span the period you want to monitor. This is the time range that Service Level Management checks for compliance to the SLA. Service Level Management includes two default time intervals: **24x7** and **Business Hours**.

The Time Intervals Page

You use this page to create time intervals or to edit or delete existing time intervals. The page includes existing time intervals and the following components:

Name – The name of the interval.

Period Type – Time intervals can be weekly, yearly, or compound. For details on these period types, see page 225.

Description – The description of the interval.

Actions – You can edit, clone, or delete a time interval. For details, see "Editing a Time Interval" on page 227, "Cloning a Time Interval" on page 228, and "Deleting a Time Interval" on page 228.

New Time Interval Button – Click this button to define a new time interval. For details, see the next section.

Defining a Time Interval

You use the Time Interval wizard to define time interval schedules.

To define a time interval:

1. Select the **Time Intervals** tab to open the Time Interval wizard (**Admin** > **Service Level Management** > **Time Intervals**). The page shows a list of existing time intervals. For details on this page, see "The Time Intervals Page" on page 224.
2. Click **New Time Interval** to open the Time Interval wizard.
3. Give a name to the time interval.

   The name should not be longer than 50 characters and can consist of any characters (including special characters) and spaces.
4. Enter a description.

   The description should not be longer than 500 characters and can consist of any characters and spaces.
5. Choose the time interval scheme:

   Weekly – The time interval is based on a weekly cycle, for example, every Sunday from 1:00 AM to 3:00 AM. Continue to the next step.

   Yearly – The time interval is based on a yearly cycle, for example, the month of December or annual vacations. Continue to the next step.

   Compound – The time interval combines existing time intervals. For example, say one yearly time interval monitors January to October, and a weekly time interval monitors business hours. You could combine the two time intervals to create a time interval that monitors business hours from January to October. Skip to step 8.
6. Click **Next** to continue to the next page.

7 If you selected **Weekly** on the previous page, the time grid displays the days of the week.

If you selected **Yearly** on the previous page, the time grid displays the months of the year.

To add a time or date to the time interval, click a cell. To remove the time or date, click the cell again. (Active cells are shown in red and free cells in gray.)

To enter a range, select the times or dates in the lower table and click **Add**.

To remove part of a time interval, select the range in the lower table and click **Clear**. For example, to quickly create a time interval that spans the whole week, apart from work days, select a start time of 12 AM and an end time of 12 AM. Select all the days of the week. Click **Add**. Select a start time of 9 AM and an end time of 5 PM. Select Monday to Friday. Click **Clear**.

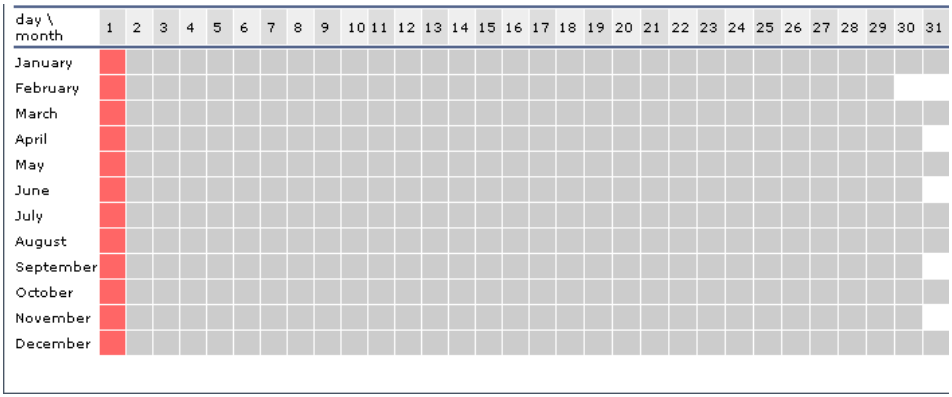
To remove all active times from the grid, click **Clear All**.

8 If you chose **Compound** in the previous page, you must now choose which time intervals to include in the new time interval.

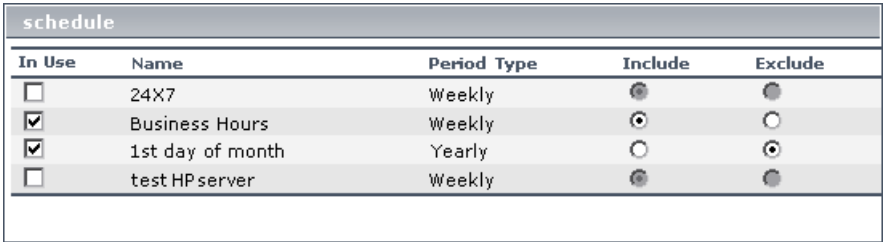
Locate the time intervals to add to the new time interval, and select their **In Use** check box.

You use the **Include** and **Exclude** buttons when you want to use an existing time interval but without all its components.

For example, say you want to define a time interval that monitors business hours but does not include the first day of the month. You define a yearly time interval (called **1st day of month**) that includes only the first day of each month:



Next, you define a **Compound** type time interval where you include the Business Hours time interval and exclude the **1st day of month** time interval.



In this example, **24x7** and **test HP server** are irrelevant to the compound time interval being defined and are not selected.

Note: If you update one of the time intervals included in a compound time interval, the compound time interval itself is also updated.

---

9 Click **Finish** to continue to the next page.

Service Level Management confirms that your settings have been saved successfully.

10 Click **Close** to close the Time Interval Wizard and return to the Time Interval page. The new time interval is displayed in the list.

Editing a Time Interval

You can make changes to an existing time interval.

To edit an existing time interval:

1 Select the **Time Intervals** tab (**Admin** > **Service Level Management** > **Time Intervals**). Locate the time interval you want to edit and click its **Edit** button.

2 Make any necessary changes, by continuing with the procedure for defining a time interval. For details, see page 225.

Cloning a Time Interval

You can clone a time interval to define a similar schedule.

To clone an existing time interval:

1 Select the **Time Intervals** tab (**Admin** > **Service Level Management** > **Time Intervals**). Locate the time interval you want to clone and click its **Duplicate** button.

The cloned time interval is displayed in the list as copy of <time interval name>.

2 Click the **Edit** button to open the Properties page and change the name.

3 Make any necessary changes to the time interval. For details, see "Defining a Time Interval" on page 225.

Deleting a Time Interval

Note: You cannot delete a time interval if it is associated with an SLA.

Select the **Time Intervals** tab (**Admin** > **Service Level Management** > **Time Intervals**). Locate the time interval you want to delete and click its **Delete** button. Answer **Yes** to the question that is displayed.

15

Outage Categories

This chapter explains how to define outage categories to be used in Service Level Management reports, to make results more meaningful.

The Outage Categories Page

You use this page to view existing outage categories and to create outage categories in addition to the default categories provided by Service Level Management.

The page includes the following components:

Name – the name of the category

Description – the description of the category

Actions – you edit an outage category by clicking the **Edit** button. For details see "Editing an Outage Category" on page 231.

New Outage Category button – to define a category, click this button. For details, see the next section.

You can sort the list by any column: An arrow next to a title shows by which column the outages are sorted, and also the direction in which the column has been sorted (that is, ascending or descending).

Note: You cannot delete an outage category.

Creating an Outage Category

You create outage categories to be used in Service Level Management reports, to make results more meaningful. For details on outage reports, see "Outage Reports" in *Using Service Level Management*.

To create an outage category:

1 Select the **Outage Categories** tab to open the Outage Categories page (**Admin** > **Service Level Management**). The page shows a list of existing categories, organized alphabetically.

For a description of this page, see "The Outage Categories Page" on page 230.

2 Click **New Outage Category** to open the Outage Category page.

3 Enter the details of the new category in the name and description fields.

4 Click **OK** to save the new category, or **Cancel** to close the window without saving the category.

When you add an outage to an SLA (during SLA creation or editing), you can choose the new category from the list.

Editing an Outage Category

You can edit outage categories, including the default categories.

To edit an outage category:

1 Select the **Outage Categories** tab to open the Outage Categories page (**Admin** > **Service Level Management**). The page shows a list of existing categories, organized alphabetically.

2 Locate the category you want to change, and click its **Edit** button.

3 In the Outage Category window, make any necessary changes.

4 Click **OK** to return to the Outage Categories page, or **Cancel** to close the window without editing the category.

16

Repositories

The Repositories tab includes data that you need when defining an SLA.

KPIs

KPIs help you to monitor your business objectives, and to track critical performance variables over time. For details on the Service Level Management KPIs, see "Service Level Management KPI Repository" in *Repositories Administration*.

Rules

Service Level Management business rules define the logic to be used when calculating measurements for a KPI. For details on the Service Level Management rules, see "Service Level Management Business Rules Repository" in *Repositories Administration*.

For details on defining a Service Level Management KPI, see "Defining an SLA: KPIs" on page 171.

Time Intervals

Service Level Management reports organize results according to time intervals. You define time intervals that span the period you want to monitor. Time intervals defined here are then available for using during the procedure for defining an SLA. For details, see Chapter 14, "Time Intervals."

Outage Categories

Outage categories are used in Service Level Management reports, to make results more meaningful. You can create outage categories in addition to the default categories provided by Service Level Management. For details, see Chapter 15, "Outage Categories."

17

Upgrading Service Level Management to Mercury Business Availability Center 6.2

This chapter describes how to upgrade service level agreements (SLAs) to work with Mercury Business Availability Center 6.2. You can upgrade SLAs, Service Level Management custom reports, and reports saved to the report repository.

Mercury Business Availability Center displays the Service Level Management Upgrade page only after all other upgrade processes have concluded. That is, before you begin the Service Level Management upgrade process, Mercury Business Availability Center has upgraded all SLAs to version 5.x.

Because of differences in architecture between Mercury Business Availability Center versions 5.x and 6.x, Service Level Management calculations may not be identical in the two versions. An SLA will probably show the same result for monitor (leaf) data, but data attached to CIs nearer the root may not be the same in both versions.

Prerequisites

This section includes issues that should be considered before beginning the upgrade procedure:

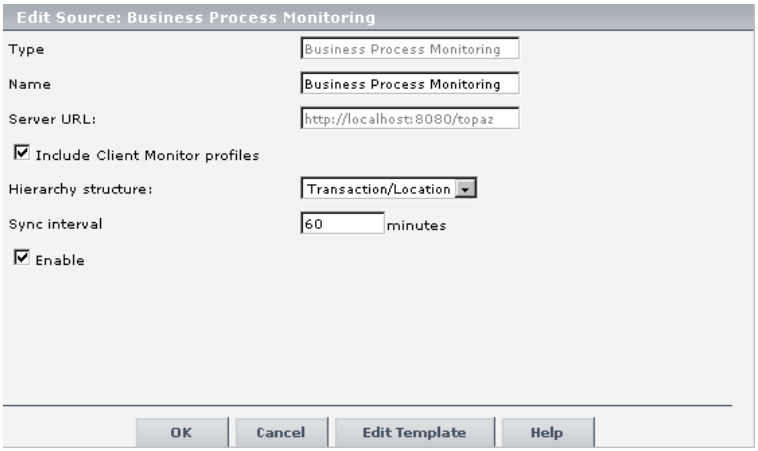
- Due to backward compatibility issues, an upgraded SLA configuration is different to the previous version. Before performing the upgrade procedure, therefore, you should save important reports to the report repository. For details, see "Saving a Report to the Report Repository" in *Working with Applications*. This step is optional.
- To verify version 5.x SLA configuration data, you can display the Service Level Panorama report to view the SLA configuration in its entirety, in report format. To access the report: **Applications** > **Service Level Management** > **Offline Reports** > **Service Level Panorama**. This step is optional.
- The version 6.x default KPI definitions for the upgrade process are stored in an XML file in the Infrastructure Settings Manager (select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Upgrade KPIs** entry in the Service Level Management – SLM Admin table). Prior to upgrade, it is recommended to view this file and make any necessary changes.
- The version 6.x default objectives are stored in an XML file in the Infrastructure Settings Manager (select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Default KPIs** entry in the Service Level Management – SLM Admin table). Prior to upgrade, it is recommended to make yourself familiar with the objective values.
- Verify that the Monitor configuration item type (CIT) has been successfully upgraded. For details, refer to *Upgrading Mercury Business Availability Center*. Verify, too, that monitors, transactions, and measurements have been successfully upgraded by viewing them in IT Universe or Monitor Administration. For details, see *Working with Monitor Administration*.
- Because you cannot roll back the custom report upgrade, before upgrading custom reports, back up the custom reports table in the database. This step is optional.

SLA Upgrade and the Business Process Monitor Adapter Source

If a 5.x transaction is filtered by location, you can avoid losing data in version 6.x SLAs by configuring the Business Process Monitor adapter source (before performing the upgrade process) so that CIs include location information.

To configure the Business Process Monitor adapter source:

1. Display the Edit Source window: **Admin** > **CMDB** > **Source Manager**.
2. Click the **Edit** button for the Business Process Monitor source adapter.
3. Select **Transaction/Location** in the Hierarchy structure field:



For details on the hierarchy structure, see "Business Process Monitor Hierarchies" in *Source Manager Administration*.

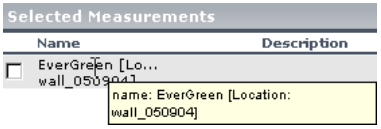
Tip: If most of the 5.x SLAs are filtered by location, set an adapter's hierarchy structure to **Transaction/Location**. If most SLAs are not filtered by location, set the hierarchy structure to **Regular**.

Example of 6.x SLA Dependent on Adapter Mode

In 5.x, an SLA may or may not include location information. The upgrade process upgrades the SLA according to:

- whether the SLA includes location information
- how the Business Process Monitor adapter source is configured

The following table shows how the upgrade process configures the 6.x SLA:

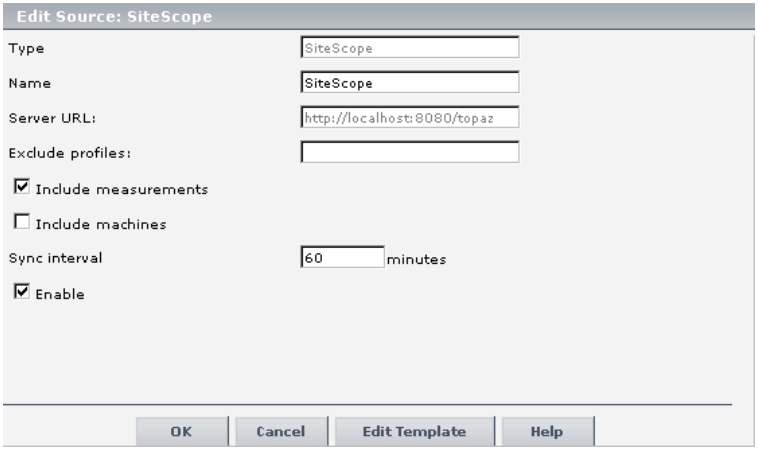
Version 5.x	**Version 6.x**	
	Business Process Monitor Adapter Source Set at Transaction/Location	**Business Process Monitor Adapter Source Set at** Regular
Transaction (EverGreen) filtered by location (wall_050904):  	EverGreen └ wall_050904 Upgrade process adds a CI of type BP Step and below it, a CI of type Transaction from Location, thereby replicating the 5.x SLA exactly.	EverGreen └ EverGreen Upgrade process does not recognize location, so adds transaction only to the SLA.
Transaction not filtered by location	EverGreen ├ wall ├ wall_05 └ wall_050904 Upgrade process adds a CI of type BP Step and below it, a CI of type Transaction from Location for all 6.2 locations.	EverGreen └ EverGreen Upgrade process replicates the 5.x SLA exactly.

SLA Upgrade and the SiteScope Adapter Source

If a 5.x monitor is filtered by monitor and measurement, you can avoid losing data in version 6.x by configuring the SiteScope source adapter (before performing the upgrade process) so that CIs include measurement performance objectives—and not only monitor objectives.

To configure the SiteScope adapter source:

1. Display the Edit Source window: **Admin** > **CMDB** > **Source Manager**.
2. Click the **Edit** button for the SiteScope source adapter.
3. Select the **Include measurements** check box in the Edit Source window:



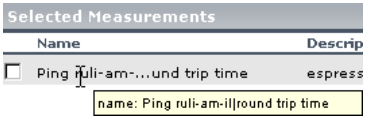
For details on editing the SiteScope source, see "SiteScope Hierarchies" in *Source Manager Administration*.

Example of 6.x SLA Dependent on Adapter Mode

In 5.x, an SLA may or may not include measurement information. The upgrade process upgrades the SLA according to:

- whether the SLA includes a SiteScope performance objective
- how the SiteScope adapter source is configured

The following table shows how the upgrade process configures the 6.x SLA:

Version 5.x	**Version 6.x**	
	SiteScope Adapter Source: Include Measurements **Check Box Selected**	**SiteScope Adapter Source:** Include Measurements **Check Box Not Selected**
Monitor (Ping ruli-am-il) filtered by measurement (round trip time):  	With measurements: Ping ruli-am-il └ round trip time Upgrade process replicates the 5.x SLA exactly.	Monitor only: Ping ruli-am-il Upgrade process adds monitor only to the SLA. **Note:** You will lose SiteScope performance objectives data for this customer.

Upgrading SLAs from 5.x to 6.2

This section explains how to upgrade service level agreements from version 5.x to 6.2 and how to delete 5.x SLAs.

The SLA table includes the following components:

- **Name.** The name of the SLA
- **Description.** The description of the SLA
- **Status**. Shows whether the upgrade process has run

You can sort the list by name, description, or status: An arrow next to a title shows by which column the SLAs are sorted, and also the direction in which the column has been sorted (that is, ascending or descending).

Actions – These buttons show the actions that you can perform on the SLA: **Simulate**, **Upgrade**, **Roll Back**, and **View Log**.

To upgrade version 5.x SLAs to version 6.2:

1. Select **Admin** > **Platform** > **Setup and Maintenance** and click the **Service Level Management Upgrade** link to open the upgrade page. The page shows a list of SLAs that are not compatible with version 6.2, organized alphabetically.
2. Locate the SLA you want to upgrade.

Note: If the SLA has the same name as a version 6.2 SLA, Service Level Management does not perform the upgrade process. You must change the name of either of the SLAs.

---

3. To view upgrade results and identify configuration changes, click **Simulate**. This step is optional but highly recommended.

   Service Level Management displays the Upgrade Warnings window. Read through the warnings. You can copy the information in this window to a text editor by copying and pasting.

   During simulation, Service Level Management updates all components of an SLA apart from its associations with KPIs and objectives.
4. If you are satisfied with the results, return to the upgrade page and click **Upgrade**. The SLA's status changes to **Upgraded** and the **Upgrade** button changes to **Roll Back**.

   At the end of the upgrade process, the Upgrade Warning window is displayed again. The first message informs you that the SLA has been upgraded successfully. The other messages are intended to help you decide whether you want to change the SLA in version 6.2 or to accept the upgraded version. Click **OK** to return to the Upgrade page.
5. To review the changes to the upgraded SLA in the Service Level Agreements page, click **Review 6.2 Configuration**. The SLA is now displayed in the list of SLAs that are compatible with version 6.2. For details on this page, see "The Service Level Agreements Page" in *Application Administration*.

Note:

- An upgraded 6.2 SLA is not identical with the original 5.x version.
- It is highly recommended to use the SLA Wizard to check the SLA, make changes to the SLA (if necessary), and save it. For details, see "SLA Definition Workflow" in *Application Administration*.

  When checking an SLA, pay special attention to the default objectives, especially if they are replacing 5.x services and groups (in the cases where the 5.x SLA does not include overall objectives).
- You must start the SLA (that is, click the **Start** button) for Service Level Management to calculate the SLA. Service Level Management calculates the SLA for the past three months only.

---

6 Click **View Log** to view a chronological account of the upgrade process and the warning messages.

Logs are saved to the Data Processing Server.

7 Continue to upgrade the SLAs. Repeat steps 2 to 5 for each SLA.

To upgrade or roll back several SLAs simultaneously:

Note: This procedure is not recommended as it slows down performance and creates many warning notifications.

---

1 Select the check boxes of the SLAs you want to upgrade or roll back.

2 Click the **Upgrade** or **Roll Back** button below the list of SLAs.

3 Continue with the upgrade process, as described in the previous section.

The next step is to upgrade the custom reports. For details, see "Upgrading Custom Reports" on page 243.

To delete version 5.x SLAs:

You can upgrade custom reports to version 6.2 only after you have upgraded all 5.x SLAs. If there are SLAs that you do not wish to upgrade (for example, because they are no longer relevant to your system), you must delete them.

1. Select the check boxes of the SLAs you want to delete.
2. Click the **Delete** button below the list of SLAs.

Upgrading Custom Reports

You can upgrade Service Level Management custom reports only when all SLAs have been upgraded.

Important: You cannot roll back custom reports. Before performing the upgrade, verify that you are satisfied with the upgraded SLAs. You can also back up the custom report tables before upgrading the SLAs.

To upgrade custom reports:

- Click **Upgrade** to update existing Service Level Management custom reports.
- Click **Review 6.2 Configuration** to access the list of custom reports.

Version 5.x Reports	Version 6.2 Report
Executive Scorecard	SLAs Summary
Availability Snapshot Performance Snapshot	SLAs Summary – only WeekToDate time range is saved, with a Day granularity
Service Status	CI Status – only the service is saved to this version
Availability Over Time vs. SLA	CIs Over Time vs. Target

Version 5.x Reports	Version 6.2 Report
Time Range Comparison	Time Range Comparison – only the service is saved to this version
Service Outages	Outages Summary – only the service is saved to this version. All outage categories are displayed.

➤ There is no Availability by Location/Group report. To produce a similar report, you must create an SLA to which you assign CIs for specific locations or groups.

Upgrading the Report Repository

Note: You can upgrade the Service Level Management report repository without upgrading the SLAs or custom reports.

➤ Click **Upgrade** to update the Service Level Management reports saved to the report repository.

➤ Click **Review 6.2 Configuration** to access the Report Repository page.

Upgrading Rules Used For SLA Conversions

Service Level Management uses a very complex algorithm to map SLAs from previous versions to version 6.2. However, due to backward compatibility issues (deriving from a difference in hierarchical structure), an upgraded 6.2 SLA is not identical with the 5.x SLA. The reasons for these differences are listed in this section.

Note: Transactions, measurements, and external data are collectively called data sources in this section.

For a note on the meaning of default objectives, see "Prerequisites" on page 236.

This section includes the following topics:

SLA Structure Issues

- The upgraded SLA structure depends on the source adapter's hierarchy structure. For details, see "Business Process Source Parameters" in *Source Manager Administration*.
- The start date is set to three months prior to the date on which the SLA is upgraded. The end date is set at a year ahead of the upgrade date.

- For a previous version's SLA groups and services, the upgrade process creates a CI for each group and service (to preserve the SLA's structure).
- Any groups or services that do not have data sources are discarded.
- For a CI created from an SLA group, SLA, or service, the upgrade process gives default objectives to the CI. For SLA groups, however, if an overall objective was set in 5.x, the CI is given the 5.x overall objective and not the default objective.

Data Source and Objective Issues

- If a group includes data sources other than Business Process Monitor and SiteScope sources (that is, Real User Monitor data or external data), the data sources are discarded and are not included in the SLA.
- Previously, a data source was filtered by location. The upgrade process adds a CI of type BP Step to the SLA for each data source. Under this CI, the upgrade process adds a CI of type BP Transaction from Location for each previously-existing location.

  If a 5.x transaction was not filtered by location and, before running the upgrade process, you set the adapter to a Transaction/Location hierarchy structure (for details, see "Prerequisites" on page 236), the upgrade process assigns each existing location to a transaction (with a CI of type BP Transaction from Location). This means that each SLA includes more information.

  If the original SLA did not have a node equivalent to the CI of type BP Step and no objectives were defined for the SLA, the upgrade process assigns default objectives for the new CIs. For details on the default KPI definitions for the upgrade process, see "Prerequisites" on page 236.
- If a data source appears more than once in the original SLA, the upgrade process maps all instances of the data source to only one CI. The upgrade process selects the first occurrence of a KPI or objective. Furthermore, identical data sources running on the same location are also mapped to one CI and here, too, the first occurrence of a KPI or objective is selected.

To retain the original 5.x data, use one of the following options:

a Create an SLA (in version 6.2) for each service.

For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Create two SLAs, SLA 1 for Service 1 and SLA 2 for Service 2. Assign an objective of 99% to SLA 1 and an objective of 97% to SLA 2.

Tip: Clone the SLA, creating the same number of SLAs as there are services. Change each SLA according to one of the services. For details, see "Cloning an SLA" in *Application Administration*.

---

b Configure the upgraded SLA so that it includes more than the Exceeded and Failed targets (for details, see "Defining an SLA: Properties" in *Application Administration*). Define an objective and set its 5.x higher value to the higher target and the lower value to the lower target.

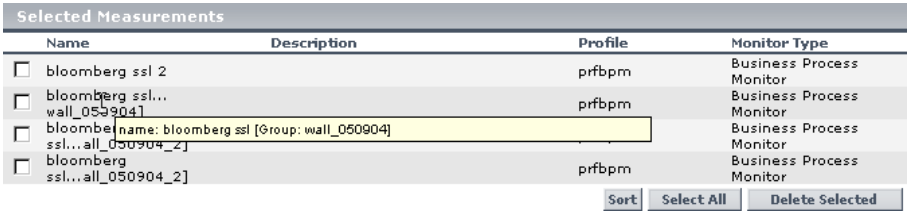
For example, a 5.x SLA includes one transaction and two services: Transaction A had an objective of 99% in Service 1, and 97% in Service 2. Set the objectives for the 6.2 SLA so that Exceeded has an objective of 99% and Met has an objective of 97%.

- If an SLA previously included a service without any data sources, the upgrade process removes the service from the SLA's hierarchy.
- If an SLA previously included a service with data sources filtered by one or more locations, the upgrade process adds a CI of type BP Step to the SLA for each location.
- If an SLA did not previously include a performance percentile objective, the upgrade process cannot add a Six Sigma performance objective to the SLA, and the objective is discarded.

  To support the Performance Six Sigma metric in version 6.2, the following objectives must have been defined for an SLA in version 5.x: percentile performance objectives and Six Sigma performance objectives.
- If the upgrade process cannot locate a Business Process Monitor or SiteScope monitor in version 6.2 that existed in version 5.x, the monitor is not added to the SLA.

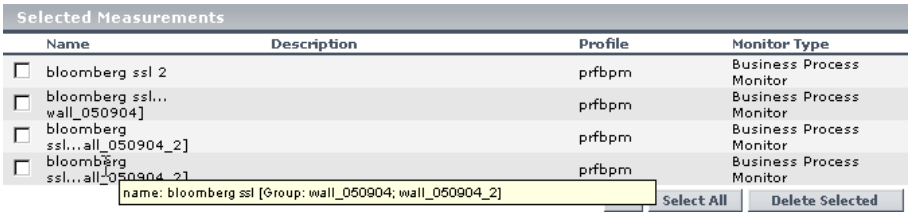
- If the upgrade process cannot locate a Business Process Monitor transaction or a SiteScope measurement in version 6.2 that existed in version 5.x, the measurement is not added to the SLA.
- Before the upgrade process, if an adapter was not configured to support CIs per measurement, the upgrade process cannot upgrade the overall performance objectives for the SLA's groups.
- The definition of a data source in version 5.x is not the same as in 6.2: a data source in version 5.x can receive data from any location, whereas a data source in version 6.2 can receive data only from locations already defined in version 6.2.
- You cannot automatically filter Business Process Monitor transactions by group. This is because groups are not included in the IT Universe. You can, however, manually define a new configuration item (CI) with dedicated selectors and associate it with the SLA.
- If a data source was previously filtered by BPM group (that do not exist in version 6.2), the upgrade process removes the group filter from the SLA for that data source. Following the upgrade, the SLA includes only one instance of the data source which does not include any group filter. Also, the SLA's objective is taken from the first occurrence found by the upgrade process.

  Example 1: a 5.x SLA contains two measurements, bloomberg ssl filtered on group wall_050409 and bloomberg ssl filtered on group wall_050409_2:



  The upgrade process creates an SLA with CI bloomberg ssl.

Example 2: a 5.x SLA contains a measurement, bloomberg ssl, filtered on two groups, wall_050904 and wall_050904_2:



The upgrade process creates an SLA with a CI named bloomberg ssl.

- Outlier trimming is not supported. Trimming is supported.

  Previously, in version 5.x, you could import outlier thresholds from the transaction threshold configuration in Monitor Administration. In version 6.2, the outlier trimming setting is no longer supported. Trimming is now calculated by the trimming condition rule parameter.

Downtime and Other Event Issues

- If an event's end date has expired (that is, the end date falls before the 6.2 SLA's start date), the upgrade process discards the event.
- Downtime granularity was changed to 5 minutes in version 6.0. Following upgrade, you should check downtime durations.

  During upgrade, event start times are rounded downwards and end times are rounded upwards. For example, the period 12:37 to 13:31 becomes 12:35 to 13:35.
- If an event is defined on a BPM group, the upgrade process discards the event (because BPM groups no longer exist in version 6.2).
- The **All SLAs** downtime value is replicated for each SLA during the upgrade process; the event receives the original name and the SLA name.
- For event CIs of type BP Group Location, the upgrade process discards the event, due to a backward compatibility issue.
- If an event's name already exists in version 6.2, the upgrade process changes the current event name by appending the SLA name in brackets to the event name.

- If an event's CI of type BP Step is not found, the upgrade process discards the event.
- If an event's CI of type BP Location is not found, the upgrade process discards the event.
- If an event's CI of type BP Transaction from Location is not found, the upgrade process discards the event.

Service Level Management Report Issues

- The following reports take a different format in version 6.2:

Version 5.x Reports	Version 6.2 Report
Executive Scorecard Availability Snapshot Performance Snapshot	SLAs Summary
Service Status	CI Status
Availability Over Time vs. SLA	CIs Over Time vs. Target
Time Range Comparison	Time Range Comparison
Service Outages	Outages Summary

- There is no Availability by Location/Group report. To produce a similar report, you must create an SLA to which you assign CIs for specific locations or groups.
- Report customizations are not upgraded.
- When upgrading custom reports, the upgrade process substitutes the SLA's creator name with the name of the user who upgraded the SLA.
- If the upgrade process does not succeed in upgrading one component of a custom report, you should use the Custom Report Manager to delete the component.
- The upgrade process calculates to-date reports till yesterday midnight.
- The upgrade process cannot upgrade reports that include active filters.

- The upgrade process can upgrade reports for predefined tracking periods only. For example, the process will not upgrade a report which includes a single value for the last three days.
- The upgrade process assigns calendar tracking periods only to reports. The minimum tracking period granularity is one hour.
- Version 6.2 does not support Service Level Management Scheduled reports produced in previous versions. That is, the reports are not upgraded.
- The upgrade process cannot assign headers or footers from version 5.x SLAs to version 6.2 SLAs Service Level Management reports. However, if the header and footer are part of a custom report, they are upgraded. You define headers and footers for reports in the Infrastructure Settings Manager. For details, see "Customizing Reports" in *Platform Administration*.
- The upgrade process stores reports in the report repository in .pdf format only.

Time Interval Issues

- Time intervals can no longer be associated with a specific SLA, but are now global functions.
- If no objectives were associated with a time interval in version 5.x, the time interval is not added to the version 6.2 SLA.
- Time intervals no longer include calculation metrics, which are now incorporated in a KPI's business rule. Therefore, you cannot now define different metrics for a CI's time intervals (for example, you cannot define an average performance metric for the 24x7 time interval, and a percentile performance metric for Business Hours).
- For version 6.2, each time interval is unique and includes a specific schedule. Previously, it was possible to define different schedules for a time interval, depending on the SLA with which the time interval was associated. During the upgrade process, only one time interval with one schedule is created, based on the time interval name. All SLAs that were associated with the previous time interval (no matter which schedule was chosen for each SLA) are now associated with the new time interval. Check each SLA; if the schedule is not suitable, create a time interval and associate it with the SLA.

Time Zone Issues

➤ If a version 5.x time zone is not supported in version 6.2, the upgrade process assigns to the SLA the first occurrence of a time zone with the same time difference as the 5.x time zone.

Day of the Week Issues

➤ During upgrade, if the first day of the week has not been defined for the same day in versions 5.x and 6.2, you are asked to choose which definition to use as a default.

Notes

➤ Any changes you make to running 6.2 SLAs (configuration changes, time interval changes, or downtime event changes) do not affect the SLA retroactively, unless the changes are made before you start the SLA. To update the SLA for previous tracking periods, you must recalculate the data. For details, see "Recalculation" in *Application Administration*.

➤ Service Level Management can recalculate SLAs for the past three months only. (This parameter is configurable in the Infrastructure Settings Manager. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Recalculation period limit** entry in the Service Level Management – SLM Admin table.)

➤ The upgrade process can fail if one of the following is exceeded: the CMDB object quota, the active TQL quota, the number of views.

Upgrade Messages

The following table includes the messages that Service Level Management displays following the successful upgrade of an SLA. The message order in this table is the same as in the Service Level Management application.

Message	Description
SLA end date is set to (<value>).	The start date is set to three months prior to the date on which the SLA is upgraded. The end date is set at a year ahead of the upgrade date. **Note:** The start date is configurable. For details, see the explanation in "Notes" on page 252.
Time zone <value> is not supported in 6.2. Assigning SLA to <value> time zone instead.	If a version 5.x time zone is not supported in version 6.2, the upgrade process assigns to the SLA the first occurrence of a time zone with the same time difference as the 5.x time zone.
SLA Owner name not found (User ID: <value>).	If a version 5.x does not include a user ID, the SLA owner name is ignored.
Time Interval (<value>) already exists. Associating it with the SLA. Verify that its scheduling matches.	For version 6.2, each time interval is unique and includes a specific schedule. Previously, it was possible to define different schedules for a time interval, depending on the SLA with which the time interval was associated. During the upgrade process, only one time interval with one schedule is created, based on the time interval name. All SLAs that were associated with the previous time interval (no matter which schedule was chosen for each SLA) are now associated with the new time interval. Check each SLA; if the schedule is not suitable, create a time interval and associate it with the SLA.
Time Interval (<value>) has no objectives in 5.x, and therefore is not added to the 6.2 SLA.	If no objectives were associated with a time interval in version 5.x, the time interval is not added to the version 6.2 SLA.
Service (<value>) had no data sources, removed from SLA's hierarchy.	If an SLA previously included a service without any data sources, the upgrade process removes the service from the SLA's hierarchy.

Message	Description
Group (<value>) contains Data Sources of type other than BPM and SiS. Those Data Sources are discarded.	The upgrade process upgrades Business Process Monitor and SiteScope data sources only. Other data sources, such as Real User Monitor and custom classes, are discarded.
Service Data Source (<value>) is filtered by several locations. Adding CI for each of the locations.	Previously, a data source was filtered by location. The upgrade process adds a CI of type BP Step to the SLA for each data source. Under this CI, the upgrade process adds a CI of type BP Transaction from Location for each previously-existing location. If the original SLA did not have a node equivalent to the CI of type BP Step and no objectives were defined for the SLA, the upgrade process assigns default objectives for the new CIs.
Service Data Source (<value>) is filtered by single location. Adding CI the location.	

Message	Description
Service Data Source (<value>) ingredients already appears in the SLA. Please note that the objectives were already upgraded.	If a data source appears more than once in the original SLA, the upgrade process maps all instances of the data source to only one CI. The upgrade process selects the first occurrence of a KPI or objective. Furthermore, identical data sources running on the same location are also mapped to one CI and here, too, the first occurrence of a KPI or objective is selected. **To retain the original 5.x data, use one of the following options:** ➤ Create an SLA (in version 6.2) for each service. For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Create two SLAs, SLA 1 for Service 1 and SLA 2 for Service 2. Assign an objective of 99% to SLA 1 and 97% to SLA 2. **Tip:** Clone the SLA, creating the same number of SLAs as there are services. Change each SLA according to one of the services. For details, see "Cloning an SLA" in *Application Administration*. ➤ Configure the upgraded SLA so that it includes more than the Exceeded and Failed targets (for details, see "Defining an SLA: Properties" in *Application Administration*). Define an objective and set its 5.x higher value to the higher target and the lower value to the lower target. For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Set the objectives for the 6.2 SLA so that Exceeded has an objective of 99% and Met has an objective of 97%.
Service Data Source (<value>) ingredients do not appear in 6.2, and therefore the data source is not added.	If the data source does not exist in the CMDB, the data source is not added to the 6.2 SLA.
Service Data Source (<value>) is filtered by Group(s). Adding CI for each of the locations.	If an SLA was previously filtered by BPM groups (that do not exist in version 6.2), the upgrade process adds a CI of type BP Step with a child for each location.

Message	Description
Service Data Source (<value>) is filtered by Location(s), but the model does not support by-location CIs.	If a 5.x SLA includes transactions filtered by one or more locations and the hierarchy structure is set to Regular, the upgrade process adds a CI of type BP Step to the SLA without any children. To include locations in the SLA, you must change the hierarchy structure. For details, see "SLA Upgrade and the Business Process Monitor Adapter Source" on page 237.
Service Data Source (<value>) is not filtered, but the model supports by-location CIs.	If a 5.x SLA includes transactions not filtered by location and the hierarchy structure is set to Transaction/Location, the upgrade process assigns all 6.2 locations to a transaction (with a CI of type BP Transaction from Location). Following the upgrade process, when you check the SLA, you can remove the unwanted locations. **Note:** Do not remove all locations from the transaction, otherwise the data is disabled. You must leave at least one location (as a data source) in the SLA.
Performance 6-Sigma Objective cannot be defined for group (<value>), because no performance objective defined.	If an SLA did not previously include an overall performance percentile objective, the upgrade process cannot add a Six Sigma performance objective to the SLA, and the objective is discarded. To support the Performance Six Sigma metric in version 6.2, the following objectives must have been defined for an SLA in version 5.x: percentile performance objectives and Six Sigma performance objectives.
The SiteScope monitor was not found in version 6.2 for the measurement (<value>).	If the upgrade process cannot locate a SiteScope monitor in version 6.2 that existed in version 5.x, the monitor is not added to the SLA. For a note on other reasons for a missing object, see "Prerequisites" on page 236.
The SiteScope measurement was not found in version 6.2 for the version 5.1 measurement (<value>).	If the upgrade process cannot locate a SiteScope measurement in version 6.2 that existed in version 5.x, the measurement is not added to the SLA.

Message	Description
SiteScope has not been configured to support by-measurement CIs, so performance objectives cannot be upgraded for measurement (<value>).	If performance objectives have been defined for a version 5.x SLA that includes a service with System class (SiteScope) measurements, you can avoid losing the measurement data in version 6.2. Configure the SiteScope source adapter so that the upgrade process upgrades measurement performance objectives—and not only monitor objectives. This must be done before performing the upgrade process. For details, see "SLA Upgrade and the SiteScope Adapter Source" on page 239.
SiteScope has not been configured to support by-measurement CIs, so the overall performance objective cannot be upgraded for group (<value>).	
Cannot upgrade event defined on BPM group. Event name: (<value>).	If an event is defined on a BPM group, the upgrade process discards the event (because BPM groups no longer exist in version 6.2).
Events on location from profile are not supported. Event: (<value>).	Due to backward compatibility issues, the upgrade process cannot upgrade events based on a specific profile's location.
Discarding event (<value>). Its end date has expired.	If an event's end date has expired (that is, the end date falls before the 6.2 SLA's start date), the upgrade process discards the event.
The event name (<value>) already exists. Changing name to (<value>).	If an event's name already exists in version 6.2, the upgrade process changes the current event name by appending the SLA name in brackets to the event name.
Location CI (<value>) was not found for event (<value>). Discarding this event.	If an event's location cannot be mapped to a 6.2 CI, the upgrade process discards the event. The reason that the event is not found in version 6.2 may be because the object on which the event is based no longer exists. For a note on other reasons for a missing object, see "Prerequisites" on page 236.
BP Group CI was not found for event (<value>). Discarding this event.	
BP Step CI was not found for event (<value>). Discarding this event.	
BP transaction from location CI was not found for event (<value>). Discarding this event.	

Message	Description
Changing event (<value>) scheduling. Previous scheduling: start limit date <value>, event range: <value> - <value>. Upgraded scheduling: start limit date <value>, event range: <value> - <value>.	➤ Due to backward compatibility issues, the upgrade process concatenates the start limit date and hour to one value. ➤ During upgrade, event start times are rounded downwards and end times are rounded upwards. For example, the period 12:37 – 13:31 becomes 12:35 – 13:35. ➤ Downtime granularity was changed to 5 minutes in version 6.0. Following upgrade, you should check downtime duration periods.
Changing event (<value>) start limit time from <value> to <value>.	
Changing event (<value>) scheduling from <value> - <value> to <value> - <value>.	

Part III

End User Management Administration

18

End User Management Report Configuration

You use the End User Management Configuration page to configure how your reports appear in Mercury Business Availability Center. You can select the order in which transactions appear in reports, use color coding to configure the appearance of transactions, and filter out transactions, locations, and groups that you do not want appearing in your reports.

About Report Configuration

You can perform the following report configuration tasks:

- You specify the order in which you want transactions that are part of a specific profile to appear in performance data reports (for details, see "Modifying Transaction Order" on page 262).
- You specify the color used to represent a transaction in reports (for details, see "Transaction Coloring" on page 262).
- You specify which transactions, locations, and/or groups to exclude from all Mercury Business Availability Center reports (for details, see "Report Filters" on page 263).

Modifying Transaction Order

You configure the transaction order for End User Management reports from End User Management Administration.

You specify the order in which you want transactions that are part of the current profile to appear in reports. You can use the links at the top of the list to sort the list by transaction name and by the appearance order within the scripts.

To modify transaction order:

1. In the **Reports** tab, select **Transaction Ordering**.
2. Select the profile whose transactions you want to order in the **Select profile** list.
3. Select a transaction in the list, and use the arrows to the right of the list to move it up or down.

   Click **Sort by name** or **Revert to original order** to sort the list by either of those criteria.
4. Click **Save** to save the settings.

Transaction Coloring

You configure transaction coloring for End User Management reports from End User Management Administration.

You can modify the color used to represent a transaction in reports.

To assign a different color to a transaction for display in reports:

1. In the Reports tab, select **Transaction Coloring**.
2. Select the profile containing the transactions whose color you want to modify in the **Select profile** list.
3. Click the color picker button, select the required color or type its hex value, and click **OK**.
4. Click **Save** to save the settings.

Report Filters

You configure filters for End User Management reports in End User Management Administration.

Report filters enable you to exclude specific transactions, locations, and/or groups from all reports for the current and future profile sessions. You configure report filters per profile.

Individual users can configure report filters only for themselves. Administrators can configure global report filters that affect all users. Any transaction, location, or group that is filtered out using the global-level report filter is unavailable at the user level (and appears disabled on the Report Filters page). For details on specifying global-level report filters, see "Configuring Report Filters Globally" in *Platform Administration*.

To configure user-level report filters:

1. In the Reports tab, select **Report Filters**.
2. Select the profile whose report filters you want to modify in the **Select profile** list.
3. Select the check box beside the transaction(s), location(s), and/or group(s) you want to exclude from reports.

Tip: To prevent old or obsolete transactions from appearing in reports, use the transaction filter.

---

4. Clear the relevant check box to display an excluded transaction, location and/or group.
5. Click **Save** to save the settings.

   Filtered values still appear in user-defined (custom and trend) reports that were created before configuring the filter. To remove newly filtered values from existing user-defined reports, you must remove and re-add the components containing the elements for which filters have been set, and save the report.

Part IV

Administering the SAP Solution

19

Deploying the SAP Solution

This chapter describes how to deploy Mercury Business Availability Center SAP solution.

SAP Solution Deployment Workflow

To work with the SAP solution you must use the following workflow:

Check	To do
	Pre-requisites. Ensure that the following software is installed before you install the SAP solution:
	➤ **Mercury Application Mapping.** Required, if you are using the Shared CMDB feature. The Shared CMDB feature provides more functionality for monitoring changes and other capabilities – For details about installing Mercury Application Mapping, see *Mercury Application Mapping Installation Guide*. For details about the Shared CMDB feature, see "Sharing the Mercury Universal CMDB Environment" in *Working with the CMDB*.
	➤ **Discovery Probe.** For details, see *Discovery Manager Administration*.
	➤ **SiteScope 8.1.2 or later.** For details, see *SiteScope Administration*.
	➤ **Business Process Monitor 5.1 or later.** For details, see *Business Process Monitor Admin*.
	➤ **Shared CMDB.** If required, install Shared CMDB. For details, refer to *Mercury Application Mapping Installation Guide*.
	Install the SAP solution. For details, see "Deploying the SAP Solution" on page 267.
	Perform Discovery. For details, see "Running SAP Discovery" on page 279.
	Create a Business Process Monitor profile. For details, see "Using a Business Process Monitor Profile to Simulate SAP Users" on page 321.
	Create monitors. For details, see "Step 7 – Creating General Monitors" on page 275.
	Perform the Shared CMDB workaround when you are using the Shared CMDB feature. For details, see "Step 8 – Shared CMDB Workaround" on page 275.

The SAP solution is ready. Once all these steps are completed, you can view SAP data in the Dashboard, view the impact of changes, and so forth.

Deploying the SAP Solution

Note:

- The following procedure assumes that Mercury Business Availability Center 6.2, SiteScope 8.1.2 or 8.2, Business Process Monitor 5.1 or 6.1, and if necessary, Mercury Application Mapping 6.2, are already installed.
- Mercury Application Mapping and Mercury Business Availability Center must not reside on the same machine.
- An existing Business Process Monitor machine can be leveraged for running SAP scripts as well.

Deploying the SAP solution includes the following steps:

Step 1 – Setting the License for the SAP Solution

When setting the SAP solution license, verify that the license also contains the Auto Discovery license (customers with the SAP solution license also receive the Auto Discovery license).

If the SAP solution license was set while installing Mercury Business Availability Center, then the SAP packages are automatically deployed and added to the CMDB.

If the SAP solution license was set after installing Mercury Business Availability Center, you must deploy the packages manually or restart Mercury Business Availability Center so the SAP packages are deployed automatically (this is the recommended procedure).

To check that the SAP packages have been deployed:

Note: The SAP-related packages: **SAP.zip**, **SAP_discovery.zip**, and **SAP_monitoring.zip** are at the following location on the machine where CMDB is installed:
<Mercury_Business_Availability_Center_root_directory>\mam_lib\packages

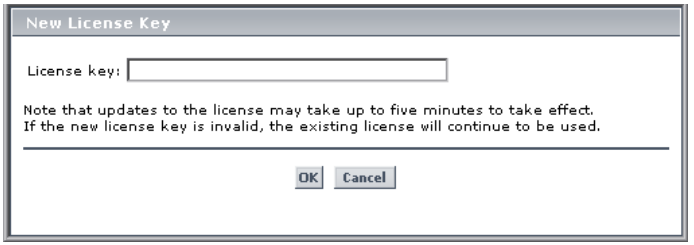
---

To check that the packages are deployed, select **Admin** > **CMDB**, click the IT Universe tab and check that the SAP_Systems view is listed in the View list in View Explorer.

To set the license for the SAP solution:

1. Log in to Mercury Business Availability Center.
2. Choose **Admin** > **Platform** > **Setup and Maintenance**.
3. Select **License Management**.

4 Click **New License Key** to open the New License Key page.



5 Enter a valid license key in the **License key** box.

The license key includes the SAP solution.

6 Click **OK** to save the change.

7 Verify that the value of **Business Availability Center for SAP** in the **Applications** area is now **Licensed**.

8 It is recommended to restart Mercury Business Availability Center at this point.

Step 2 – Performing the SiteScope Post-Installation Procedure

Once SiteScope 8.1.2 or 8.2 is installed, install SAP Java connector on the SiteScope machine and set the appropriate license.

To install the SAP Java connector (JCo) on the SiteScope machine:

1 Download the SAP JCo package from the Tools & Services window of SAP JCo in SAP Service Marketplace:

https://websmp101.sap-ag.de/~form/sapnet?_SHORTKEY=01100035870000463649

2 Extract **sapjco-ntintel-2.0.8.zip** to a temporary directory (for example: C:\temp) on the SiteScope machine.

3 Copy **sapjco.jar** from the temporary directory to the **<SiteScope_root_directory>\SiteScope\WEB-INF\lib** directory on the SiteScope machine.

4 Copy **sapjcorfc.dll** from the temporary directory to the **<SiteScope_root_directory>\SiteScope\bin** directory on the SiteScope machine.

5 Copy **librfc32.dll** from the temporary directory, in the SiteScope machine to:

- the **%winnt%\system32** directory
- the **<SiteScope_root_directory>\SiteScope\bin** directory

If there is an old version of the **librfc32.dll** file already in the **<SiteScope_root_directory>\bin** or in the **%winnt%\system32** directory, you should replace it.

6 Restart SiteScope as follows: on the SiteScope machine, go to **Start** > **Programs** > **Administration Tools** > **Services**, find SiteScope service and restart it.

To set the appropriate license:

1 Launch SiteScope by entering the following URL in a browser: **http://<SiS_machine_name>:8080**

2 Choose **Preferences** > **General Preferences**.

3 Click **Edit**.

4 Click **Insert valid license keys**.

5 In the **License Number** box, enter a valid SiteScope license key.

6 In the **Option Licenses** box, enter the SiteScope license keys appropriate for the SAP solution.

Make sure to insert a license for: EMS monitors, SAP monitors, and the SAP R/3 solution template.

7 Click **OK** to approve the changes.

Step 3 – Performing the Discovery Probe Post-Installation Procedure

After installing the Discovery Probe, perform the post-installation procedure (see below) and restart the Discovery Probe. If the Discovery Probe is already running before you perform the post-installation procedure, stop it and restart it afterwards.

To perform the Discovery Probe post-installation procedure:

1. Download the SAP JCo package from the Tools & Services window of SAP JCo in SAP Service Marketplace:

   https://websmp101.sap-ag.de/~form/sapnet?_SHORTKEY=01100035870000463649

2. Extract **sapjco-ntintel-2.0.8.zip** to a temporary directory (for example: C:\temp) on the Mercury Business Availability Center machine.

3. Create a new **sap** directory (in lowercase) in the **<Mercury Business Availability Center home directory>\DiscoveryProbe\root\ext** directory on the machine where the Discovery Probe is installed.

4. Copy **sapjco.jar** from the temporary directory to the **<Mercury Business Availability Center home directory>\DiscoveryProbe\root\ext\sap** directory on the machine where the Discovery Probe is installed.

5. Copy **sapjcorfc.dll** from the temporary directory to the **<Mercury Business Availability Center home directory>\DiscoveryProbe\root\ext\sap** directory on the machine where the Discovery Probe is installed.

6. Copy **librfc32.dll** from the temporary directory to the **%winnt%\system32** directory.

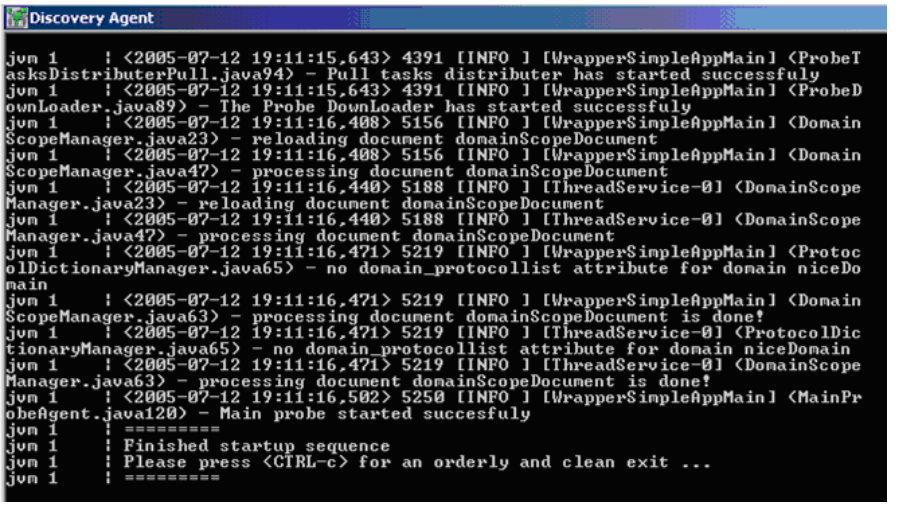
7. Verify that the **MSVCR71.dll** and **MSVCP71.dll** files are located in the **%winnt%\system32** directory.

To start the Discovery Agent:

1 On the Discovery Probe machine, access: **Start** > **Programs** > **Business Availability Center** > **Administration** > **Discovery Agent**

This starts the Discovery Probe and opens a CMD console.

2 Wait until the console displays the following lines: **Finished startup sequence**



Step 4 – Running SAP Discovery

You run SAP discovery to discover SAP elements and SAP topology – for details, see “Running SAP Discovery” on page 279.

Step 5 – Creating a Business Process Monitor Profile

To create a Business Process Monitor profile, see “Managing Business Process Profiles and Creating Client Monitor Profiles” in *End User Management Data Collector Configuration*.

Step 6 – Creating a SAP CCMS Monitor

The SAP CCMS monitor retrieves and reports measurements using SAP centralized monitoring system CCMS. CCMS is used to monitor all servers, components, and resources in the SAP R/3® System from one single centralized server facilitating problem discovery and problem diagnosis. For details, see "SAP CCMS Monitor" in *Configuring SiteScope Monitors*.

To create a SAP CCMS monitor, see "Configuring the SAP CCMS Monitor" in *Configuring SiteScope Monitors*.

SAP CCMS Monitor solution template is the most effective way to deploy a CCMS monitor – for details, see "Using SiteScope CCMS Solution Template" on page 339.

Step 7 – Creating General Monitors

You create general SiteScope monitors to get the complete picture: Database Query Monitor, Ping Monitor, and so forth – for details, see *Configuring SiteScope Monitors*.

Step 8 – Shared CMDB Workaround

Perform this step only if you plan to work with the Shared CMDB feature. In this case, you must undeploy the MAM Service package and then redeploy it.

For more details about Shared CMDB capabilities, see "Sharing the Mercury Universal CMDB Environment" in *Working with the CMDB*.

To undeploy the MAM Service package:

1 In the browser, enter **http://<Mercury_Business_Availability_Center_server_name>:8080/jmx-console/**

2 Double-click **service=Package manager** listed under **MAM**.

3 In the undeployPackage section, enter the customer Id number in the **customerId** box and **SAP_discovery.zip** in the **packageName** box, and click **Invoke**.

4 In the deployPackage section, enter the customer Id number in the **customerId** box and **SAP_discovery.zip** in the **packageName** box, and click **Invoke**.

20

Performing a SAP Discovery

This chapter describes the specific tasks involved running a SAP discovery.

Note: For details about how to perform a discovery, see "Running the Discovery Process" in *Discovery Manager Administration*.

Running SAP Discovery

The SAP discovery process enables you to discover SAP elements and SAP topology. The SAP discovery process consists of the following steps:

- "Step 1 – Installing the Java Connectors" on page 280
- "Step 2 – Preparing for a SAP Discovery" on page 280

- "Step 3 – Adding a Network CI to Trigger the Discovery of SAP System Networking" on page 284
- "Step 4 – Running the Discovery Patterns" on page 288
- "Step 5 – Checking that the Discovery Ran Correctly" on page 300
- "Step 6 – Running SAP Solution Manager Discovery" on page 301

The first step is a pre-requisite to the other steps. Steps 2 to 5 discover different SAP elements and different parts of SAP topology.

Step 1 – Installing the Java Connectors

Before you run a SAP discovery, you install the Java connectors, if you have not already done so. For details, see "Step 3 – Performing the Discovery Probe Post-Installation Procedure" on page 273.

Step 2 – Preparing for a SAP Discovery

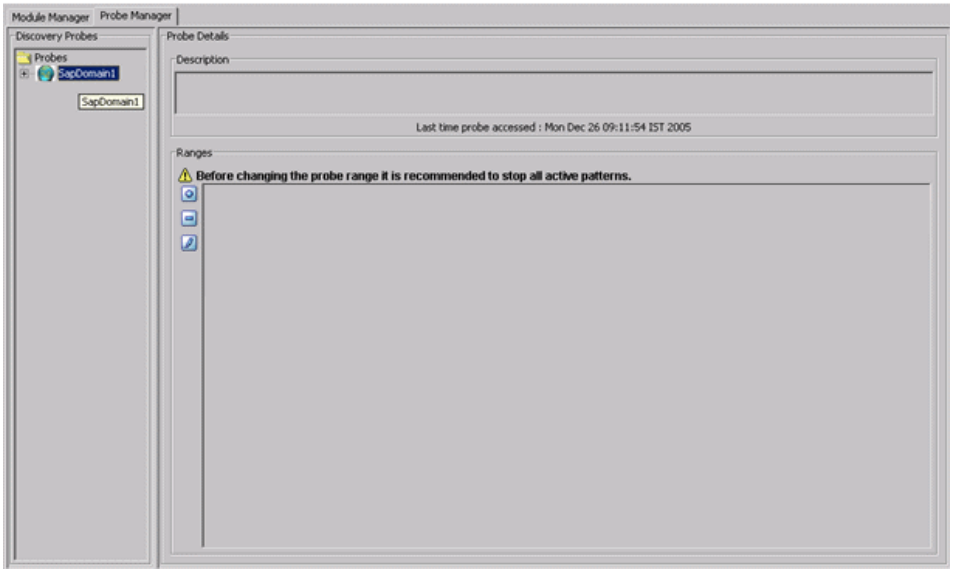
Before you run a SAP discovery, you must add a discovery probe and then define the protocols as indicated in this section.

Note: Ensure that the Discovery Probe is running.

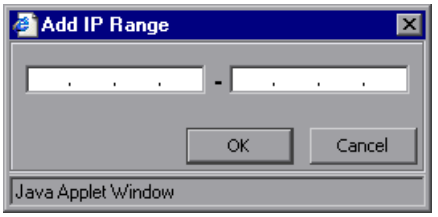
To prepare for a SAP discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the Probe Manager pane.

4 In the Discovery Probes pane, select the relevant domain.



5 Click the **Add IP Range** button to open the Add IP Range window.



6 Enter the range of IP addresses that includes the IP address of the probe you want to discover. If there is only one address, enter its value in both boxes.

7 Click **OK**.

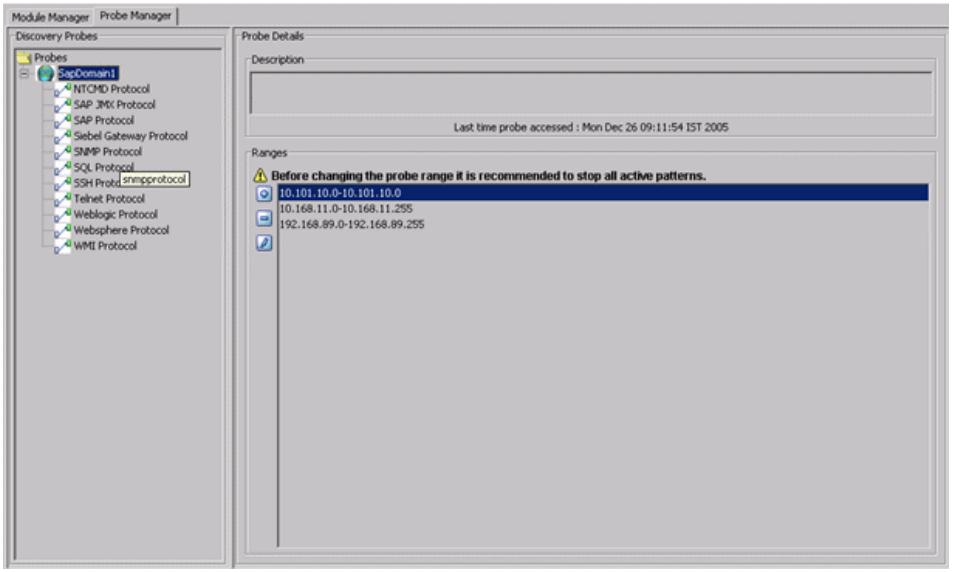
8 Click the **Add IP Range** button to open the Add Range window once more.

9 Enter the range of IP addresses that includes the IP address of the SAP system you want to discover. If there is only one address, enter its value in both boxes.

10 Click **OK**.

11 Click **Apply** to save the changes you have made.

12 Expand the domain:



13 Define the following protocols:

➤ Select **SNMP Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following field:

- **Community** – Enter the password you used when connecting to the SNMP service community you defined while configuring the SNMP service (for example, a community for read-only or read/write).

➤ Select **WMI Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:

- **NT Domain** – The name of the host where the Discovery Probe is installed.
- **User Name** – The name of the user you use to connect to the host as administrator.
- **User Password** – The password of the user you use to connect to the host as administrator.

➤ Select **NTCMD Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:

- **NT Domain** – The name of the host where the Discovery Probe is installed.
- **User Name** – The name of the user you use to connect to the host as administrator.
- **User Password** – The password of the user you use to connect to the host as administrator.

➤ Select **SAP Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:

- **SAP Client** – The default value is 800. It is recommended to use the default value.
- **SAP System Number** – The default value is 00. It is recommended to use the default value.
- **User Name** – The name of the user you use to log on to the SAP system.
- **User Password** – The password of the user you use to log on to the SAP system.

Note: If you want to discover more than one SAP System, it is recommended to create a SAP Protocol for each SAP system with different users and passwords.

---

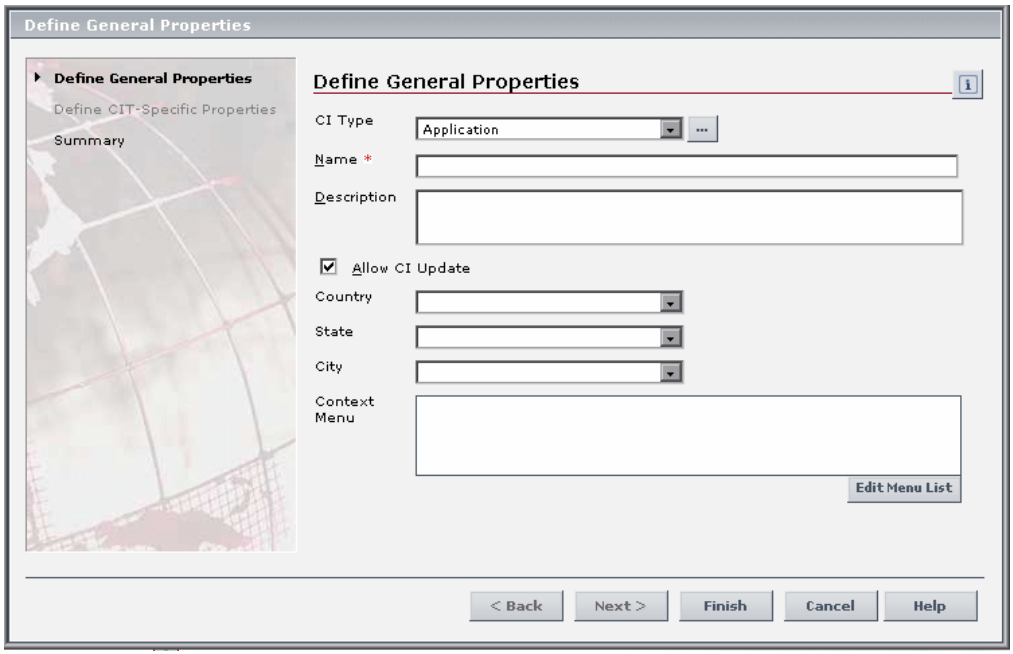
14 Click **Apply** to save the changes.

Step 3 – Adding a Network CI to Trigger the Discovery of SAP System Networking

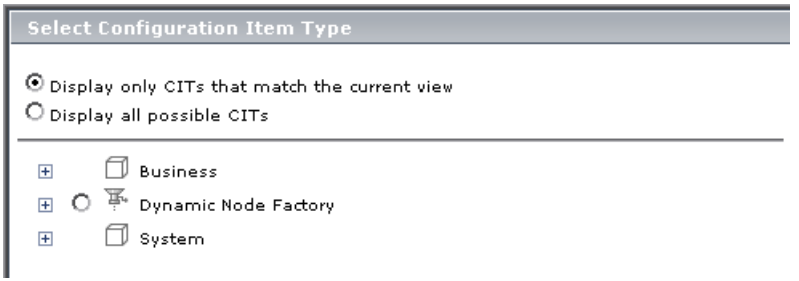
To trigger the discovery of SAP System networking features, you must add a Network CI to the CMDB.

To add a Network CI to trigger a discovery of SAP System networking:

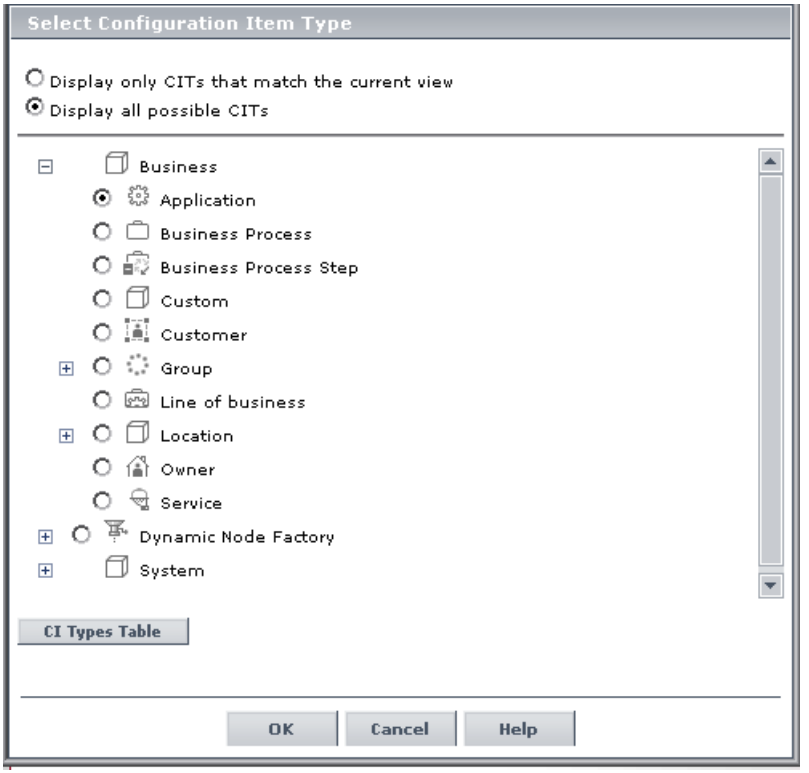
1. In Mercury Business Availability Center, select **Admin** > **CMDB**, and click the **IT Universe Manager** tab in CMDB Administration.
2. Select the **SAP Systems** view.
3. In the right pane, click **Create new CIs** under How to get started.
4. A wizard opens.



5 Click the more button to the right of the **CI Type** box, to display the full CI Type list.

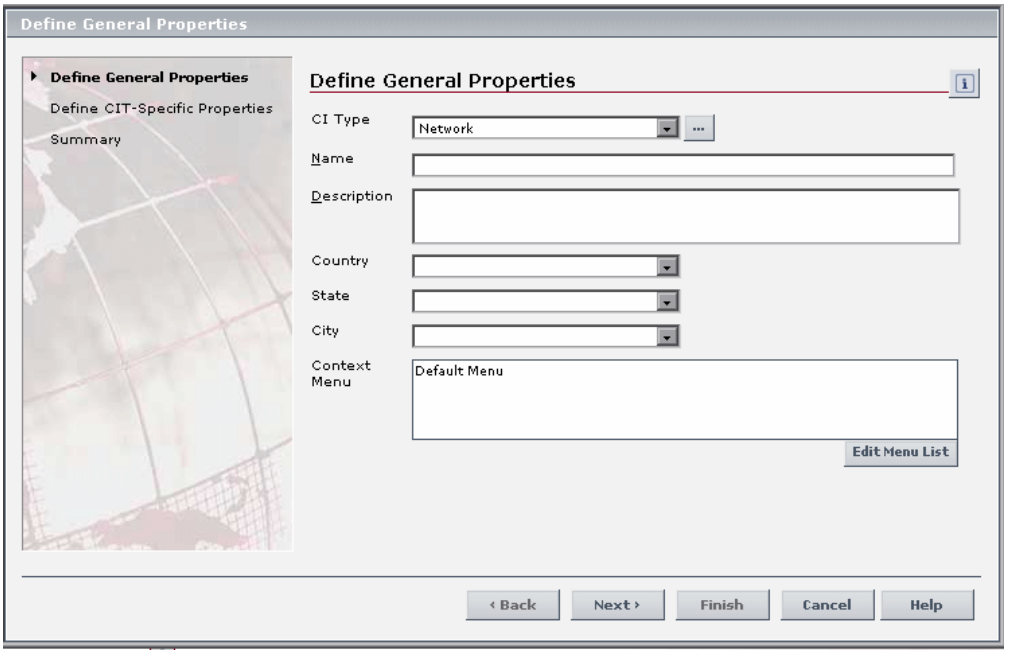


6 Select **Display all possible CITs** to display the list of all possible CITs.

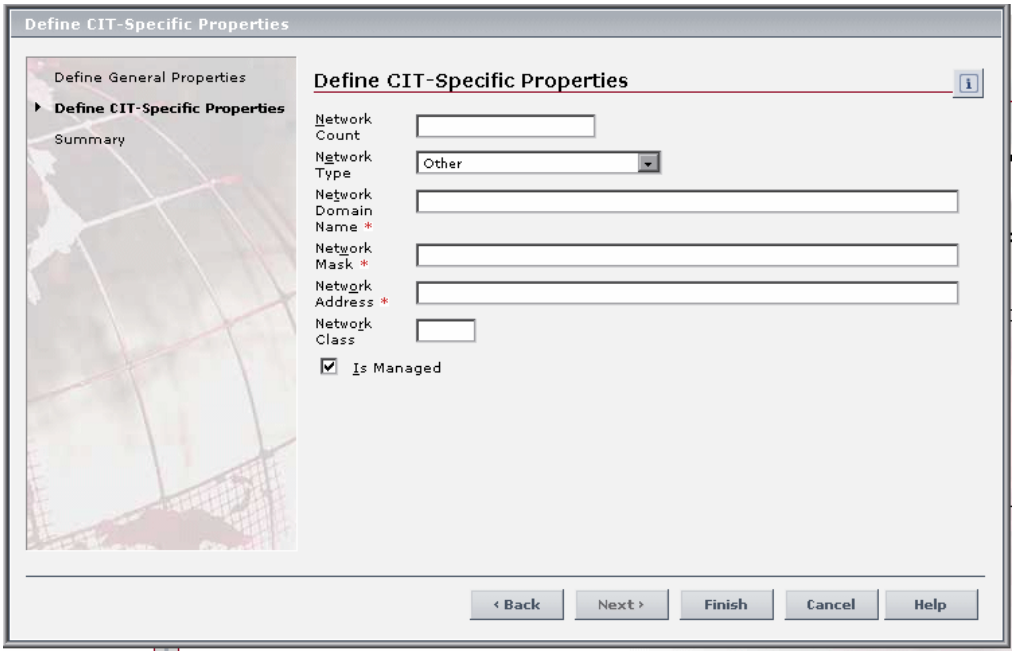


7 Expand **System** and then expand **Network Resource**.

8 Select **Network** and click **OK**. The Define General Properties page opens.



9 Click **Next**.



10 Enter the following information:

- In the **Network Domain Name** box, enter the name of the domain as it was specified during SAP installation.
- In the **Network Mask** box, enter the mask for the IP address of the SAP System network.
- In the **Network Address** box, enter the IP address of the SAP system network.

11 Click **Finish** to save the changes.

If the Network CI was added successfully, you get the following message: Network CI was added successfully.

Step 4 – Running the Discovery Patterns

To run the discovery patterns, you must trigger them in the order described in this section. Each discovery pattern discovers different components – for details on the components and their hierarchy structure, see "SAP Solution CIs" on page 303.

This section includes the following topics:

Accessing the Discovery Modules

Access the discovery modules and then run each discovery pattern in the proper order.

To access the discovery modules:

1 Click the **Discovery Manager** tab in CMDB Administration.

2 Click the **Module Manager** tab.

Note: It is very important, the first time you run discovery, to start the next pattern only after you verify that the activated pattern has successfully discovered all the required elements.

---

3 Go to the next procedure.

Running the ICMP_NET_Dis_IpC Discovery Pattern

Run the ICMP_NET_Dis_IpC discovery pattern to discover which machines are active in the range of given IP addresses.

To run the ICMP_NET_Dis_IpC discovery pattern:

1 Expand **Network - Basic** and select **ICMP_NET_Dis_IpC**. This pattern pings the machines within the IP address range that you provided in "Step 2 – Preparing for a SAP Discovery" on page 280.

2 Click the **Activate** button to start the discovery.

3 Go to the next discovery procedure.

Running the SNMP_NET_Dis_Connection Discovery Pattern

Run the SNMP_NET_Dis_Connection discovery pattern to discover, in the range of given IP addresses, the hosts that communicate using the SNMP protocol.

To run the SNMP_NET_Dis_Connection discovery pattern:

1 Expand **Network - Protocol Connections** and select **SNMP_NET_Dis_Connection**.

2 Click the **Activate** button to start the discovery.

3 Go to the next discovery procedure.

Running the NTCMD_NET_Dis_Connection Discovery Pattern

Run the NTCMD_NET_Dis_Connection discovery pattern to discover, in the range of given IP addresses, the hosts that communicate using the NTCMD protocol.

To run the NTCMD_NET_Dis_Connection discovery pattern:

1 Expand **Network - Protocol Connections** and select **NTCMD_NET_Dis_Connection**.

2 Click the **Activate** button to start the discovery.

3 Go to the next discovery procedure.

Running the WMI_NET_Dis_Connection Discovery Pattern

Run the WMI_NET_Dis_Connection discovery pattern to discover, in the range of given IP addresses, the hosts that communicate using the WMI protocol.

To run the WMI_NET_Dis_Connection discovery pattern:

1 Expand **Network - Protocol Connections** and select **WMI_NET_Dis_Connection**.

2 Click the **Activate** button to start the discovery.

3 Go to the next discovery procedure.

Running the WMI_HR_Process Discovery Pattern

Run the WMI_HR_Process discovery pattern to discover the processes that are running on the server.

If the SAP system you are discovering has an ITS configuration and you want to discover the ITS entities of the SAP system, run this pattern as a prerequisite to the SAP discovery that discovers ITS entities.

To run the WMI_HR_Process discovery pattern:

1. Expand **Host Resources - WMI** and select **WMI_HR_Process**.
2. Click the **Activate** button to start the discovery.
3. Go to the next discovery procedure.

Running the TCP_NET_Dis_Port Discovery Pattern

Run the TCP_NET_Dis_Port discovery pattern to discover the server's open active ports.

To run the TCP_NET_Dis_Port discovery pattern:

1. Expand **Network - Advanced** and select **TCP_NET_Dis_Port**.
2. Click the **Activate** button to start the discovery.
3. Go to the next discovery procedure.

Running the TCP_Webserver_Detection Discovery Pattern

Run the TCP_Webserver_Detection discovery pattern to discover the Web servers running on this host.

If the SAP system you are discovering has an ITS configuration and you want to discover the ITS entities of the SAP system, run this pattern as a pre-requisite to the SAP discovery that discovers ITS entities.

To run the TCP_Webserver_Detection discovery pattern:

1. Expand **Web Servers - Basic** and select **TCP_Webserver_Detection**.
2. Click the **Activate** button to start the discovery.
3. Go to the next discovery procedure.

Running the SAP_Dis_Site Discovery Pattern

Run the SAP_Dis_Site discovery pattern to discover infrastructure entities in the SAP System: Hosts, R/3 Application server/s, Work Processes, databases, SAP clients, Configuration files, software components (discovered as a configuration file), and support packages (discovered as a configuration file).

To run the SAP_Dis_Site discovery pattern:

1 Expand **Application - SAP (R/3)** and select **SAP_Dis_Site**.

2 Click the **Activate** button to start the discovery.

3 Go to the next discovery procedure.

Running the SAP_Dis_ITS Discovery Pattern

Run the SAP_Dis_ITS discovery pattern to discover Internet Transaction Server (ITS) entities (Application Gateway and Web Gateway).

To run the SAP_Dis_ITS discovery pattern:

1 Expand **Application - SAP (R/3)** and select **SAP_Dis_ITS**.

2 Click the **Activate** button to start the discovery.

3 Go to the next discovery procedure.

Running the SAP_Dis_Applications Discovery Pattern

Before you run the SAP_Dis_Applications discovery pattern to discover application components, SAP transactions and transports, you must set the discovery mode.

If you want to discover changed SAP transactions you must determine the appropriate range of dates (for details, see "Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery" on page 297).

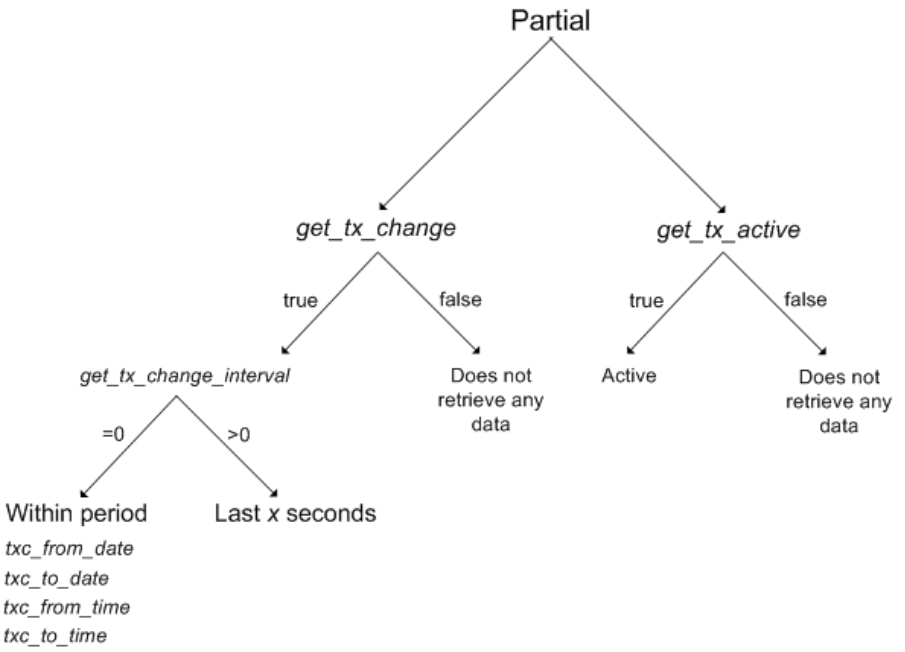
This section includes:

➤ "Discover Active and Changed SAP Transactions" on page 296

➤ "Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery" on page 297

Selecting the Discovery Modes for Discovering Application Components, SAP Transactions, and Transports

You can use the following parameter's structure to run the required discovery pattern.



Depending on the combination of parameters and their values you can discover all SAP transaction, active SAP transactions, the SAP transactions that were modified by a SAP transport, or both.

Once you have selected what you want to discover, run the appropriate discovery:

➤ "Discover Active SAP Transactions" on page 294

➤ "Discover Changed SAP Transactions" on page 295

➤ "Discover Active and Changed SAP Transactions" on page 296

Discover Active SAP Transactions

You can discover active SAP transactions.

To discover active SAP Transactions:

1. Double-click **SAP_Dis_Application** discovery pattern to open the Pattern Editor page.
2. Set **get_tx_all** to **false**.
3. Set **get_tx_active** to **true**.
4. Click **OK** to save the changes.
5. Go to the next procedure. For details, see "Running the SAP_Dis_Solution_Manager Discovery Pattern" on page 300.

Discover Changed SAP Transactions

You can discover the SAP transactions that have been changed by discovered transports.

To run changed SAP Transactions:

1. Double-click **SAP_Dis_Application** discovery pattern to open the Pattern Editor page.
2. Set **get_tx_all** to **false**.
3. Set **get_tx_active** to **false**.
4. Set **get_tx_change** to **true**.
5. Set **get_tx_change_interval** to one of the following:
   - **0** – to discover the changes to transactions in the period of time specified in the **txc_from_date, txc_from_time**, **txc_to_date,** and **txc_to_time** parameters. For details about the range to specify, see "Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery" on page 297.
   - **x** – (where x > 0) to discover the changes to transactions in the last **x** seconds
6. Click **OK** to save the changes.
7. Go to the next procedure – for details, see "Running the SAP_Dis_Solution_Manager Discovery Pattern" on page 300.

Discover Active and Changed SAP Transactions

You can discover the SAP transactions that are active and have changed since the last discovery.

To discover active and changed SAP Transactions:

1. Double-click **SAP_Dis_Application** discovery pattern to open the Pattern Editor page.
2. Set **get_tx_all** to **false**.
3. Set **get_tx_active** to **true**.
4. Set **get_tx_change** to **true**.
5. Set **get_tx_change_interval** to one of the following:
   - **0** – to discover the changes to transactions in the period of time specified in the **txc_from_date, txc_from_time**, **txc_to_date,** and **txc_to_time** parameters. For details about the range to specify, see "Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery" on page 297.
   - **x** – (where x > 0) to discover the changes to transactions in the last **x** seconds
6. Click **OK** to save the changes.
7. Go to the next procedure. For details, see "Running the SAP_Dis_Solution_Manager Discovery Pattern" on page 300.

Determining the Appropriate Range of Dates for Changed SAP Transaction Discovery

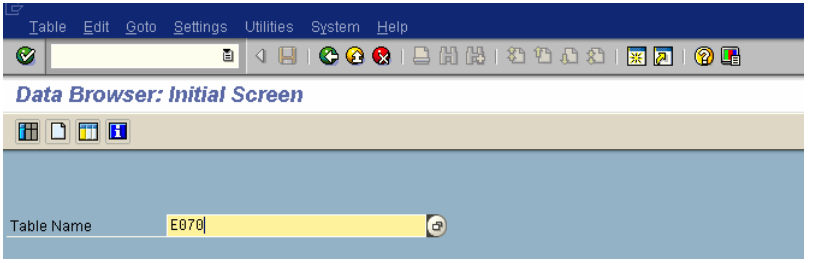
---

Note: This procedure is only required if the parameter **get_tx_change_interval** = 0. For details, see "Selecting the Discovery Modes for Discovering Application Components, SAP Transactions, and Transports" on page 293.

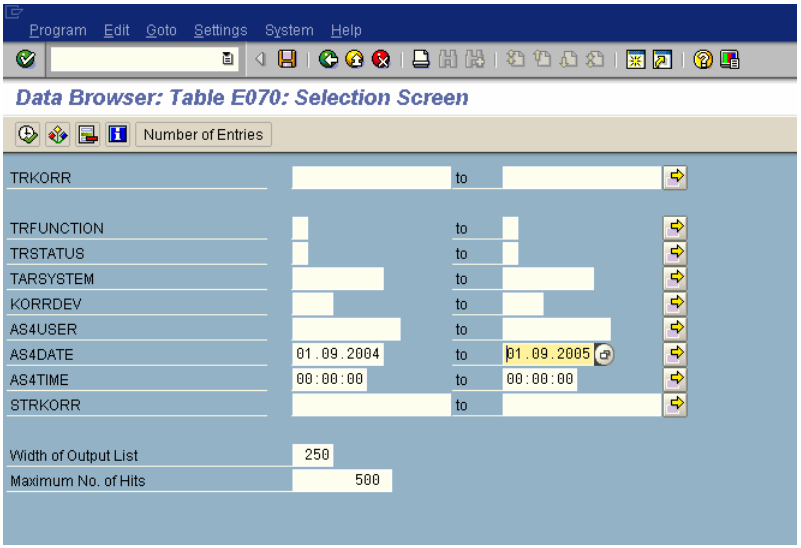
To discover the SAP transactions that have changed, you must determine the appropriate range of dates before entering them in the appropriate discovery pattern – for details, see "Selecting the Discovery Modes for Discovering Application Components, SAP Transactions, and Transports" on page 293.

To determine the appropriate range of dates for changed SAP transactions discovery:

1. Click the SAP Logon icon to log in to SAP.
2. Activate SE16 in SAPGUI to open table E070.



3 Enter the range of dates for which you want to display the transports deployed



4 Press the **Execute** button, in the top left corner.

The outcome is the result of the query you just defined in SAP. The time range is indicated in the AS4DATE and AS4TIME columns.

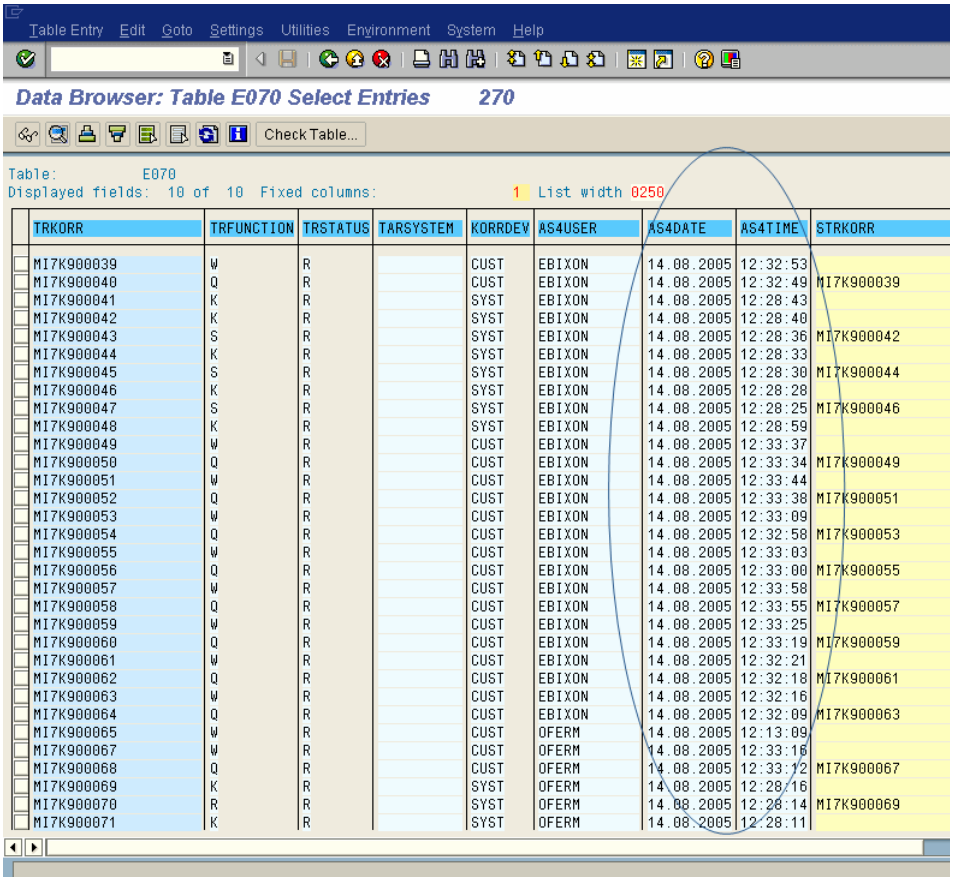


Table Entry Edit Goto Settings Utilities Environment System Help

Data Browser: Table E070 Select Entries 270

Check Table...

Table: E070
Displayed fields: 10 of 10 Fixed columns: 1 List width 0250

TRKORR	TRFUNCTION	TRSTATUS	TARSYSTEM	KORRDEV	AS4USER	AS4DATE	AS4TIME	STRKORR
MI7K900039	W	R		CUST	EBIXON	14.08.2005	12:32:53	
MI7K900040	Q	R		CUST	EBIXON	14.08.2005	12:32:49	MI7K900039
MI7K900041	K	R		SYST	EBIXON	14.08.2005	12:28:43	
MI7K900042	K	R		SYST	EBIXON	14.08.2005	12:28:40	
MI7K900043	S	R		SYST	EBIXON	14.08.2005	12:28:36	MI7K900042
MI7K900044	K	R		SYST	EBIXON	14.08.2005	12:28:33	
MI7K900045	S	R		SYST	EBIXON	14.08.2005	12:28:30	MI7K900044
MI7K900046	K	R		SYST	EBIXON	14.08.2005	12:28:28	
MI7K900047	S	R		SYST	EBIXON	14.08.2005	12:28:25	MI7K900046
MI7K900048	K	R		SYST	EBIXON	14.08.2005	12:28:59	
MI7K900049	W	R		CUST	EBIXON	14.08.2005	12:33:37	
MI7K900050	Q	R		CUST	EBIXON	14.08.2005	12:33:34	MI7K900049
MI7K900051	W	R		CUST	EBIXON	14.08.2005	12:33:44	
MI7K900052	Q	R		CUST	EBIXON	14.08.2005	12:33:38	MI7K900051
MI7K900053	W	R		CUST	EBIXON	14.08.2005	12:33:09	
MI7K900054	Q	R		CUST	EBIXON	14.08.2005	12:32:58	MI7K900053
MI7K900055	W	R		CUST	EBIXON	14.08.2005	12:33:03	
MI7K900056	Q	R		CUST	EBIXON	14.08.2005	12:33:00	MI7K900055
MI7K900057	W	R		CUST	EBIXON	14.08.2005	12:33:58	
MI7K900058	Q	R		CUST	EBIXON	14.08.2005	12:33:55	MI7K900057
MI7K900059	W	R		CUST	EBIXON	14.08.2005	12:33:25	
MI7K900060	Q	R		CUST	EBIXON	14.08.2005	12:33:19	MI7K900059
MI7K900061	W	R		CUST	EBIXON	14.08.2005	12:32:21	
MI7K900062	Q	R		CUST	EBIXON	14.08.2005	12:32:18	MI7K900061
MI7K900063	W	R		CUST	EBIXON	14.08.2005	12:32:16	
MI7K900064	Q	R		CUST	EBIXON	14.08.2005	12:32:09	MI7K900063
MI7K900065	W	R		CUST	OFERM	14.08.2005	12:13:09	
MI7K900067	W	R		CUST	OFERM	14.08.2005	12:33:16	
MI7K900068	Q	R		CUST	OFERM	14.08.2005	12:33:12	MI7K900067
MI7K900069	K	R		SYST	OFERM	14.08.2005	12:28:16	
MI7K900070	R	R		SYST	OFERM	14.08.2005	12:28:14	MI7K900069
MI7K900071	K	R		SYST	OFERM	14.08.2005	12:28:11	

Running the SAP_Dis_Solution_Manager Discovery Pattern

Run the SAP_Dis_Solution_Manager discovery pattern if you are using SAP Solution Manager and you want to discover the SAP Solution Manager components.

To run the SAP_Dis_Solution_Manager discovery pattern:

1 Expand **Application - SAP (R/3)** and select **SAP_Dis_Solution_Manager**.

2 Click the **Activate** button to start the discovery.

For details on the SAP Solution Manager components, see "SAP Solution CIs" on page 303.

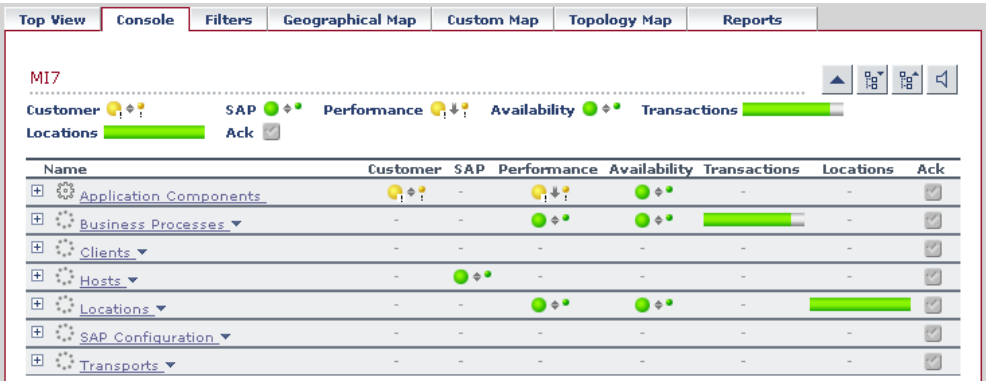
Step 5 – Checking that the Discovery Ran Correctly

After running all the discoveries, check that all the information is displayed correctly.

To check that the discovery ran correctly:

Select **Application** > **Dashboard**, click the **Console** tab, and open the SAP Systems view or select **Admin** > **CMDB**, and click the **IT Universe Manager** tab.

The view is as follows if Business Process Monitor profiles and CCMS monitors were configured before running discovery. Otherwise, the view is similar but the status indicators are grey:



Step 6 – Running SAP Solution Manager Discovery

You run the SAP Solution Manager discovery to discover the business process hierarchy.

To run SAP Solution Manager Discovery:

1. Select **Admin** > **CMDB** and click the **Discovery Manager** tab to open the Discovery Management page.
2. Click the **Module Manager** tab.
3. In the Discovery Modules pane, expand **Application - SAP (R/3)**.
4. Select the **SAP_Dis_SolutionManager** discovery pattern.
5. Click the **Activate** button to start the discovery.

   The outcome is the business process hierarchy – for details, see "SAP Solution CIs" on page 303.

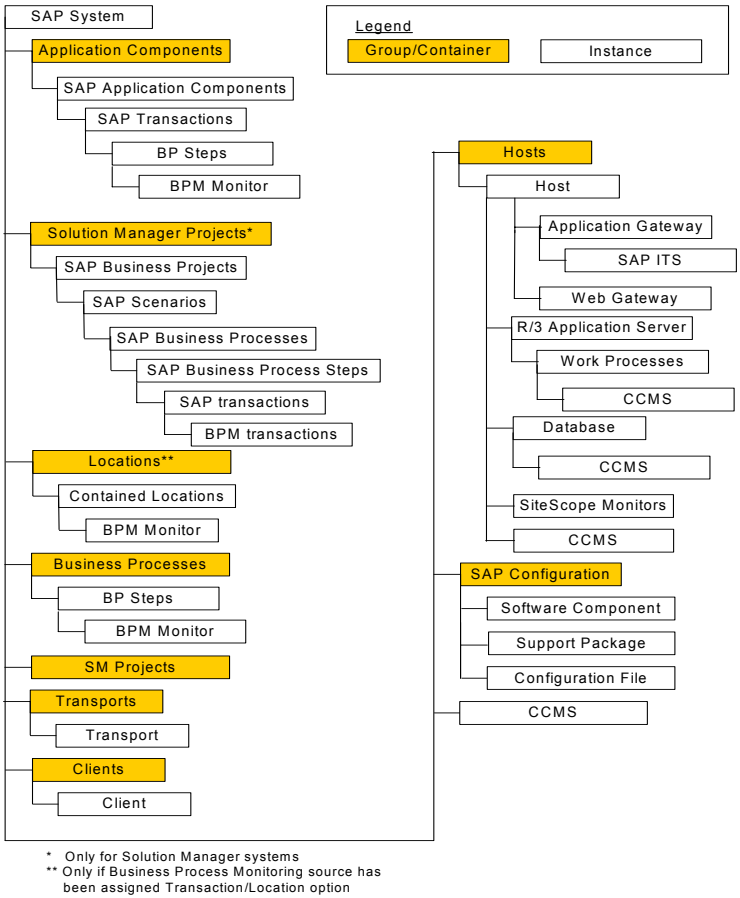
21

SAP Solution CIs

SAP discovery package discovers SAP-related CIs and general CIs (such as hosts) that are related to them. This chapter describes the CI types and the full hierarchy of SAP CIs that appear in Mercury Business Availability Center (depending on the specific SAP deployment discovered).

Hierarchy

The CIs hierarchy is as follows:



SAP System

SAP System is a logical unit, grouping together SAP-related CIs (and possibly other CIs as well) into one homogenous SAP deployment.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth) – for details, see "System" in *Repositories Administration*. By default, the System KPI does not appear in the view. If you are using a regular SiteScope monitor (which creates the System KPI) and you want to display the System KPI in the view, you have to add the System KPI manually to the CI.	SiteScope
SAP	Indicates problems related to the SAP infrastructure – for details, see "SAP" in *Repositories Administration*. The data that is reported by this KPI comes from CCMS measurements.	SiteScope

KPIs	Description	Source
Transactions	A bar that includes up to six colored sections. Each colored section represents the relative amount of Business Process Steps with the end-user experience status (the worst status between **Performance** and **Availability**) that corresponds to the color – for details, see "Transactions" in *Repositories Administration*.	Business Process Monitor
Locations	A bar that includes up to six colored sections. Each colored section represents the relative amount of Business Process Steps with the end-user experience status (the worst status between **Performance** and **Availability**) that corresponds to the color, at the specified location – for details, see "Locations" in *Repositories Administration*.	Business Process Monitor

SAP Applications

SAP Applications is a logical unit, grouping together Application Components.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor

SAP Application Component

A SAP Application Components may include other SAP Application Components and some SAP transactions with some common denominator.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor

SAP Transaction

A SAP Transaction CI is part of a business process defined in the SAP System. It is comprised of request-response couples called dialog steps. The end user uses SAP transactions to carry out actions on the SAP System.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor

Business Process Step

Business Process Steps (BPM transactions inside a script) are emulated SAP transactions executed on a Business Process Monitor machine. They are used to supply proactive monitoring of end user experience.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor

BPM Monitor

The BPM Monitor CIs represent Business Process Monitor entities used to monitor user experience.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor

Solution Manager Projects

The Solution Manager Projects CI type includes SAP Business Project CIs, SAP Scenario CIs, SAP Business Process CIs, and SAP Business Process Step CIs.

The Solution Manager Projects hierarchy is specified by the user in SAP Solution Manager.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor

Locations

The Contained Group Locations is a logical unit, grouping together Contained Locations CIs.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Locations	A bar that includes up to six colored sections. Each colored section represents the relative amount of BP Steps with the end-user experience status (the worst status between performance and availability) that corresponds to the color – for details, see "Locations" in *Repositories Administration*.	Business Process Monitor

Contained Location

Location CIs are created as part of the Business Process Monitor hierarchy when working with the **Transactions/locations** option.

To separate the SAP Business Process steps locations status from the Location CI (from the Business Process Monitor), the Contained Location CIs are created by the SAP solution and are connected to the SAP Business Process steps (identified by following the naming convention or by manually linking them).

The regular Location CI is connected to all Business Process steps both regular and SAP, but the Contained Location CI is connected only to the SAP Business Process steps.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor

Business Processes

The Contained Group called Business Processes is a logical container that contains all the Business Process steps attached to all the SAP transactions.

The default CI KPIs are:

KPIs	Description	Source
Performance	Indicates the performance of SAP transactions – for details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Availability	Indicates the availability of SAP transactions – for details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Transactions	A bar that includes up to six colored sections. Each colored section represents the relative amount of BP Steps with the end-user experience status (the worst status between performance and availability) that corresponds to the color – for details, see "Transactions" in *Repositories Administration*.	Business Process Monitor

Transports

A Transport represents packaged change requests that include the changes that are to be deployed onto the system.

This CI does not have KPIs.

Client

A client is an organizational and legal CI in the SAP system. The main objective of the client is to keep the data isolated: the data in a client can only be visible within that client; it cannot be displayed or changed from another client. Each client on a system can represent a unique working environment.

This CI does not have KPIs.

Hosts

Hosts is a logical unit, grouping together Host CIs.

A Host CI represents the physical machine on which a server is installed. This is not a SAP-specific element.

The default CI KPIs are:

KPIs	Description	Source
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth) – for details, see "System" in *Repositories Administration*. By default, the System KPI does not appear in the view. If you are using a regular SiteScope monitor (which creates the System KPI) and you want to display the System KPI in the view, you have to add the System KPI manually to the CI.	SiteScope
SAP	Indicates problems related to the SAP infrastructure – for details, see "SAP" in *Repositories Administration*. The data that is reported by this KPI comes from CCMS measurements.	SiteScope

Application Gateway

An Internet Transaction Server (ITS) component. Establishes the connection to the R/3 System and performs the processing of tasks that are required to move data between R/3 applications and the Internet.

This CI does not have KPIs.

Web Gateway

An ITS component. A web server extension that establishes the connection between ITS and the Web server and forwards user requests to the Application Gateway.

This CI does not have KPIs.

R/3 Application Server

SAP® R/3 Application Server is SAP's integrated software solution for client/server and distributed open systems.

The default CI KPIs are:

KPIs	Description	Source
SAP	Indicates problems related to the SAP infrastructure – for details, see "SAP" in *Repositories Administration*. The data that is reported by this KPI comes from CCMS measurements.	SiteScope

Work Processes

Each work process CI is a logical, single-instance representation of all the work processes of the same type existing on the R/3 server.

There are several available types of work processes:

- **Dialog Work Process** – Executes dialog programs (ABAP).
- **Update Work Process** – Responsible for asynchronous database changes (controlled by a COMMIT WORK statement in a dialog work process).
- **Update2 Work Process** – Used for statistical, non-critical updates (for example, result calculations).
- **Background Work Process** – Executes time-dependent or event-controlled background jobs.
- **Enqueue Work Process** – Executes locking operations (if SAP transactions have to synchronize themselves).
- **Spool Work Process** – Performs print formatting (to printer, file, or database).

The default CI KPIs are:

KPIs	Description	Source
SAP	Indicates problems related to the SAP infrastructure – for details, see "SAP" in *Repositories Administration*. The data that is reported by this KPI comes from CCMS measurements.	SiteScope

Database

A database management system holding the data tier, including all the SAP elements: SAP transactions, programs, work processes, and so forth. This is not a SAP-specific CI.

The default CI KPIs are:

KPIs	Description	Source
SAP	Indicates problems related to the SAP infrastructure – for details, see "SAP" in *Repositories Administration*. The data that is reported by this KPI comes from CCMS measurements.	SiteScope
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth) – for details, see "System" in *Repositories Administration*. By default, the System KPI does not appear in the view. If you are using a regular SiteScope monitor (which creates the System KPI) and you want to display the System KPI in the view, you have to add the System KPI manually to the CI.	SiteScope

Software Component

A software component installed on the SAP System, for example: SAP_ABA (cross-application component), SAP_HR (human resources), and so forth.

This CI does not have KPIs.

Support Package

A Support Package contains quality improvements for the SAP system, or adjustments due to legal changes.

This CI does not have KPIs.

Configuration File

Configuration files are used to enter configuration parameters into the system/servers.

This CI does not have KPIs.

CCMS Counters

CCMS Counters (also called Measurements) are pieces of information elements, relevant to SAP, retrieved from SAP CCMS (Computer Center Management System).

The default CI KPI is:

KPIs	Description	Source
SAP	Indicates problems related to the SAP infrastructure – for details, see "SAP" in *Repositories Administration*. The data that is reported by this KPI comes from CCMS measurements.	SiteScope

Monitor

The monitors are SiteScope entities used to monitor the various CIs that exist in the CMDB. The monitors that are most likely to appear in the SAP view are host monitors: CPU, memory, disk space, and so forth. These monitors appear in the SAP view only if they are manually attached to the Host CI.

The default CI KPIs are:

KPIs	Description	Source
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth) – for details, see "System" in *Repositories Administration*. By default, the System KPI does not appear in the view. If you are using a regular SiteScope monitor (which creates the System KPI) and you want to display the System KPI in the view, you have to add the System KPI manually to the CI.	SiteScope

22

Administering the SAP Solution

This chapter describes the specific tasks involved in administering the SAP solution.

Using a Business Process Monitor Profile to Simulate SAP Users

Business Process Monitor profiles are used to simulate SAP users To obtain performance and availability information on the SAP transactions.

You can view Business Process Steps under the SAP view to enable you to analyze what happens in the SAP system.

This section includes the following topics:

➤ "Attaching Business Process Monitor Transactions to SAP Application Components" on page 328

➤ "Checking/Viewing the Business Process Monitor Measurements in the SAP Systems View" on page 332

Creating a Business Process Monitor Profile

You create a Business Process profile in Monitor Administration – for details, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

This section includes the following topics:

➤ "Selecting the Appropriate Protocol" on page 322

➤ "Selecting the Appropriate Run-Time Settings" on page 324

➤ "Editing the Script" on page 326

Selecting the Appropriate Protocol

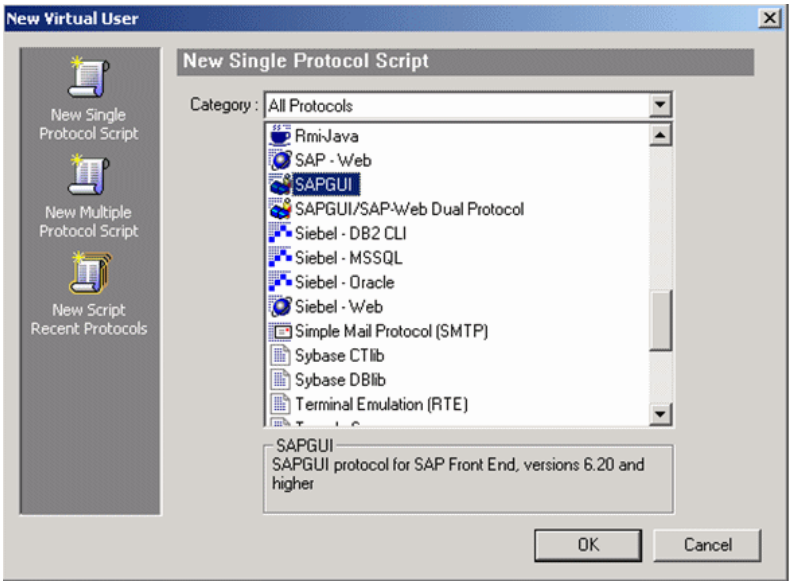
In Mercury Virtual User Generator (VuGen), SAP scripts are recorded using the SAPGUI protocol. You must select the SAPGUI protocol when you create a new script – for details, see "Creating New Virtual User Scripts" in *Using Mercury Virtual User Generator*.

To select the appropriate protocol:

1 In VuGen, select **New** to open the New Virtual User page.

2 Select **New Single Protocol Script**.

3 Select the **SAPGUI** protocol.

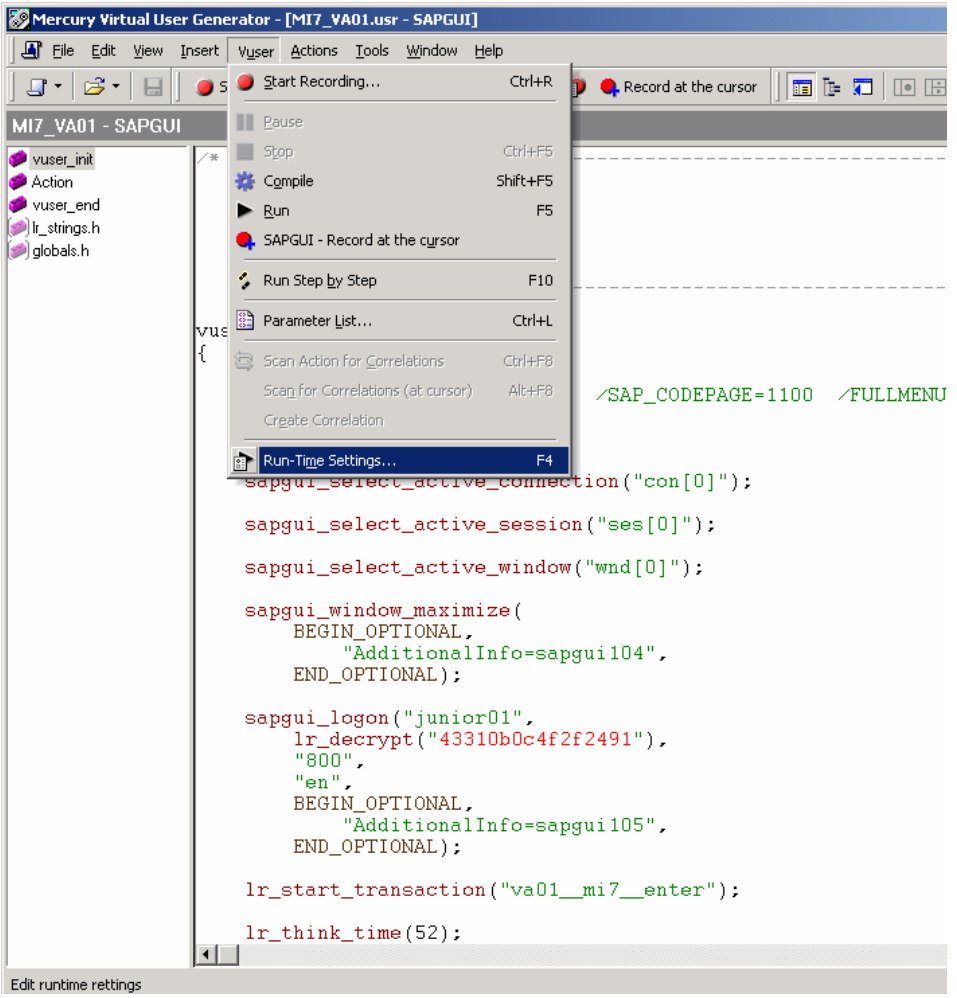


Selecting the Appropriate Run-Time Settings

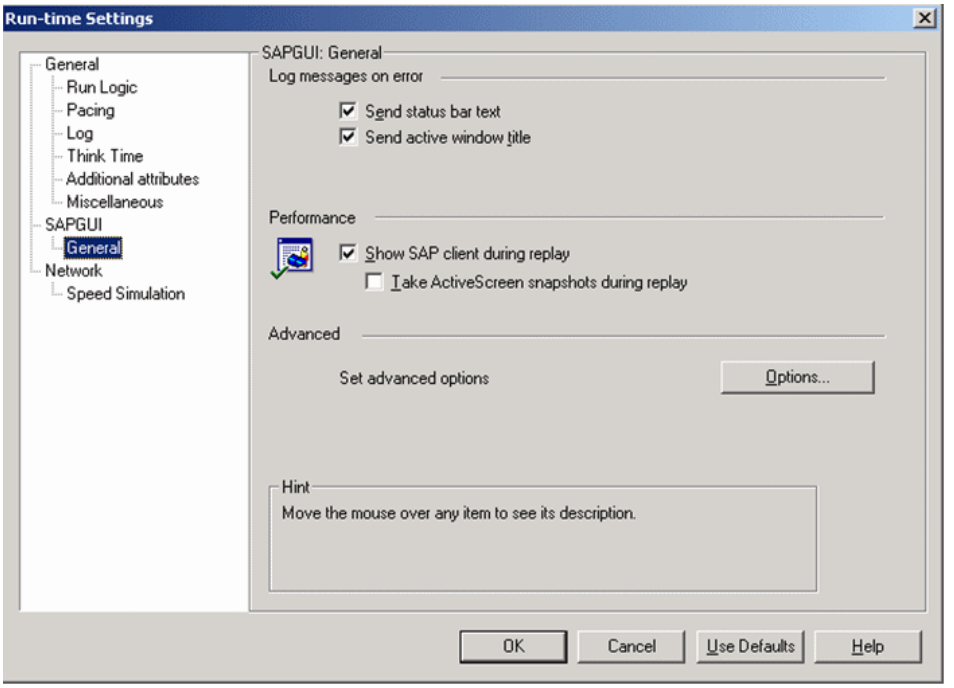
In VuGen, open the Run-Time settings window, and in the Performance area, select **Show SAP client during replay** to give more accurate user experience times – for details, see "Configuring Run-Time Settings" in *Using Mercury Virtual User Generator*.

To select the appropriate run-time settings:

1 After recording the script in VuGen, select **Vuser** > **Run-Time Settings**.



2 The Run-time Settings page opens. Select **Show SAP client during replay**, and clear **Take ActiveScreen snapshots during replay**.



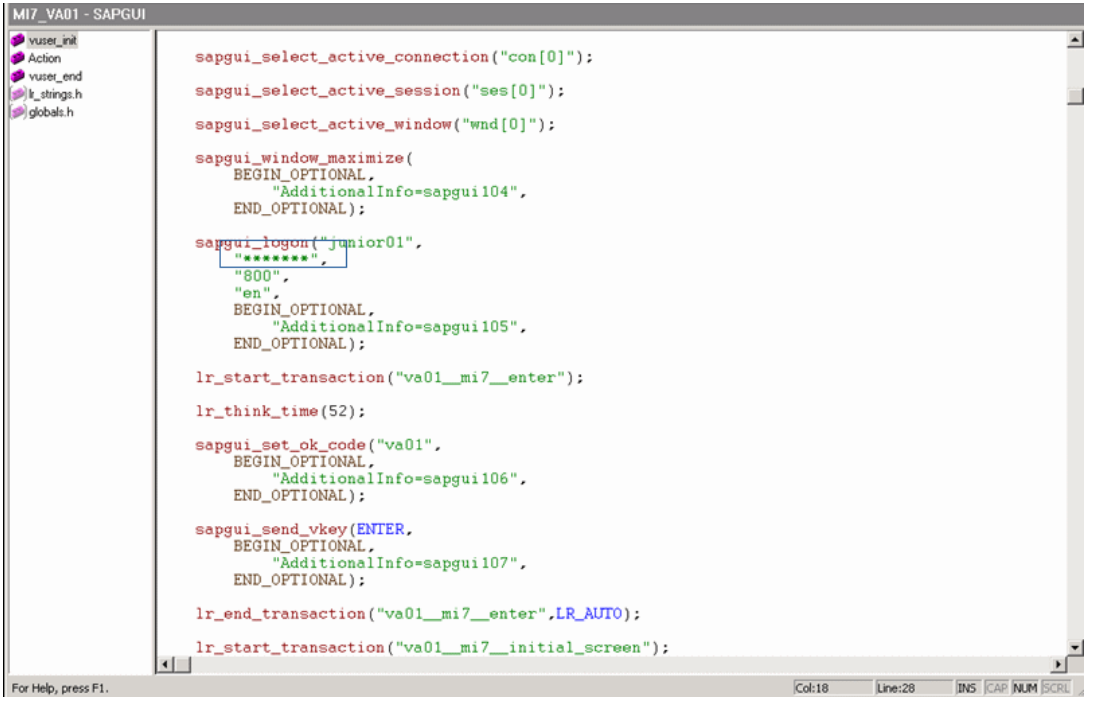
3 Click **OK**.

Editing the Script

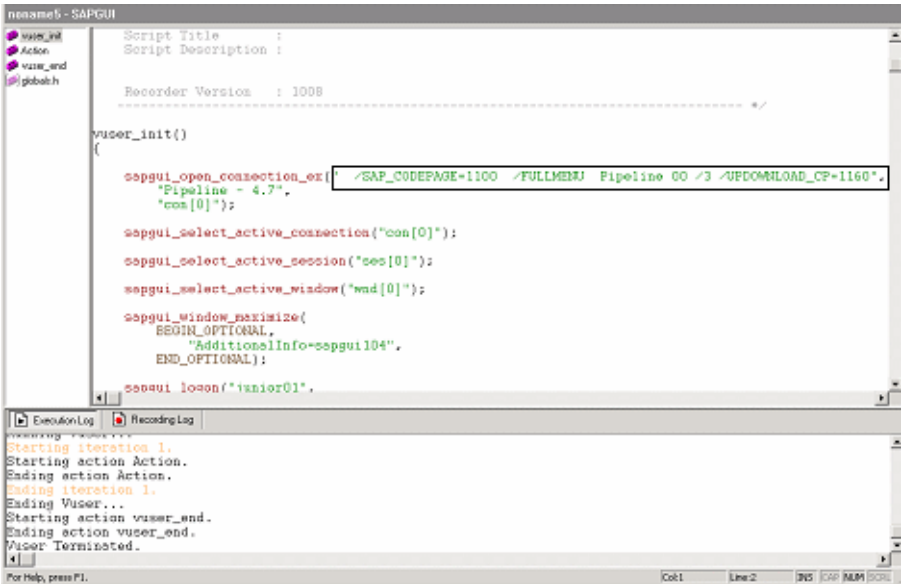
You can edit the script to make sure the password is recorded properly and to check and correct the script's connection parameters.

To edit the script:

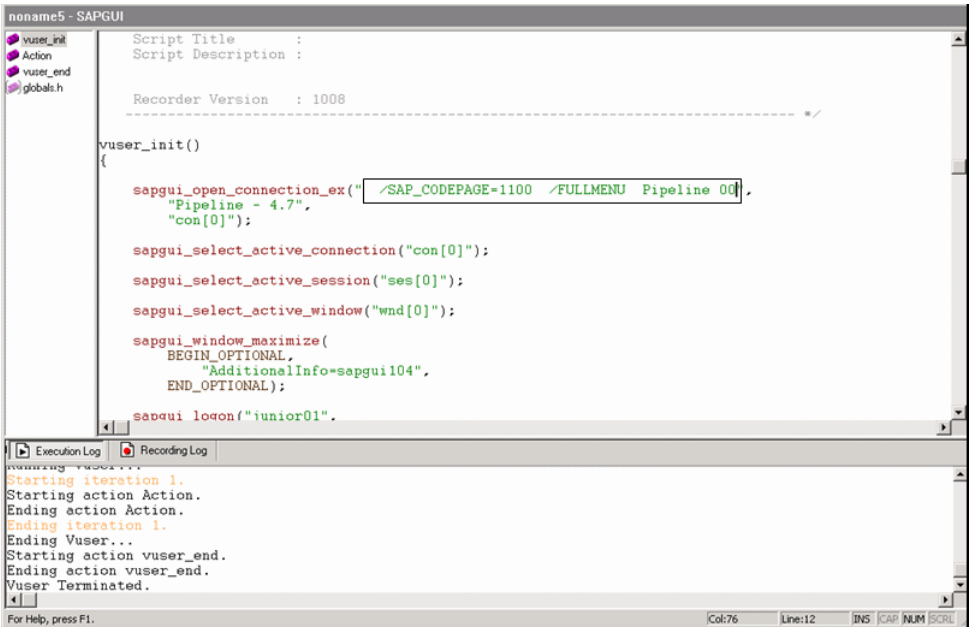
1 Make sure the password is recorded correctly. Remove the stars and replace with the required password.



2 Check the script's connection parameters and if necessary, delete the string that appears after the system number in the first parameter.



The result is as follows:



Synchronizing the Business Process Monitoring Source Adapter

You can synchronize the Business Process Monitoring source adapter immediately or you can wait for the automatic synchronization to take place – for details, see "Administering the SAP Solution" in *Source Manager Administration*.

Attaching Business Process Monitor Transactions to SAP Application Components

To display Performance and Availability information, Business Process Steps must be attached to SAP transactions.

You can connect BMP transactions to a SAP transaction in two different ways:

➤ by following the naming conventions for the BMP transaction names. For details, see "Following the Naming Conventions for Naming Business Process Steps" on page 329.

➤ by **not** following the naming conventions for the BMP transaction names and manually linking a Business Process Step to a SAP transaction. For details, see "Attaching Business Process Steps to a SAP Transaction without Following the Naming Conventions" on page 330.

If you do not follow the naming conventions, be careful when deleting links between SAP transactions and Business Process Steps. For details, see "Deleting Links Between SAP Transactions and Business Process Steps" on page 331.

Following the Naming Conventions for Naming Business Process Steps

To logically connect Business Process Steps to a SAP transaction, the Business Process Step name should have the following format: **<tran_name>_ _<sys_name>_ _<BPM_tran_name>**

➤ **tran_name** – the name, in lowercase, of the SAP transaction to which you want to attach the Business Process Step.

➤ **sys_name** – the name, in lowercase, of the SAP System on which the transaction is run (for example, MI7).

➤ **BPM_tran_name** – the unique name of the Business Process Step. Any set of alphanumeric and mixed case characters are supported (special characters are not allowed). It is good practice to name the transaction so that the name indicates what occurs in that set of dialog steps.

Note: You assign the appropriate name to a Business Process Step when you record it – for details, see "Recording with VuGen" in *Using Mercury Virtual User Generator*.

For example, the names of the Business Process Steps assigned to the SAP transaction VA01 in the MI7 SAP System should start with: va01_ _mi7_

In the SAP Systems View, a **Business Process Steps** node that is displayed under a specific SAP transaction is a container under which all relevant transactions are located.

It is important to split a SAP transaction into a few Business Process Monitor transactions so that you are able to pinpoint the problem. For example, if each step of the SAP transaction is a separate Business Process Monitor transaction, you can find the exact part of the SAP transaction where the problem occurs.

Attaching Business Process Steps to a SAP Transaction without Following the Naming Conventions

If you do not want to follow the naming conventions for the Business Process Steps, go to Monitor Administration and build a Business Process Monitor profile. You can then manually connect Business Process Steps with SAP transactions.

To attach Business Process Steps to a SAP transaction without following the naming convention:

1. Select **Admin** > **CMDB**.
2. Click the **IT Universe Manager** tab.
3. Select **SAP View** in the **View** list.
4. Right-click the SAP transaction that you want to monitor using the BPM profile and select **Attach Related CI** to open the **Attach Related CIs** wizard.
5. Select **Monitors View** in the **Views** list.
6. Expand and select the Business Process Step to which you want to connect the SAP transaction.

7. Click the right arrow to move the CI to the right-hand box.
8. Click **Next**.
9. In the **Relationship Type** list, select **Monitored By for SAP**.
10. Select **Allow CI Update.**
11. Click **Finish**.

Deleting Links Between SAP Transactions and Business Process Steps

SiteScope measurements and Business Process Monitor transactions are attached under the appropriate level of the SAP hierarchy – for details, see "SAP Solution CIs" on page 303.

A TQL runs in the background and returns:

- **CCMS measurements that are not linked to SAP entities** – most of the CCMS measurements' names indicate to which SAP entities they should be attached in the hierarchy.

- **Business Process Monitor transactions that are not attached to a SAP and follow the naming convention** – the name of the Business Process Monitor transaction indicates to which SAP entity it should be attached – for details about the naming convention, see below.
- **Business Process steps that are manually attached to a SAP transaction** – a Business Process Step is automatically attached to the Business Process container that was created by the Business Process Step, the Business Process Step is monitored by SAP – for details, see "Attaching Business Process Steps to a SAP Transaction without Following the Naming Conventions" on page 330.

  If the Business Process Monitor source adapter was assigned the **Transaction/Location** option (for details, see "Business Process Monitoring" in *Source Manager Administration*) a copy of the location information is attached to the Locations container.

If you delete a link between a SAP transaction and its child Business Process Step transaction, then the following happens:

- If you followed the naming convention for the Business Process Step transaction, the link between the SAP transaction and its child Business Process Step is automatically recreated at the next synchronization
- If you did not follow the naming convention and created a manual link between the SAP transaction and a Business Process Step transaction, then when you delete the link:
  - if the Business Process Monitoring source adapter was assigned the **Transactions/locations** option, the Location container is not deleted.

    You can manually delete it. Delete the Location container only if the deleted Business Process Step transaction is the only CI attached to this location. If other Business Process Step transactions are attached to this location, delete only the links between the Business Process Monitor (BPM transaction from location) and the Location container.
  - if the Business Process Monitoring source adapter was assigned the **Regular** option, the Business Process container is not deleted. You must manually delete the links between the Business Process container and the detached Business Process Step transaction.

For details about the **Transactions/locations** or **Regular** options, see "Business Process Monitoring" in *Source Manager Administration*.

Checking/Viewing the Business Process Monitor Measurements in the SAP Systems View

You can view the Business Process Measurement in the SAP Systems view in different locations in the SAP hierarchy.

This section includes the following topics:

- "Naming Conventions for Business Process Steps and Transaction/Location Hierarchy Structure" on page 333
- "No Naming Convention for Business Process Steps and Transaction/Location Hierarchy Structure" on page 335

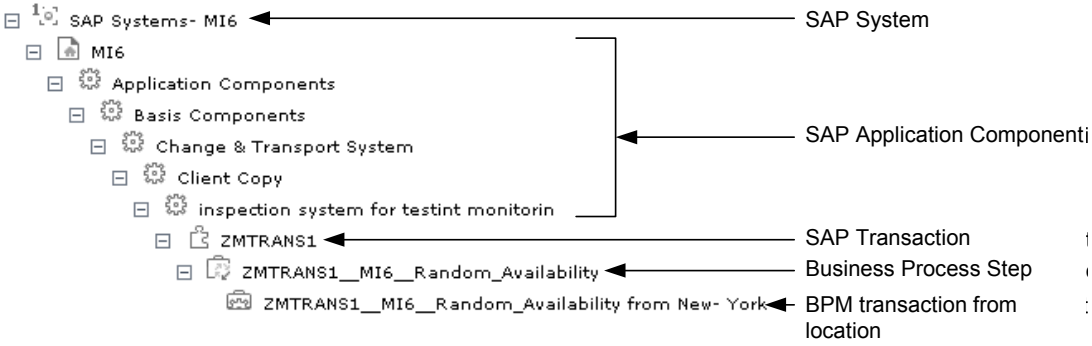
➤ "Naming Conventions for Business Process Steps and Regular Hierarchy Structure" on page 336

➤ "No-Naming Convention for Business Process Steps and Regular Hierarchy Structure" on page 337

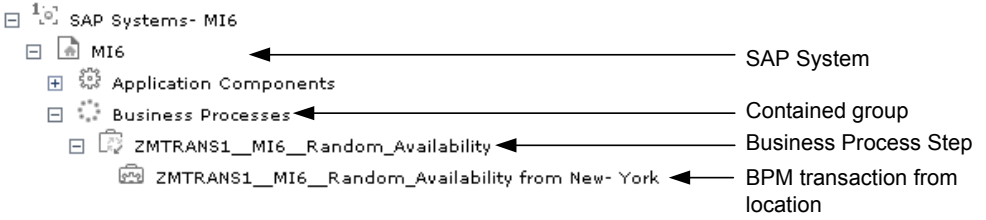
Naming Conventions for Business Process Steps and Transaction/Location Hierarchy Structure

If you have used the naming convention for the Business Process Step, and you have set the Hierarchy structure of the Business Process Monitoring source adapter to **Transaction/Location** (for details, see "Business Process Monitoring" in *Source Manager Administration*) then the view displays the following structure:

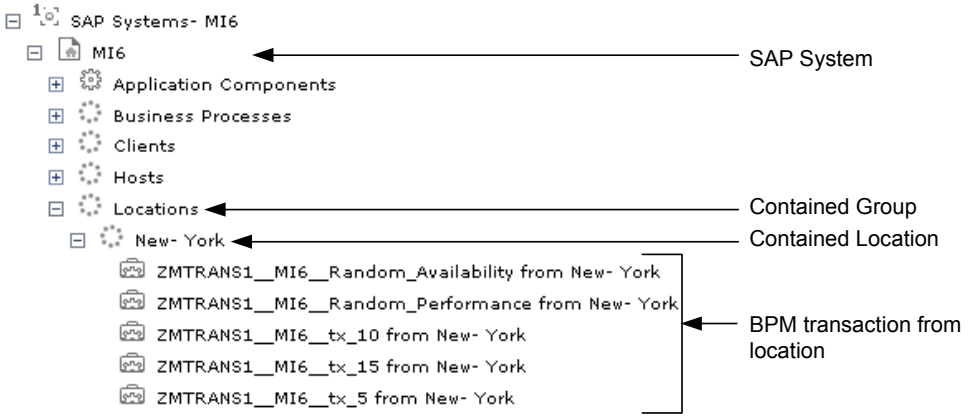
➤ the BPM Monitor (BPM transaction from location CIT) is displayed under a Business Process Step CI, under a SAP transaction CI, under several levels of SAP Application Component CIs, under a SAP System CI. For example:



- the BPM Monitor (BPM transaction from location CIT) is also displayed under a Business Process Step CI under the Contained group CI (Business Processes). For example:



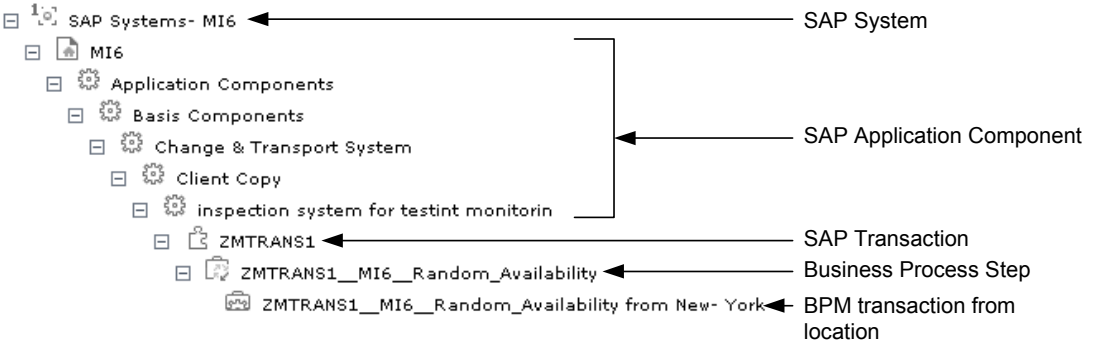
- the BPM Monitor (BPM transaction from location CIT) is displayed under a Contained Location CI itself under a Contained group CI (Locations) under the SAP System CI. For example:



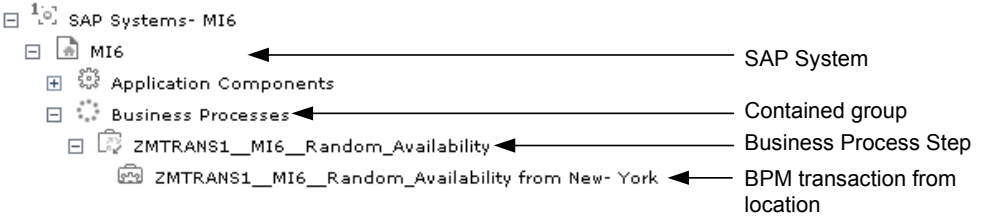
No Naming Convention for Business Process Steps and Transaction/Location Hierarchy Structure

If the Business Process Steps do not follow the naming conventions, and you have set the Hierarchy structure of the Business Process Monitoring source adapter to **Transaction/Location** (for details, see "Business Process Monitoring" in *Source Manager Administration*) then the view displays the following structure:

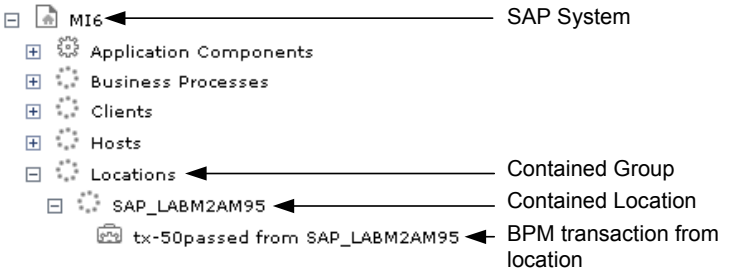
- the BPM Monitor (BPM transaction from location CIT) is displayed under a Business Process Step CI, under a SAP transaction CI, under several levels of SAP Application Component CIs, under a SAP System CI. For example:



- the BPM Monitor (BPM transaction from location CIT) is also displayed under a Business Process Step CI under the Contained group CI (Business Processes). For example:



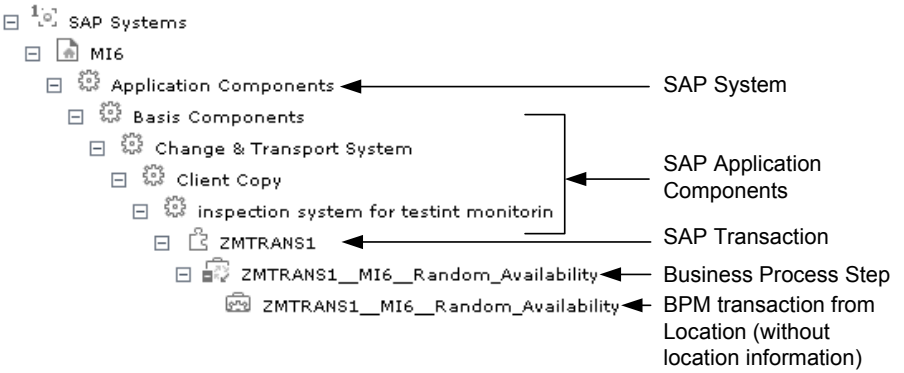
- the BPM Monitor (BPM transaction from location CIT) is also displayed under a Contained Location CI, under a Contained group CI (Locations), under a SAP System CI. For example:



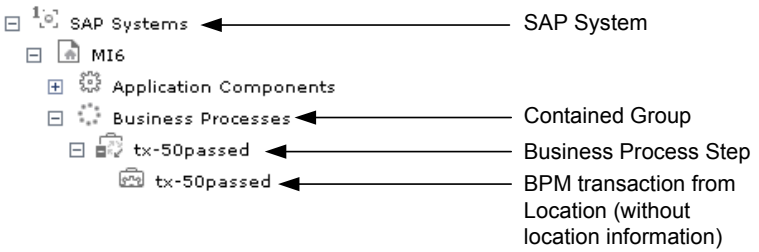
Naming Conventions for Business Process Steps and Regular Hierarchy Structure

If the Business Process Steps follow the naming conventions and you have set the Hierarchy structure of the Business Process Monitoring source adapter to **Regular** (for details, see "Business Process Monitoring" in *Source Manager Administration*), then the view displays the following structure:

- the BPM Monitor (BPM transaction from location CIT) is displayed without the location information, under a Business Process Step CI, under a SAP transaction CI, under several levels of SAP Application Component CIs, under a SAP System CI. For example:



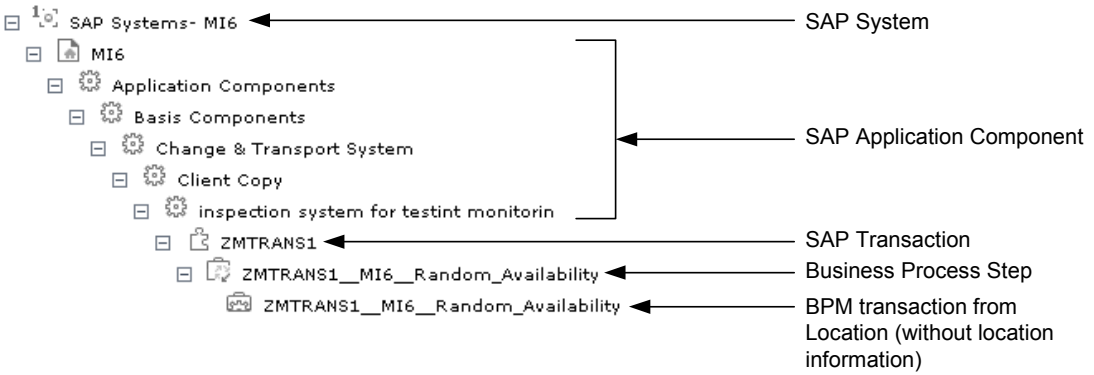
➤ the BPM Monitor (BPM transaction from location CIT) without location information, is also displayed under a Business Process Step CI under the Contained group CI (Business Processes). For example:



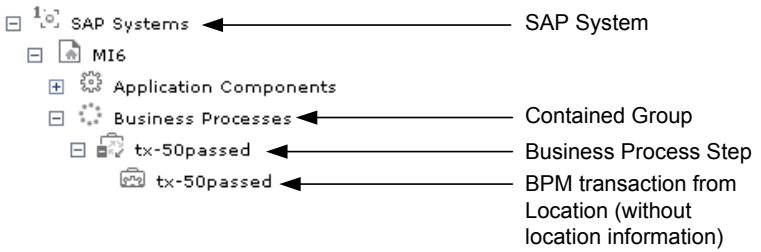
No-Naming Convention for Business Process Steps and Regular Hierarchy Structure

If a Business Process Step does not follow the naming conventions and you have set the Hierarchy structure of the Business Process Monitoring source adapter to **Regular** (for details, see "Business Process Monitoring" in *Source Manager Administration*), then the view displays the following structure:

➤ the BPM Monitor (BPM transaction from location CIT) is displayed under a Business Process Step CI, under a SAP transaction CI, under several levels of SAP Application Component CIs, under a SAP System CI, without the location information. For example:



➤ the BPM Monitor (BPM transaction from location CIT) without location information, is also displayed under a Business Process Step CI under the Contained group CI (Business Processes). For example:



Using the SAP CCMS Monitor to Retrieve Measurements from SAP System

The SAP CCMS monitor retrieves and reports measurements from SAP's centralized monitoring system CCMS. CCMS is used to monitor all servers, components and resources in the SAP R/3® System from one single centralized server, facilitating problem discovery and problem diagnosis. For details, see "SAP CCMS Monitor" in *Configuring SiteScope Monitors*.

Note: The SAP CCMS Monitor is an optional SiteScope feature whose license is provided with the SAP solution.

This section includes the following topics:

➤ "Connecting the SAP CCMS Measurements to the Appropriate Elements of the SAP Hierarchy" on page 341

➤ "Checking/Viewing the SiteScope Measurements in the SAP View" on page 343

Using SiteScope CCMS Solution Template

The **MonitorSetSSServer.mset** solution template is the most effective way to deploy a CCMS monitor.

To use the SiteScope CCMS solution template:

1. Access SiteScope via Monitor Administration in Mercury Business Availability Center or directly using the URL: **http://<SiteScope_server>:8080/topaz/**.
2. Click the **Monitors** tab.
3. Right-click the appropriate SiteScope in the Enterprise tree, and select **New Group**.
4. Enter the name of the group in the **Group Name** box in the Main Settings area.
5. Click **OK**.
6. Expand **Solution Sets**, right-click **SAPR3Solution**, and select **Copy**.
7. Right-click the new group you have created, and select **Paste**.
8. In the Main Settings area, enter the following information:
   - ➤ the name of the SAP System in the **TARGET_SERVER_NAME** box
   - ➤ the user name in the **USER_NAME** box
   - ➤ the password in the **Password** box
   - ➤ the number of the SAP system in the **SYSTEM_NUMBER** box
   - ➤ the number of the client to which you connect SiteScope in the **CLIENT_NUMBER** box
9. Click **OK**.

Attaching SiteScope to Mercury Business Availability Center

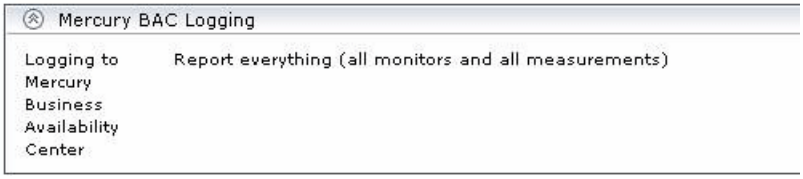
You must now attach SiteScope to Mercury Business Availability Center – for details, see "Managing SiteScope in the Monitor Tree" in *Managing SiteScope*.

Checking that the Monitor is Set to Report All Monitors and Measurements

To view SiteScope measurements, you must make sure that the monitor is set to report all monitors and measurements information.

To check that the monitor is set to report all monitors and measurements:

1. Select **Admin** > **Monitors**.
2. Click the **Monitors** tab.
3. Double-click the appropriate CCMS monitor under the appropriate group, select **Properties**, and expand the Mercury BAC Login area.
4. Make sure that the value of the **Logging to Mercury Business Availability Center** is **Report everything (all monitors and all measurements)**.



Synchronizing the SiteScope Source Adapter

You can synchronize the SiteScope source adapter immediately or you can wait for the automatic synchronization to take place – for details, see "Administering the SAP Solution" in *Source Manager Administration*.

Connecting the SAP CCMS Measurements to the Appropriate Elements of the SAP Hierarchy

The SAP CCMS measurements are connected to the appropriate elements of the SAP hierarchy as follows:

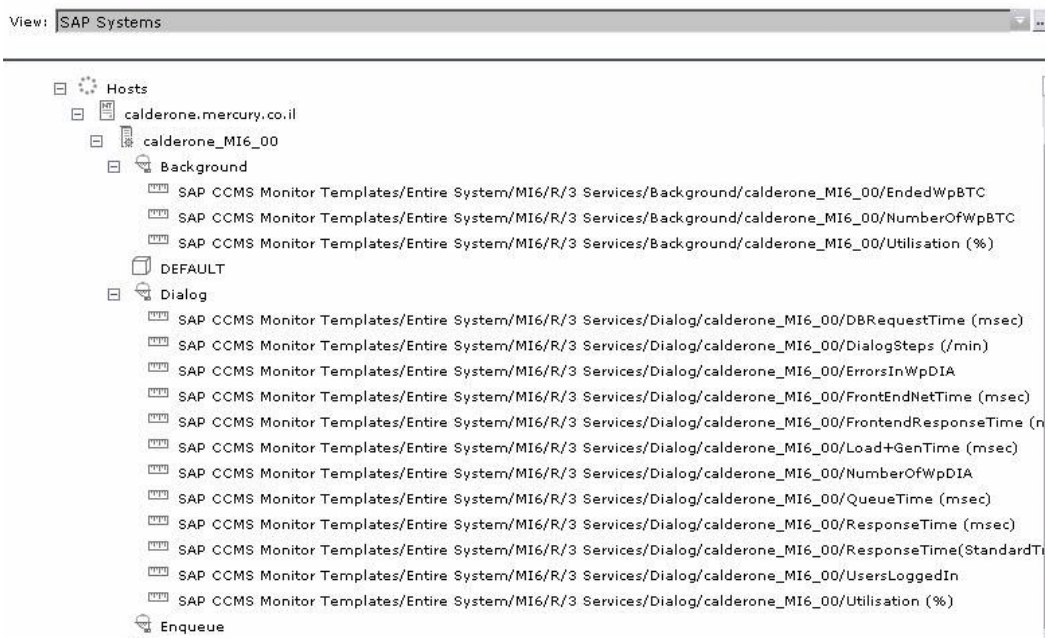
1. A SAP CCMS measurement can reside only under a System, R/3 Application Server, Work Process, or Database CIT.
2. The linkage is performed based on the CCMS measurement's name that includes the name of the appropriate CI.

   A CCMS measurement name has the following syntax: **<field1>/<field2>/<field3>**. If the fields in the CCMS name include the name of an R/3 Application Server, System ID, Work Process name, or Database name, the CCMS measurement is attached to the appropriate CI as follows:

<field1>	<field2>	<field3>	Attached to CI
R/3 Application Server name	System ID	Work Process name	Attached to the specified work process
R/3 Application Server name	System ID	N/A	Attached to the specified R/3 application server
System ID	N/A	N/A	Attached to the specified SAP system
System ID	Database name	N/A	Attached to the specified database

For more details about SAP hierarchy, see Chapter 21, “SAP Solution CIs”.

For example, if you have the following CCMS measurements:



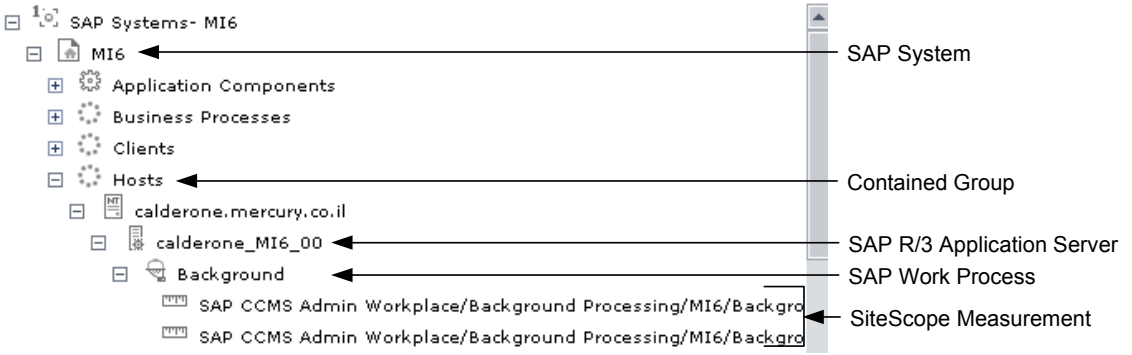
The first three CCMS measurements in the above figure are attached to the Background CI (Work Process) under the R/3 Services CI (R/3 Application Server), under the Host CI.

The other group of measurements are attached to the Dialog Work Process under the R/3 Services (R/3 Application Server) under the Host calderone_MI6_00.

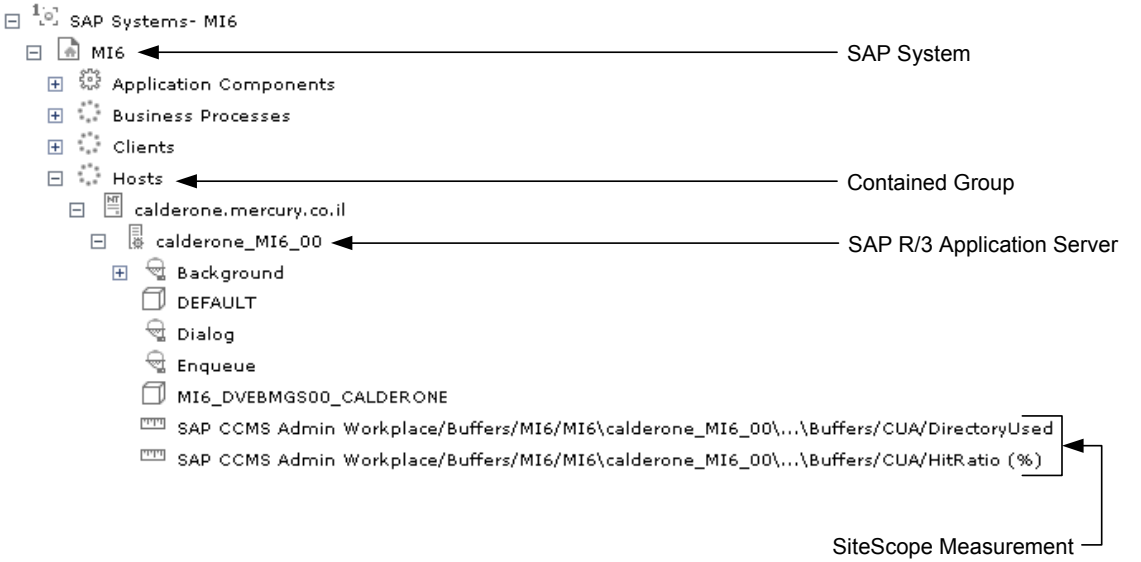
Checking/Viewing the SiteScope Measurements in the SAP View

SiteScope monitors are displayed in the SAP view only if they are connected to hosts. To display them elsewhere in the hierarchy, advanced users must modify the TQL of the SAP System.

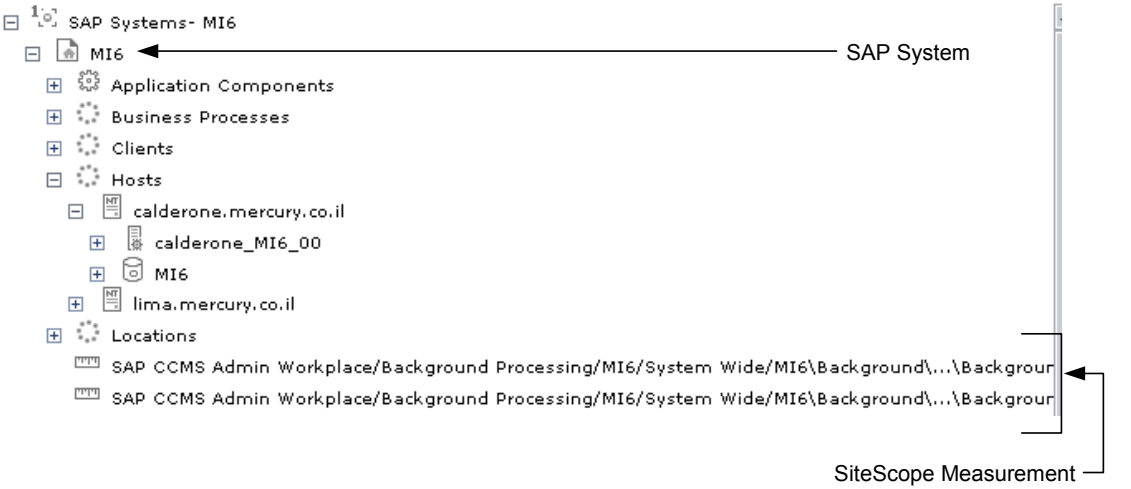
➤ The SiteScope Measurement is displayed under a SAP Work Process CI, under SAP R/3 Application Server CI, under an instance of a Contained Group CI, under a SAP System CI. For example:



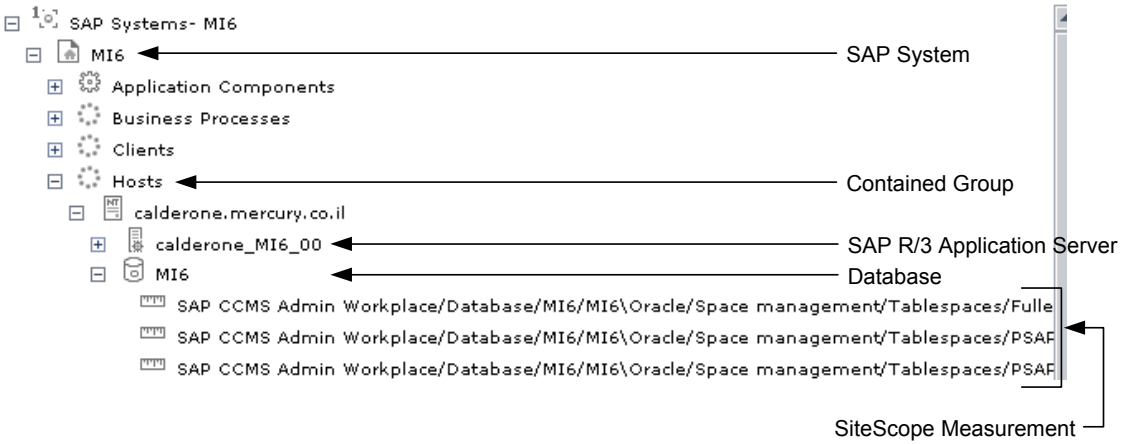
➤ The SiteScope Measurement is displayed under a SAP R/3 Application Server CI, under an instance of a Contained Group CI, under a SAP System CI. For example:



➤ The SiteScope Measurement is displayed under a SAP System CI. For example:



➤ The SiteScope Measurement is displayed under a Database CI, under an instance of a Contained Group CI, under a SAP System CI. For example:



Administering SAP Service

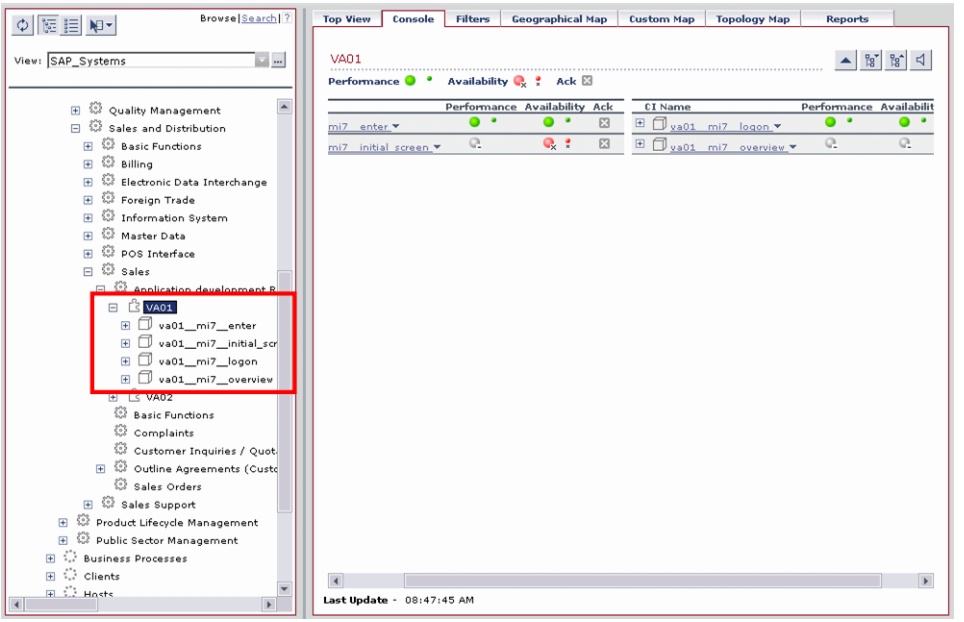
The SAP service is assigned to the Modeling Data Processing Server. It is a configuration service that enables Mercury Business Availability Center to work with data that is in SAP format.

For details about how to view a service status via the JMX Web console, see "High Availability for the Data Processing Server" in *Deploying Servers*.

The SAP Service provides the following advantages:

- Responsible for intelligent relation of monitoring information
- Installed on the modeling processing server (5 server installation)
- Loaded after the CMDB and Viewing System services are loaded
- Registers on 3 TQLs and gets notification on every change in those TQLs
- Check if the service is up/activated in the JMX console – for details, see "Activating the SAP Service" on page 346
- Responsible for automatic linkage of SiteScope measurements or BPM scripts with standardized names – for details, see "Following the Naming Conventions for Naming Business Process Steps" on page 329

- Creating a Business Process and Locations container and connecting the appropriate Business Process Steps to the containers. A Business Process Step connected manually to the SAP transaction would also be connected to those containers – for details, see "Attaching Business Process Steps to a SAP Transaction without Following the Naming Conventions" on page 330.
- Works after BPM and SiteScope source adapters have been synchronized
- Business Process Step that follows the naming convention



Activating the SAP Service

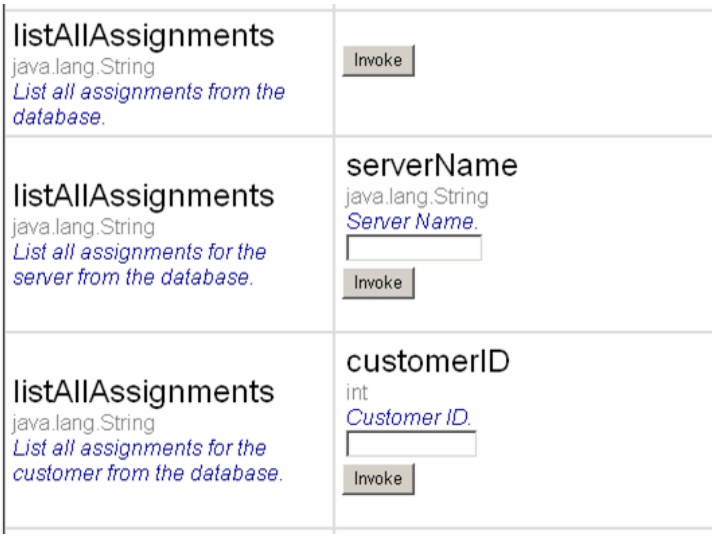
Check that the SAP Service is activated (it is activated by default). If necessary activate it manually.

To view if the SAP Service is activated:

1 In the browser, enter **http://<Mercury_Business_Availability_Center_server_name>:8080/jmx-console/**

2 Double-click **service=hac-manager** listed under **Topaz**.

3 The JMX MBean View for hac-manager opens.



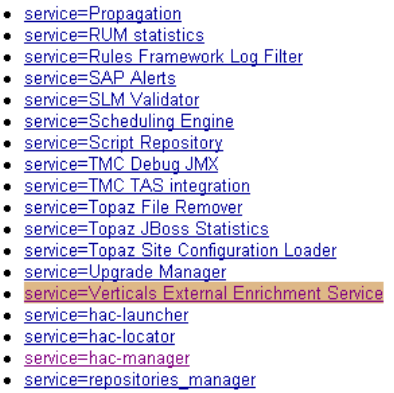
4 Click the **Invoke** button corresponding to the **listAllAssignments** parameter. The result is as follows:

Service	Customer	Process - [Start] - [Ping]	Assigned - [Since] - [Duration]	State - [Since] - [Duration]	Srv. Sign	State Sign
LRDT	-1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:41:21] - [16h:45m:20s]	1	1
CDM	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:47:42] - [16h:38m:59s]	1	1
CMDB	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:41:51] - [16h:44m:50s]	1	1
VIEWSYS	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:42:02] - [16h:44m:39s]	1	1
VERTICALS	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [08/Jun/2006 07:21:25] - [5m:16s]	1	1
PACKAGER	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:46:58] - [16h:39m:43s]	1	1
DASHBOARD	1	smart : mercury_online_engine - [16h:43m:5s] - [3s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:53:42] - [16h:32m:59s]	1	1
NOA	-1	smart : mercury_offline_engine - [16h:43m:6s] - [3s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:43:36] - [16h:43m:5s]	1	1
PM	-1	smart : topaz_pm - [16h:43m:10s] - [18s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:43:33] - [16h:43m:8s]	1	1

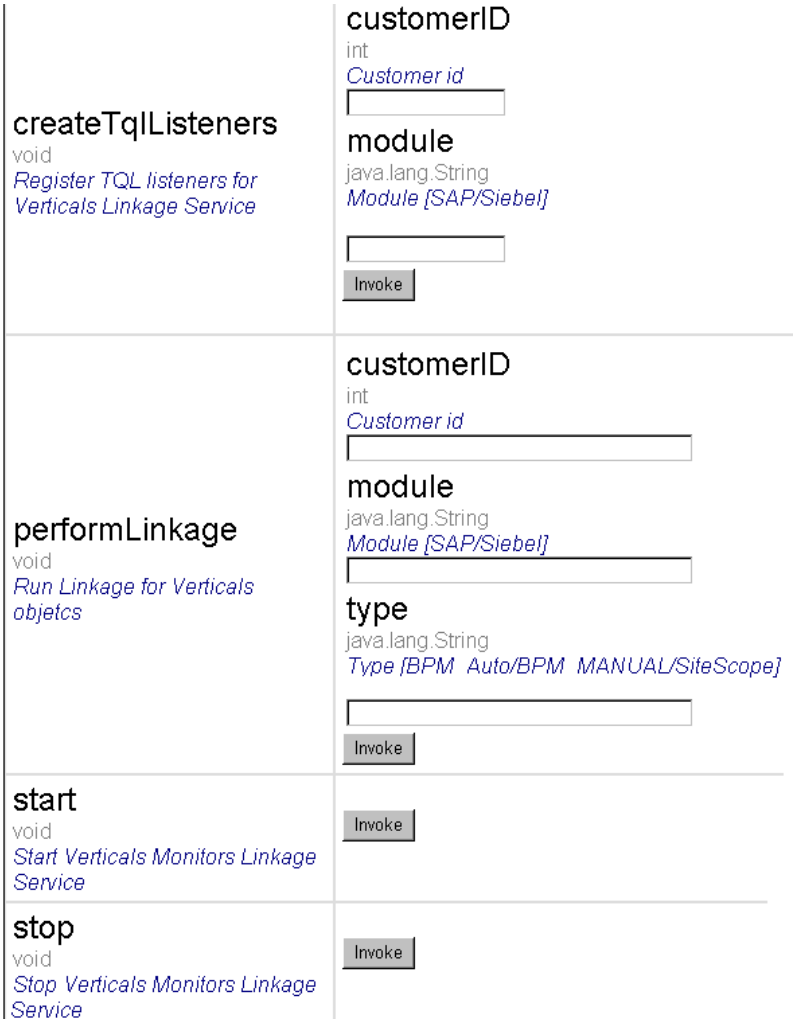
To manually activate the SAP Service:

1 In the browser, enter **http://<Mercury_Business_Availability_Center_server_name>:8080/jmx-console/**

2 Double-click **service=Verticals External Enrichment Service** listed under **Topaz**.



3 The JMX MBean View for Verticals External Enrichment Service opens:



4 Specify:

- **performLinkage** – gets customer ID and the relevant linkage to perform (CCMS/BPM AUTO/BPM manual
- **createTqlListeners** – mainly for debugging

- **Start** – starts the service
- **Stop** – stops the service

Understanding the Change Reports

Changes made to the properties of all types of CIs are discovered by different types of discoveries – for details, see "Running SAP Discovery" on page 279. Those changes are displayed in the Change report available as a right-click menu option for each one of the relevant CI types – for details about the Change report, see "Change Report" in *Using Dashboard*.

Some of the changes made to the SAP Transactions CIs are caused by changes made to the corresponding Transport CIs. Those specific changes are processed by correlation rules in discovery and are displayed in the SAP Transaction Changes report and the SAP Transport Changes report. For details, see "SAP Transaction Changes Report" on page 252 and "SAP Transport Changes Report" on page 254.

23

Troubleshooting the SAP Solution

This chapter provides information that can help troubleshooting the SAP solution.

The SAP KPI Remains Uninitialized

If the SAP KPI remains uninitialized, check these possible solutions in the following order:

1. Make sure the SAP CCMS monitor is set to send samples to Mercury Business Availability Center in the monitor's **Logging to Mercury AM** property in Monitor Administration.
2. Check that the samples arrive to the Business Logic Engine, in the following file:
<Mercury_Business_Availability_Center_root_directory>\log\EJBContainer\TrinitySamples.log
3. Check that the samples arrive to the bus in the following file:
<Mercury_Business_Availability_Center_root_directory>\log\core\dispatcher_log.txt
4. Check that the samples are sent in the following file:
<SiteScope_root_directory>\logs\topaz_all.log.1
5. If you see values in the measurements' KPIs, but they are not colored, check the threshold definition in Monitor Administration.
6. Restart SiteScope, detach it, and reattach it.
7. Check time synchronization between Mercury Business Availability Center and its management database.

CCMS Does Not Manage to Monitor a SAP System

If CCMS does not manage to monitor a SAP System, check these possible solutions in the following order:

1. If you are able to connect to the SAP System using SAP Logon.
2. If yes, run the **rz20** transaction.
3. Open **SAP CCMS Monitor Templates** > **Entire System**, and check if a tree is displayed.
   - ➤ If there is no tree, there might be a problem with the job that is collecting CCMS information. Contact your SAP administrator.
   - ➤ If there is a tree, check that the names of the application server and of the system match, in content and case, the ones used in SiteScope.

The Performance and Availability KPIs Remain Uninitialized

If the Performance and Availability KPIs remain uninitialized, check these possible solutions in the following order:

1. Check that the samples arrive, in the following file: **<Mercury_Business_Availability_Center_root_directory>\log\EJBContainer\TrinitySamples.log**
2. Try and run Business Process Monitor as a specific user.
3. Check time synchronization between Mercury Business Availability Center and its Management database.
4. Check the minute's synchronization between Business Process Monitor and Mercury Business Availability Center.

SAP Business Process Monitor Scripts Do Not Execute

If the SAP Business Process Monitor scripts do not execute, check these possible solutions in the following order:

1. Verify that SAP Logon is installed on the Business Process Monitor server.
2. Make sure that the SAP Business Process Monitor scripts run in Mercury Virtual User Generator (VuGen) and check the script's connection parameters – for details, see "Editing the Script" on page 326.
3. Register dlls under **<Business_Process_Monitor_install_directory>\bin**, as follows:
   - **regsvr32 SapGuiActiveScreen.dll**
   - **regsvr32 SapGuiReplayEvents.dll**
   - **regsvr32 ActiveScreen.dll**

Unable to Log Into Mercury Business Availability Center

If you are unable to log into Mercury Business Availability Center, check these possible solutions in the following order:

1. Check that the last line in the following file:
   <SiteScope_root_directory>\log\jboss_boot.log
   displays the following information: JBoss .... started in ...
2. If you are able to connect using port **8080** explicitly, give the **Read and Execute** permission to **Everyone** for the following dlls in **<Windows_installation_directory>\System32**:
   - **msvcr71.dll**
   - **msvcp71.dll**
   - **mfc71.dll**
   - **atl71.dll**

3 If you have SiteScope installed on the same machine as Mercury Business Availability Center, make sure that Mercury Business Availability Center is already running before you start SiteScope.

Note: It is not recommended to install Mercury Business Availability Center and SiteScope on the same machine.

Part V

Administering the Siebel Solution

24

Deploying the Siebel Solution

This chapter describes how to install Mercury Business Availability Center Siebel solution.

Requirements

- Mercury Business Availability Center 6.2
- Siebel 7.5.3, 7.7, or 7.8
- SiteScope 8.1 or 8.2
- Business Process Monitor 4.5.2 and later
- Discovery Probe 6.2
- The version of Siebel Application Response Measurement Analyzer (SARM) package that is appropriate for the Siebel version you have installed
- The version of Server Manager that is appropriate for the Siebel version you have installed.

Siebel Solution Deployment Workflow

To deploy the Siebel solution use the following workflow:

Check	To do
	Pre-requisites. Ensure that the following software is installed before you install the Siebel solution: ➤ **Discovery Probe.** For details, see *Discovery Manager Administration*. ➤ **SiteScope with the appropriate Siebel license.** For details, see *SiteScope Administration*. ➤ **Business Process Monitor 5.1 or later.** For details, see *Business Process Monitor Admin*. ➤ **Siebel.** For details, refer to Siebel documentation.
	Optional: ➤ **Mercury Application Mapping.** Required if you are using Shared CMDB. For details about installing Mercury Application Mapping, see *Mercury Application Mapping Installation Guide Version 6.2*. For details about the Shared CMDB feature, see "Sharing the Mercury Universal CMDB Environment" in *Working with the CMDB*.
	Enter the appropriate Siebel license in Mercury Business Availability Center. For details, see "Licenses" on page 362.
	Deploy the Siebel_monitoring package. For details, see "Deploying the siebel_monitoring Package" on page 363.
	Copy the srvrmgr tool to the Discovery Probe Server. For details, see "Copying the srvrmgr Tool to the Discovery Probe Server" on page 367.
	Copy SARM Analyzer and srvrmgr tool to the SiteScope Server. For details, see "Copying the srvrmgr Tool and the SARM Analyzer Tool to the SiteScope Server" on page 365.
	Perform Discovery. For details, see Chapter 25, "Performing a Siebel Discovery".
	Record the Business Process Monitor transactions for Siebel. For details, see "Record the Business Process Monitor Transactions for Siebel" on page 368.
	Create a Business Process Monitor profile. For details, see "Using a Business Process Monitor Profile to Simulate SAP Users" on page 321.

Check	To do
	Deploy the Siebel monitors. For details, see "Deploying the Siebel Monitors" on page 409.
	Synchronize the source adapters to enter SiteScope and Business Process Monitor measurements into the CMDB. For details, see "Synchronize the Source Adapters to Enter SiteScope and Business Process Monitor Measurements into the CMDB" on page 369.

Mercury Business Availability Center Siebel solution is ready. After all these steps are completed, you can view Siebel data in the Dashboard, use diagnostic tools, and so forth.

Note: If the SiteScope machine is located outside the Mercury Business Availability Center LAN, the Virtual Private Network (VPN) should be configured to enable SiteScope to communicate with the Centers Server.

Licenses

Add the following licenses:

1. In Mercury Business Availability Center, the license for running the Business Availability Center for Siebel solution.

   This license can be configured in Mercury Business Availability Center as follows: select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**.

2. In Mercury Business Availability Center, the license to enable the necessary amount of Business Process transactions to run.

   This license can be configured in Mercury Business Availability Center as follows: select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**.

3. The license that enables the definition of SiteScope Siebel monitors and deployment of Siebel solution templates. For details, see *SiteScope Administration*.

For details about entering a license in SiteScope, see "Performing an Upgrade Installation" in *SiteScope Administration*.

For details about Siebel solution templates, see "Siebel Solution Templates" in *Configuring SiteScope Monitors*.

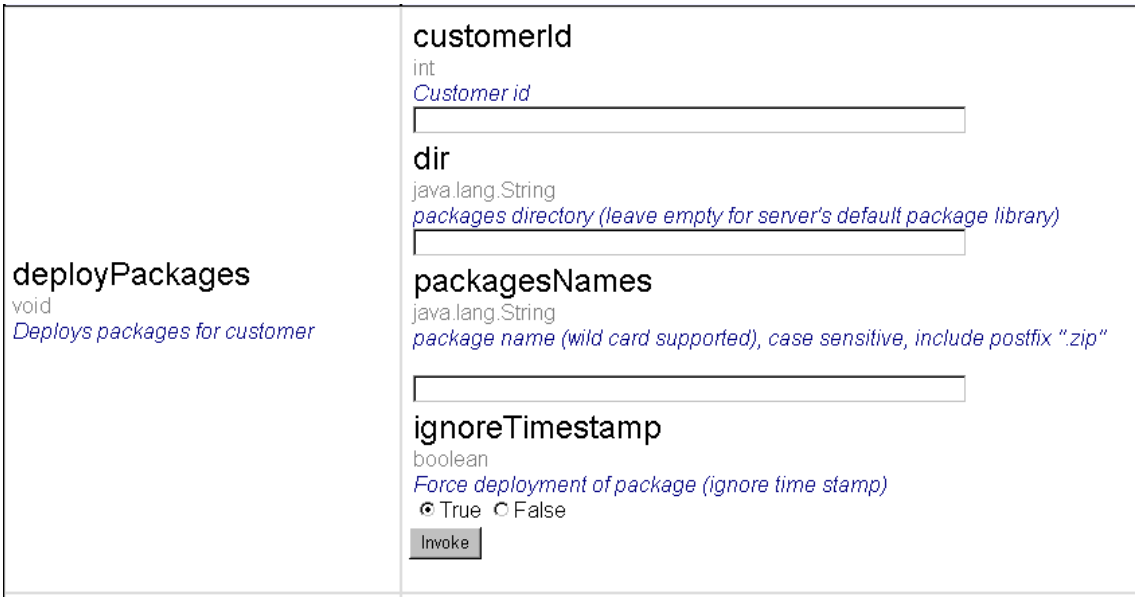
Deploying the siebel_monitoring Package

Before you run the discovery process, start the siebel_monitoring package.

To start the siebel_monitoring package:

1. In the browser, enter **http://<Modeling_server_name>:8080/jmx-console/**
2. Click **service=Package manager** listed under **MAM**.

3 The JMX MBean View for Package manager opens:



4 Specify:

- **customerId.** Enter the Mercury Business Availability Center customer ID.
- **packagesNames.** Enter: **Siebel_monitoring.zip**.

5 Click **Invoke**.

6 To check that the package has been deployed, go to **<Mercury_Availability_Center_home_directory>\log\packaging.log**, check that you have the following entry at the end of the log:
Finished installing package for <customer_ID>.

Copying the srvrmgr Tool and the SARM Analyzer Tool to the SiteScope Server

The SiteScope Siebel monitors require that the srvrmgr tool and the SARM Analyzer tool to be copied to the SiteScope server.

Make sure that you install the appropriate version.

To copy the srvrmgr tool and the SARM Analyzer tool to the SiteScope server:

1 Copy the srvrmgr Command Line Interface (CLI) tool from the Siebel server to a folder on the SiteScope server.

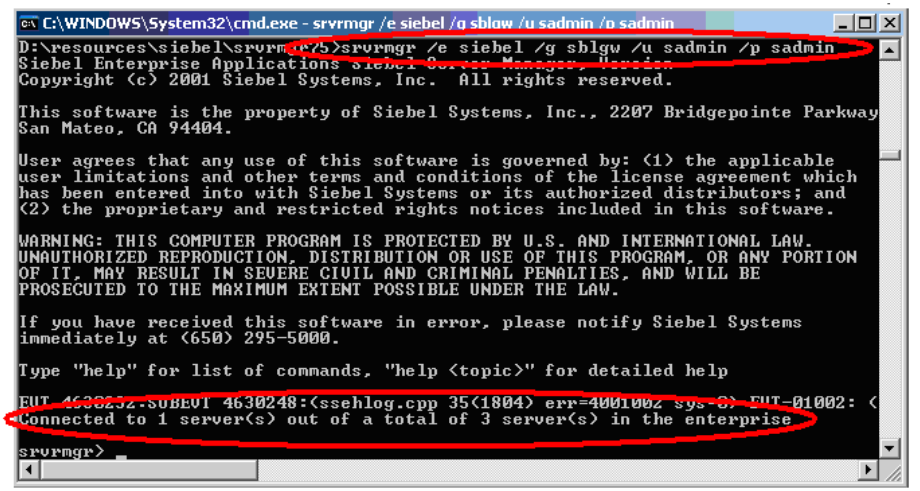
Note: It is recommended to run the Siebel connection test to validate the srvrmgr installation.

---

2 To run a connection test, open the command line on the SiteScope server and change directory to the location of the **srvrmgr.exe** file.

3 Run from the command line:
>srvrmgr /e [site_name] /g [gateway_host] /u [username] /p [password]

If the connection is established successfully, you should see the srvrmgr prompt and the status message about number of connected servers, as follows:



Note: For the connection to work properly you must make sure that the user and password you are using have the correct permission for a remote connection. For details, see below.

Performing the Remote Connection from SiteScope to Siebel

All Siebel servers (Windows and Unix) must be defined as remote servers on SiteScope server.

Copying the srvrmgr Tool to the Discovery Probe Server

Siebel protocol requires that a srvrmgr tool with the appropriate version, be copied to the Discovery Probe server.

Note: Ask the Siebel system administrator to copy the srvrmgr tool to the Discovery Probe machine.

Copying the srvrmgr tool to the Discovery Probe server:

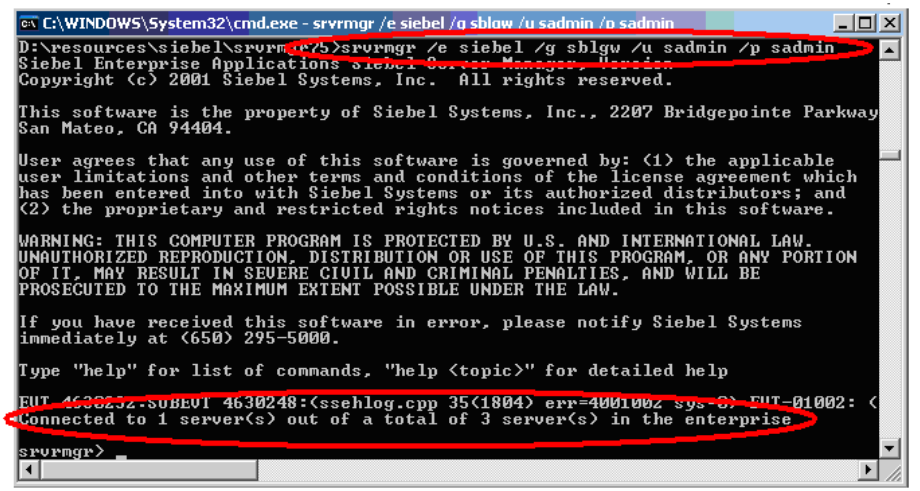
1. Copy the srvrmgr Command Line Interface (CLI) tool form the Siebel server to a folder on the SiteScope server.

Note: It is recommended to run the Siebel connection test to validate the srvrmgr installation.

---

2. To run the connection test, open the command line on the Discovery Probe server and change directory to the location of the **srvrmgr.exe** file.
3. Run from the command line:
>srvrmgr /e [site_name] /g [gateway_host] /u [username] /p [password]

If the connection is established successfully, you must see the srvrmgr prompt and the status message about number of connected servers, as follows:



Record the Business Process Monitor Transactions for Siebel

Make sure that:

- When recording scripts on Siebel you only use the Siebel-Web Multiple protocol (use Multiple Protocol; for details, see “Creating Web Vuser Scripts” in *Using Mercury Virtual User Generator*).
- You record scripts with a special user created for monitoring/diagnostics purposes on Siebel.
- You set a think time separator of 10 seconds for the script transactions used for Siebel diagnostics.

- The VuGen script includes discrete transactions (transactions that do not include **lr_think_time()**) and that it uses the **lr_think_time(…)** functions to separate between the VuGen transactions. The script should not be very long (recommended no more than five transactions per script) since the Diagnostics tools need to run the whole script every time you want to analyze a specific transaction. For example, if a problematic transaction is located close to the end of the script, you would have to run all the previous transactions to reach the problematic one. If you need to record more transactions, record an additional script.
- Sometimes, the Run-Time Settings should be configured for setting appropriate values: **Think-Time-Replay policy**, **Timeout values**, logging options, **Proxy**, **Browser Emulation**, and so forth.

Using a Business Process Monitor Profile to Simulate Siebel Users

Make sure that when creating the profile, to enable the script for Siebel Diagnostic Breakdown, select **Enable Siebel Breakdown** in **Admin** > **Monitor Admin**. For details, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

Synchronize the Source Adapters to Enter SiteScope and Business Process Monitor Measurements into the CMDB

To view data in the Siebel Enterprises view in Dashboard, you must synchronize the Business Process Monitor source adapter and the SiteScope source adapter. For details, see "Actions Buttons" in *Source Manager Administration*.

25

Performing a Siebel Discovery

This chapter describes the steps involved in discovering Siebel.

Note: For details about how to perform a discovery, see "Running the Discovery Process" in *Discovery Manager Administration*.

About Performing a Siebel Discovery

You can run an automatic Siebel discovery to create the Siebel world, with all its components inside Mercury Business Availability Center, using the Siebel patterns.

During the discovery process:

- All discovered Siebel-related configuration items (CIs) are entered into the CMDB. The Siebel-related CIs located in the CMDB are equivalent to actual IT entities that reside in the organization.

- The necessary relationships between the elements are created and saved in the CMDB. These relationships can be used as a baseline, which you can update manually.
- The newly-generated CIs appear in the View Explorer tree when the Siebel Enterprises view is selected and appear under the Siebel Enterprises root node.
- When a new Siebel Application is created, two KPIs are created under it: Transactions and Locations.
- In addition, four logical containers: Applications, Business Processes, Hosts and Locations are also created.
- After the discovery has been performed, you must manually update some of the discovered CI's properties. For details, see "Manual Configuration for Specific Siebel CIs" on page 416.

Running Siebel Discovery

The Siebel discovery process enables you to discover Siebel elements and Siebel topology. The Siebel discovery process consists of the following steps:

- "Step 1 – Preparing for a Siebel Discovery" on page 373
- "Step 2 – Adding a Network CI to Trigger the Discovery of Siebel System Networking" on page 376
- "Step 3 - Accessing the Discovery Modules" on page 381
- "Step 4 - Discovering the Network" on page 382
- "Step 5 – Running the Pre-Discovery Patterns for the Web Tier" on page 383
- "Step 6 – Running the Siebel Discovery" on page 384
- "Step 7 – Checking that Discovery Ran Correctly" on page 385

Steps 1 to 4 are a pre-requisite to the other steps. Steps 5 to 7 discover different Siebel elements and different parts of Siebel topology.

Step 1 – Preparing for a Siebel Discovery

Before you run a Siebel discovery, you must define the protocols as indicated in this section.

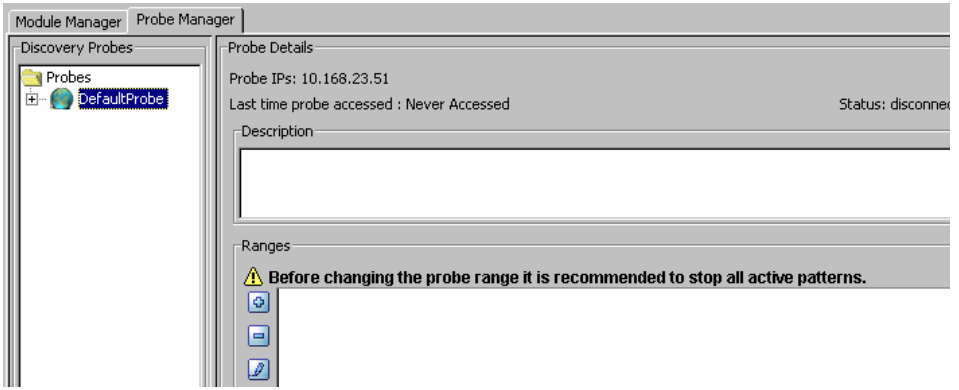
Note: Ensure that the Discovery Probe is running.

To define Siebel protocols, ask the Siebel system administrator for the following information:

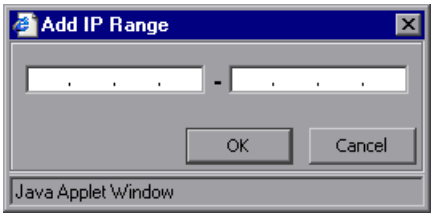
- Siebel enterprise name
- Gateway host
- User name
- Password
- The path to the srvrmgr directory on the Discovery Probe server. For details, see "Copying the srvrmgr Tool to the Discovery Probe Server" on page 367.

To prepare for a Siebel discovery:

1. In Mercury Business Availability Center, select **Admin** > **CMDB**.
2. Click the **Discovery Manager** tab.
3. Click the **Probe Manager** tab.
4. In the Discovery Probes pane, select the relevant domain.



5 Click the **Add IP Range** button to open the Add IP Range dialog box.



6 Enter the range of IP addresses that includes the IP address of the discovery probe. If there is only one address, enter its value in both boxes.

7 Click **OK**.

8 Click the **Add IP Range** button to open the Add IP Range dialog box once more.

9 Enter the range of IP addresses that includes the IP address of the Siebel server(s) you want to discover. If there is only one address, enter its value in both boxes.

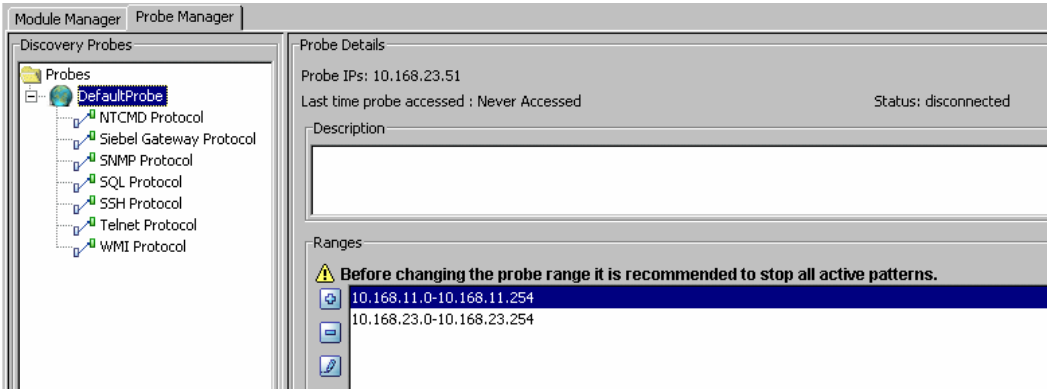
Note: Make sure that all the Siebel servers IP addresses are included in the range.

---

10 Click **OK**.

11 Click **Apply**.

12 Expand the domain:



13 Define the following protocols:

➤ Select **SNMP Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following field:

- **Community.** Enter the value you used when connecting to the SNMP service community you defined while configuring the SNMP service (for example, a community for read only or read/write).

➤ Select **WMI Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:

- **NT Domain.** The name of the domain that includes the host where discovery probe is installed.
- **User Name.** The name of the user you use to connect to the host as administrator.
- **User Password.** The password of the user you use to connect to the host as administrator.

➤ Select **NTCMD Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:

- **NT Domain.** The name of the domain that includes the host where discovery probe is installed.
- **User Name.** The name of the user you use to connect to the host as administrator.

- **User Password.** The password of the user you use to connect to the host as administrator.

➤ Select **Siebel Gateway Protocol**, and click the **Add new connection details for the selected protocol type** button. Populate the following fields:

- **Siebel Enterprise Name.** The name of the Siebel enterprise.
- **srvrmgr path.** The location where you copied **srvrmgr** on the Probe server.
- **User Name.** The name of the user you use to log on to the Siebel system.
- **User Password.** The password of the user you use to log on to the Siebel system.

If you want to discover more than one Siebel System, it is recommended to create separate credentials for each Siebel system with different users and passwords, in the Siebel Gateway Protocol entries page.

If you have several protocol entries with different srvrmgr versions, the client with the newer version should appear before the client with the older version. For example, if you want to discover Siebel 7.5.3. and Siebel 7.7, define the protocol parameters for Siebel 7.7 and then the protocol parameters for Siebel 7.5.3.

14 Click **Apply** to save the changes.

Step 2 – Adding a Network CI to Trigger the Discovery of Siebel System Networking

To trigger the discovery of Siebel System networking features, you must add Network CI to the CMDB.

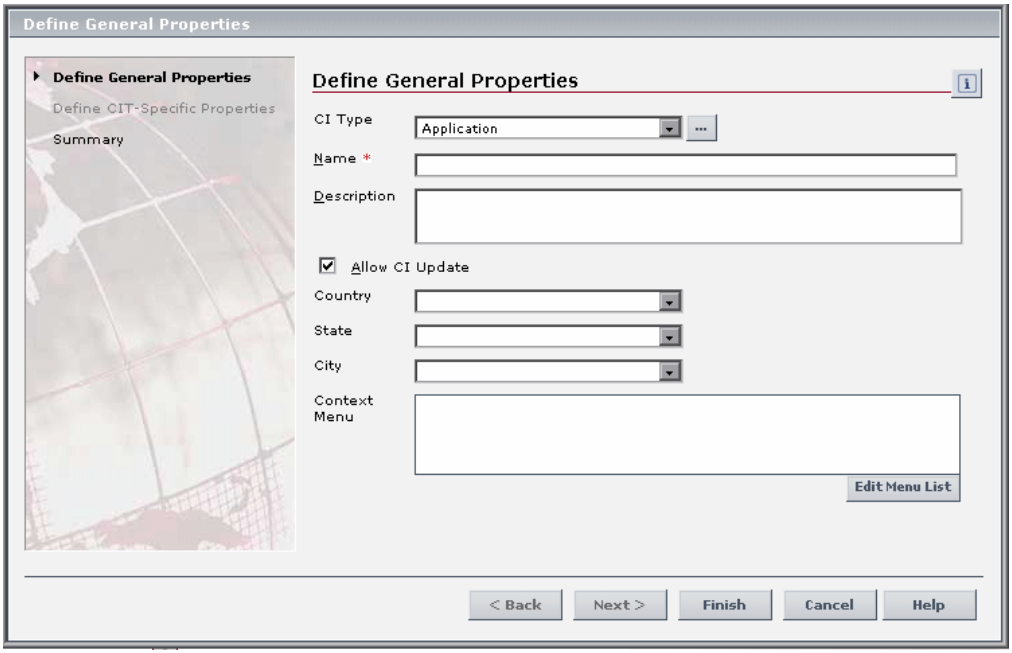
To add Network CI to trigger a discovery of Siebel System networking:

1 In Mercury Business Availability Center, select **Admin** > **CMDB**, and click the **IT Universe Manager** tab in CMDB Administration.

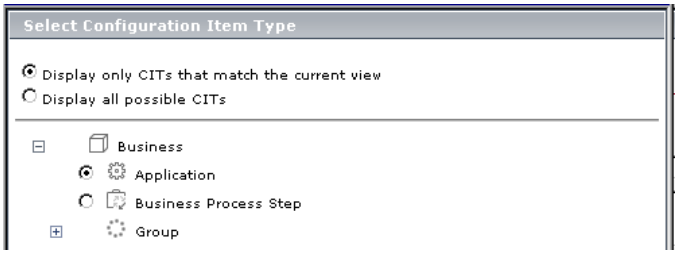
2 Select any view.

3 In the right pane, click **Create new CIs** under How to get started.

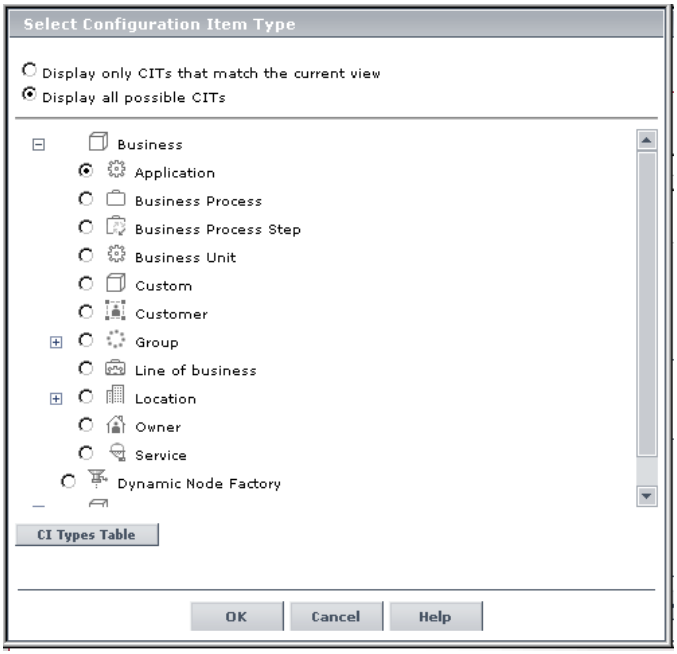
4 A wizard opens.



5 Click the more button to the right of the **CI Type** box, to display the full CI Type list.

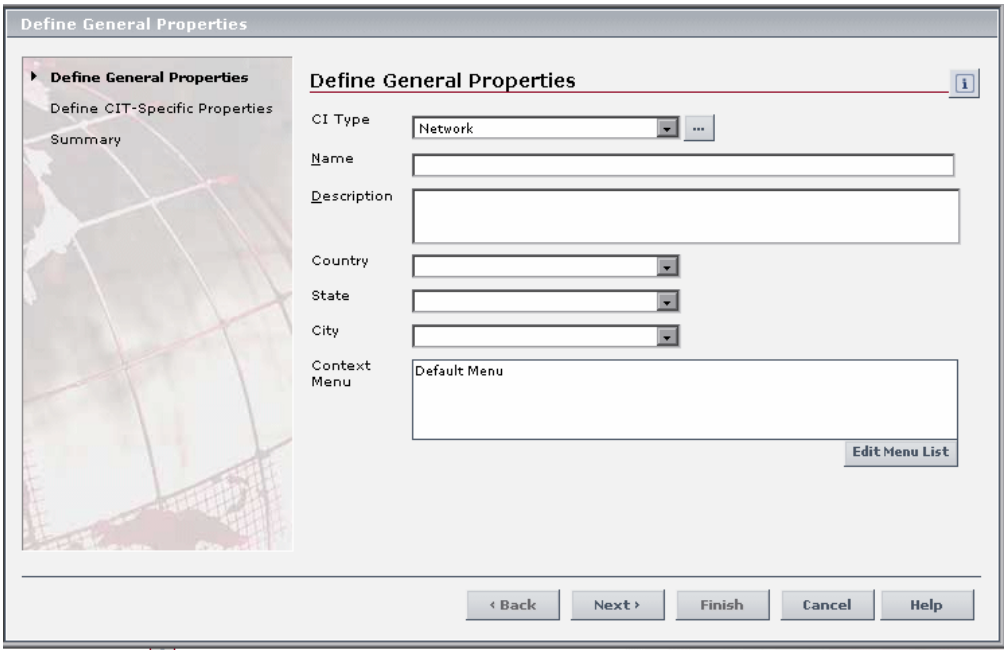


6 Select **Display all possible CITs** to display the list of all possible CITs.

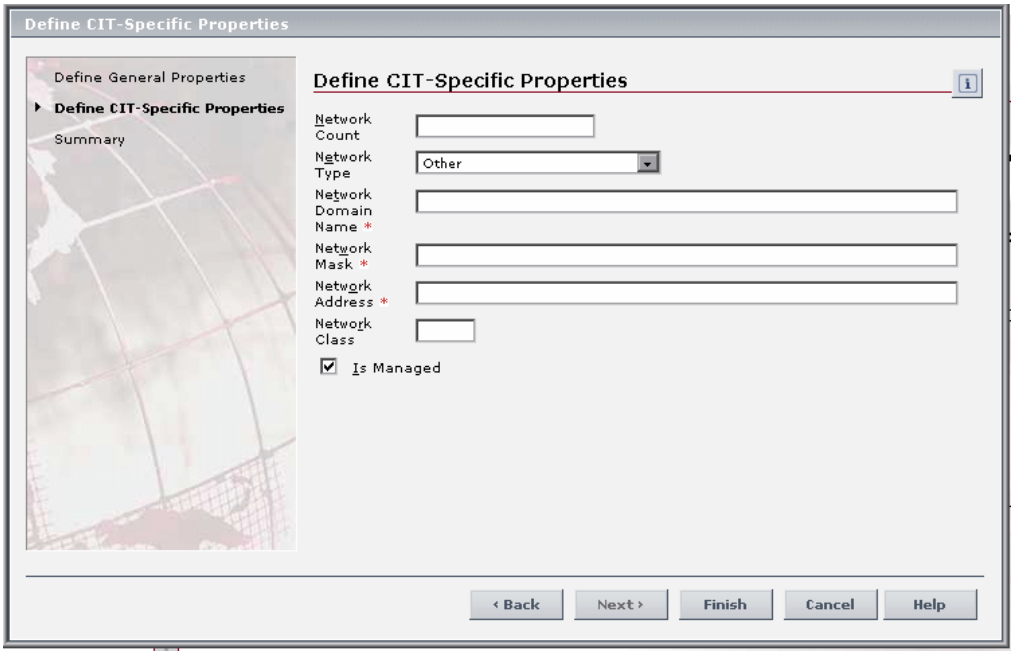


7 Expand **System** and then expand **Network Resource**.

8 Select **Network** and click **OK**. The Define General Properties page opens.



9 Click **Next**.



10 Enter the following information:

- In the **Network Domain Name** box, enter the name of the domain that was specified during the probe's installation.
- In the **Network Mask** box, enter the mask for the IP address of the Siebel System network.
- In the **Network Address** box, enter the IP address of the Siebel system network. For example: 10.168.11.0.

11 Click **Finish** to save the changes.

You should get the following message: Network CI was added successfully.

Step 3 - Accessing the Discovery Modules

Access the discovery modules and then run each discovery pattern in the proper order. You can proceed using two different procedures:

1. The first procedure consists of creating a new module, adding the elements listed below to the new module, and activating the new module.
2. The second procedure consists of selecting and activating the elements listed below one by one, or selecting all the elements and then activating them.

   For details on how to activate a discovery pattern, see *Discovery Manager Administration*.

To access the discovery modules:

1. Click the **Discovery Manager** tab in CMDB Administration.
2. Click the **Module Manager** tab.

Note: It is very important, the first time you run discovery, to start the next pattern only after you verify that the activated pattern has successfully discovered all the required elements.

---

3. Go to the next procedure.

Step 4 - Discovering the Network

To run the discovery patterns, you must trigger them in the order described in this section. Each discovery pattern discovers different components – for details on the components and their hierarchy structure, see "CIs Discovered by the Discovery Process" on page 386.

To discover the network:

1 In the **Module Manager** tab, proceed as follows:

Expand Module	Activate Pattern	Description
Network - Basic	**ICMP_NET_Dis_IpC**	Discovers which machines are active in the range of given IP addresses by pinging the machines in the IP address range that you provided in "Step 1 – Preparing for a Siebel Discovery" on page 373.
Network - Protocol Connections	**NTCMD_NET_Dis_Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the NTCMD protocol.
Network - Protocol Connections	**WMI_NET_Dis_Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the WMI protocol.
Network - Protocol Connections	**TTY_NET_Dis_Connection**	Discovers, in the range of given IP addresses, the hosts that communicate using the SSH/Telnet protocol.

Step 5 – Running the Pre-Discovery Patterns for the Web Tier

This step must be performed before the discovery takes place.

To run the discovery patterns, you must trigger them in the order described in this section. Each discovery pattern discovers different components – for details on the components and their hierarchy structure, see "CIs Discovered by the Discovery Process" on page 386.

To run the discovery:

1 In the **Module Manager** tab, proceed as follows:

Expand Module	Activate Pattern	Description
Network - Advanced	**TCP_NET_Dis_Port**	Discovers the http_80 port server's open active ports. If the port is not 80, the discovery procedure update the **portNumberToPortName.xml** file.
Host Resource-Registry	**NTCMD_HR_Reg_ Software**	Discovers the installation path of the Siebel Web Server Extension.
Web Server - Basic	**TCP_Webserver_ Detection**	Discovers the Web servers running on this host. If the Siebel system you are discovering has an ITS configuration and you want to discover the ITS entities of the Siebel system, run this pattern as a pre-requisite to the Siebel discovery that discovers ITS entities.

2 Click the **Activate** button to start the discovery.

Step 6 – Running the Siebel Discovery

Siebel discovery can be performed using Discovery Manager by activating all the patterns in the Siebel module. The patterns are scheduled to run every 24 hours.

You can select all the discovery patterns and activate them at once. Each discovery pattern discovers different components. For details on the components and their hierarchy structure, see "CIs Discovered by the Discovery Process" on page 386.

To run the discovery:

1 In the **Module Manager** tab, proceed as follows:

Expand Module	Activate Pattern	Description
Application - Siebel	**SIEBEL_DIS_ WEBAPPS_NT** (for Windows platform) **or SIEBEL_DIS_ WEBAPPS_UNIX** (for Unix platform)	Discovers the Siebel Web Server Extensions, Siebel Web Application, and Siebel Gateway CIs. Siebel Gateway CIs are discovered by the **SIEBEL_DIS_WEBAPPS_NT** discovery pattern when the load balancing of web requests is performed by the gateway
Application - Siebel	**SIEBEL_DIS_ GATEWAY_ CONNECTION (GTWY)**	Select this pattern if load balancing of web requests is not performed by the gateway but by an external load balancer Discovers Siebel Gateway CIs.
Application - Siebel	**SIEBEL_DIS_APP_ SERVERS**	Discovers Siebel Application Server, Component Group, and Component CIs.
Application - Siebel	**SIEBEL_DIS_APP_SER VER_CONFIG**	Discovers the **Siebel.cfg** file.
Application - Siebel	**SIEBEL_DIS_DB_NT** (for the Windows platform) or **SIEBEL_DIS_DB_ UNIX** (for the Unix platform)	Discovers the Siebel Database CIs.

2 Click the **Activate** button to start the discovery.

3 Note that the following enrichment patterns are automatically running in the background while the discovery is taking place:

- **Siebel_Route_WebApp_To_Component.** Builds the route between Siebel Web Application CIs and Siebel Component CIs
- **Siebel_Web_To_Middle_Tier.** Builds the route between the web tier and the middle tier when the Siebel system uses a Resonate server for load balancing.

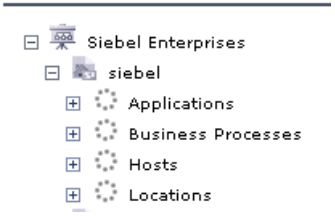
Step 7 – Checking that Discovery Ran Correctly

After running all the discovery patterns, check that all the information in the Siebel view is displayed correctly.For information on which CIs are discovered, see "CIs Discovered by the Discovery Process" on page 386.

To check that the discovery ran correctly:

Select **Application** > **Dashboard**, click the **Console** tab, and open the Siebel Systems view or **Admin** > **CMDB**, and click the **IT Universe Manager** tab.

The view is as follows:



Note: Some of the properties of some of the CIs must be entered manually in order for data to be inserted properly in the Siebel Enterprises view. For details, see "Manual Configuration for Specific Siebel CIs" on page 416.

CIs Discovered by the Discovery Process

The following Siebel CIs are discovered:

Siebel Entities/CIs	Icon	Description
Web Server		Represents the Web server that forwards requests to the Siebel system. Currently, Siebel discovery discovers IIS and SunOne (iPlanet).
Siebel Web Server Extension		Represents the Siebel Web Server Extension installed on the web server.
Siebel Web Application		Represents the application URL that appears in Siebel Web Server Extension.
Siebel Enterprise		Logical grouping of Siebel Application Servers that support the same group of users accessing a common database server.
Siebel Gateway		The Siebel gateway server provides enhanced scalability, load balancing, and high-availability across the site.
Siebel Application Server		The middle-tier platform that supports both back-end and interactive processes for every Siebel client.
Siebel Component Group		A certain type of application running on the Siebel Application Server.
Siebel Component		A process on the Siebel Application Server encapsulating some Siebel application functionality

Siebel Entities/CIs	Icon	Description
Database		The Database CI represents the database that is holding the data tier. This is not a Siebel-specific CI.
Configuration Files		The Configuration File CIs represent the **siebel.cfg** configuration file that includes information from the application server installation or the **parameters.cfg** that includes the output of the **list parameters for component** command using srvrmgr.

This section includes the following topics:

Siebel Enterprise

The Siebel Enterprise CI represents a group of servers that function together to build a complete Siebel toolset experience.

The default KPIs are:

KPIs	Description	Source
Availability	Indicates the availability of Siebel transactions. For details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Locations	A bar that includes up to six colored sections. Each colored section represents the amount of locations with the status corresponding to the section's color, from which Siebel-related transactions are running. For details, see "Locations" in *Repositories Administration*.	Business Process Monitor
Performance	Indicates the performance of Siebel transactions. For details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Sessions	Displays the sum of running sessions measurement on all underlying hosts (a session is a task that is in running mode and interactive state), provided by the SiteScope measurement. The resulting display is a number that is colored according to the objectives set for the rule. For details, see "Sessions" in *Repositories Administration*.	SiteScope Siebel monitor
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor

KPIs	Description	Source
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth). For details, see "System" in *Repositories Administration*.	SiteScope
Transactions	A bar that includes up to six colored sections. Each colored section represents the relative amount of Business Process Steps with the end-user experience status (the worst status between **Performance** and **Availability**) that corresponds to the color. For details, see "Transactions" in *Repositories Administration*.	Business Process Monitor

Contained Group

The Group CI is a logical container. This is not a Siebel-specific CI. The Siebel Enterprises view includes the following groups: Applications, Business Processes, Hosts, and Locations.

The default KPIs are:

KPIs	Description	Source
Availability	Indicates the availability of Siebel transactions. For details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Locations	A bar that includes up to six colored sections. Each colored section represents the amount of locations with the status corresponding to the section's color, from which Siebel-related transactions are running. For details, see "Locations" in *Repositories Administration*.	Business Process Monitor

KPIs	Description	Source
Performance	Indicates the performance of Siebel transactions. For details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Sessions	Displays the sum of running sessions measurement on all underlying hosts (a session is a task that is in running mode and interactive state), provided by the SiteScope measurement. The resulting display is a number that is colored according to the objectives set for the rule. For details, see "Sessions" in *Repositories Administration*.	SiteScope Siebel monitor
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth). For details, see "System" in *Repositories Administration*.	SiteScope
Transactions	A bar that includes up to six colored sections. Each colored section represents the relative amount of Business Process Steps with the end-user experience status (the worst status between **Performance** and **Availability**) that corresponds to the color. For details, see "Transactions" in *Repositories Administration*.	Business Process Monitor

Siebel Application

The Siebel Application CI represents the Siebel complete solution for an organization's needs in a certain area. For example: marketing, call center, and so forth.

The default KPIs are:

KPIs	Description	Source
Availability	Indicates the availability of Siebel transactions. For details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Performance	Indicates the performance of Siebel transactions. For details, see "Performance" in *Repositories Administration*.	Business Process Monitor
Sessions	Displays the sum of running sessions measurement on all underlying hosts (a session is a task that is in running mode and interactive state), provided by the SiteScope measurement. The resulting display is a number that is colored according to the objectives set for the rule. For details, see "Sessions" in *Repositories Administration*.	SiteScope Siebel monitor

Business Process Step

The Business Process Steps (BPM transactions inside a script) CIs are emulated Siebel transactions executed on a Business Process Monitor machine. They are used to supply proactive monitoring of end user experience.

The default KPIs are:

KPIs	Description	Source
Availability	Indicates the availability of Siebel transactions. For details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Performance	Indicates the performance of Siebel transactions. For details, see "Performance" in *Repositories Administration*.	Business Process Monitor

Contained Location

The Contained Location CIs are created as part of the Business Process Monitor hierarchy when working with the **Transactions/locations** option. They represent the location to which the BP Steps are referenced. Those BP Steps correspond only to the transactions that analyze Siebel.

The default KPIs are:

KPIs	Description	Source
Availability	Indicates the availability of Siebel transactions. For details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Performance	Indicates the performance of Siebel transactions. For details, see "Performance" in *Repositories Administration*.	Business Process Monitor

BPM Transaction/Location

The BPM Transaction/Location CIs represent a BP Step/Location intersection (a specific transaction running at a specific location).

The default KPIs are:

KPIs	Description	Source
Availability	Indicates the availability of Siebel transactions. For details, see "Availability" in *Repositories Administration*.	Business Process Monitor
Performance	Indicates the performance of Siebel transactions. For details, see "Performance" in *Repositories Administration*.	Business Process Monitor

Host

A Host CI represents the physical machine on which a server is installed. This is not a Siebel-specific element.

The default KPIs are:

KPIs	Description	Source
Sessions	Displays the sum of running sessions measurement on all underlying hosts (a session is a task that is in running mode and interactive state), provided by the SiteScope measurement. The resulting display is a number that is colored according to the objectives set for the rule. For details, see "Sessions" in *Repositories Administration*.	SiteScope Siebel monitor
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth). For details, see "System" in *Repositories Administration*.	SiteScope

Web Server

The Web Server CI represents a standard web server. This is not a Siebel-specific element.

The default KPIs are:

KPIs	Description	Source
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth). For details, see "System" in *Repositories Administration*.	SiteScope

Siebel Web Server Extension

The Siebel Web Server Extension CI represents the Siebel extension to a web server, running the Siebel Web tier.

The default KPIs are:

KPIs	Description	Source
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor

Siebel Web Application

The Siebel Web Application CI represents the location of the Siebel application on the Siebel Web Server Extension.

The default KPIs are:

KPIs	Description	Source
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor

Siebel Gateway

The Siebel Gateway CI represents a coordinating server that routes requests to the correct component.

This CI does not have KPIs.

Siebel Application Server

The Siebel Application Server CI represents a server running the business logic tier.

The default KPIs are:

KPIs	Description	Source
Sessions	Displays the sum of running sessions measurement for that specific application server (a session is a task that is in running mode and interactive state), provided by the SiteScope measurement. The resulting display is a number that is colored according to the objectives set for the rule. For details, see "Sessions" in *Repositories Administration*.	SiteScope Siebel monitor
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor
Tasks in Error	Displays the number of tasks that are in error, provided by the SiteScope Number of tasks in error measurement. For details, see "Tasks in Error" in *Repositories Administration*.	Siebel monitor

Siebel Component Group

The Component Group CI represents an administrative grouping of components running on the Siebel Application Server.

The default KPIs are:

KPIs	Description	Source
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor

Siebel Component

The Component CI represents a process running on the Siebel Application Server, which encapsulates some Siebel application functionality.

The default KPIs are:

KPIs	Description	Source
Sessions	Displays the sum of running sessions measurement for that specific component (a session is a task that is in running mode and interactive state), provided by the SiteScope measurement. The resulting display is a number that is colored according to the objectives set for the rule. For details, see "Sessions" in *Repositories Administration*.	SiteScope Siebel monitor

KPIs	Description	Source
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor
Tasks in Error	Displays the number of tasks that are in error, provided by the SiteScope measurement Number of Tasks in Error measurement. For details, see "Tasks in Error" in *Repositories Administration*.	Siebel monitor

Database

The Database CI represents the database that is holding the data tier. This is not a Siebel-specific CI.

The default KPIs are:

KPIs	Description	Source
System	Indicates physical problems with underlying hosts, provided by SiteScope physical monitors (for example: CPU monitor, disk space monitor, and so forth). For details, see "System" in *Repositories Administration*.	SiteScope

SiteScope Measurement

The SiteScope Measurement CI is not a Siebel-specific CI. However, in the Siebel Enterprises view, it usually represents a metric of a Siebel monitor. For example, the Application Server monitor.

The default KPIs are:

KPIs	Description	Source
Siebel	Provides Siebel-specific data such as number of tasks, processes, and so forth. For details, see "Siebel" in *Repositories Administration*.	SiteScope Siebel monitor

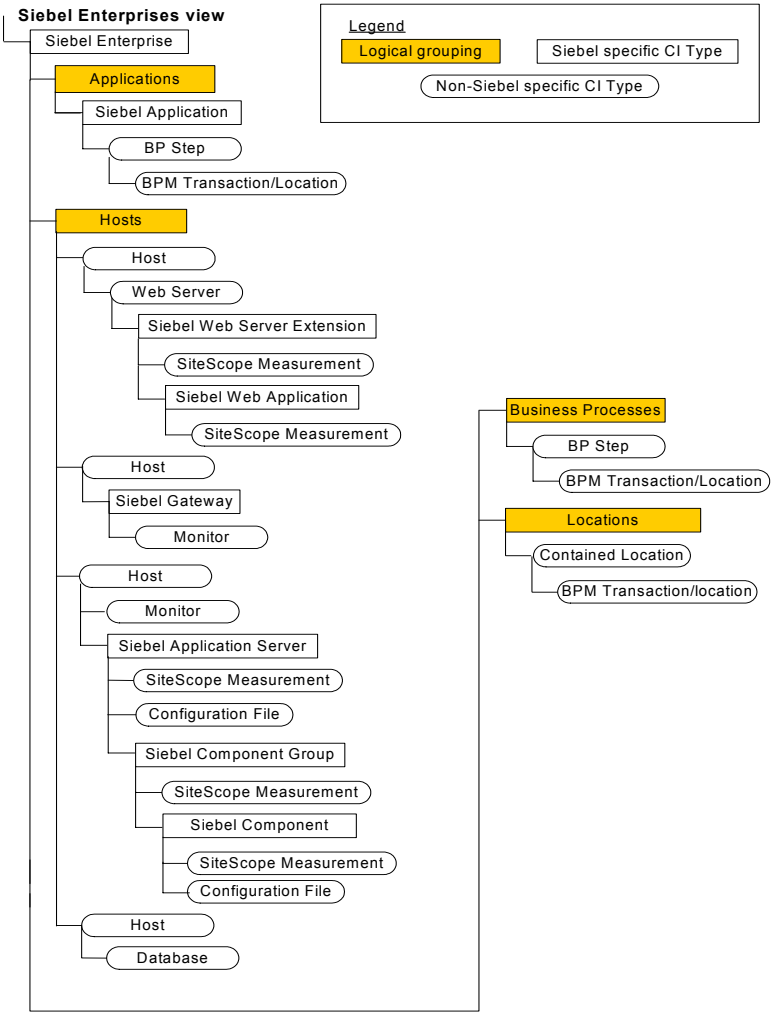
Configuration File

The Configuration File CIs represent the **siebel.cfg** configuration file that includes information from the application server installation or the **parameters.cfg** that includes the output of the list parameters for component command using srvrmgr.

The Configuration File CIs have no KPIs.

Hierarchy

The CIs hierarchy is as follows:



26

Configuring the Siebel Solution

This chapter describes the steps involved in configuring the Mercury Business Availability Center Siebel solution that you use to monitor Siebel enterprises.

About Configuring the Siebel Solution

To monitor your Siebel eBusiness applications and servers using Business Availability Center for Siebel, you must first set up the Siebel monitoring environment by performing the following steps:

1 **Create Business Process profiles that emulate Siebel application users.**

For information on creating Business Process Monitor profiles, see "Using a Business Process Monitor Profile to Simulate Siebel Users" on page 405.

2 **Manually configure some of the parameters in the discovered CIs.** For details, see "Manual Configuration for Specific Siebel CIs" on page 416.

3 **Deploy SiteScope monitors for the Siebel templates using the MDW.** For details, see "Deploying the Siebel Monitors" on page 409.

Note:

- If you are a system administrator, you may want to perform advanced configuration procedures on the Infrastructure Settings Manager page. To access the page, click **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, and select **Siebel** in the **Applications** context.
- To see the breakdown features for Business Process Monitor scripts you must upgrade the Business Process Monitor using the Siebel Web scripts for which you want to see transaction breakdown, to the appropriate version. For details, see "Deploying Business Process Monitor" in *Business Process Monitor Administration*.
- To see Siebel Application Response Measurement (SARM) data coloring BP steps in the Mercury Business Availability Center Siebel solution SARM tool, you must also select **Enable Siebel Breakdown** in **Admin** > **Monitor Admin**. For details, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

Using a Business Process Monitor Profile to Simulate Siebel Users

Business Process Monitor profiles are used to simulate Siebel users To obtain performance and availability information on the Siebel transactions.

You can view Business Process Steps under the Siebel view to enable you to analyze what happens in the Siebel system.

This section includes the following topics:

Creating a Business Process Monitor Profile

You create Business Process profiles in Monitor Administration – for details, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*.

In Mercury Virtual User Generator (VuGen), Siebel scripts are recorded using the Siebel-Web protocol. You must select the Siebel-Web protocol when you create a new script – for details, see "Creating New Virtual User Scripts" in *Using Mercury Virtual User Generator*.

To select the appropriate protocol:

1. In VuGen, select **New** to open the New Virtual User page.
2. Select **New Single Protocol Script**.
3. Select the **Siebel-Web** protocol.

Synchronizing the Business Process Monitoring Source Adapter

You can synchronize the Business Process Monitoring source adapter immediately or you can wait for the automatic synchronization to take place – for details, see "Business Process Monitoring" in *Source Manager Administration*.

Attaching Business Process Monitor Transactions to Siebel Application Components

To display Performance and Availability information on Siebel applications, Business Process Steps must be attached to Siebel Application CIs.

You can connect Business Process Steps to a Siebel application in two different ways:

- by following the naming conventions for the Business Process Steps names. For details, see "Following the Naming Conventions for Naming Business Process Steps" on page 406.
- by **not** following the naming conventions for the Business Process Steps names. In this case, you must manually link a Business Process Step to a Siebel application. For details, see "Attaching Business Process Steps to a Siebel Application CI without Following the Naming Conventions" on page 407.

  If you do not follow the naming conventions, be careful when deleting links between Siebel applications and Business Process Steps. For details, see "Deleting Links Between Siebel Applications and Business Process Steps" on page 408.

Following the Naming Conventions for Naming Business Process Steps

To automatically connect Business Process Steps to a Siebel application, the Business Process Step name should have the following format:
<app_name>_ _<ent_name>_ _<BPM_tran_name>

- **app_name.** The name, in lowercase, of the Siebel application to which you want to attach the Business Process Step.
- **ent_name**. The name, in lowercase, of the Siebel enterprise on which the application is run.
- **BPM_tran_name.** The unique name of the Business Process Step. Any set of alphanumeric and mixed case characters are supported (special characters are not allowed). It is good practice to name the transaction so that the name indicates what occurs in it.

Note: You assign the appropriate name to a Business Process Step when you record it – for details, see "Recording with VuGen" in *Using Mercury Virtual User Generator*.

Attaching Business Process Steps to a Siebel Application CI without Following the Naming Conventions

After you have built a Business Process Monitor profile, you must manually connect Business Process Steps with Siebel Application CIs.

To attach Business Process Steps to a Siebel Application CI without following the naming convention:

1. Select **Admin** > **CMDB**.
2. Click the **IT Universe Manager** tab.
3. Select **Siebel Enterprises** in the **View** list.
4. Right-click the Siebel Application CI that you want to monitor using the BPM profile and select **Attach Related CI** to open the **Attach Related CIs** wizard.
5. Select **Monitors View** in the **Views** list.
6. Expand and select the Business Process Step to which you want to connect the Siebel Application CI. You can select more than one.
7.  Click the right arrow to move the CI to the right-hand box.
8. Click **Next**.
9. In the **Relationship Type** list, select **Monitoring By Siebel**.
10. Select **Allow CI Update.**
11. Click **Finish**.

Deleting Links Between Siebel Applications and Business Process Steps

SiteScope measurements and Business Process Monitor transactions are attached under the appropriate level of the Siebel hierarchy – for details, see "Hierarchy" on page 401.

A TQL runs in the background and returns:

- **Business Process Monitor transactions that are not attached to a Siebel entity and follow the naming convention** – the name of the Business Process Monitor transaction indicates to which Siebel entity it should be attached – for details about the naming convention, see below.
- **Business Process steps that are manually attached to a Siebel transaction** – a Business Process Step is automatically attached to the Business Process container that was created by the Business Process Step, the Business Process Step is monitored by Siebel – for details, see "Attaching Business Process Steps to a Siebel Application CI without Following the Naming Conventions" on page 407.

  If the Business Process Monitor source adapter was assigned the **Transaction/Location** option (for details, see "Business Process Monitoring" in *Source Manager Administration*) a copy of the location information is attached to the Locations container.

  If you delete a link between a Siebel transaction and its child Business Process Step transaction, then the following happens:

- If you followed the naming convention for the Business Process Step transaction, the link between the Siebel transaction and its child Business Process Step is automatically recreated at the next synchronization.
- If you did not follow the naming convention and created a manual link between the Siebel transaction and a Business Process Step transaction, then when you delete the link:
  - if the Business Process Monitoring source adapter was assigned the **Transactions/locations** option, the Contained Location CI is not deleted.

You can manually delete it. Delete the Contained Location CI only if the deleted Business Process Step transaction is the only CI attached to this location. If other Business Process Step transactions are attached to this location, delete only the links between the Business Process Monitor (BPM transaction from location) and the Location container.

- if the Business Process Monitoring source adapter was assigned the **Regular** option, the Business Process container is not deleted. You must manually delete the links between the Business Process container and the detached Business Process Step transaction.

For details about the **Transactions/locations** or **Regular** options, see "Business Process Monitoring" in *Source Manager Administration*.

Deploying the Siebel Monitors

There are two ways of deploying the Siebel monitors:

- Using the Monitor Deployment Wizard to deploy SiteScope monitors.
- Running one or more of the Siebel solution templates.

This section includes the following topics:

- "Deploying Siebel Monitors Using the Monitor Deployment Wizard" on page 409
- "Deploying Siebel Monitors Using the Siebel Solution Templates" on page 411

Deploying Siebel Monitors Using the Monitor Deployment Wizard

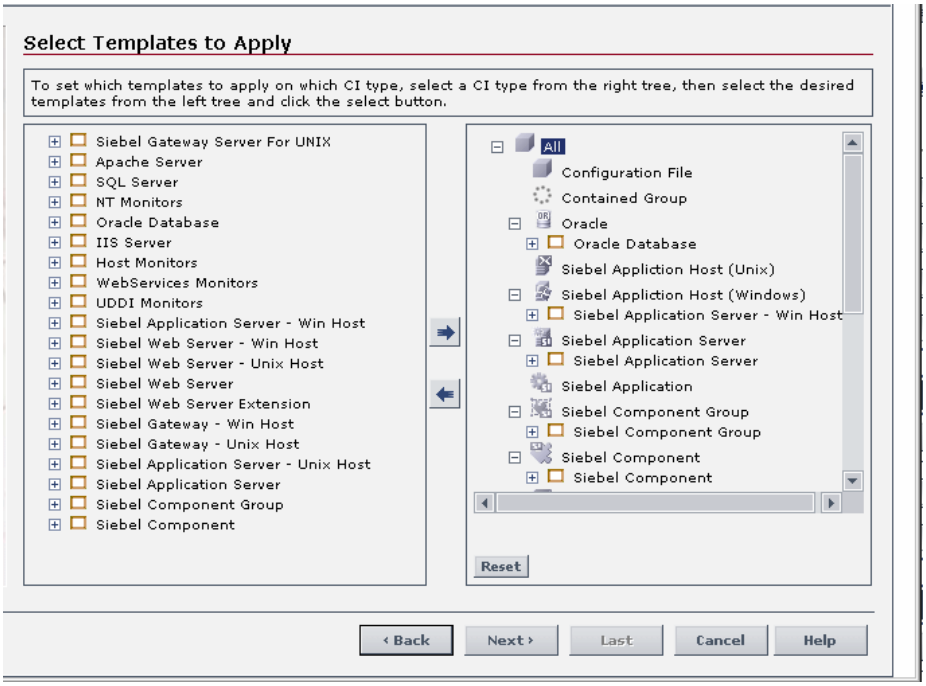
Use the Monitor Deployment Wizard to deploy Siebel monitors.

To deploy Siebel Monitors Using the Monitor Deployment Wizard:

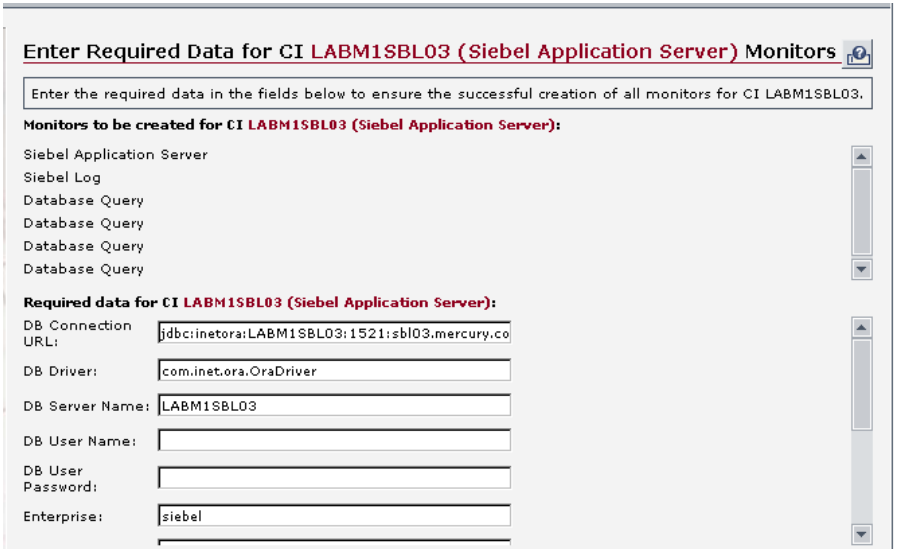
1 Follow the wizard as indicated in "Monitor Deployment Wizard" in *Configuring SiteScope Monitors*.

In the Select Templates to Apply page, note that the right pane lists the CI Types of all the CIs selected in the previous page.

If the wizard was able to match templates to the selected CI Types, the CI Type is listed with the applicable template as a child object.



2 In the Enter Required Data for CI page, enter the following information:



- In the **DB User Name** box, enter the name of the user used to login the database located on the Siebel server.
- In the **DB User Password** box, enter the password of the user used to login the database located on the Siebel server.

3 Proceed with the wizard as indicated in "Monitor Deployment Wizard" in *Configuring SiteScope Monitors*.

Deploying Siebel Monitors Using the Siebel Solution Templates

To create a SiteScope monitor that can monitor a Siebel Enterprise site, you can run one or more of the following dedicated solution templates:

- **Siebel Application Server Solution Template.** The SiteScope Siebel Application Server Solution Template provides tools you use to monitor the availability, usage statistics, and server performance statistics for Siebel Application servers installed on Windows platforms. This solution template will deploy a set of monitors that test the health, availability, and performance of Siebel Application Servers.

  For details about running the solution template, see "Using the Siebel Application Server Solution Template" in *Configuring SiteScope Monitors*.

- **Siebel Gateway Server Solution Template.** The SiteScope Siebel Gateway Server Solution allows you to monitor the availability and server statistics for Siebel Gateway servers installed on Windows platforms.

  This solution template will deploy a set of monitors that test the health, availability, and performance of Siebel Gateway Servers. You can use this solution template to deploy monitors for server-wide resources and metrics.

  For details about running the solution template, see "Using the Siebel Gateway Server Solution Template" in *Configuring SiteScope Monitors*.

- **Siebel Web Server Solution Template.** The SiteScope Siebel Web Server Solution allows you to monitor the availability and server statistics for Siebel Web servers installed on Windows platforms. This solution template will deploy a set of monitors that test the health, availability, and performance of Siebel Web Servers.

  For details about running the solution template, see "Using the Siebel Web Server Solution Template" in *Configuring SiteScope Monitors*.

Provide the Appropriate Path to SiteScope

If you are using the Siebel Application Server monitor (which is part of the Application Server solution template), and Mercury Business Availability Center sends a request for information to SiteScope, a temporary monitor is created, run, and then erased. Access to SiteScope is done using connection parameters. When you configure Siebel sites, you give information about the Application Server, the Gateway Server, the server Manager path (which is the path to the srvrng.exe file), and so forth.

Each request has a key that consists in the following information: **<application_server><gateway_server><server_manager>**

The key is followed by the rest of the parameters.

If the problem occurs, check the SiteScope error log (in SiteScope under the logs directory) and the Siebel log and check the list of parameters used to access SiteScope and Siebel. For details about the Siebel log, see "Errors that Occur when Running One of the Diagnostics Tools" on page 419.

Services for Siebel

The Siebel Service is a configuration service that enables Mercury Business Availability Center to work with data that is in Siebel format. It performs an Auto Link between the Business Process Monitor and SiteScope data and the relevant Siebel CIs for which this data is relevant. It also groups the applications, locations, Business Processes, and hosts CIs into the appropriate containers.

For details about how to view a service status via the JMX Web console, see "High Availability for the Data Processing Server" in *Deploying Servers*.

The Siebel Service provides the following advantages:

- Responsible for intelligent relation of monitoring information
- Responsible for automatic linkage of SiteScope measurements or BPM scripts with standardized names. For details, see "Following the Naming Conventions for Naming Business Process Steps" on page 406.

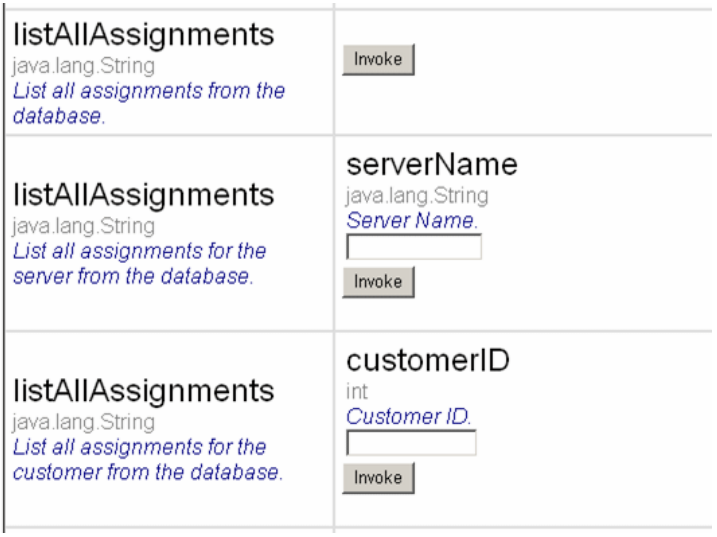
- Creating a Business Process and Locations container and connecting the appropriate Business Process Steps to the containers. A Business Process Step connected manually to the Siebel transaction would also be connected to those containers. For details, see "Attaching Business Process Monitor Transactions to Siebel Application Components" on page 406.
- Works after BPM and SiteScope source adapters have been synchronized.

Activating the Siebel Service

Check that the Siebel Service is activated (it is activated only if you have a license). If necessary activate it manually.

To view if the Siebel Service is activated:

1. In the browser, enter **http://<Mercury_Business_Availability_Center_server_name>:8080/jmx-console/**
2. Double-click **service=hac-manager** listed under **Topaz**.
3. The JMX MBean View for hac-manager opens.



4 Click the **Invoke** button corresponding to the **listAllAssignments** parameter. The result is as follows:

Service	Customer	Process - [Start] - [Ping]	Assigned - [Since] - [Duration]	State - [Since] - [Duration]	Srv. Sign	State Sign
LRDT	-1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:41:21] - [16h:45m:20s]	1	1
CDM	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:47:42] - [16h:38m:59s]	1	1
CMDB	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:41:51] - [16h:44m:50s]	1	1
VIEWSYS	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:42:02] - [16h:44m:39s]	1	1
VERTICALS	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [08/Jun/2006 07:21:25] - [5m:16s]	1	1
PACKAGER	1	smart : mercury_as - [16h:46m:20s] - [16s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:46:58] - [16h:39m:43s]	1	1
DASHBOARD	1	smart : mercury_online_engine - [16h:43m:5s] - [3s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:53:42] - [16h:32m:59s]	1	1
NOA	-1	smart : mercury_offline_engine - [16h:43m:6s] - [3s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:43:36] - [16h:43m:5s]	1	1
PM	-1	smart : topaz_pm - [16h:43m:10s] - [18s]	Yes(1) - [07/Jun/2006 14:40:21] - [16h:46m:20s]	RUNNING - [07/Jun/2006 14:43:33] - [16h:43m:8s]	1	1

5 Check that the Assigned column for the VERTICALS service includes **Yes**.

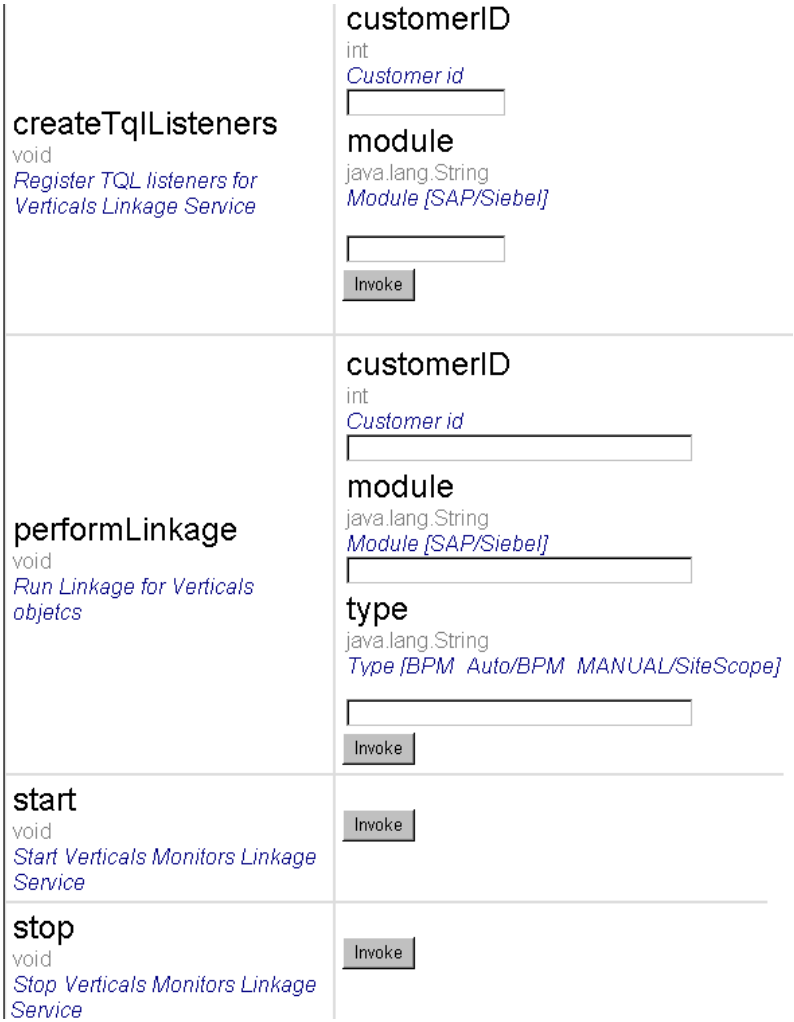
To manually activate the Siebel Service:

1 In the browser, enter **http://<Mercury_Business_Availability_Center_server_name>:8080/jmx-console/**

2 Double-click **service=Verticals External Enrichment Service** listed under **Topaz**.

- service=Propagation
- service=RUM statistics
- service=Rules Framework Log Filter
- service=SAP Alerts
- service=SLM Validator
- service=Scheduling Engine
- service=Script Repository
- service=TMC Debug JMX
- service=TMC TAS integration
- service=Topaz File Remover
- service=Topaz JBoss Statistics
- service=Topaz Site Configuration Loader
- service=Upgrade Manager
- service=Verticals External Enrichment Service
- service=hac-launcher
- service=hac-locator
- service=hac-manager
- service=repositories_manager

3 The JMX MBean View for Verticals External Enrichment Service opens:



4 Specify:

- **performLinkage.** Gets customer ID and the relevant linkage to perform (BPM AUTO/BPM manual/module).
- **createTqlListeners.** Mainly for debugging.

- **Start.** Starts the service.
- **Stop.** Stops the service

Manual Configuration for Specific Siebel CIs

When the Siebel discovery process is run, the CIs that appear in the Siebel Enterprises view have most of their properties' values automatically entered in the CMDB. Some of the properties of some of the CIs must be entered manually in order for data to be inserted properly in the Siebel Enterprises view. For details, see "CIT-Specific Properties" in *IT Universe Manager Administration*.

The following properties remain empty and must be entered manually.

CI Type	Properties	Description
Siebel Enterprise	**Admin user name**	The name of the user used to login to the Server Manager.
	Admin password	The password of the user used to login to the Server Manager.
	SARM Script Path	The path to the location of the SARM Analyzer package on the SiteScope server. The path is relative to the SiteScope server.
	Server Manager Script Path	The path to the location of the Server Manager package on the SiteScope server. The path is relative to the SiteScope server.
Siebel Application	**Emulated Transaction User Name**	The name of the user used in the script that analyzes the application. It is the default user name that appears when configuring the Database Breakdown tool. For details, see "Creating Siebel Database Logs" in *Using Dashboard*.
Siebel Web Server Extension	**SARM Log Folder**	The path to the log folder where the SARM files are written, relative to the Web Server Extension server. The path is relative to the SiteScope server. The folder should be shared. The format should be: **\\<siebel_web_server_extension_name>\ <log_directory>**

CI Type	Properties	Description
Siebel Application Server	**SARM Log Folder**	The path to the log folder where the SARM files are written, relative to the server where the Application Server is installed. The path is relative to the SiteScope server. The folder should be shared. The format should be: \\<**siebel_web_server_name**>\<**log_directory**>
	Log Folder	The path to the log folder where Siebel general log files are written, relative to the server where the Application Server is installed. The path is relative to the SiteScope server. The folder should be shared. The format should be: \\<**siebel_web_server_name**>\<**log_directory**>

SARM and SARM Benefits

Siebel Application Response Monitoring (SARM) is a Siebel process that produces User Session Trace output files.

For details, see "Siebel Application Response Monitoring (SARM)" on page 12.

Dedicated SiteScope Monitor for the Siebel Solution (Diagnostics)

Mercury Business Availability Center for Siebel SARM Diagnostics is a user trace breakdown diagnostic tool that processes the data in the User Session Trace output files produced by Siebel's SARM process (available to Siebel users from version 7.5.3 and above). This data can be retrieved for a specific user in a specific time frame. It is also retrieved for a specific transaction of a prerecorded script.

SARM data helps you find how long, on average, have sessions answering the criteria spent in each tier: Network, Web Server, Application Server and database, as well as underlying sub-layers. Furthermore, you can compare this breakdown by user sessions, user transactions, or even the different application servers. This enables you to identify the prime suspect for the performance problems.

SARM Ability to Use Multiple SiteScopes

If your site includes a large number of web servers, it is better to use multiple SiteScopes to distribute the work done by the SARM Analyzer tool between those SiteScopes.

Errors in Logs

Logs are available to help you debug problems with Siebel views and problems that occur when using the Siebel diagnostics tools.This section includes the following topics:

➤ "Errors that Occur when Building the Siebel Enterprises View" on page 418

➤ "Errors that Occur when Running One of the Diagnostics Tools" on page 419

Errors that Occur when Building the Siebel Enterprises View

The **Siebel.ejb.log** file (on the Modeling server) includes information about all the automatic links between the Business Process Monitor or SiteScope and the Siebel CIs whether those links worked correctly or not.

For details about the automatic links, see "SARM and SARM Benefits" on page 417.

To debug the log:

1 Open the **<Mercury_Business_Availability_Center_home_directory>\conf\core\Tools \log4j\EJB\topaz.properties** file

2 In the line that follows, change **${loglevel}** to debug. The lines should be as follows:
log4j.category.com.mercury.topaz.vertical=debug, vertical.appender
log4j.category.com.mercury.am.bac.vertical.rules=debug, vertical.appender

3 Open the error log, located on the Modeling server at the following location:
<Mercury_Business_Availability_Center_home_directory>\log \EJBContainer\Siebel.ejb.log

4 Locate the **#define appender for vertical module** line.

5 You can now view the log information.

6 After you have completed the debugging tasks, make sure to change **debug** back to **${loglevel}** in the lines that follows **#define appender for vertical module**. The lines should be as follows:
log4j.category.com.mercury.topaz.vertical=${loglevel}, vertical.appender
log4j.category.com.mercury.am.bac.vertical.rules=${loglevel}, vertical.appender

Errors that Occur when Running One of the Diagnostics Tools

The **Siebel.ejb.log** file (on the Center server) includes detailed information about the operations that take place in the Siebel Diagnostics tools.

For details about the Siebel Diagnostics tools, see "Working with the Siebel Solution" on page 261 in *Using Dashboard*.

To debug the log:

1 Open the error log, located on the Center server at the following location:
<Mercury_Business_Availability_Center_home_directory>\log \EJBContainer\Siebel.ejb.log

2 Locate the **#define appender for siebel** line.

3 In the line that follows, change **${loglevel}** to debug. The line should be as follows:
log4j.category.com.mercury.topaz.siebel=debug, siebel.appender

4 Open the
<Mercury_Business_Availability_Center_home_directory>\conf\core\Tools \log4j\EJB\topaz.properties file

5 You can now view the log information.

6 After you have completed the debugging tasks, make sure to change **debug** back to **${loglevel}** in the line that follows **#define appender for siebel**. The line should be as follows:
log4j.category.com.mercury.topaz.siebel=${loglevel}, siebel.appender

How Values are Calculated in Tasks and Processes

The CPU usage is calculated as follows:
CPU = 100 * (current_measurement - last_measurement)) / interval

where:

- **current_measurement.** The value of the measurement in the current CPU sample.
- **last_measurement.** The value of the measurement in the previous CPU sample.
- **interval.** The time period that occurred between the time the current measurement was collected and the time when the previous measurement was collected. interval = current measurement time - last measurement time.

General Administration

This section describes some of the settings that can be modified to customize the Siebel solution.

This section includes the following topics:

Increasing the Default Timeout for Either a SARM Task or a SARM Analyzer Execution

If the sarmanalyzer.log (SiteScope) indicates that a SARM task or sarmanalyzer execution has been timed-out, increase the default timeout for either a SARM task or a SARM analyzer execution.

To increase the default timeout for either a SARM task or a SARM analyzer execution:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Applications** and select **Siebel**.

3 Locate the **Siebel - Siebel SARM Breakdown** area.

4 Modify the following parameters:

- **SARM task timeout in seconds.** Indicates the default timeout for the execution of a SARM task (analyzing Web Server file, analyzing Application Server files, and so forth).
- **sarmanalyzer command timeout in seconds.** Indicates the default timeout for the execution of sarmanalyzer.exe (used to generate CSV or XML files).

Changing the Default Timeout for the Execution of a SiteScope Monitor

If the **Siebel.ejb.log**, located on the Center server, indicates that an execution of a SiteScope monitor got timed-out, change the default timeout for the execution of this monitor.

To change the default timeout for the execution of a SiteScope Monitor:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.

2 Click **Foundations** and select **Verticals**.

3 Locate the **Vertical - SiteScope Remote Control Settings** area.

4 Modify the **SiteScope monitor timeout in seconds** parameter. The parameter indicates the default timeout for the execution of a SiteScope monitor.

Monitoring a Siebel Application in Mercury Business Availability Center

This section describes the SiteScope monitors and solution sets that can be used to monitor a Siebel application.

This section includes the following topics:

- "Siebel App Server Solution Set Counters" on page 442
- "Siebel Gateway Server Solution Set Counters" on page 451
- "Siebel Web Server Solution Set Counters" on page 452

SiteScope Monitors

You can use one or more monitors and solutions sets offered by SiteScope to monitor Siebel (for more details, see *Configuring SiteScope Monitors* and "Introducing SiteScope Solution Templates" in *Configuring SiteScope Monitors*). Solution sets automate the creation of the monitors you want to use, and include threshold information. It is recommended to use the solution sets via the Monitor Deployment Wizard. For details about the Monitor Deployment Wizard, see "Monitor Deployment Wizard" in *Configuring SiteScope Monitors*.

- The monitors are:
  - **Siebel Application Server.** Uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.

    Details about the Siebel Application Server monitor counters are available in "Siebel Application Server Counters" on page 423.

    For details about the monitor, see "Siebel Application Server Monitor" in *Configuring SiteScope Monitors*.
  - **Siebel Web Server.** Monitors statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database.

    Details about the Siebel Web Server monitor counters are available in "Siebel Web Server Counters" on page 441.

    For details about the monitor, see "Siebel Web Server Monitor" in *Configuring SiteScope Monitors*.
  - **Siebel Log Monitor.** Monitors the log file entries added to a group of log files by looking for entries containing a specific event type or subtype.

    For details about the monitor, see "Siebel Log File Monitor" in *Configuring SiteScope Monitors*.

- The solution sets are:
  - **Siebel Application Server Solution Set.** Monitors the availability and server statistics for Siebel application servers (see "Siebel Solution Templates" in *Configuring SiteScope Monitors*). Available for Windows NT/2000 only. This is not a Monitor Administration monitor.

    Details about the Siebel App Server solution set counters are available in "Siebel App Server Solution Set Counters" on page 442.

    For details about the solution set, see "Using the Siebel Application Server Solution Template" in *Configuring SiteScope Monitors*.
  - **Siebel Web Server Solution Set.** Monitors the availability and server statistics for Siebel web servers (see "Siebel Solution Templates" in *Configuring SiteScope Monitors*). Available for Windows NT/2000 only. This is not a Monitor Administration monitor.

    For details about the solution set, see "Using the Siebel Web Server Solution Template" in *Configuring SiteScope Monitors*.
  - **Siebel Gateway Solution Set.** Monitors the availability and server statistics for Siebel web servers (see "Siebel Solution Templates" in *Configuring SiteScope Monitors*). Available for Windows NT/2000 only. This is not a Monitor Administration monitor.

    Details about the Siebel Web Server Solution Set counters are available in "Siebel Gateway Server Solution Set Counters" on page 451.

    For details about the solution set, see "Using the Siebel Gateway Server Solution Template" in *Configuring SiteScope Monitors*.

Siebel Application Server Counters

This section describes the SiteScope Siebel counters used by the SiteScope Siebel Application Server monitor.

This section includes:

➤ "Components Stat Counters" on page 432

➤ "Component Objects" on page 438

Server Statistics Counters

The counters used to calculate and display server statistics information are:

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Average Connect Time	Average connect time for Object Manager sessions	List statistics in Siebel	Regular counter under the specific Application Server
Average Reply Size - Siebel	Average size of reply messages (in bytes)	List statistics in Siebel	Regular counter under the specific Application Server
Average Request Size	Average size of request messages (in bytes)	List statistics in Siebel	Regular counter under the specific Application Server
Average Requests Per Session	Average number of requests per Object Manager session	List statistics in Siebel	Regular counter under the specific Application Server
Average Response Time	Average Object Manager response time	List statistics in Siebel	Regular counter under the specific Application Server
Average Think Time	Average end-user think time between requests	List statistics in Siebel	Regular counter under the specific Application Server
Avg SQL Execute Time	Average time for SQL execute operations (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server
Avg SQL Fetch Time	Average time for SQL fetch operations (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Avg SQL Parse Time	Average time for SQL parse operations (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server
CPU Time	Total CPU time for component tasks (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server
Elapsed Time	Total elapsed (running) time for component tasks (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server
Maximum Peak Memory Usage	Peak memory used by task. Rolls up differently from MinPeakMemory	List statistics in Siebel	Regular counter under the specific Application Server
Minimum Peak Memory Usage	Peak Mem used by task. Rolls up differently than MaxPeakMemory	List statistics in Siebel	Regular counter under the specific Application Server
Num of DBConn Retries	Number of Retries due to DB Connection Loss	List statistics in Siebel	Regular counter under the specific Application Server
Num of DLRbk Retries	Number of Retries due to Deadlock Rollbacks	List statistics in Siebel	Regular counter under the specific Application Server
Num of Exhausted Retries	Number of Times All Retries are Exhausted	List statistics in Siebel	Regular counter under the specific Application Server
Number of SQL Executes	Total number of SQL execute operations	List statistics in Siebel	Regular counter under the specific Application Server

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Number of SQL Fetches	Total number of SQL fetch operations	List statistics in Siebel	Regular counter under the specific Application Server
Number of SQL Parses	Total number of SQL parse operations	List statistics in Siebel	Regular counter under the specific Application Server
Number of Sleeps	Total number of sleeps for component tasks	List statistics in Siebel	Regular counter under the specific Application Server
Object Manager Errors	Number of errors encountered during Object Manager session	List statistics in Siebel	Regular counter under the specific Application Server
Reply Messages	Number of reply messages sent by the server	List statistics in Siebel	Regular counter under the specific Application Server
Request Messages	Number of request messages received by the server	List statistics in Siebel	Regular counter under the specific Application Server
SQL Execute Time	Total elapsed time for SQL execute operations (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server
SQL Fetch Time	Total elapsed time for SQL fetch operations (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server
SQL Parse Time	Total elapsed time for SQL parse operations (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server
Sleep Time	Total amount of sleep time for component tasks (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Tasks Exceeding Configured Cap	Number of tasks stated that exceeded configured capacity	List statistics in Siebel	Regular counter under the specific Application Server
Tests Attempted	Number of tests that were started.	List statistics in Siebel	Regular counter under the specific Application Server
Tests Failed	Number of tests that failed.	List statistics in Siebel	Regular counter under the specific Application Server
Tests Successful	Number of tests that were successful.	List statistics in Siebel	Regular counter under the specific Application Server
Total Database Response Time	Total Database Response/Processing Time (in milliseconds)	List statistics in Siebel	Regular counter under the specific Application Server
Total Reply Size	Total size (in bytes) or reply messages	List statistics in Siebel	Regular counter under the specific Application Server
Total Request Size	Total size (in bytes) of request message	List statistics in Siebel	Regular counter under the specific Application Server
Total Tasks	Total number of tasks completed for server components	List statistics in Siebel	Regular counter under the specific Application Server
Total Think Time	Total end-user think time (in seconds)	List statistics in Siebel	Regular counter under the specific Application Server

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
No. of tasks in error	The number of tasks in error	Lists tasks and counts the tasks that are running	Affects the number of sessions in the sites view of the Application Server and allows viewing the list of tasks that are **Exited with error** for that Application Server
No. of tasks Running	The number of tasks that are running	Lists tasks and counts the tasks that are running	Regular counter under the specific Application Server
No. of tasks Completed	The number of tasks that have completed	Lists tasks and counts the tasks that are completed	Regular counter under the specific Application Server

Server Processes Counters

The counters used to calculate and display server processes information are:

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Siebel Application Server Process (SIEBSVC): 1 No. of Running Instances 2 Max %CPU Time 3 Max Memory Used 4 Total %CPU Time 5 Total Memory Used	SIEBSVC is an executable that starts up the Siebel Service.	The data is taken from the Task Manager of Windows. For each process type the number of running process types is counted and the maximum CPU time	Affects the list of processes. It is displayed as counters under the Application Server in the Server Processes section.
Siebel Components (SIEBMTSH / SIEBMTSHMW): 1 No. of Running Instances 2 Max %CPU Time 3 Max Memory Used 4 Total %CPU Time 5 Total Memory Used	SIEBMTSH is an executable that runs multi-threaded process (**mtsh suffix**).	The data is taken from the Task Manager of Windows. For each process type the number of running process types is counted and the maximum CPU time	Affects the list of processes. It is displayed as counters under the Application Server in the Server Processes section.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Siebel Background Tasks (SIEBPROC /SIEBSH) 1 No. of Running Instances 2 Max %CPU Time 3 Max Memory Used 4 Total %CPU Time 5 Total Memory Used	The **siebproc** process is invoked when one of the Server Tasks has its Default Tasks parameter set to a value larger than 0. For example, these processes can be **siebproc** or **siebsh** depending on the sequence of events and setting of **Default Tasks**.	The data is taken from the Task Manager of Windows. For each process type the number of running process types is counted and the maximum CPU time	Affects the list of processes. It is displayed as counters under the Application Server in the Server Processes section.
Siebel SrvrMgr Session (SIEBSESS) 1 No. of Running Instances 2 Max %CPU Time 3 Max Memory Used 4 Total %CPU Time 5 Total Memory Used	SIEBSESS is the Siebel server manager server task.	The data is taken from the Task Manager of Windows. For each process type the number of running process types is counted and the maximum CPU time	Affects the list of processes. It is displayed as counters under the Application Server in the Server Processes section.

The types of Siebel processes are:

- **SIEBSVC.** This executable starts up the Siebel service.
- **SIEBMTSH.** (**siebmtsh.exe**) is an executable that runs multi-threaded process (**mtsh suffix**). Some of the Components that run under multi-thread are:
  - Assignment Manager
  - Batch Assignment
  - Object Manager
  - Server Request Manager
  - Siebel Call Center

- Siebel Internet Self Service
- Siebel Sales Enterprise
- Siebel Service Enterprise
- Synchronization Manager

- **SIEBPROC** and **SIEBSH.** The **siebproc** process is invoked when one of the Server Tasks has its Default Tasks parameter set to a value larger than 0 (for example, these processes can be **siebproc** or **siebsh** depending on the sequence of events and setting of **Default Tasks**):
  - If the components have **Default Tasks** set to a value larger than 0 and the NT Service is stop/started then the process will be **siebproc**.
  - If the Enterprise/Server is stop/started using the GUI via Server Administration screens or using **srvrmgr**, the process will always be **siebsh**.
- **SIEBSESS.** The Siebel server manager server task. A **SIEBSESS** task runs for each session of server manager that is running.

Components Groups Counters

The counters used to calculate and display component groups information are:

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
CG_RUN_STATE	A component group can have several states. The run state depends on the enable state; only component groups with an Online enable state when the Siebel Server was started can have an Online or Running run state	List component group	Displayed under the Component group under the counter **state**

Components Stat Counters

The counters used to calculate and display component statistics information are:

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Average Connect Time	Average connect time for Object Manager sessions	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Average Reply Size - Siebel	Average size of reply messages (in bytes)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Average Request Size	Average size of request messages (in bytes)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Average Requests Per Session	Average number of requests per Object Manager session	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Avg. Response Time (name in SiteScope: Average Response Time)	Average Object Manager response time	List statistics in Siebel	Displayed as counter of the component.
Avg. Think Time (name in SiteScope: Average Think Time)	Average end-user think time between requests	List statistics in Siebel	Displayed as counter of the component.
Avg. SQL Time (name in SiteScope: Avg SQL Execute Time)	Average time for SQL execute operations (in seconds)	List statistics in Siebel	Displayed as counter of the component.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Avg SQL Fetch Time	Average time for SQL fetch operations (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Avg SQL Parse Time	Average time for SQL parse operations (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
CPU Time	Total CPU time for component tasks (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Elapsed Time	Total elapsed (running) time for component tasks (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Maximum Peak Memory Usage	Peak Mem used by task Rolls up differently from MinPeakMemory	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Minimum Peak Memory Usage	Peak memory used by task. Rolls up differently from MaxPeak Memory	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Num of DBConn Retries	Number of retries due to database connection loss	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Num of DLRbk Retries	Number of retries due to Deadlock Rollbacks	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Num of Exhausted Retries	Number of times all retries are exhausted	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Number of SQL Executes	Total number of SQL execute operations	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Number of SQL Fetches	Total number of SQL fetch operations	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Number of SQL Parses	Total number of SQL parse operations	List statistics in Siebel	Displayed as counter of the component.
Number of Sleeps	Total number of sleeps for component tasks	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Object Manager Errors	Number of errors encountered during Object Manager session	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Reply Messages	Number of reply messages sent by the server	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Request Messages	Number of request messages received by the server	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
SQL Execute Time	Total elapsed time for SQL execute operations (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
SQL Fetch Time	Total elapsed time for SQL fetch operations (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
SQL Parse Time	Total elapsed time for SQL parse operations (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Sleep Time	Total amount of sleep time for component tasks (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Tasks Exceeding Capacity (name in SiteScope: Tasks Exceeding Configured Cap)	Number of tasks stated that exceeded configured capacity	List statistics in Siebel	Displayed as counter of the component.
Tests Attempted	Number of tests that were started.	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Tests Failed	Number of tests that failed.	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Tests Successful	Number of tests that were successful.	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Total Database Response Time	Total database response/processing time (in milliseconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Total Reply Size	Total size (in bytes) of reply messages	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Total Request Size	Total size (in bytes) of request messages	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Total Tasks	Total number of tasks completed for server components	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.
Total Think Time	Total end-user think time (in seconds)	List statistics in Siebel	Not displayed by default, unless added to the **monitor_measurements.xml file**.

Component Objects

The counters used to calculate and display component object information are:

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
CP_MAX_TASK	A parameter used with the Command Line (CLI) tool.	List tasks in Sitescope	Not displayed by default, unless added to the **monitor_measurements.xml** file.
CP_ACTV_MTS	A parameter used with the Command Line (CLI) tool.	List tasks in Sitescope	Not displayed by default, unless added to the **monitor_measurements.xml** file.
CP_MAX_MTS	A parameter used with the Command Line (CLI) tool.	List tasks in Sitescope	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Running State (name in SiteScope: CP_DISP_RUN_STATE)	A parameter used with the Command Line (CLI) tool.	List tasks in Sitescope	Displayed as counter of the component.
CP_NUM_RUN	A parameter used with the Command Line (CLI) tool.	List tasks in Sitescope	Not displayed by default, unless added to the **monitor_measurements.xml** file.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Tasks Error (name in SiteScope:No. of tasks in error)	A parameter used with the Command Line (CLI) tool.	List tasks in Sitescope	Displayed as counter of the component. Affects list tasks on a specific component and on the count of sessions for an Application Server and of the Application if this is a component object manager.
No. of tasks Running	The number of tasks that are running	List tasks in Sitescope	Not displayed by default, unless added to the **monitor_measurements.xml** file.
No. of tasks Completed	The number of tasks that have completed	List tasks in Sitescope	Not displayed by default, unless added to the **monitor_measurements.xml** file.
No. of Running Instances	The number of instances that are running	Data is taken from Windows Task Manager. The correlation between a process and a component is done by identifying the component running tasks for that have a process ID.	Not displayed by default, unless added to the **monitor_measurements.xml** file.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
CPU Status (name in SiteScope:Max %CPU Time)	The maximum CPU time in percentages	Data is taken from Windows Task Manager. The correlation between a process and a component is done by identifying the component running tasks for that have a process ID.	Displayed as counter of the component.
Max Memory Used	The maximum amount of memory used	Data is taken from Windows Task Manager. The correlation between a process and a component is done by identifying the component running tasks for that have a process ID.	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Total %CPU Time	The total CPU time in percentages	Data is taken from Windows Task Manager. The correlation between a process and a component is done by identifying the component running tasks for that have a process ID.	Not displayed by default, unless added to the **monitor_measurements.xml** file.

Counter Name	Description	Data Retrieval	Effect in Mercury Business Availability Center
Total Memory Used	The total amount of memory used	Data is taken from Windows Task Manager. The correlation between a process and a component is done by identifying the component running tasks for that have a process ID.	Not displayed by default, unless added to the **monitor_measurements.xml** file.
Max Task Run Time	The maximum time spent by a running task	Data is taken from Windows Task Manager. The correlation between a process and a component is done by identifying the component running tasks for that have a process ID.	Not displayed by default, unless added to the **monitor_measurements.xml** file.

Siebel Web Server Counters

This section describes the counters used by the SiteScope Siebel Web Server monitor.

This section includes:

- "System Stats" on page 441
- "Applications" on page 442

System Stats

The counters used to calculate and display system statistics information are:

- Anonymous sessions requested from the pool
- Open Session Time

- Anon Session Available
- Close Session Time
- Request Time
- Anon Session Removed
- Response Time
- Anonymous sessions returns to the pool

For more details about the counters, see "Siebel Solution Templates" in *Configuring SiteScope Monitors*.

Applications

The counters used to calculate and display application information are:

- /callcenter_enu/
- /sales_enu/
- /callcenter_jpn/
- /callcenter_enu/Session Lifespan
- /callcenter_jpn/Session Lifespan
- /sales_enu/Session Lifespan
- Anon Session Available
- Close Session Time
- Request Time
- Anon Session Removed
- Response Time
- Anonymous sessions returns to the pool

Siebel App Server Solution Set Counters

This section describes the SiteScope App Server Solution Set counters used by the SiteScope Siebel Application Server monitor.

Siebel App Server Solution Set includes a subset of the counters of selected monitors.

The Siebel App Server Solution Set includes a subset of the counters of the following monitors:

- Siebel Application Server
- CPU Utilization
- Memory
- Ping
- Siebel Server Service
- Directory
- Disk Space
- Siebel Application Server Log
- Siebel Transaction Logging process
- Siebel Workflow Rules process
- Siebel Transaction Router process
- Siebel Integration Enterprise Manager process
- siebel_solution_<cannon>_web
- Service: Siebel Server [siebel_cannon] Service on <cannon>
- Siebel Transaction Router Process

The Siebel App Server Solution Set counters are:

- "Siebel Call Center Component" on page 444
- "Siebel Call Center Object Manager (ENU) Component" on page 444
- "Siebel eService Object Manager (ENU) Component" on page 445
- "Siebel System Component Group" on page 446
- "Siebel SRBroker Component" on page 446
- "Siebel SRProc Component" on page 447
- "Siebel ServerMgr Component" on page 447
- "Siebel FSMSrv Component" on page 448

➤ "Siebel ClientAdmin Component" on page 449

➤ "Siebel Application Server: Siebel Process" on page 449

➤ "Siebel Transaction Logging Process" on page 450

Siebel Call Center Component

The counters used to calculate and display Call Center component information are:

➤ Server Stats/cannon/No. of tasks in error

➤ Component Groups/Siebel Call Center/CG_RUN_STATE

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel Call Center Object Manager (ENU) Component

The counters used to calculate and display Call Center Object Manager information are:

➤ Component Objects/Siebel Call Center/Call Center Object Manager (ENU)/ CP_DISP_RUN_STATE

➤ Component Stats/Siebel Call Center/Call Center Object Manager (ENU)/ Average Response Timer

➤ Component Stats/Siebel Call Center/Call Center Object Manager (ENU)/ Avg SQL Execute Time

➤ Component Stats/Siebel Call Center/Call Center Object Manager (ENU)/ Average Think Time

➤ Component Objects/Siebel Call Center/Call Center Object Manager (ENU)/ No. of tasks in error

➤ Component Stats/Siebel Call Center/Call Center Object Manager (ENU)/ Tasks Exceeding Configured Cap

➤ Component Objects/Siebel Call Center/Call Center Object Manager (ENU)/ Max Memory Used

➤ Component Objects/Siebel Call Center/Call Center Object Manager (ENU)/ Max %CPU Time

- Component Objects/Siebel Call Center/Call Center Object Manager (ENU)/ No. of Running Instances

  For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel eService Object Manager (ENU) Component

The counters used to calculate and display eService Object Manager component information are:

- Component Objects/Siebel Call Center/eService Object Manager (ENU)/ CP_DISP_RUN_STATE
- Component Stats/Siebel Call Center/eService Object Manager (ENU)/ Average Response Time
- Component Stats/Siebel Call Center/eService Object Manager (ENU)/ Avg SQL Execute Time
- Component Stats/Siebel Call Center/eService Object Manager (ENU)/ Average Think Time
- Component Objects/Siebel Call Center/eService Object Manager (ENU)/ No. of tasks in error
- Component Stats/Siebel Call Center/eService Object Manager (ENU)/ Tasks Exceeding Configured Cap
- Component Objects/Siebel Call Center/eService Object Manager (ENU)/ Max Memory Used
- Component Objects/Siebel Call Center/eService Object Manager (ENU)/ Max %CPU Time
- Component Objects/Siebel Call Center/eService Object Manager (ENU)/ No. of Running Instances

  For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel System Component Group

The counters used to calculate and display System Component Group information are:

- Server Stats/cannon/ No. of tasks in error
- Component Groups/System Management/CG_RUN_STATE

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel SRBroker Component

The counters used to calculate and display Service Request Broker (SRBroker) Component information are:

- Component Objects/System Management/Server Request Broker/ CP_DISP_RUN_STATE
- Component Stats/System Management/Server Request Broker/ Avg SQL Execute Time
- Component Objects/System Management/Server Request Broker/ No. of tasks in error
- Component Stats/System Management/Server Request Broker/ Tasks Exceeding Configured Cap
- Component Objects/System Management/Server Request Broker/ Max Memory Used
- Component Objects/System Management/Server Request Broker/ Max %CPU Time
- Component Objects/System Management/Server Request Broker/ No. of Running Instances

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel SRProc Component

The counters used to calculate and display Server Request Processor (SRProc) Component information are:

- Component Objects/System Management/Server Request Processor/ CP_DISP_RUN_STATE
- Component Stats/System Management/Server Request Processor/ Avg SQL Execute Time
- Component Objects/System Management/Server Request Processor/ No. of tasks in error
- Component Stats/System Management/Server Request Processor/ Tasks Exceeding Configured Cap
- Component Objects/System Management/Server Request Processor/ Max Memory Used
- Component Objects/System Management/Server Request Processor/ Max %CPU Time
- Component Objects/System Management/Server Request Processor/ No. of Running Instances

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel ServerMgr Component

The counters used to calculate and display ServerMgr Component information are:

- Component Objects/System Management/Server Manager/ CP_DISP_RUN_STATE
- Component Stats/System Management/Server Manager/ Avg SQL Execute Time
- Component Objects/System Management/Server Manager/ No. of tasks in error
- Component Stats/System Management/Server Manager/ Tasks Exceeding Configured Cap

- Component Objects/System Management/Server Manager/ Max Memory Used
- Component Objects/System Management/Server Manager/ Max %CPU Time
- Component Objects/System Management/Server Manager/ No. of Running Instances

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel FSMSrv Component

The counters used to calculate and display File System Manager (FSMSrv) Component information are:

- Component Objects/System Management/File System Manager/ CP_DISP_RUN_STATE
- Component Stats/System Management/File System Manager/ Avg SQL Execute Time
- Component Objects/System Management/File System Manager/ No. of tasks in error
- Component Stats/System Management/File System Manager/ Tasks Exceeding Configured Cap
- Component Objects/System Management/File System Manager/ Max Memory Used
- Component Objects/System Management/File System Manager/ Max %CPU Time
- Component Objects/System Management/File System Manager/ No. of Running Instances

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel ClientAdmin Component

The counters used to calculate and display ClientAdmin Component information are:

- Component Objects/System Management/Client Administration/ CP_DISP_RUN_STATE
- Component Stats/System Management/Client Administration/ Avg SQL Execute Time
- Component Objects/System Management/Client Administration/ No. of tasks in error
- Component Stats/System Management/Client Administration/ Tasks Exceeding Configured Cap
- Component Objects/System Management/Client Administration/ Max Memory Used
- Component Objects/System Management/Client Administration/ Max %CPU Time
- Component Objects/System Management/Client Administration/ No. of Running Instances

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel Application Server: Siebel Process

The counters used to calculate and display Siebel Process information are:

- Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)/ Max Memory Used
- Server Processes/Siebel Application Server Process (SIEBSVC)/ Max Memory Used
- Server Processes/Siebel SrvrMgr Session (SIEBSESS)/ Max %CPU Time
- Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW)/ No. of Running Instances
- Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)/ No. of Running Instances

- Server Processes/Siebel SrvrMgr Session (SIEBSESS)/ No. of Running Instances
- Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW)/ Max %CPU Time
- Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)/ Max %CPU Time
- Server Processes/Siebel SrvrMgr Session (SIEBSESS)/ Max Memory Used
- Server Processes/Siebel Application Server Process (SIEBSVC)/ No. of Running Instances
- Server Processes/Siebel Application Server Process (SIEBSVC)/ Max %CPU Time
- Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW)/ Max Memory Used

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel Transaction Logging Process

The counters used to calculate and display Siebel Transaction Logging Process information are:

- Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)/ Max Memory Used
- Server Processes/Siebel Application Server Process (SIEBSVC)/ Max Memory Used
- Server Processes/Siebel SrvrMgr Session (SIEBSESS)/ Max %CPU Time
- Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW)/ No. of Running Instances
- Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)/ No. of Running Instances
- Server Processes/Siebel SrvrMgr Session (SIEBSESS)/ No. of Running Instances

- Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW)/ Max %CPU Time
- Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)/ Max %CPU Time
- Server Processes/Siebel SrvrMgr Session (SIEBSESS)/ Max Memory Used
- Server Processes/Siebel Application Server Process (SIEBSVC)/ No. of Running Instances
- Server Processes/Siebel Application Server Process (SIEBSVC)/ Max %CPU Time
- Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW)/ Max Memory Used

For more details about those counters, see "Siebel Application Server Counters" on page 423.

Siebel Gateway Server Solution Set Counters

This section describes the SiteScope Gateway Server Solution Set counters used by the SiteScope Siebel Application Server monitor.

The Siebel Gateway Server Solution Set includes a subset of the counters of the following monitors:

- CPU Utilization
- Disk Space (Disk space - % full, Disk space - MB free, Disk space - total disk)
- Directory (#of files in gtwysrvr/LOG directory)
- Memory (% used, MB free, pages/sec.)
- Ping
- Service: Siebel Gateway Name Server Service

Siebel Web Server Solution Set Counters

This section describes the SiteScope Web Server Solution Set counters used by the SiteScope Siebel Application Server monitor.

The Siebel Web Server Solution Set includes the a subset of the counters of following monitors:

- CPU Utilization
- Disk Space (Disk space - % full, Disk space - MB free, Disk space - total disk)
- Directory (# of files in SWEApp/LOG directory)
- Memory ($ used, MB free)
- Ping
- Service: IIS Admin Service on \\CANNON
- http://CANNON/callcenter_enu/start.swe?SWECmd=Start Monitor
- Port 80 on CANNON

The Siebel Web Server Solution Set counters are:

- "IIS Server Monitor" on page 452
- "Siebel Server Monitor" on page 453

IIS Server Monitor

The counters used to calculate and display IIS Server Monitor information are:

- Web Service -- Bytes Sent/sec -- Default Web Site
- Web Service -- Bytes Received/sec -- Default Web Site
- Web Service -- Bytes Total/sec -- Default Web Site
- Web Service -- Get Requests/sec -- Default Web Site
- Web Service -- Post Requests/sec -- Default Web Site
- Web Service -- Current Connections -- Default Web Site
- Web Service -- Maximum Connections -- Default Web Site

- Web Service -- Current NonAnonymous Users -- Default Web Site
- Web Service -- Total Not Found Errors -- Default Web Site

For more details, see "IIS Server Monitor" in *Configuring SiteScope Monitors*.

Siebel Server Monitor

The counters used to calculate and display Siebel Server Monitor information are:

- System Stats/Request Time/Frequency mean
- Applications//callcenter_enu//Frequency mean

For more details, see "Siebel Web Server Monitor" in *Configuring SiteScope Monitors*.

Siebel Solution Hints and Tips

This section provides hints and tips that can help you use the Siebel solution more efficiently. It includes the following topics:

Siebel Configuration

This section describes how to improve Siebel configuration.

Large Log Files

The Siebel logging mechanism for the CallCenter application (or any other application) is sometimes configured in such way that all log data is written to a few large log files instead of creating a separate log file per task. Large log files are a problem because parsing takes a long time.

To solve the problem:

Two solutions are available:

- The Siebel administrator should configure the relevant parameters so that each task writes to a separate log data file.
- The Siebel administrator should provide:
  - A script to be used before running the diagnostic tools. That script should set the logging mechanism to log each task into a separate file. This is required when you want to use the Database Breakdown reports and may also be relevant when the Siebel Log Monitors is configured. You can configure the flush rate at the environment variables level of the operating system of the machine where Siebel Server is installed (this can be a problem when both the Web Server and the Application Server are installed on same machine, since the environment variables of the two servers override each other). Consult Siebel documentation for more detailed instructions.
  - A script to be used after running the diagnostics tool. That script should switch the log level back to its initial state.

Diagnostics Checklist

This section describes the Diagnostics-related settings that ensure that the Diagnostics work properly.

This section includes:

Diagnostics-Related Settings for Siebel

Make sure that:

- The SiteScope user has at least read-only access to the log directories of all Web and Application Servers.
- The SiteScope user has administrative privileges on all Siebel servers or, if this is not possible, give the permissions specified at the following location: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q300702.
- You have defined a special Siebel user to be used by Business Process Monitor profiles. Note that this user should be used only for that purpose.
- **Siebel Breakdown** is enabled for the script that monitors the Siebel application (for details, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*).
- **Siebel Server Manager and SARM Analyzer.** Make sure that:
  - The **srvrmgr** package and **SARM Analyzer** package are installed on a SiteScope machine (they are needed for running the Diagnostics tools). You copy the Siebel Server Manager and the SARM Analyzer to a SiteScope machine (preferably) or, if this is not possible, to another machine where it can be executed by a SiteScope user.
  - The SiteScope user on the Siebel Server Manager has execution permissions when both SiteScope and Siebel are running on UNIX.

➤ The SARM Analyzer package includes the following files:

Siebel 7.5.3	Siebel 7.7
➤ change_siebel_db_log_level.bat ➤ collect_sarm_web_files.bat ➤ collect_user_session_trace_files_753.bat ➤ copy_remote_file.bat ➤ sarmanalyzer.exe ➤ srm.exe ➤ sslcosa.dll ➤ sslcshar.dll ➤ sslcsym.dll ➤ sslcver.dll	➤ libarm.dll ➤ msvcp70.dll ➤ msvcr70.dll ➤ sarmanalyzer.exe ➤ srm.exe ➤ sslcacln.dll ➤ sslccore.dll ➤ sslcevt.dll ➤ sslcos.dll ➤ sslcosa.dll ➤ sslcosd.dll ➤ sslcrsa.dll ➤ sslcscr.dll ➤ sslcshar.dll ➤ sslcsrd.dll ➤ sslcsym.dll ➤ sslcver.dll

➤ The **srvrmgr** package includes the following files:

Siebel 7.5.3	Siebel 7.7
➤ srvmgr.exe ➤ srvmgr.zip ➤ sslcacln.dll ➤ sslccca.dll ➤ sslccore.dll ➤ sslcctmrclnt.dll ➤ sslcdb.dll ➤ sslcdbgengw.dll	➤ srvmgr.exe ➤ CharsetConverter51U.dll ➤ libarm.dll ➤ msvcp70.dll ➤ msvcr70.dll ➤ siebsrvr.dll ➤ SiteXSpecificDllNew51U.dll ➤ srcesatme.dll

Siebel 7.5.3	Siebel 7.7
➤ sslcdock.dll ➤ sslcevt.dll ➤ sslcfsm.dll ➤ sslckm.dll ➤ sslclm.dll ➤ sslcnapi.dll ➤ sslcns.dll ➤ sslcnscl.dll ➤ sslcos.dll ➤ sslcosa.dll ➤ sslcosd.dll ➤ sslcrsa.dll ➤ sslcrsa56.dll ➤ sslcsa.dll ➤ sslcsac.dll ➤ sslcsc.dll ➤ sslcscc.dll ➤ sslcscstr.dll ➤ sslcscr.dll ➤ sslcshar.dll ➤ sslcsmgr.dll ➤ sslcsndk.dll ➤ sslcsnfl.dll ➤ sslcsnns.dll ➤ sslcsnom.dll ➤ sslcsnsa.dll ➤ sslcsnsc.dll ➤ sslcsnsm.dll ➤ sslcsnsq.dll ➤ sslcsnsr.dll ➤ sslcsobj.dll ➤ sslcspck.dll ➤ sslcsrcn.dll ➤ sslcsrd.dll	➤ ssan3v2.dll ➤ sslcacln.dll ➤ sslcafx.dll ➤ sslcasgn.dll ➤ sslcasrv.dll ➤ sslccachev2.dll ➤ sslccca.dll ➤ sslccore.dll ➤ sslcctmr.dll ➤ sslcctmrclnt.dll ➤ sslcdb.dll ➤ sslcdbgengw.dll ➤ sslcdock.dll ➤ sslcevt.dll ➤ sslcfsm.dll ➤ sslckm.dll ➤ sslclm.dll ➤ sslcmsagent.d ➤ sslcnapi.dll ➤ sslcns.dll ➤ sslcnscl.dll ➤ sslcntfy.dll ➤ sslcom.dll ➤ sslcos.dll ➤ sslcosa.dll ➤ sslcosd.dll ➤ sslcrsa.dll ➤ sslcrsa56.dll ➤ sslcrsh.dll ➤ sslcrti.dll ➤ sslcsa.dll ➤ sslcsac.dll ➤ sslcsc.dll ➤ sslcscc.dll

Siebel 7.5.3	Siebel 7.7
➤ sslcsrms.dll ➤ sslcsrqc.dll ➤ sslcsrs.dll ➤ sslcsrtr.dll ➤ sslcsrvr.dll ➤ sslcsssm.dll ➤ sslcstax.dll ➤ sslcsul.dll ➤ sslcsvrq.dll ➤ sslcsym.dll ➤ sslctutl.dll ➤ sslcupg.dll ➤ sslcver.dll ➤ sslcwath.dll ➤ sslczlib.dll	➤ sslcscstr.dll ➤ sslcscr.dll ➤ sslcsdm.dll ➤ sslcsecc.dll ➤ sslcsecm.dll ➤ sslcshar.dll ➤ sslcsmgr.dll ➤ sslcsndk.dll ➤ sslcsnfl.dll ➤ sslcsnns.dll ➤ sslcsnom.dll ➤ sslcsnsa.dll ➤ sslcsnsc.dll ➤ sslcsnsq.dll ➤ sslcsnsr.dll ➤ sslcsobj.dll ➤ sslcspck.dll ➤ sslcsrcn.dll ➤ sslcsrd.dll ➤ sslcsrms.dll ➤ sslcsrqc.dll ➤ sslcsrs.dll ➤ sslcsrtr.dll ➤ sslcsrvr.dll ➤ sslcsssm.dll ➤ sslcstax.dll ➤ sslcsul.dll ➤ sslcsvpr.dll ➤ sslcsvrq.dll

Siebel 7.5.3	Siebel 7.7
	➤ sslcsym.dll ➤ sslcsysstat.dll ➤ sslctutl.dll ➤ sslcupg.dll ➤ sslcupgutl.dll ➤ sslcver.dll ➤ sslcwath.dll ➤ sslcwork.dll ➤ sslczlib.dll ➤ tlib.dll

Diagnostics-Related Settings for SiteScope

Make sure that:

- SiteScope service is running under a domain account (not a local system). This domain account (SiteScope user) must have the permissions specified in "Diagnostics-Related Settings for Siebel" on page 455.
- Each Siebel Web and Application Server is defined as Remote NT or Remote UNIX appropriately. Remote UNIX machines must be defined using the Telnet protocol. Additionally, in the **initialize shell environment** field, enter **stty cols 1024; stty tabs; $SHELL**.
- SiteScope has access permissions to the Siebel machines. Check that the account SiteScope Service is running in Services (in Windows NT) or in the process (on UNIX).
- The **log** and **SARM log** folders on Siebel Web Server and Application Server are accessible from the SiteScope machine.
- SiteScope is attached to the Core Server.
- SiteScope has an additional license for Siebel Monitors.

Diagnostics-Related Settings for Mercury Business Availability Center

Make sure that:

- all the Business Availability Center for Siebel configuration parameters of the Enterprise, and Siebel Servers are spelled correctly, the appropriate case is used, and there are no blank spaces at the end of the parameter string.
- there is no inconsistency in the treatment of the SiteScope host name between the SiteScope profile and Monitor Administration (either defined with domain or as an IP address). Diagnostics cannot access a SiteScope located in an outer LAN; the solution is to define SiteScope in Monitor Administration using the host name provided by the SiteScope server. If the SiteScope server cannot be accessed using such a host name from the Centers Server the host name must be defined in the hosts file in the operating system of all the Centers Servers (for NT, the location is: **C:\WINNT\system32\drivers\etc\hosts**; for some Unix environments, the location is: **/etc/hosts**; in other Unix environments it is in the **.rhosts** file).
- the SiteScope you are using for diagnostics is attached (click **Admin** > **Monitors** > **Monitors** in Mercury Business Availability Center).
- you are using a dedicated SiteScope for diagnostics purposes, when working with medium to large Siebel deployments.
- you have network access (without firewalls or via VPN) to the Business Process Monitor servers (port ***2696***) you are going to use for diagnostics purposes.
- for each Business Process Monitor server used for Diagnostics, you can open the **http://<BPM_server>:2696/** page from the Centers Server.
- all paths you set in Business Availability Center for Siebel configuration are relative to SiteScope; for example: if they are local on SiteScope (Server Manager, SARM analyzer) use the local path, otherwise use the complete network path.
- you have a license for Siebel on the Centers Server (click **Admin** > **Platform** > **License Management** to verify this).

- SiteScope data arrives to Mercury Business Availability Center:
  - Verify that the SiteScope clock is synchronized with the Mercury Business Availability Center Management Database machine. You can verify that by using the start > command and run **net time \\<machine_name>** command. If necessary, you can set the clock using the same command.
  - Consult the SARM log file or the **dispatcher.txt** log file with the appropriate log level to check that information. You can update the log level of the dispatcher log in the first line of the **<Mercury Business Availability Center home directory>\conf\dispatcher_log.cfg** file on the Centers Server. Change the value of **LogLevel** to **debug5**. This causes the samples from SiteScope to appear in the **dispatcher.txt** file.

Note: It is recommended to increase the log level only for a short period, so Mercury Business Availability Center performance is not affected.

- only one script is monitoring your Siebel Application inside the Business Process Monitor profile that will be associated with that Siebel Application.
- the user of your Siebel Application in Business Availability Center for Siebel Configuration has appropriate permissions in the Siebel Site and the password is correct.

Topology View

This section describes issues related to the Topology View and how to solve those problems.

Session Data is Not Available

Session data is available only if the following conditions are met:

- **Session data for a server** – If **No. of Running Sessions** is assigned to the Application Server or to components of the Application Server, then the number of sessions is displayed for the appropriate server.

Task Data is Not Available

Task data is displayed only for tasks in error.

If task data is not available, either the appropriate counter (**No. of tasks in error**) was not defined or none of the tasks is in error.

Siebel Application Response Monitoring (SARM)

This section describes how to improve Siebel configuration so SARM works properly and how to solve SARM-related issues.

This section includes:

Note: You can run SARM manually. For details, see *Technote XXX SARM.doc* (for Siebel 7.5.3) or Chapter 12: "Monitoring Siebel Application Performance" in *PerformTun.pdf* (for Siebel 7.0).

Enabling SARM for Siebel

You control SARM using Siebel server parameters and environment variables. To enable SARM, you must enable specific SARM parameters for the Web server using environment variables and for the Siebel Server using the Server Manager or the Siebel Server Manager Graphical User Interface. When a component starts up in the Siebel Enterprise, it will check the status of the following SARM parameters:

➤ **For Siebel 7.5.3**:

Name of SARM Parameter in the Web Server	Name of SARM Parameter for Application Server	Description
SIEBEL_SarmEnabled	SARMEnabled	Indicates whether SARM is enabled or disabled for a Siebel Server Component. The default value is **false**. This parameter can be set at the Siebel Enterprise level, Siebel Application Server level, or Siebel Component level.
SIEBEL_SarmMaxMemory	SARMMaxMemory	The maximum size of the SARM memory. This parameter can be set at the Siebel Server or Siebel Server Component level.
SIEBEL_SarmMaxFileSize	SARMMaxFileSize	The maximum size of a SARM file. SARM continues to append file segments to the current file until the maximum size is reached. When the limit is reached, SARM starts a new file. The default value is **20000000** (~20 MB) and is specified in bytes.

➤ **For Siebel 7.7**:

Name of SARM Parameter in the Web Server	Name of SARM Parameter for Application Server	Description
SIEBEL_SARMBufferSize	SARMBufferSize	The size of the SARM buffer. The default value is 5,000,000 bytes (~5MB).
SIEBEL_SARMLevel	SARMLevel	The SARM Granularity level. The default value is **0**. This parameter can be set at the Siebel Server or Siebel Server Component level.
SIEBEL_SARMFileSize	SARMFileSize	The maximum size of a SARM data file. The default value is 15,000,000 bytes (~15MB).
SIEBEL_SARMMaxFiles	SARMMaxFiles	The maximum number of SARM files determines how many SARM files should be saved for a session. The recommended value is 5.
SIEBEL_SarmPeriod	SARMPeriod	The SARM period is the time when SARM outputs the stored data to the SARM log file regardless of the Buffer size. The default value is 3.

You can enable SARM for Siebel either at the web server level, at the Application Server level, or at the component level (see the procedures below for more details).

To enable SARM for Siebel at the Web server level:

1. Update the values of the appropriate environment variables parameters listed in the table above.
2. Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see “Calculating the SarmMaxFileSize Parameter for Siebel 7.5.3” on page 467 or “Calculating the SarmMaxFileSize Parameter for Siebel 7.7” on page 468.
3. Restart the Siebel server for the new values to take effect.

Note: SARM is disabled by default.

To enable SARM for Siebel at the Application level from the environment variables:

Note: The Application Server Parameters can be updated from either the environment variables or from the Siebel Server user interface (follow the procedure below). If the parameters are defined both in the user interface and the environment variables, the environment variables override the user interface definitions.

---

1. Update the values of the appropriate environment variables parameters listed in the table above.
2. Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see "Calculating the SarmMaxFileSize Parameter for Siebel 7.5.3" on page 467 or "Calculating the SarmMaxFileSize Parameter for Siebel 7.7" on page 468.
3. Restart the Siebel server for the new values to take effect.

Note: SARM is disabled by default.

To enable SARM for Siebel at the Application Server level from the Siebel Server user interface:

Note: The Application Server Parameters can be updated from either the environment variables (follow the procedure above) or from the Siebel Server user interface (follow the procedure below). If the parameters are defined both in the user interface and the environment variables, the environment variables override the user interface definitions.

---

1. In Siebel Server Manager Graphical User Interface, click **Site Map** > **Server Administration** > **Servers** > **Server Parameters**.
2. In the Server Parameters List Applet, query for SARM.
3. Update the values of the appropriate parameters listed in the table above.

Note: SARM is disabled by default.

---

4. Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see “Calculating the SarmMaxFileSize Parameter for Siebel 7.5.3” on page 467 or “Calculating the SarmMaxFileSize Parameter for Siebel 7.7” on page 468.

To enable SARM for Siebel at the component level:

1 In Siebel Server Manager Graphical User Interface, click **Site Map** > **Server Administration** > **Servers** > **Component Parameters**.

2 In the Component Parameters List Applet, query for SARM.

3 Update the values of the appropriate parameters listed in the table above.

Note: SARM is disabled by default.

---

4 Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see "Calculating the SarmMaxFileSize Parameter for Siebel 7.5.3" on page 467 or "Calculating the SarmMaxFileSize Parameter for Siebel 7.7" on page 468.

Calculating the SarmMaxFileSize Parameter for Siebel 7.5.3

This section describes the **SarmMaxFileSize** parameter settings recommended for working with SARM.

The amount of data that is written per second can be calculated in the following way:
37kb/min*<nbr_of_concurrent_users>*<required_time_frame_saved>/<nbr_of_server_components_instances>

For example, if your site has 20 concurrent users, you want to save the data of the last hour for all users, and you have 3 instances of the Object Manager component of the application, the file size should be:
37*20*60/3 = 14800Kb. Therefore the SARM Data File Size Limit should be set to 15,000,000. The buffer size should be set to 4,000,000. The growth rates of the Web server data is 1/5 the growth of the Application Server data.

Calculating the SarmMaxFileSize Parameter for Siebel 7.7

This section describes the **SarmMaxFileSize** parameter settings recommended for working with SARM.

The amount of data that is written per second in Siebel 7.7 depends on the granularity level and can be calculated in the following way:

- **Level 1 (SIEBEL_SarmLevel=1).** The calculation is as follows:
  10kb/min*<nbr_of_concurrent_users>*<required_time_frame_saved>/<nbr_of_server_components_instances>

  For example, if your site has 20 concurrent users, you want to save the data of the last hour for all users, and you have 3 instances of the Object Manager component, the file size should be: 10*20*60/3 = 4,000 Kb. Therefore, the SARM Data File Size Limit should be set to: 4,000,000.

- **Level 2 (SIEBEL_SarmLevel=2).** To store more data. The calculation is as follows:
  60kb/min*<nbr_of_concurrent_users>*<required_time_frame_saved>/<nbr_of_server_components_instances>

  For example, if your site has 20 concurrent users, you want to save the data of the last hour for all users, and you have 3 instances of the Object Manager component, the file size should be: 60*20*60/3 = 24,000 Kb. Therefore, the SARM Data File Size Limit should be set to: 24,000,000.

Tips

1. To save disk space, it is recommended to enable SARM only for Object Manager components since Siebel is only measuring the Object Managers time for the User Session trace.
2. If you restart the Siebel Application Server or the Web server regularly it is recommended to search, in the log folder, for old SARM files that can be deleted. Every time you restart the server a new log file, which includes the Process Id, is created. Only five log files with the same Process Id are kept at a time (the older ones are overwritten). Files with other Process Ids must be deleted manually. This procedure will save disk space and will also improve the efficiency of the User Session Breakdown.

It is best if the number of SARM files saved in the SARM folders is minimal. Save only the files you want to retrieve data from. Other files can be moved to another folder (not to a sub-directory of the SARM folder) and can be used later. Too many SARM files in the SARM directories cause the SARM tool to work more slowly.

SARM on the UNIX Platform

To activate SARM on a UNIX platform, make sure that the following requirements are met:

- **For Siebel 7.7**
  - The SARM feature is supported only if SiteScope is installed on an NT platform.
  - A mount point must exist between SiteScope and the Siebel machine. The SiteScope user must have permission to read from the relevant directories (it means that the user has to be declared as a mounting point machine user and as a UNIX user).
- **For Siebel 7.5.3**

Note: The SARM user trace breakdown diagnostic tool is not recommended for use on Siebel 7.5.3 running on Unix.

  - If you work with SARM Analyzer on SiteScope, make sure that SiteScope is installed on a UNIX machine.
  - A mount point must exist between the SiteScope machine and the Siebel machine.
  - The updated **csh** scripts (**collect_sarm_web_files** and **collect_user_session_trace_files_753**) are located in the **templates.applications\scripts.siebel** directory in the SiteScope installation directory.
  - The SiteScope user must have permissions to read from the relevant directories on the Siebel machine.

- Make the following changes to the **start-monitor** and **start-service** scripts located in the <**SiteScope**>/**classes** directory: insert all the variables that are related to **LD_LIBRARY_PATH** from the **siebenv.sh** file (generally located in the **siebsrvr** directory), and set them to be accurate (insert all the definitions from the **siebenv.sh** file). This definition is needed to run **srvrmgr** and **sarmanalyzer** on the SiteScope machine with mount. It is recommended to copy the **srvrmgr** and **sarmanalyzer** directories to SiteScope for better performance.

Troubleshooting SARM-Related Issues

This section includes:

SARM Does Not Work

Make sure that all steps of the following checklist are followed.

Note: The following is applicable for Siebel servers installed on the NT environment only.

---

1. Check that the SARM Analyzer path that you defined for the site is accessible via SiteScope.
2. Check that at least one Web Server, one Application Server, and one Gateway Server have been defined for the Site.
3. Check that the log folder defined for the Web Server is accessible via SiteScope.
4. Check that the log folder defined for the Application Server is accessible via SiteScope.
5. Check that SiteScope is running with a user on the SiteScope machine:
   - ➤ In the SiteScope machine, open **Services**.
   - ➤ Right-click the SiteScope service to open its properties.
   - ➤ Click the **Log On** tab.
   - ➤ Make sure that **This Account** is checked.
   - ➤ Make sure that the user name and password are correct.
6. To run the SARM Analyzer tool, make sure that the directory **<SiteScope_home_directory>\tools\sarmdiagnostics** exists on the SiteScope server.
7. Check that the Siebel Server Manager properties are defined properly for the site, in Siebel configuration in Mercury Business Availability Center (for more information, see “Manual Configuration for Specific Siebel CIs” on page 416).
8. Make sure that SiteScope is attached.
9. If you checked the entire list and SARM still does not work, check the following options:

➤ "SARM Data Does Not Generate Properly" on page 472

➤ "SARM Analyzer Crashes" on page 473

SARM Data Does Not Generate Properly

If the **No Relevant Sessions** error message is issued when you know that you should have data, SARM might not generate properly.

To identify the problem:

1 Open one the .xml files located in the relevant SiteScope in the following directory:
<SiteScope_Install>\cache\tempbyage\<TimeStamp>_SIEBEL_SARM\<web_server>_<App_server>

Note: If there are no .xml files in that directory follow the next procedure.

---

2 Select any of the last requests in the .xml file:

➤ If the request doesn't include a **<SiebsrvrDetails>** section with a **<Group>** node under it, then Siebel is not generating the SARM data properly.

➤ If the request does include a **<SiebsrvrDetails>** section with a **<Group>** node under it, then follow the procedures below (for details, see below or "SARM Analyzer Fails to Run" on page 473).

To solve the problem:

Delete all the SARM files from the Application Server and from the Web server.

If this does not help, restart the Siebel machine.

SARM Analyzer Crashes

If the **No Relevant Sessions** error message is issued when you know that you should have data, SARM Analyzer might have crashed because the requests counter was reset to **0** in the middle of the session without any logical reason. Another indication is that it takes at least five minutes for this error to appear, because the execution of the batch files in SiteScope times out.

To identify the problem:

SARM Analyzer has crashed if any one of the following situations occurs:

- A message (**No relevant sessions were found**) is issued, indicating that there are no sessions when you know there should be sessions.
- This indication almost always occurs – The timestamp of the **crash<nnn>** file in the SARM Analyzer folder corresponds to the time when you ran the User Session Trace.
- This indication is rare – An error message is issued in the SiteScope machine.

To solve the problem:

Using PC Anywhere, connect to the Siebel web server, and delete (locally) the last SARM binary file from the web server log folder.

If this does not help and the problem occurs again, restart the Siebel machine.

SARM Analyzer Fails to Run

When you run the SARM Analyzer from a remote machine (not locally on the SiteScope machine), the SARM Analyzer fails to run.

To identify the problem:

SARM Analyzer failed to run if any one of the following situations occurs:

- A message ((**No relevant sessions were found**) is issued, indicating that there are no sessions when you know there should be sessions.
- One of the following errors was added to the SiteScope **sarmAnalyzer.log** log in **<SiteScope installation directory>\Tools\sarmDiagnostics\log\sarmAnalyzer.log** during the execution of the SARM diagnostics:

- **Failed to analyze app server SARM files**
- **SarmAnalyzer failed**
- **Error running command: <command_name>**

Note: The problem occurs because of a different domain or because of permissions issues.

To solve the problem:

Copy the SARM Analyzer to reside locally on the SiteScope machine.

SARM Configuration Issues

SARM configuration is not correct, if one of the following situations occurs:

- SARM is configured to store data for long time period (several days). Processing takes too long.
- The flush ratio on the Web server is approximately 45 minutes.

To identify the problem:

Configure SARM correctly.

A Sitescope Server Failed to Access a Siebel SARM Folder or File

After running SARM Diagnostics, the error message **A Sitescope server failed to access a Siebel SARM folder or file. Make sure all SiteScope servers have the proper permissions.** is displayed.

This usually happens because either the user used to log to the SiteScope Service does not have the appropriate permissions to access the SARM web or the application folders, or because the user running the SiteScope service does not have the appropriate permissions to access those log folders.

To solve the problem:

1 Go through steps 3-8 of the SARM Does Not Work procedure above. For details, see "SARM Does Not Work" on page 471.

2 Log in to one of the SiteScope machines with the SiteScope username and password, and try to access the SARM folders defined in BAC.

The Operation Completed with Several Errors

After running SARM Diagnostics, the error message **The operation completed with several errors. Please check the logs for more information.** is displayed.

This error can be caused by a number of reasons, including unexpected SarmAnalyzer output, network issues, or Server manager errors.

No working SiteScope server could be found to process SARM dataTo check which errors happened, go through the following log files and search for error messages logged around the time you invoked User Session Breakdown:

- On the Mercury Business Availability Center machine: **<Mercury Business Availability Center home directory> /log/EJBContainer/siebel.ejb.log**
- On the SiteScope machine: **<SiteScope home directory>/tools/sarmDiagnostics/log/sarmAnalyzer.log**

Timed-out Execution of a SARM Task or sarmanalyzer Execution

If the sarmAnalyzer.log (SiteScope) indicates that a SARM task or sarmanalyzer execution has been timed-out, increase the default timeout for either a SARM task or a SARM analyzer execution. For details, see "Increasing the Default Timeout for Either a SARM Task or a SARM Analyzer Execution" on page 420.

If the **Siebel.ejb.log** (on the Centers server) indicates that an execution of a SiteScope monitor got timed-out, change the default timeout for the execution of this monitor. For details, see "Changing the Default Timeout for the Execution of a SiteScope Monitor" on page 421.

No Working Sitescope Server Could Be Found

If the message **No working SiteScope server could be found to process SARM data.** is issued when running SARM Diagnostics, proceed as explained in this section.

To solve the problem:

1. Open the **Advanced Options** section of the User Trace Breakdown page in Mercury Business Availability Center. For details, see "Running the SARM - User Trace Breakdown Diagnostic Tool" on page 298.
2. Verify that the SiteScope servers that are selected in **Using SiteScope:** list are the servers you want to use for SARM diagnostics.
3. Go through steps 5-8 of SARM does not work above (for details, see "SARM Does Not Work" on page 471), for these servers.
4. If this doesn't help, restart the SiteScope servers.

Database Breakdown

This section describes how to solve Database Breakdown-related issues.

Problem with looking for a task using the Siebel Database Breakdown tool

If the Siebel Site uses a gateway with an additional SSL that supplies dynamic IDs for every user session, searching for the proper tasks using the Siebel Database Breakdown tool may be problematic.

To solve the problem:

A possible solution is to find the correlation in the VuGen script and to update the Siebel Application's user in the Siebel Application Configuration.

To do so, click **Admin** > **Siebel Configuration**, click the appropriate site, click the **Edit Application** button for the appropriate application, and update the Siebel Application's user in the **Script user name** box.

Note: It is recommended to use a script with no more than five transactions when using the Database Breakdown diagnostics.

Processes

This section describes how to solve processes-related issues.

Processes tool does not function or files do not get through SiteScope

- Make sure that the SiteScope user has permission to log to the Siebel machines.
- If another user is currently running SiteScope or ran SiteScope when the SiteScope server had not been booted, restart the SiteScope machine and the SiteScope service.

Tasks

This section describes how to solve task-related issues.

No. of tasks in error Counter

Note: The **No. of tasks in error** counter affects the number of sessions that is displayed in BAC for Siebel Dashboard because sessions are a subset of tasks and the list of tasks is sent with this counter.

- In **SiteScope 8.2** – The **No. of tasks in error** counter reports all the running tasks (regardless of their start time), and all the tasks that started in the last hour and have completed or exited with error in the last hour.

  If you configure, in the advanced options of the SiteScope monitor, the **Siebel Tasks Time Window** parameter to **0**, the **No. of tasks in error** counter will display all the tasks regardless of their start time.
- In **SiteScope 7.9.5** with **Cumulative patch 12** – The behavior of the **No. of tasks in error** counter is like in SiteScope 8.0.
- In **SiteScope 7.9.5** – the **No. of tasks in error** counter is, by default, defined to report only the tasks that started in the last hour.

  You can set the **No. of tasks in error** counter to display all the tasks by configuring, in the advanced options of the SiteScope monitor, the **Siebel Tasks Time Window** parameter to **0**.

Troubleshooting

This section describes how to troubleshoot some of the problems. It includes the following topics:

Specifying the Default SiteScope Monitors

To specify the default SiteScope monitors you want to work with, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Siebel**, and locate the **Default SiteScopes for SARM diagnostics** entry in the **Siebel - Siebel SARM Breakdown** table. Modify the value to one of the following:

- the SiteScope monitor names separated by semicolons (for example: rca3;rca4)
- **ALL** if you want to use all attached SiteScope monitors

Correct Location

In the SiteScope machine, check that the following files are located in the corresponding location:

Folder	File name
<SiteScope_Installation_directory>\Tools\sarmDiagnostics\lib	➤ sarmDiagnostics.jar ➤ javacore.jar ➤ log4j.jar ➤ logger.jar
<SiteScope_Installation_directory>\Tools\sarmDiagnostics\bin	sarmDiagnostics.bat
<SiteScope_Installation_directory>\Tools\sarmDiagnostics\conf	log4j.properties

If any of those files are missing, re-install the SARM diagnostics patch or the SiteScope 7.9.5 cumulative patch 17 or higher.

27

Upgrading from Mercury Business Availability Center for Siebel 5.1 SP1

This chapter describes the steps involved in upgrading Mercury Business Availability Center from 5.1 SP1 to 6.2. The upgrade is performed automatically. Some configuration may be lost during the upgrade. Some manual procedures are available to recover some of the configuration.

Upgrade Procedure

When upgrading an existing implementation of Mercury Business Availability Center for Siebel version 5.1 to the Siebel solution (Mercury Business Availability Center version 6.2), proceed as follows:

1 If, in version 5.1, you had defined servers:

➤ Check that all the IP addresses of the Siebel server that were defined in version 5.1 are in the IP addresses range that is used in the discovery process.

If they are, the discovery process discovers them and connects them to the Siebel topology.

If not, add them manually. For details, see step 3.

➤ If you have a license for other discovery patterns, run them to discover these servers (a load balancer, for example). These servers are discovered but are not part of the regular architecture (Application Server, Web Server, Database Server, and Gateway Server). Connect them manually to the Siebel topology. For details, see step 4.

2 Run the Siebel automatic discovery patterns.

3 If some of the Siebel servers that were added in version 5.1 are not in the IP addresses range that is used in the discovery process, add them manually to the Siebel topology after you have run discovery. For details, see "Working with CIs in IT Universe Manager" in *IT Universe Manager Administration*.

4 Connect manually the servers that are discovered by the discovery process but are not part of the regular architecture), to the Siebel topology. For details, see "Working with CIs in IT Universe Manager" in *IT Universe Manager Administration*.

5 For each Siebel Application CI, use the **Attach Monitoring CI** option in the IT Universe to relate the application to the Business Process Steps monitoring it. For details, see "Attaching Business Process Monitor Transactions to Siebel Application Components" on page 406.

6 For each Siebel Application CI that is entered manually, enter the appropriate value in the **Emulated Transaction User Name** box. For details, see "CIT-Specific Properties" in *IT Universe Manager Administration*. For details about the **Emulated Transaction User Name** property, see "General Administration" on page 420.

7 For each Siebel Component and Siebel Application Server monitored by SiteScope, add the **Number of sessions** counter to the existing monitor, in SiteScope. For details, see SiteScope documentation.

8 Enter manually, the user-defined server types and CIs that were lost using the CMDB Administrator, using the **Add Related CIs** option. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.

9 If automatic discovery did not discover all Siebel Applications you defined in version 5.1, recreate them manually, using the **Add Related CIs** option. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.

10 Recreate manually the missing links between Siebel CIs (entities) and other CIs (if automatic discovery fails to create them), before you run Siebel diagnostics. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.

11 Reports:

- ➤ Recreate the customized Siebel-related reports and the Siebel-customized trend reports you defined in 5.1.
- ➤ The network analysis and the multi-profile summary reports are not upgraded and are not be available.

12 Recreate the custom-made Siebel Dashboard views you defined in 5.1.

13 Redefine the thresholds that you defined through Dashboard Admin, overriding Monitoring Administration definitions.

Notes and Limitations

- ➤ The split screen that showed both the topology and the KPIs on the selected element/CI is not available in 6.1.
- ➤ The Sites View is replaced by the standard Dashboard views and appropriate KPIs. The Siebel Enterprises view is created.
- ➤ The SiteScope adapter creates the monitors and measurements CIs, therefore, historical samples data will still be available, after the upgrade of the profile database is performed.
- ➤ A dimension/Key Performance Indicator (KPI) that appeared for a Siebel element/configuration item (CI) will appear as a measurement for the Siebel KPI.
- ➤ The feature displaying the Web Extension Server and the Siebel Application Server CIs used when an Application is clicked in the topology is replaced by the **Show Related CIs** context menu. For details, see Show Related CIs in "Searching for Configuration Items" in *Working with the CMDB*.
- ➤ The capability to customize trend reports per CI has been replaced by the capability to customize trend reports per CI type.

- The Component Group, Component, and Siebel Web Application CIs exist now in the CMDB. They are not monitoring information linked to the Siebel Application Server CI as in version 5.1.
- A user sees the Siebel Enterprises view in Dashboard or is able to configure the Siebel Enterprises view, only after a user with the appropriate administration privileges has granted that user the appropriate permissions.

Part VI

Administering the SOA Solution

28

Service-Oriented Architecture Solution

This chapter describes how to implement the first stage of the Mercury Business Availability Center solution for monitoring your Service-Oriented Architecture (SOA) enterprise environment. (Further stages will be supported in future Mercury Business Availability Center versions.)

Overview of the SOA Solution

Mercury Business Availability Center enables you to monitor your SOA environment, by monitoring the performance of SOA components within the environment. The data is collected by different Mercury Business Availability Center components:

- Discovery packages identify and map the SOA-based applications in your system from the UDDI registry, and from the Web services deployed on top of IBM WebSphere and BEA WebLogic containers.
- Web service metrics and UDDI server health data is collected by dedicated SiteScope monitors.
- Web service performance is monitored by creating Business Process Monitor transactions that run Web services scripts.

You map the CIs created by the discovery process with the CIs created for the monitoring data (either using the Monitor Deployment Wizard, or by manually attaching the CIs), to produce an integrated Web Services view.

Using Discovery for SOA

Mercury Business Availability Center includes discovery packages and out-of-the-box views for monitoring your SOA environment. The Discovery packages are deployed from **Admin** > **CMDB Administration** > **Discovery Manager**.

The UDDI Registry module, part of the Webservice Discovery package, maps the nodes, Web services, and Web service operations that are discovered from the UDDI registry (for UDDI versions 2 and 3).

Running the module automatically populates the Web Services view with the created CIs, according to the TQL for the view. For examples of the Web Services view and TQL, see "Web Services View and Reports" on page 491.

In addition, running the J2EE - WebLogic and J2EE - WebSphere packages discovers Web services deployed on top of these containers. CIs are automatically created for the discovered Web services and added to the Web Services view.

For information on deploying and running Discovery packages, see "Deploying Packages" and "Running the Discovery Process" in *Discovery Manager Administration*.

Limitations

- Segmented WSDL files are not supported. If you use the import mechanism to break down the WSDL file into several segments, it will cause data inconsistency in the discovery.
- The WSDL file should be placed in the UDDI registry according to the following UDDI hierarchy (from the UDDI technical specification by OASIS): **BusinessService** > **TemplateBinding** > **TModel** > **OverViewDoc**. In any other location it will not be found.

SiteScope Monitors for SOA

SiteScope provides three monitors that are tailored to monitoring your SOA environment, configured in **Admin** > **Monitor Administration**:

- **UDDI Monitor:** For details on using this monitor, see "UDDI Monitor" in *Configuring SiteScope Monitors*.
- **Web Service Monitor:** For details on using this monitor, see "Web Service Monitor" in *Configuring SiteScope Monitors*.
- **Technology Web Service Integration Monitor:** For details on using this monitor, see "Technology Web Service Integration Monitor" in *Configuring SiteScope Monitors*.

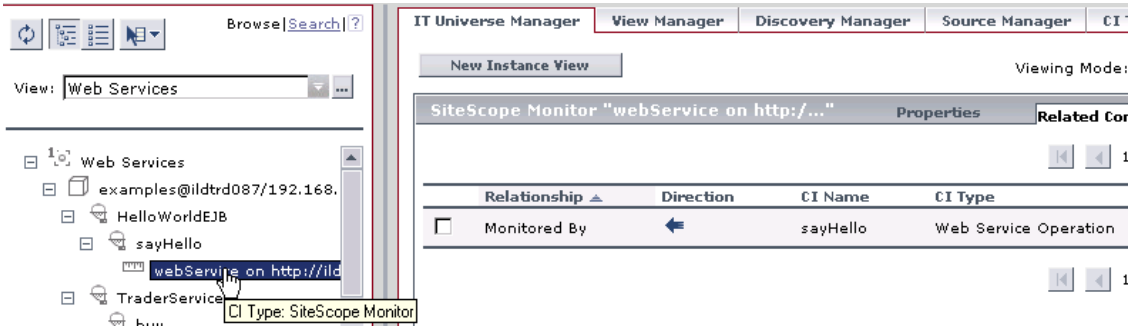
Using the Monitor Deployment Wizard to Map SiteScope Monitors to the Web Services View

You can map the SiteScope monitors for SOA (the **UDDI Monitor**, the **Web Service Monitor**, and the **Technology Web Service Integration Monitor**) directly onto the CIs added by the discovery process to the Web Services view, using the Monitor Deployment Wizard. This deploys the SiteScope monitoring CIs generated by the relevant SiteScope monitors, onto the higher level UDDI Registry, Web Service, and Web Service Operation CIs, creating a Monitored By relationship between them.

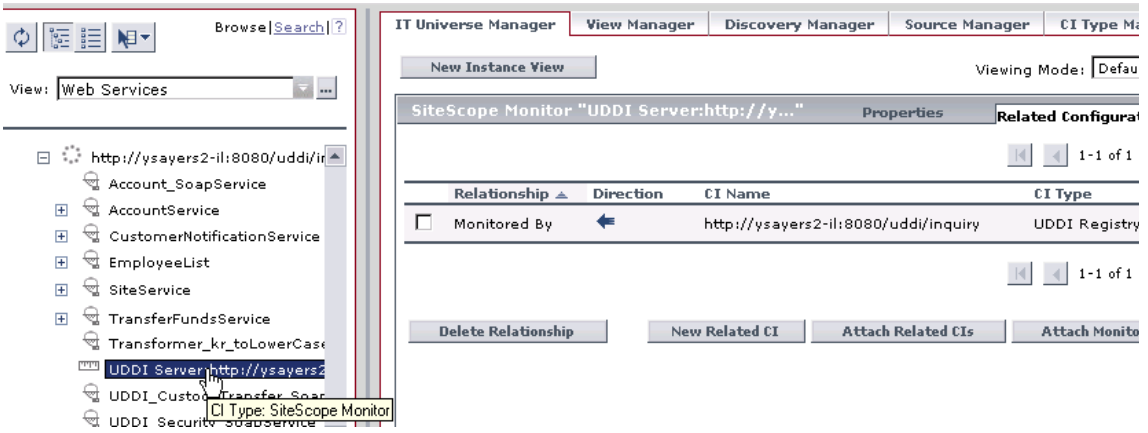
For details on using the Monitor Deployment Wizard, see "Monitor Deployment Wizard" in *Configuring SiteScope Monitors*.

In **Admin** > **CMDB Administration** > **IT Universe Manager**, you can view the resulting hierarchy after using the Monitor Deployment Wizard to deploy SiteScope monitors onto the Web Services view CIs.

The following example shows, for a J2EE Domain containing Web Service and Web Service Operation CIs (discovered by a J2EE - WebLogic discovery module), a SiteScope Monitor CI of Web Service type deployed onto a Web Service Operation CI:



The following example shows, for a UDDI Registry (discovered by a UDDI Registry discovery module), a SiteScope Monitor CI of UDDI Monitor type deployed onto the UDDI Registry CI.



Business Process Monitor Transactions for SOA

In **Admin > Monitor Administration**, you can use the Business Process Profile Wizard to define Business Process profiles, containing transaction monitors that run scripts to check Web service performance. For more information, see "Creating Business Process Profiles" in *End User Management Data Collector Configuration*.

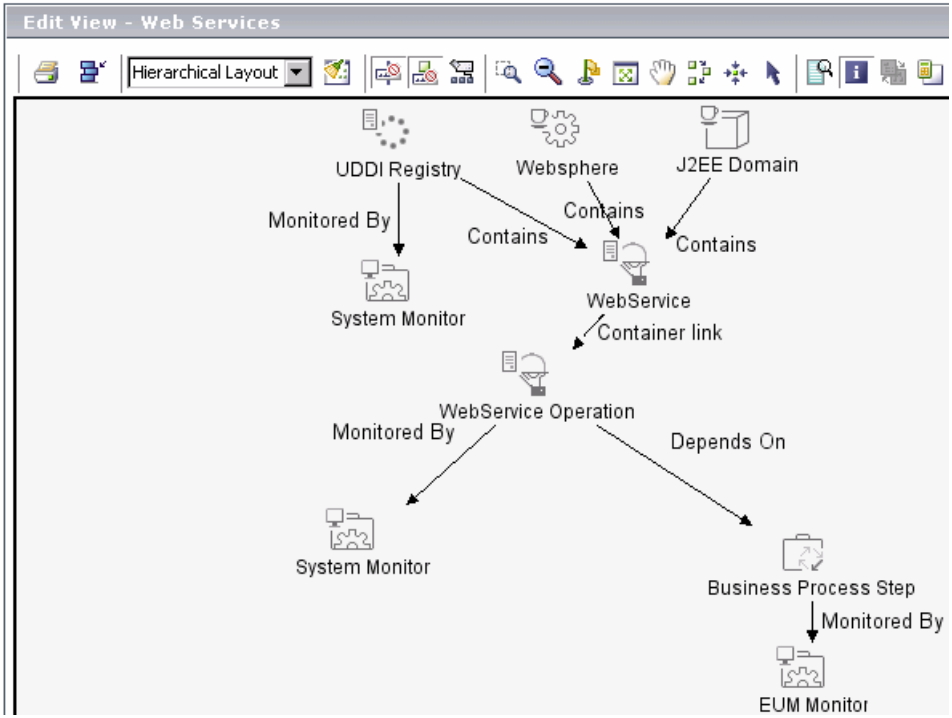
After Business Process Monitor has run the scripts, the resulting BPM Transaction from Location CIs are added to the Monitors View and End Users Monitors View.

To map the SOA CIs in the Web Services view (discovered during the discovery process) to the relevant BPM Transaction from Location CIs, you must manually attach the monitoring CIs to the higher level CIs. This is done in **Admin > CMDB Administration > IT Universe Manager**. For details, see "Attaching Existing CIs" in *IT Universe Manager Administration*.

Web Services View and Reports

The SOA folder containing the Web Services pattern view is part of the list of available views in **Admin** > **CMDB Administration** > **View Manager**.

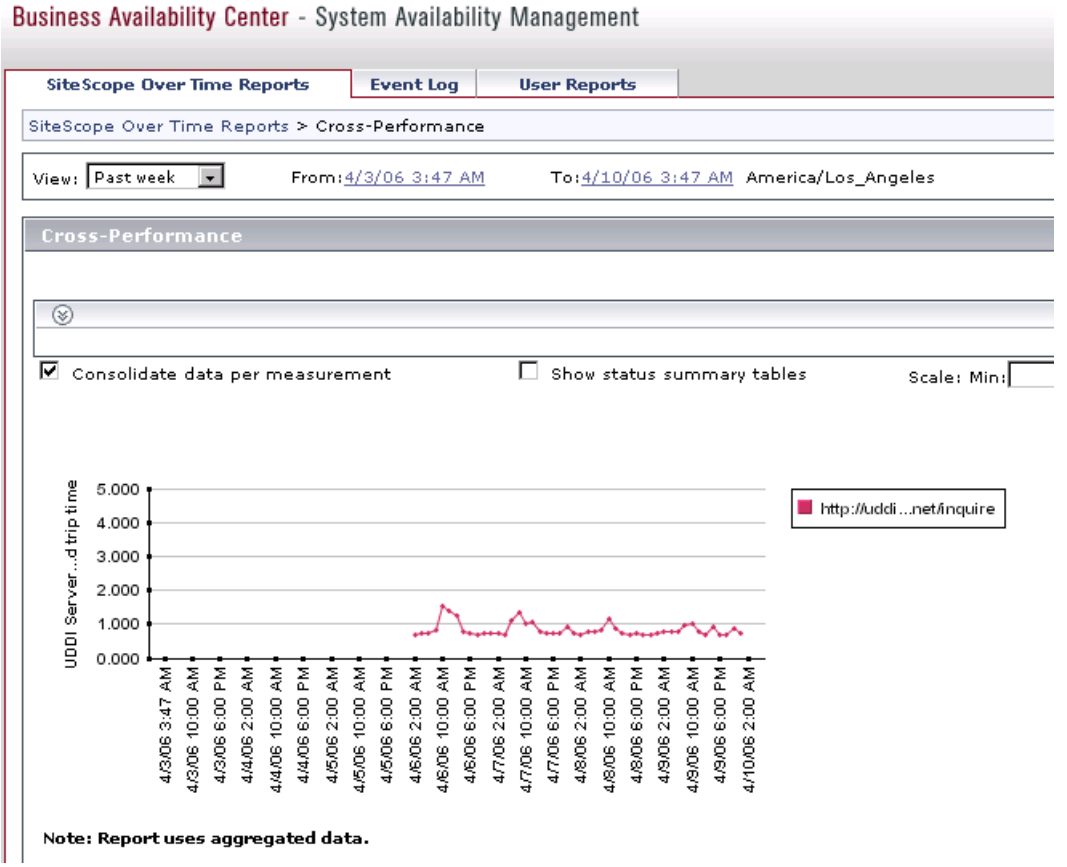
In View Manager you can open and edit the TQL for the view. The TQL is set up as follows:



For more information, see "Working with Pattern Views" in *View Manager Administration*.

The Web Services view reflects the UDDI business hierarchy, Web services, and underlying infrastructure, and is available in Dashboard and Service Level Management (accessed from the **Applications** menu).

Reports and alerts are available for the SOA data as with any other monitoring data.



Part VII

Appendixes

A

Mercury Diagnostics and Mercury Business Availability Center Integration

If you are a licensed user, you can integrate Mercury Diagnostics with Mercury Business Availability Center. This appendix explains how to begin the Mercury Diagnostics registration procedure.

The Mercury Diagnostics application is used to gain end-to-end visibility and comprehensive diagnostics for Java 2 Enterprise Edition (J2EE), .NET-connected, SAP, Oracle, and other complex environments.

Setting Up Mercury Business Availability Center for Mercury Diagnostics

To view Mercury Diagnostics data in Mercury Business Availability Center, you must register the Mercury Diagnostics server machine in Mercury Business Availability Center.

To register Mercury Diagnostics:

1 Access **Admin** > **Diagnostics**, to open the Mercury Diagnostics Server Details page.

If the user name with which you logged in does not have permissions for making changes on the Mercury Diagnostics server, a message is displayed instead of the Mercury Diagnostics page.

2 Enter the details of the server as follows:

Diagnostics server host name – enter the name of the machine on which the Mercury Diagnostics server is running

Diagnostics server port number – accept the port number or enter the port number through which Mercury Diagnostics listens to server traffic

Diagnostics server protocol – select the communication protocol (HTTP or HTTPS) through which Mercury Business Availability Center connects to Mercury Diagnostics

If the server name is incorrect or the server is unavailable, an error message is displayed.

3 Click **Submit** to register the server with Mercury Business Availability Center.

4 For help with the remainder of this procedure for registering the server, refer to *Mercury Diagnostics Installation and Configuration Guide* (**Help** > **Diagnostics Help**).

For information on viewing Mercury Diagnostics data in Mercury Business Availability Center, refer to *Mercury Diagnostics User's Guide*.

Troubleshooting

Problem: After connecting Mercury Business Availability Center to the Mercury Diagnostics server, a message is displayed: "Session does not exist."

Solution: Check that Internet Explorer is set up to allow the browser to submit cookies to the Mercury Diagnostics server:

To set up Internet Explorer to allow the browser to submit cookies:

1. In Internet Explorer (version 6.0), select **Tools** > **Internet Options** > **Privacy**.
2. In the Web Sites section, click the **Edit** button.
3. In the Per Site Privacy Actions dialog box, enter the Mercury Diagnostics server DNS domain name.
4. Click **Allow**, **OK**, and **OK**.

Index

C

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W