Configuring AdminPoint settings

This section includes the following topics:

Changing passwords in AdminPoint

You can change your password from the Settings menu in StartPoint or AdminPoint.

To change a password.

1. On the Settings menu, click **Change Password**.
2. In the **Current password** field, enter your current password.
3. In the **New password** field, enter your new password.
4. Confirm the new password by typing the new password again.
5. Click **OK** to save the new password, or **Cancel** to close the dialog box without saving.

Defining roles and users in Precise

The following section describes how to define the roles and users in Precise.

About roles and users in Precise

Precise provides a centralized role management capability across the entire Precise deployment, including granting specific users the ability to access a specified technology/environment/AppTier/instance and perform restricted actions on it. Furthermore, Precise administrators are able to delegate sub-sets of their permissions to other users, thus allowing them to manage their own users and permissions.

User permissions are role-based. This means that each user that is defined in Precise should have at least one role that is assigned to him. A role defines the allowed permissions on a sub-set of resources.

Permissions can be defined for the following resources:

- Technology
- Environment
- AppTier
- Instance

Each role can have resources assigned only from one of the above-named scopes. The following table describes the predefined roles for Precise.

Table 4-1 Pre-defined roles for Precise

Role	Description
Precise manager	Allowed to install all technologies, administrate all technologies, monitor and tune all technologies. Included permissions: • ADMINISTRATE.FULL_CONTROL on ALL technologies. • MONITOR.FULL_CONTROL on ALL technologies. • TUNE.FULL_CONTROL on ALL technologies. This role cannot be modified or deleted.
Precise guest	Allowed to monitor the default environment.
<Techology> manager	Allowed to install, monitor and administer the specified technology. Included permissions: • ADMINISTRATE.FULL_CONTROL on <Technology> and operating system technologies. • MONITOR.FULL_CONTROL on ALL <Technology> and operating system technologies. • TUNE.FULL_CONTROL on <DB Technology> (if a database).

Precise Monitor	Allowed to monitor and tune all technologies. Included permissions: • MONITOR.FULL_CONTROL on ALL technologies. • TUNE.FULL_CONTROL on ALL technologies.

Delegating permissions

Any user assigned with the ADMINISTRATE.EXECUTE permission on the Precise technology can customize roles and permissions. This user can customize roles and permissions only in the context of the permissions assigned to him, for example: a user with MONITOR.VIEW permission on the environment “Production Environment” can grant the monitor view permission on the “Production Environment” environment to other users.

If a user has permissions on all resources of a specific scope, he can delegate all resources belonging to all other scopes too. For example: a user with the following roles:

- Role that includes user assigned with the ADMINISTRATE.EXECUTE permission on the Precise technology
- Role that includes all environments (The "All Environments" check box is checked for the role) can delegate this permission on all technologies, AppTiers, and instances.

To delegate a user’s permission(s) to other users

1. Create a new role with the appropriate permissions
2. Assign the role to another existing user, or to a new user

Performing activities on roles

You can define, edit, clone, and delete roles. To be able to define, edit, clone, and delete roles, you must have ADMINISTRATE.EXECUTE permission on the Precise technology. See Delegating permissions.

To define, edit, clone, or delete roles

1. From AdminPoint, on the Settings menu, click **Roles**.
2. Specify the permissions for the role.

About nodes as they apply to roles and users

Roles apply on all nodes in an installation. Resource-permissions are node related; each node will have only the relevant resource-permissions assigned to it, based by its scope.

Table 4-2 Resource permissions for nodes based by scope

Scope	Description
Technology	You need to specify in the role dialog the nodes it is associated to. The role can be associated to a specific node, or to the “all” node option. If the “all” (default) node option is selected, new attached nodes are added automatically to the existing list of roles for that role.
Environment	The node association is based on the environment's node. monitor.view permission can only be set on the environment scope.
AppTier	The node association is based on the AppTier's node.
Instance	The node association is based on the instance's node.

Defining a role

You can define a role via the Role Settings dialog box.

> The case-sensitive role name can have a maximum length of 50 characters. The valid characters are A-Z, a-z, -, _, , space, @, and 0-9.

To define a role

1. In the Role Settings dialog box, click **Add**.
2. In the Role Settings - Add dialog box, insert a role name for the new role.
3. Select a role scope: **technology**, **instance**, **environment**, or **AppTier**.
4. Select the resources to which this role will apply.

When you select “ALL parameters for the technology (or other selected scope),” all of the resources for the selected scope are included.

1. Select the permissions for the selected resources.
2. For the technology scope, click **Change node** to select the nodes this role applies. By default, “all” is selected.
3. Click **OK** to save your settings.

Editing a role

You can edit a role via the Role Settings dialog box.

To edit a role

1. In the Role Settings dialog box, select the role you want to edit and click **Edit**.
2. Make the required changes (where needed) for role name, scope, resources, permissions and nodes.
3. Click **OK** to save your settings. The changes are immediately applied to all logged users.

Cloning a role

You can clone a role via the Role Settings dialog box.

To clone a role

1. In the Role Settings dialog box, click **Clone**.
2. Make the required changes (where needed) for role name, scope, resources, permissions and nodes.
3. Click **OK** to save your settings.

Deleting a role

You can delete a role via the Role Settings dialog box.

> Apart from the Precise manager entity, you are able to delete all available roles.

To delete a role

1. In the Role Settings dialog box, select the role you want to edit and click **Delete**.
2. Click **Yes** to confirm, if you want to delete this role.

Performing activities on users

You can define, edit, and delete users. A user can only give or revoke permissions he is permitted to delegate. Whether you define, edit, or delete a user, you need to start in the Users dialog box, and must have ADMINISTRATE.EXECUTE permission on Precise technology.

> If using LDAP integration, a Precise user can only manage resources and assign permissions. All other user and role-related operations will be blocked. For more information on LDAP, see the "Configuring a secured Precise system" section in the *Precise Installation Guide*.

To define, edit, or delete users

- From AdminPoint, on the Settings menu, click **Users**.

Defining a user

You can define a user via the Users dialog box.

> The user name (not case-sensitive) can have a maximum length of 50 characters. The valid characters are A-Z, a-z, -, _, space, and 0-9.

To define a user

1. In the User Settings dialog box, click **Add**.
2. Insert a user name for the new user.
3. Insert a password for this user and confirm this password.
4. Click an arrow to add one or more roles, by moving the appropriate role(s) from the left pane to the right pane.
5. Click **OK** to save your settings.

Editing a user

You can edit a user via the User Settings dialog box.

To edit a user

1. In the User Settings dialog box, select a user from the list, and click **Edit**.
2. Insert a password and confirm it. The user can change this password after login.

3. Click an arrow to connect this user to one or more roles, by moving the appropriate role(s) from the left pane to the right pane.
4. Click an arrow to disconnect this user to one or more roles, by moving the appropriate role(s) from the right pane to the left pane.

> “Admin” user roles cannot be changed.

5. Click **OK** to save your settings.

Deleting a user

You can delete a user via the User Settings dialog box.

> “Admin” user roles cannot be changed.

To delete a user

1. In the User Settings dialog box, select a user from the list.
2. Click **Delete**.
3. Click **Yes** to confirm if you want to delete this user.

About role-based access

The following table describes the permissions needed to perform an operation.

The user can view the environment in StartPoint; the data which the user can view, and the operations he can perform are based on the roles given to him. See “About role management in Alerts” on page 169.

Table 4-3 Permissions needed to perform an operation

Operation	Required permission	Required resource
Install instance	ADMINISTRATE. INSTALL	The instance’s technology. To install an instance, the ADMINISTRATE.INSTALL permission is also required on each environment where the user can install the instance.
Edit/uninstall instance	ADMINISTRATE. INSTALL	The instance.
Set instance AppTiers	ADMINISTRATE. EXECUTE	The instance.
Set instance customized columns	ADMINISTRATE. EXECUTE	The instance.
Apply update	ADMINISTRATE. INSTALL	Precise technology on all nodes.
Change instances customized column headers	ADMINISTRATE. EXECUTE	Precise technology on all nodes.
Apply license	ADMINISTRATE. EXECUTE	Precise technology on all nodes.
Add node	ADMINISTRATE. INSTALL	Precise technology on all nodes.
Edit/remove node	ADMINISTRATE. INSTALL	Precise technology on the node.
Add environment	ADMINISTRATE. EXECUTE	Precise technology on the node the environment belongs.
Edit/remove/customize columns environment	ADMINISTRATE. EXECUTE	The environment.
Change environments customized column header	ADMINISTRATE. EXECUTE	Precise technology on all nodes.

Add AppTier	ADMINISTRATE.EXECUTE	The AppTier's environment.
Edit/remove AppTier	ADMINISTRATE.EXECUTE	The AppTier.
Manage roles and users	ADMINISTRATE.EXECUTE	Precise technology on all nodes.
Manage clusters	ADMINISTRATE.EXECUTE	The cluster's technology.
Manage downtime	ADMINISTRATE.EXECUTE	The instance.
Manage SLA availability	ADMINISTRATE.EXECUTE	The instance's technology.
Manage SLA response time or service time	ADMINISTRATE.EXECUTE	The instance's and Precise technology on the nodes the user wants to manage.
Manage grouping	ADMINISTRATE.EXECUTE	Precise technology on the node the group is defined and on the technology the group is defined.
Manage locations	ADMINISTRATE.EXECUTE	Precise technology on the node the location is defined.
View Environment in StartPoint	MONITOR.VIEW	The environment.
Create Support file	ADMINISTRATE.EXECUTE	Precise technology

About configuring planned downtimes

A planned downtime is a period during which an instance is considered not available, for example for maintenance. During a planned downtime, no data is collected for the specified time period so that availability calculations remain accurate. For example using Precise for SAP, no data is displayed for a planned downtime period in the Availability tab. In addition, Alerts does not report instance-related problems during this planned downtime period.

A planned downtime can be defined as a regular downtime, which occurs only once, or as recurring downtime, which returns periodically. You can define, update, and delete planned downtime periods for all instances by using the Planned Downtime dialog box. In this dialog box, scheduled planned downtimes appear in both the Instance table and in the calendar. You can use the arrow buttons above the calendar to scroll to a wider time frame for planned downtimes.

Adding a planned downtime

You can add a planned downtime via the Planned Downtime Settings dialog box.

To add a planned downtime

1. On the Settings menu, click **Downtime**.
2. From the technologies drop-down list, select the technology you want to define the downtime for.
3. In the Planned Downtime Settings dialog box, below the table, click **Add**.
4. In the Planned Downtime Settings — Add dialog box, from the Instance list, select the instance for which you want to add a planned downtime.
5. Set the time range during which the planned downtime must occur. Use the From/To dates and time settings.
6. If the downtime is recurrent, click **Recurrence**.
7. In the Planned Downtime Settings — Add Recurring Downtime dialog box, define how often you want the downtime to recur.
    - **Daily**. The interval in days at which the downtime is to recur.
    - **Weekly**. The weekday and interval in weeks at which the downtime is to recur.
    - **Monthly**. One of the following definitions:
        - On which day (numeral) of the month and at which interval in months the downtime is to recur
        - On which weekday of the month and at which interval in months the downtime is to recur
8. If the downtime period is limited, select the **End by** option and set the date.
9. Click **OK**.

Editing a planned downtime

You can edit a planned downtime via the Planned Downtime Settings dialog box.

To edit a planned downtime

1. On the Settings menu, click **Downtime**.
2. From the technologies drop-down list, select the technology you want to edit the downtime for.
3. In the Planned Downtime Settings dialog box, below the table, click **Edit**.
4. In the Planned Downtime Settings — Edit dialog box, from the Instance list, select the instance for which you want to edit a planned downtime.

5. If the downtime is recurrent, click **Recurrence**.
6. In the Planned Downtime Settings — Edit Recurring Downtime dialog box, define how often you want the downtime to recur.
    - **Daily**. The interval in days at which the downtime is to recur.
    - **Weekly**. The weekday and interval in weeks at which the downtime is to recur.
    - **Monthly**. One of the following definitions:
        - On which day (numeral) of the month and at which interval in months the downtime is to recur
        - On which weekday of the month and at which interval in months the downtime is to recur
7. If the downtime period is limited, select the **End by** option and set the date.
8. Click **OK**.

Deleting a planned downtime

You can delete a planned downtime via the Planned Downtime Settings dialog box.

To delete a planned downtime

1. On the Settings menu, click **Downtime**.
2. From the technologies drop-down list, select the technology and instance you want to delete.
3. In the Planned Downtime Settings dialog box, below the table, click **Delete**.

About configuring SLAs

Service Level Agreements (SLAs) define the performance goals of an information system. They help you identify when the service level that is associated with your information system as a whole, or with some parts of it (such as Web pages), fall below a threshold. When you discover a drop in performance, further investigation and drill down operations are required to isolate the location of the drop and to pinpoint its cause.

You can define three types of SLAs:

- **Service Time**. Defined for activities of a specific technology. Service Time SLAs refer to the net duration needed to process a request, from the time the request arrived until the time the service that is associated with the request was completed. For this SLA type, you define threshold values for activity durations. These values represent units of time and distinguish between the different levels of service.
  Service Time SLAs are available for the following technologies: .NET, J2EE, Oracle, SQL Server, Web, Tuxedo, Oracle Applications, WebSphere MQ, and other technologies that are defined as part of the ‘Other’ AppTier.
- **Response Time**. Defined for activities of a specific application. Response Time SLAs refer to the total duration needed to process an application request, from the time the user initiated the request until that time when the response to the request is returned to the user. For this SLA type, you define threshold values for activity durations. These values represent units of time and distinguish between the different levels of service.
  Response Time SLAs are available for the following technologies: Web and SAP.
- **Availability**. Indicate the lowest acceptable level of an instance's availability. For Availability SLAs, you define a threshold value for each instance. The value represents the minimum percentage of time an instance should be up for its availability to still be considered acceptable.
  Availability SLAs are available for the following technologies: .NET, J2EE, Oracle, SQL Server, Sybase, Web, Tuxedo, Oracle Applications, WebSphere MQ, and Oracle Applications.

Further, to help you manage your information system proactively, you can define a near-breach threshold for each Response Time and Service Time SLA. The near-breach threshold identifies situations where the SLA has not yet been breached but the service level approaches an unacceptable level. You can then take the necessary steps and precautions to assure this situation does not deteriorate further and does not become a performance problem.

The SLA Settings dialog box lets you manage SLAs. You may also add, edit, or delete Response Time and Service Time SLA definitions. Availability SLA definitions are created per instance during the installation of the instance, and they are removed when the instance is uninstalled. Therefore, you cannot add or delete Availability SLA definitions, but you can edit them any time.

The SLA Settings dialog box opens, displaying a list of all SLA definitions currently defined under the selected SLA type, the activity or activities this SLA definition refers to, the near-breach and breach threshold values, and the last time the SLA definitions was updated.

> An SLA definition for a specific activity is assigned by best fit. For example, if a specific Human Resource transaction - such as “HR12” - should have a different SLA threshold than other transactions, you could define an additional SLA definition for it. In this case, all transactions starting with “HR” would be assigned to the first SLA definition, while “HR12” would be assigned by best fit to its specific SLA definition.

Viewing SLA settings

You can view SLA settings via the SLA Settings dialog box.

To view SLA settings

1. On the Settings menu, click **SLA**.
2. In the SLA Settings dialog box, to view the Service Time SLA table, the Response Time SLA table, or the Availability SLA table, click the relevant tab.
3. From the Technology list, select the technology for which you want to view SLAs.

Managing response time

Response time SLAs refer to the total duration needed to process an application request, from the time the user initiated the request until that time when a response to the request is returned to the user.

Adding a response time SLA definitions

You can add a response time SLA definition via the SLA Settings dialog box.

To add a response time SLA definition

1. On the Settings menu, click **SLA**.
2. In the SLA Settings dialog box, on the relevant tab, from the Technology list, select the technology for which you want to add an SLA definition and click **Add**.
3. In the SLA Settings - Add SLA Definition dialog box, perform one of the following steps:
    - **For all technologies except 'Other'**. In the SLA name text box, type the name of the new SLA definition.
    - **For a technology of type 'Other'**. From the AppTier list, select an AppTier.
    - **For SAP**. From the Activity type list, select the relevant activity type.
4. Select a value in the node list; the SLA can be defined on a single node, or on all nodes.
5. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
   Click **Filter** to populate the Select list with items. To display a smaller, more focused set of items, type a string expression that contains the character string common to all the items that you want to add to the SLA definition, combined with wildcard characters, into the text box. For example, suppose you want to define an SLA definition for the SAP AppTier that contains only the SAP transactions that are executed by the Human Resources department. If all such SAP transactions start with the letters "HR," you can type the string HR% in the Filter text box to display only Human Resources department transactions in the Select list. If the name of the item that you want to add to the SLA definition does not appear in the Select list, type its name into the Free text box. You can also use this text box to add a pattern to the SLA definition instead of selecting distinct transactions. To add a pattern to the SLA definition
6. Use the arrow buttons to move items to the list on the right. To delete an item from the list, select it and click **Remove**.
7. Specify time values, in seconds, for Near-breach and Breach thresholds and click **OK**. You can fine-tune the threshold up to milliseconds, for example 1.02 seconds.

Editing a response time SLA definition

You can edit a response time SLA definition via the SLA Settings dialog box.

To edit a response time SLA definition

1. On the Settings menu, click **SLA**.
2. In the SLA Settings dialog box, on the relevant tab, from the Technology list, select the technology for which you want to add an SLA definition and click **Edit**.
3. In the SLA Settings - Edit SLA Definition dialog box, perform one of the following steps:
    - **For all technologies except 'Other'**. In the SLA name text box, type the name of the new SLA definition.
    - **For a technology of type 'Other'**. From the AppTier list, select an AppTier.
    - **For SAP**. From the Activity type list, select the relevant activity type.
4. Select a value in the node list; the SLA can be defined on a single node, or on all nodes. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
5. Click **Filter** to populate the Select list with items.
   To display a smaller, more focused set of items, type a string expression that contains the character string common to all the items that you want to add to the SLA definition, combined with wildcard characters, into the text box. For example, suppose you want to define an SLA definition for the SAP AppTier that contains only the SAP transactions that are executed by the Human Resources department. If all such SAP transactions start with the letters "HR," you can type the string HR% in the Filter text box to display only Human Resources department transactions in the Select list.
   If the name of the item that you want to add to the SLA definition does not appear in the Select list, type its name into the Free text box. You can also use this text box to add a pattern to the SLA definition instead of selecting distinct transactions.

To add a pattern to the SLA definition

1. Use the arrow buttons to move items to the list on the right. To delete an item from the list, select it and click **Remove**.
2. Specify time values, in seconds, for Near-breach and Breach thresholds and click **OK**. You can fine-tune the threshold up to milliseconds, for example 1.02 seconds.

Deleting a response time SLA definition

You can delete a response time SLA definition via the SLA Settings dialog box.

To delete a response time SLA definition

1. On the Settings menu, click **SLA**.
2. In the SLA Settings dialog box, on the relevant tab, from the Technology list, select the technology for which you want to add an SLA definition and click **Delete**.

Managing service time

Service Time SLAs refer to the net duration needed to process a request, from the time the request arrived until the time the service that is associated with the request was completed.

Adding a service time SLA definition

You can add a service time SLA definition via the SLA Settings dialog box.

To add a service time SLA definition

1. On the Settings menu, click **SLA**.
2. In the SLA Settings dialog box, on the relevant tab, from the Technology list, select the technology for which you want to add an SLA definition and click **Add**.
3. In the SLA Settings - Add SLA Definition dialog box, perform one of the following steps:
    - **For all technologies except 'Other'**. In the SLA name text box, type the name of the new SLA definition.
    - **For a technology of type 'Other'**. From the AppTier list, select an AppTier.
4. Select a value in the node list; the SLA can be defined on a single node, or on all nodes.
5. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
   Click **Filter** to populate the Select list with items.
   To display a smaller, more focused set of items, type a string expression that contains the character string common to all the items that you want to add to the SLA definition, combined with wildcard characters, into the text box. For example, suppose you want to define an SLA definition for the SAP AppTier that contains only the SAP transactions that are executed by the Human Resources department. If all such SAP transactions start with the letters "HR," you can type the string HR% in the Filter text box to display only Human Resources department transactions in the Select list. If the name of the item that you want to add to the SLA definition does not appear in the Select list, type its name into the Free text box. You can also use this text box to add a pattern to the SLA definition instead of selecting distinct transactions.

To add a pattern to the SLA definition

1. Use the arrow buttons to move items to the list on the right. To delete an item from the list, select it and click **Remove**.
2. Specify time values, in seconds, for Near-breach and Breach thresholds and click **OK**.

You can fine-tune the threshold up to milliseconds, for example 1.02 seconds.

Editing a service time SLA definition

You can edit a service time SLA definition via the SLA Settings dialog box.

To edit a service time SLA definition

1. On the Settings menu, click **SLA**.
2. In the SLA Settings dialog box, on the relevant tab, from the Technology list, select the technology for which you want to add an SLA definition and click **Edit**.
3. In the SLA Settings - Edit SLA Definition dialog box, perform one of the following steps:
    - **For all technologies except 'Other'**. In the SLA name text box, type the name of the new SLA definition.
    - **For a technology of type 'Other'**. From the AppTier list, select an AppTier.
4. Select a value in the node list; the SLA can be defined on a single node, or on all nodes.
5. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
   Click **Filter** to populate the Select list with items.
   To display a smaller, more focused set of items, type a string expression that contains the character string common to all the items that you want to add to the SLA definition, combined with wildcard characters, into the text box. For example, suppose you want to define an SLA definition for the SAP AppTier that contains only the SAP transactions that are executed by the Human Resources department. If all such SAP transactions start with the letters "HR," you can type the string HR% in the Filter text box to display only Human Resources department transactions in the Select list.
   If the name of the item that you want to add to the SLA definition does not appear in the Select list, type its name into the Free text box. You can also use this text box to add a pattern to the SLA definition instead of selecting distinct transactions.

To add a pattern to the SLA definition

1. Use the arrow buttons to move items to the list on the right. To delete an item from the list, select it and click **Remove**.
2. Specify time values, in seconds, for Near-breach and Breach thresholds and click **OK**.

You can fine-tune the threshold up to milliseconds, for example 1.02 seconds.

Deleting a service time SLA definition

You can delete a service time SLA definition via the SLA Settings dialog box.

To delete a service time SLA definition

1. On the Settings menu, click **SLA**.
2. In the SLA Settings dialog box, on the relevant tab, from the Technology list, select the technology for which you want to add an SLA definition and click **Delete**.

Managing availability

Availability SLAs indicate the lowest acceptable level of an instance's availability.

Editing an availability SLA definition

You can edit an availability SLA definition via the SLA Settings dialog box.

> You cannot add or delete Availability SLA definitions, but you can edit them at any time.

To edit availability SLA definitions

1. From the Settings menu, click **SLAs**.
2. In the SLA Settings dialog box, click the Availability tab.
3. From the Technology list, select the technology for which you want to edit an SLA definition.
4. In the table, select an instance. Then click **Edit**.
5. In the SLA Settings - Edit SLA Definition dialog box, type the new SLA value (in percent) and click **OK**.

About configuring locations

By defining Precise locations, you can logically divide your organization into geographical or organizational groups. Defining locations this way can help you to isolate local performance problems and also gain a better understanding of system behavior patterns.

Location definitions are based on the IP addresses of client machines. You can define a location that is based on one IP address or based on a range of IP addresses. Location definitions affect Insight and Precise for Web.

The table in the Location Settings dialog box displays a list of all locations currently defined, the specific IP addresses or IP address ranges that are part of the location, and the time and date of the last update. You can only define locations for newly loaded data, not for previously loaded data.

An activity with a specific IP address is assigned to the best-fit location. For example: Location A has an IP address range from 10.1.0.0 to 10.1.0.255 while location B is defined for IP addresses 10.1.0.77 and 10.1.0.79. In this case, an activity with the IP address 10.1.0.79 is assigned to location B, not A.

Adding a location

You can add a location via the Location Settings dialog box.

> When you insert IP ranges, verify that you do not create an invalid overlap. For example: 211.2.2.2-223.0.0.0 and 222.2.2.2-224.0.0.0 overlap and create an invalid overlap. 211.2.2.2-223.0.0.0 and 223.0.0.1-224.0.0.0 or 211.2.3.3-222.1.2.9 are valid overlaps, if overlapping is checked as the selected node. If all nodes was selected, the overlapping check will be performed on all nodes.

To add a location

1. On the Settings menu, click **Location**.
2. In the Location Settings dialog box, click **Add**.
3. Select a value from the node list; the location can be defined on a single node or on all nodes.
4. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
5. In the Location Settings - Add dialog box, click **Filter** to populate the Select list with items.
   To display a smaller, more focused set of items in the Select list, type a string expression that contains the character string common to all the IP addresses you want to add to the SLA definition, combined with wildcard characters, into the text box.
   For example: If you define a Chicago location and all IP addresses in this location start with “10.6,” you could type the string 10.6* in the Filter box to display only IP addresses that belong to this location.
6. To specify a range of IP addresses for the location, type the first and last address into the From...To text boxes.
7. Use the arrow buttons to move items to the list on the right.
8. To delete an item from the right list, select it and click **Remove**.
9. Click **OK**.

Editing a location

You can edit a location via the Location Settings dialog box.

> When you insert IP ranges, verify that you do not create an invalid overlap. For example: 211.2.2.2-223.0.0.0 and 222.2.2.2-224.0.0.0 overlap and create an invalid overlap. 211.2.2.2-223.0.0.0 and 223.0.0.1-224.0.0.0 or 211.2.3.3-222.1.2.9 are valid overlaps, if overlapping is checked as the selected node. If all nodes was selected, the overlapping check will be performed on all nodes.

To edit a location

1. On the Settings menu, click **Location**.
2. In the Location Settings dialog box, click **Edit**.
3. Select a value from the node list; the location can be defined on a single node or on all nodes.
4. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
5. In the Location Settings - Edit dialog box, click **Filter** to populate the Select list with items.
   To display a smaller, more focused set of items in the Select list, type a string expression that contains the character string common to all the IP addresses you want to edit to the SLA definition, combined with wildcard characters, into the text box. For example: If you define a Chicago location and all IP addresses in this location start with “10.6,” you could type the string 10.6* in the Filter box to display only IP addresses that belong to this location.
6. To specify a range of IP addresses for the location, type the first and last address into the From...To text boxes.
7. Use the arrow buttons to move items to the list on the right.
8. To delete an item from the right list, select it and click **Remove**.
9. Click **OK**.

Deleting a location

You can delete a location via the Location Setting dialog box.

To delete a location

1. On the Settings menu, click **Location**.
2. In the Location Settings dialog box, select the location you want to remove and click **Delete**.

About configuring grouping settings

Grouping settings are relevant for displaying information in Insight. In Insight, the graphs in the AppTier area compare performance attributes of various entities for each AppTier. This can be useful in pinpointing problem areas. In cases where the information in the graphs is too granular, you can create a higher-level view of the graph by grouping entities together.

For example, examining a graph that shows SQL Server Login Names reveals that many users use the system. It is difficult to understand from the graph who actually uses the database for normal application purposes and who uses it for administrative or other purposes. It is even more difficult to understand the geographical or organizational distribution of system users.

An effective way to obtain such information is to group entities (Login Names in this example). By grouping login names into designated groups, you can obtain a higher-level understanding of system usage and performance.

Viewing existing groups

You can view existing groups via the Grouping Settings dialog box.

To view existing groups

1. On the Settings menu, click **Grouping**.
2. In the Grouping Settings dialog box, from the Technology list, select the technology for which you want to view existing groups. The values in the Group list change according to the selected technology.
3. From the Group list, select the group whose definition you want to view. The group table populates with information on the selected group.

Adding a group

You can add a group via the Grouping Settings dialog box.

To add a group

1. On the Settings menu, click **Grouping**.
2. In the Grouping Settings dialog box, select a technology and group.
3. Click **Add**.
4. In the Grouping Settings — Add dialog box, in the Group text box, type the name for the group you want to create.
5. Select a value from the node list; the grouping can be defined on a single node or on all nodes.
6. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
7. Click **Filter** to populate the Select list with items.
   To display a smaller, more focused set of items in the Select list, type a string expression that contains the character string common to all the values you want to add to the group, combined with wildcard characters, into the text box.
   For example: If you define a group of login names and you want to view a list of all the login names that start with “U,” you can type the string U% (or %) in the Filter box to display only login names that start with “U.” If a specific value does not appear in the list, use the Free text box to enter the value.
8. Use the arrow buttons to move items to the list on the right.
9. To delete an item from the right list, select it and click **Remove**.
10. Click **OK**. A new group is added to the group list.

Editing a group

You can edit a group via the Group Settings dialog box.

To edit a group

1. On the Settings menu, click **Grouping**.
2. In the Grouping Settings dialog box, select a technology and group.
3. Click **Edit**.
4. In the Grouping Settings — Edit dialog box, in the Group text box, edit those fields for the group that need to be changed.
5. The filter button will retrieve the data from the selected node. If all nodes was selected, the operation will be performed on all nodes and the result will be a combination of all results.
6. Click **Filter** to populate the Select list with items.
   To display a smaller, more focused set of items in the Select list, type a string expression that contains the character string common to all the values you want to add to the group, combined with wildcard characters, into the text box.
   For example: If you define a group of login names and you want to view a list of all the login names that start with “U,” you can type the string U% (or %) in the Filter box to display only login names that start with “U.” If a specific value does not appear in the list, use the Free text box to enter the value.
7. Use the arrow buttons to move items to the list on the right.

8. To delete an item from the right list, select it and click **Remove**.
9. Click **OK**. An existing group is edited for the group list.

Deleting a group

You can delete a group via the Grouping Settings dialog box.

To delete a group

1. On the Settings menu, click **Grouping**.
2. In the Grouping Settings dialog box, select a technology and group to remove.
3. Click **Delete**.

Configuring hour groups

PMDB data is summarized into hourly-based time units. In large environments with a high volume of transactions, the PMDB can use a lot of disk space. To reduce disk space consumption, Precise automatically aggregates hourly data into daily, weekly, and monthly data. Aggregation saves space, but it eliminates the raw details of hourly performance data. To specify the hours for which you want data maintained, use the Hour Group option.

The Hour Group option divides the week into hour groups. The default groups are day, morning, night, and weekend. During the installation process, you can create your own hour groups or change the defaults to whatever is appropriate for your environment. For example, you could define a peak hour every day between 10 AM and 11 AM.

When you have declared the hour groups you want, you can further define which performance data is collected within each hour group.

> Changing the hour group settings does not apply to information already stored in the PMDB. The new information will only be used for calculations that are related to future information.

To configure hour groups

1. On the Configuration bar, click **Hour Groups**.
2. In the Hour Group Settings dialog box, do one of the following tasks:
    a. Disable the use of hour groups by clearing the **Use hour group definition for calculations** check box. Disabling hour groups affects the baseline calculation. Old hour groups already stored in the PMDB remain enabled.
    b. Mark an hour or a sequential set of hours with the mouse. The Hour Group Settings - Edit dialog box opens with the day and time duration set. Select the preferred hour group from your organization's hour groups as listed in the table. Each group appears in a different color.
    c. Click **Edit**. The Hour Group Settings - Edit dialog box opens with no day or time duration set. Specify the day of the week and the time duration you want and select the preferred hour group from your organization's hour groups, as listed in the table. Each group appears in a different color.
3. To change the name of a group, click **Rename** and type the new name in the relevant table cell. For example, to change “Customized 4” to “Peak,” select the **Customized 4** row, click **Rename**, and type `Peak` in the name text box on the table.
4. Click **OK**.

Configuring Alerts general settings

The Alerts, issued by Alerts, are based on information collected by Insight agents, agents of Precise products, or Report Manager agents. For most of the metrics, Alerts enables you to launch the relevant Precise product without returning to the StartPoint screen.

> In order to enable the Alerts settings screen, the user must have ADMIN.VIEW role permissions.

To configure Alerts general settings

1. On the Settings menu, click **Alerts General Settings**.
2. In the Alerts General Settings dialog box, select the appropriate tab.

Setting alerts defaults on the General tab

The alert defaults affect the view of the various tables and graphs in Alerts. You can set the alert defaults to fine-tune the view according to your preferences.

The General tab includes the following parameters:

- **Display alert history over the last [hours]**. This parameter affects all history table columns (in the Metric tab, Instances tab, and AppTiers table), maximum, minimum, and average counters (in the Current tab). You can set the history period up to 168 hours (week).
  After modifying this parameter you must restart the Alerts FocalPoint to apply the new setting.
- **Display only top *n* metrics or events**. Sets the maximum number of Metrics or Events to display in the Metric viewer, Event viewer, and the Main Area of the Metric tab. Lowering the value improves the User Interface response time.

To set alerts defaults on the General tab

1. Specify the display parameters.
2. Click **OK** to save the parameters.

Setting an Email server for actions on the Email tab

The Email tab allows you to set an external email server, through which Alerts can send email actions to a specified address. The email actions are automatically triggered by alerts, after configuring email actions for a metric.

The Email tab includes the following parameters:

- **Integrate Alerts with an email server**. Select this option box to enable Alerts to send email actions.
- **Email server name or IP address**. Set the mail server name or IP address. The mail server must be recognized by the network of the Precise installation.
- **Alerts email messages should be sent by**. Set the address you want to appear in the sent by field in email actions.

To set an Email server for actions on the Email tab

1. From the Email tab, check mark **Integrate Alerts with an Email server**.
2. Specify the details regarding the Email server.

Setting an SNMP server for actions on the SNMP tab

The SNMP tab lets you set the details of an external SNMP manager that receives the metric status from Alerts through SNMP traps, and to configure a port through which you can perform SNMP Get commands. See “About setting Alerts SNMP connectivity” on page 176.

The SNMP tab includes the following parameters:

- **Integrate Alerts with SNMP console**. Select this option box to enable SNMP functionality.
- **Server name or IP address**. Set the server name or IP address of the SNMP manager.
- **SNMP Trap Port**. Set the SNMP Trap port of the SNMP manager.
- **SNMP Trap version**. Set the SNMP Trap version of the SNMP manager.
- **SNMP Port**. Set the SNMP port of the Alerts FocalPoint server that listens to the SNMP requests.
- **SNMP Version**. Set the SNMP version of the Alerts FocalPoint server that listens to the SNMP requests.

To set an SNMP server for actions on the SNMP tab

1. From the SNMP tab, check mark **Integrate Alerts with SNMP console**.
2. Specify the details of the SNMP console for receiving Alerts SNMP traps.

Setting a MOM server for actions on the MOM tab

The MOM tab lets you set the details of an external MOM server that receives the metric status from Alerts. Specify the details of the MOM application server that will receive the alerts from Precise Alerts. See “About Alerts MOM connectivity” on page 182.

The MOM tab includes the following parameters:

- **Integrate Alerts with Microsoft Operations Manager**. Select this option box to enable MOM functionality.
- **Server name or IP address**. Insert the server name or IP address of the MOM server.
- **User name**. Insert the user name of the administrator on the MOM server.
- **Password**. Insert the password.
- **Domain**. Insert the domain.

To set a MOM server for actions on the MOM tab

1. From the MOM tab, check mark **Integrate Alerts with Microsoft Operation Manager**.
2. Specify the details of the MOM application server that will receive the alerts from Precise Alerts.

Editing instance settings on the Instances tab

The Instances tab allows you to modify the association properties of all instances within a selected AppTier. You can associate or disassociate instances with alerts, enable or disable SNMP actions for each instance, and add a default email address for each server.

You can display instances within a specific AppTier and their general settings, by selecting it from the AppTier list box. The following table describes the properties displayed for each instance.

Table 4-4 Instance association table

Properties	Description
Instance	Instance name.
Server	Indicates the server name where the instance is running.
Alerts Reported	Indicates whether alerts are reported for the instance or not.

SNMP	Indicates whether SNMP actions are enabled for the instance or not. When enabled, all the metrics that sample the instance are automatically set with SNMP actions. When disabled, all metrics that sample the instance are set with no SNMP actions.
Default email	Displays the default email address of the recipient. This email address is used as a default in the email definition in the Actions tab. See About metric properties for Action settings.

To edit instance settings

1. From the Instances tab, select the instance that you want to edit and then click **Edit**.
2. In the Instance Settings dialog box, set the Instance properties and click **OK**.

In case of a busy system, to improve the system performance, you can check the Do not report alerts for this instance option box of instances that are not important to sample.

Configuring Alerts metric settings

The Alerts, issued by Alerts, are based on information collected by Insight agents, agents of Precise products, or Report Manager agents. For most of the metrics, Alerts enables you to launch the relevant Precise product without returning to the StartPoint screen.

> In order to enable the Alerts Metrics settings screen, the user must have ADMIN.VIEW or ADMIN.UPDATE role permissions.

To configure Alerts metric settings

1. On the Settings menu, click **Alerts Metric Settings**.
2. In the Alerts Metric settings dialog box, select the appropriate tab.

Setting alerts metrics on the Settings tab

The Settings dialog box allows you to edit the properties of each metric that is available in your Precise environment, and the Cross-AppTiers metrics (FocalPoints, Agents, Processes, and Licenses) available in the Precise-generated ‘i3 Status’ environment. You can also add customized metrics to an AppTier (excluding the Cross-AppTiers), or delete customized metrics.

To edit a metric setting for one or all instances, from an AppTier (or Cross-AppTier) of the same technology

1. From the AppTier list box, select the required AppTier (or Cross-AppTiers). The table in the Settings tab displays all the metrics and their metric set.
2. From the Metrics table, select the required metric.
3. Click **Edit**.

If you click **Edit** according to the instructions above, you next need to edit the metric properties. See Editing metric properties.

To add a customized metric to an AppTier of the same technology

1. From the AppTier list box, select the required AppTier. The table in the Settings tab displays all the metrics and their metric set of the selected AppTier.
2. Click **Add**.

If you click Add according to the instructions above, you next need to create a customized metric. See Creating customized metrics.

Creating customized metrics

Alerts allows you to monitor any performance aspects using pre-defined metrics for each AppTier. For data that is not collected by any of the pre-defined metrics, you can create new customized metrics. (Only users with Administrator privilege are allowed to define customized metrics.)

For example, you can create a customized metric that uses a UNIX shell that collects data about the memory size allocated for specific processes (in this case, the metric type is Table because it collects multiple values). The metric will return the data by using a host script. Alerts will display the collected data as a list in the Current tab. The History tab will display the processes behavior over time. The Events tab will trace the alert levels produced by this metric including its failures (Not Sampled status).

When creating a customized metric, it is associated with all instances of an existing AppTier. The customized metrics are part of the Customized set. You can also edit the Thresholds, Sampling, and Actions for each customized metric individually.

> To support customized metrics that use scripts in Precise servers, Alerts InformPoint must be installed. If InformPoint is not automatically installed on the specific server where you want to run customized metrics, you can install InformPoint on that particular server manually. Use the Agent Installer's Servers screen to install the InformPoint. For more information, see the *Precise Installation Guide*.

See “About creating customized metrics” on page 184.

To create a customized metric

1. On the Precise bar, click **Settings>Alerts Metric Settings**.

2. Select the Settings tab. From the AppTier list box, select the AppTier for which you want to create the customized metric (Cross-AppTiers cannot include customized metrics).
3. Click **Add**.
4. On the Metric Properties dialog box, in the Metric name text box, type a name for the new metric.
5. From Sample this metric by running options, select either stored procedure or executable file.
6. In the Executable/Stored procedure textbooks, type the command line that runs the required stored procedure or executable file.
7. In the Metric's response type option, select the metric type, either single value or item list (multiple values).
8. If necessary, select **Alert** when value drops below the designated thresholds and click **Save**.
9. Select the Description tab. In the Description box, type a description of the new metric and click **Save**.

> To move from one tab to the next you must first save the changes made in the previous tab.

10. Edit the settings of the customized metric in the remaining tabs (Scheduling, Thresholds, Actions, and Customize) as required. Click **Save** after editing each tab's settings.
11. Click **Close**. The new customized metric is created.

To delete a customized metric from an AppTier

1. On the Precise bar, click **Settings>Alerts Metric Settings**. The Settings dialog box opens.
2. Select the Settings tab.
3. On the Settings tab, from the AppTier list box, select the AppTier for which you want to delete the customized metric.
4. From the Metrics list, select the metric you want to delete (only metrics of the Customized set can be deleted).
5. Click **Delete**.

Enabling and disabling metrics on the Activities tab

In the Activities tab, you have quick customization options to enable or disable metrics. These operations can also be performed in the settings tab of this dialog, except the focus in the settings tab is on only enabling or disabling metrics.

To disable all metrics for all instances of all environments

1. From the AppTier list box, select the required AppTier (or Cross-AppTiers). The table in the Activities tab displays all the enabled metrics and their metric set.
2. Click **Disable all metrics**.
3. Click **Save** to save the settings.

To enable an Availability metric for all instances of all environments

1. From the AppTier list box, select the required AppTier (or Cross-AppTiers). The table in the Activities tab displays all the enabled Availability metrics and their metric set.
2. Click **Enable Availability metrics**.
3. Click **Save** to save the settings.

To enable/disable metrics from the various sets for a specific instance

1. Select the Environment, AppTier, and instance.
2. Check any metric to enable it, or uncheck any metric to disable it.
3. Click **Save** to save the settings.

Copying metric properties on the Copy Metric Settings tab

Metric settings you set on the Activities tab, or in the settings tab, can be copied to other instances using the Copy Metric Settings tab. To copy the settings to other instances, follow the steps as given on the Copy Metric Settings tab.

To copy metric properties on the Copy Metric Settings tab:

1. Under Source Definitions, select the Environment, AppTier, and Instance you want to copy.
2. On the table, check mark the metrics you want to copy.
3. Check mark the settings group you want to copy.
4. Under Destination Instances, click **Populate destination Instances**.
5. On the table, check mark the destination instance(s).
6. Click **Execute** to copy the selected metric settings.

Editing metric properties

You can edit the properties of each metric that is available in your Precise environment, including Cross-AppTiers metrics, such as: FocalPoints, Agents, Processes, and Licenses.

Alerts issues alerts according to the metric properties, which must be adjusted to your individual environment and organization preferences. The metric definitions must be accurate and adequate. Sampling frequencies and periods require careful considerations. Thresholds need to be set in accordance with the performance level you want to meet.

In addition, alerts must reach the relevant personnel, or in severe cases, management representatives immediately and regardless of their location. Subsequently, the threshold-exceeding values must be examined.

Alerts enables you to adjust the metric definitions through the Metric Properties dialog box.

If you had previously selected Edit or Add for alerts metric settings on the Settings tab, you next need to edit the metric properties.

The Metric Properties dialog box includes the following tabs:

- Description
- Scheduling
- Threshold
- Actions

To edit metric properties for one or all instances, from an AppTier (or Cross-AppTier) of the same technology

1. In the Settings tab, click **Edit** or **Add**. See Setting alerts metrics on the Settings tab.
2. Click the appropriate settings tab (Scheduling, Threshold, or Action)

About setting metric sampling properties on the Scheduling tab

Alerts copies the scheduling settings for the source instance.

To set the metric sample properties

1. From the Metric Properties dialog box, select the Scheduling tab.
2. To set the sampling rate, in the Sample metric every <...> boxes, set the time (day, hours, and minutes) to the frequency, in which you want Alerts to sample the metric. If you do not want to sample this metric, select the Disable metric sampling radio button.

   > Time slice metrics' sampling parameters are usually disabled for editing.

3. To modify the sampling base, in Start sampling at <...> boxes, set the time (day, hours, and minutes) in which Alerts starts to sample the metric (the day parameter is available in case the sampling rate is a week and above). The default is: Sunday, 00:00 AM.

   > These sampling parameters are useful for metrics whose sampling rate is once a day or more. For example, if sampling every 24 hours (1 day), the metric will be sampled every midnight. For sampling it at 3:00 am, change the time parameters to 3:00.

4. In the Analyze metric over the last <...> boxes, set the sampling period for which you want to analyze the metric. The Sampling period is the time frame for retrieving statistical data from the monitored product. The sampling period is used only in metrics that return statistics for a period of time.
5. To sample the metric during downtime period, check **Sample this metric even during downtime**.
6. If the metric monitors an important performance aspect, check **This is a key metric**. Critical alerts related to a key metric are indicated by an exclamation point.

Defining thresholds on the Thresholds tab

Alerts defines "copy threshold settings" from the source instance.

The Thresholds tab allows you to define your performance requirements, and to ignore or consider specific items or conditions. Alerts will then be issued logically and according to your specific configuration.

Because some alerts are calculated based upon total instance running time, a false alert may sometimes be issued. For example, assume the Top Programs sub-metric of the Top Activities metric for SQL Server AppTier is assigned a 10% Near-Critical threshold and a 20% Critical threshold. If a program runs only 10 seconds during the time slice and there are no other programs running on the instance, it will issue a false alert because it exceeds the defined threshold (10 seconds out of a total running time of 10 seconds is 100% of instance running time). This occurs though the program ran for only 1.1% of the time slice total time [10 seconds/(60 seconds x 15 min)]. This false alerts issue is resolved by using a Minimum value setting defined on the Thresholds tab of the Metric Properties dialog box.

The Minimum value setting is a minimum value in seconds of MS-SQL time below which an alert will not be issued. Suppose you do not want to issue an alert for the Top Programs sub-metric if it does not reach 15% of the MS-SQL time. You would then set a Minimum value of 135 seconds (15 min time slice x 60 seconds/min x 15%). No alarm will be issued until the defined minimum value is exceeded.

> Minimum value is only relevant for list metrics whose unit value is given as a percentage.

Alerts comes with a default set of thresholds defined to suit general needs. You should tune these thresholds, as required, in relation to the setup and definitions of your environment.

There are two types of metrics:

- **Single value metrics**. These are metrics that collect only a single value. An alert is issued when its value exceeds the predefined threshold (for example the Availability metric). Parent Single Value metrics include sub-metrics (child metrics). Each child metric has its own thresholds and may be enabled or disabled individually (for example the General Behavior metric).
- **List metrics**. These are metrics that collect a dynamic list of items identifying each item by its description and value (for example the Locked sessions metric). Parent List metrics include sub-metrics (child metrics). Each child metric has its own thresholds and may be enabled or disabled individually (for example the Top Activities metric).

To edit a Sub-Metrics threshold

1. From the Metric Properties dialog box, select the Thresholds tab.
2. Select the sub-metric you want to edit.
3. Click **Edit**.
4. In the Metric Properties - Edit thresholds dialog, enter the required value in the Critical Threshold and Near-critical Threshold text boxes.
5. To consider only specific items when sampling data, include them in the Include list text box.
6. To ignore specific items when sampling data, include them in the Exclude list text box.
   When entering list items, verify that they are separated by a semicolon. Use the percent sign (%) as a wildcard. For example, Alerts%; %Alerts; % Alerts%.
7. To disable a sub-metric, clear the check mark in the Enable Sub-Metric checkbox. If a List metric type, a disabled sub-metric will not be sampled. If a Single value metric type, a disabled sub-metric will be sampled (retrieve a value), however, this will not generate an alert (the sub-metric will always be green).
8. Click **OK**. Repeat steps 2 through 7 for each sub-metric to be defined.
9. In the Minimum value <...> text box at the bottom of the Threshold tab dialog, enter the minimum value necessary for Alerts to consider the item.
10. To save your definitions, choose whether to save them either for the selected instance, or for all the environments" instances. Then click **Save** and **Close**.

About metric properties for Action settings

Alerts copies the action settings from the source instance. Alerts provides the following action types when an alert is raised:

- Email
- Message Box
- Program
- SNMP
- MOM

See About metric properties for Action settings, "About setting Alerts SNMP connectivity" on page 176, and "About Alerts MOM connectivity" on page 182.

Configuring Admin Dashboard settings

The Admin Dashboard settings enable you to set additional report triggers and the Refresh Rate of the data on the screen.

The following options can be selected:

- Report also when one or more instances are not loading data into the PMDB.
- Report also when the status of one or more agent is Stopped.

The default Refresh Rate setting is 15 minutes and this amount can be changed.