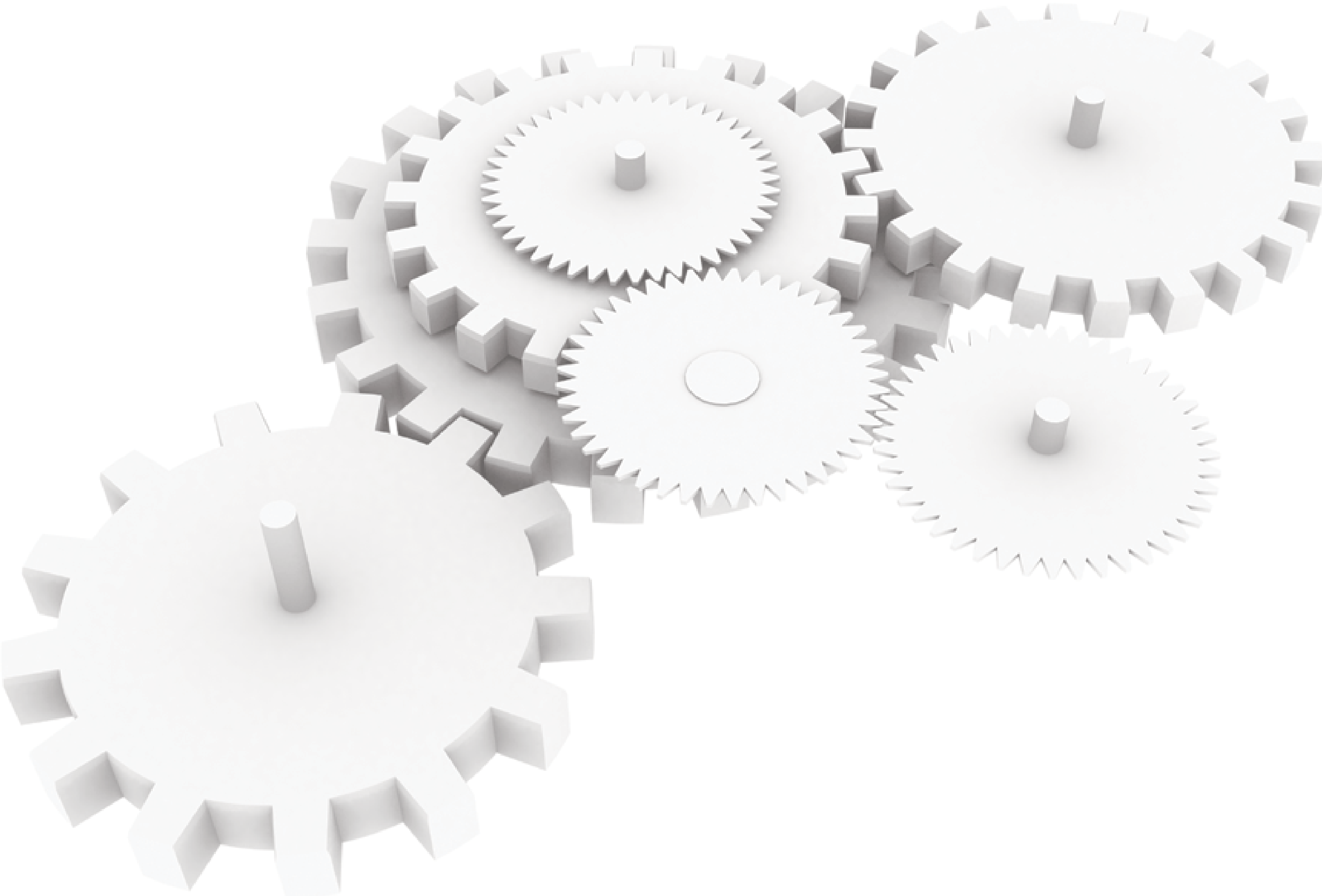
Richmond Systems

SupportDesk Administrator Guide



Contents

SupportDesk Setup Console

Welcome

The SupportDesk Setup Console is the main component for configuring Richmond SupportDesk.

What can be configured in the Setup Console?

The list below show the areas of Richmond SupportDesk that can be configured with the Setup Console, as you progress through this document each configuration will be covered in detail:

General
- Categories
- Groups
- Rights
- Users
- Skills Matrix

Configuration Management
- Inventory Styles
- Inventory Icons
- External Database Integration

Incident Management
- Statuses
- Priorities
- Terminology
- Extended Incident Options
- Category UDF Setup
- Resolution Codes
- Satisfaction Survey
- Terminology
- Extended Incident Options

Problem Management
- Enable/Disable Problem Management
- Known Errors
- Fixed Problems
- Misc

Service Level Management
- Service Hours
- Closed Days
- Escalation Types
- SLA User Defined Fields

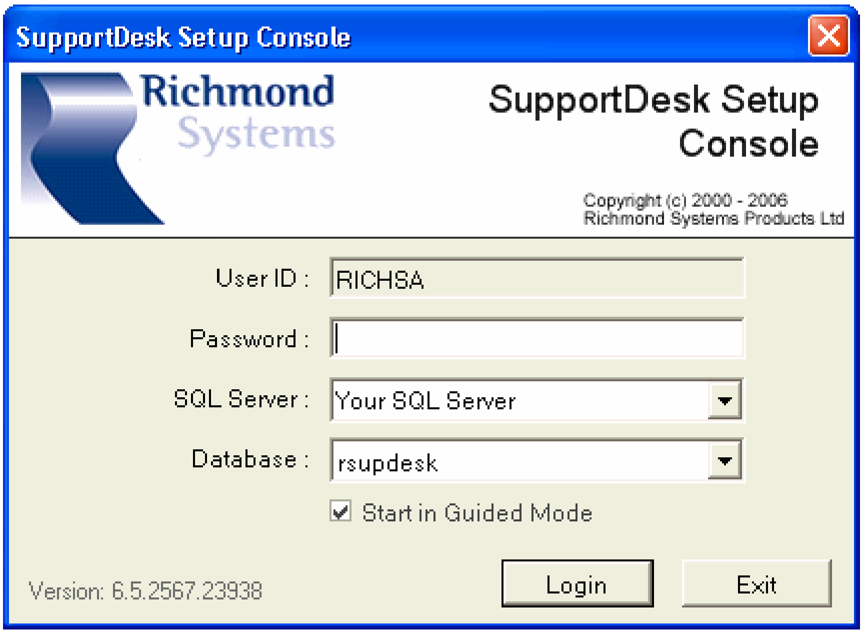
Change Management
- Configuration
- CAB Setup

Miscellaneous
- Web Interface Settings
- Icon Library
- PC Remote control
- Time Zones
- Delete Records

Resource Management
- Resource Settings
- Specialist Availability Calendar

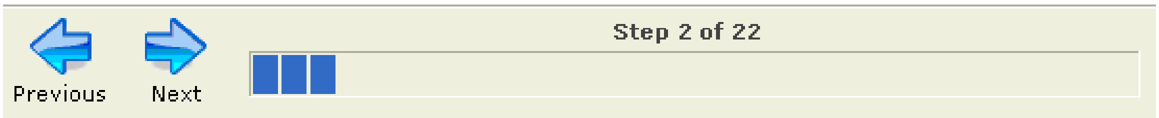
The SupportDesk Setup Console can be launched from the Windows Start menu in the Start→Program Files→ Richmond Systems→SupportDesk program group.

The Setup Console requires authentication using the RICHSA user.



The *Start in Guided Mode* check box can be selected to have the Setup Console step through each of the different areas of configuration. This is beneficial for the initial configuration of SupportDesk.

The Setup Console Navigation bar provides a *Next* and *Previous* option to step through each configuration screen.



The Guided mode offers *Tips* for each screen.

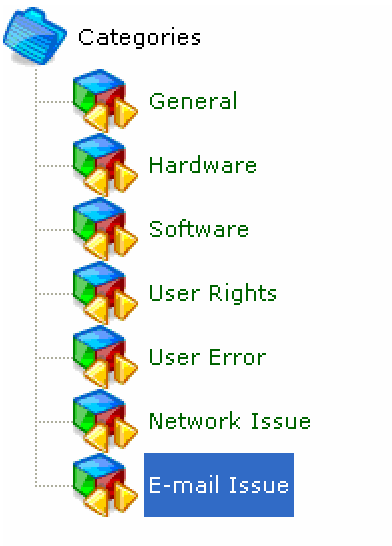
The *Tips* provide a brief description of each configuration step. *Tips* can be turned off by selecting the *Don't show any more tips* check box.

General

Categories

Categories provide a way to group related records. Categories are stored in a hierarchical structure which can be customised to suit different types of support functions and environments.

Reporting takes advantage of the categorisation of records. Considerations should be made when constructing your category structure to reflect your reporting needs. The Category structure is also used to define which Categories particular Specialists are skilled in and to arrange Knowledge Base articles.



Right clicking on existing categories will bring up a context menu.

- **Add New Category**. This option will add a new category beneath the selected Category.

- **Rename**. This option will rename an existing category.
- **Delete.** This option will delete the selected Category
- **Service Level Agreement**. This option will open a window to configure SLA information for the selected Category.
- **Bulk Move Requests**. This option will move all requests that are linked to the selected Category to another Category.
- **End-User Visibility**. This has two options. Category can be set to be either visible or not visible to the End Users of the Web Interface.
- **Skills**. This option is used to select which Specialists are able to be assigned records under particular Categories. . Specialists can also be prevented from taking ownership of records belonging to specific Categories.

Adding New Categories

- Select the appropriate node that you wish to add the new Category to and then right click and select *Add New* from the context menu.
- Enter a name for the new category in the popup dialog and click *OK*.
- The new category will be added to the tree.

Renaming Categories

- Select the category the needs renaming.
- Right click on the Category and then select *Rename* from the context menu.
- Enter the new name in the Rename Category dialog box and click *OK*.

Deleting a Category

- Select the Category to be deleted.
- Right click on the selected Category and select *Delete* from the context menu.
- Confirm the deletion of the Category.

Note: *A* Category can not be deleted if:

- Requests are logged against the Category.
- The Category is set as the default for E-mail requests
- The Category is set as the default for customers that log requests via the Web Interface.
- The Category is set as the default for NetOp Help Requests.
- Any users have the Category selected as their *Add Request default* in their SupportDesk User Profile.

To reassign all calls against a category see **Bulk Move.**

SLA

Any Category can have an SLA defined against it. When a Category is selected on a new Incident record, the SLA of the Category will automatically be applied to the Incident.

Bulk Move

Bulk Move allows for the reassigning of all records logged against a particular Category. This is required if you wish to delete a Category with records logged against it.

- Right click on the category you wish to move records from and select *Bulk Move Requests*.
- A dialog box will appear informing you that all records in the selected will be moved, click OK.
- The mouse pointer will now have a question mark next to it prompting you to select the category you wish to move the records to. Left click on the relevant category.

- A dialog box will appear asking you to confirm the moving of records from one category to another, click *Yes*.
- A dialog box will appear confirming the number of records that have been moved. Click OK

End User Visibility

End User Visibility defines which Categories are visible or hidden from SupportDesk Web Interface End Users. By default categories are visible to End Users using the Web Interface. Some categories may only be required for Service Desk personnel and using the feature, select Categories can be hidden when End Users log a Request in the Web Interface.

- Right click on the Category you wish to set End-User Visibility.
- Select End User Visibility and then choose one of the following options:
  - **Visible to Web End Users –** End-Users of the Richmond Web Interface will be able to see and select this Category when logging an Incident.
  - **Hidden from Web End Users –** End-Users of the Richmond Web Interface will not able to see or select this Category when logging an Incident.

Skills

To make all Specialists Skilled in All Categories

- Right click any Category and from the context menu select **Make All Users Skilled in All Categories**.

To make all Specialists Skilled in a particular Category:

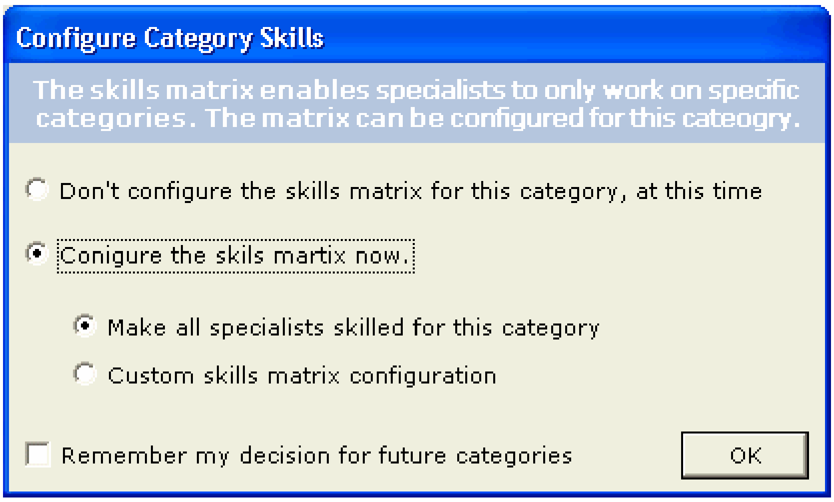
- Right click the relevant Category and select **Skills → Make All Users Skilled In the Selected Category**.
- A dialog box will prompt you to confirm this action, click OK.
- All Specialists will now be skilled in the chosen Category.

To configure the Skills Matrix

- Right click any Category and from the context menu select **Configure Skill Matrix**. See the Skills Matrix section for more details.

The Skills Matrix and new Categories

When creating a new Category you will be presented with the following dialog box:



- **Don't configure the skills matrix for this category, at this time –** All Specialists will have a competencies level of **Not Enforced** against the new Category.

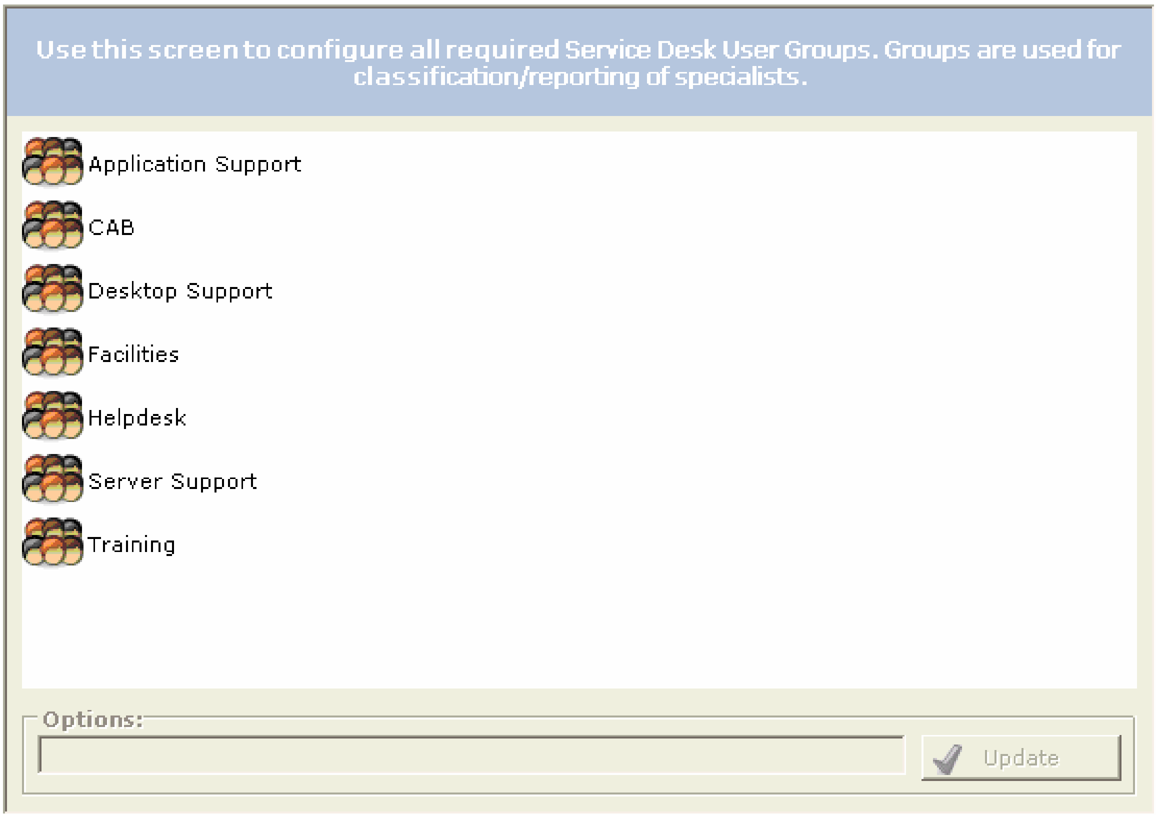
- **Configure the skills matrix now:**
    - **Make all Specialists skilled for this category -** All Specialists will have a competencies level of **Skilled** against the new Category.
    - **Custom Skills Matrix configuration –** When you click **OK** to create the new Category you will be taken straight to the '**Configure Skills Matrix**' screen for the new Category.

Remember my decision for future Categories – The options chosen above will be remembered and applied to any other new Categories created during this session.

User Groups

User Groups allow you to assign Users to individual departments within SupportDesk. Each SupportDesk User must be assigned to a User Group. A User can only belong to one User Group.

- User Groups can be defined as individual departments within the helpdesk dealing with different areas, for example Helpdesk or Training. As many User Groups as needed can be created.



Note: This screen is only used to create the User Groups. Users are assigned to groups through the Setup Users screen.

The advantages with using User Groups are:

- The creation of statistical information by User Group.
- The creation of performance reports by User Group.
- User Groups can be sent an alarm when a new Request is logged or updated.
- Define different support functions within SupportDesk

Adding a new User Group

- Right Click in the User Group section.
- Select *Add New* from the context menu.
- Enter a description for the new Group.
- Click on *OK* to add the new Group.

Modify a User Group

- Select the Group to be amended.
- Amend the Group's description in the Option box.
- Click on *Update* to save your changes.

Deleting a User Group

- Highlight the Group to be deleted.
- Right Click on the highlighted Group
- Select *Delete* from the context menu.
- You will then be asked to confirm the deletion of the Group.

Note: You will not be able to delete a Group if:

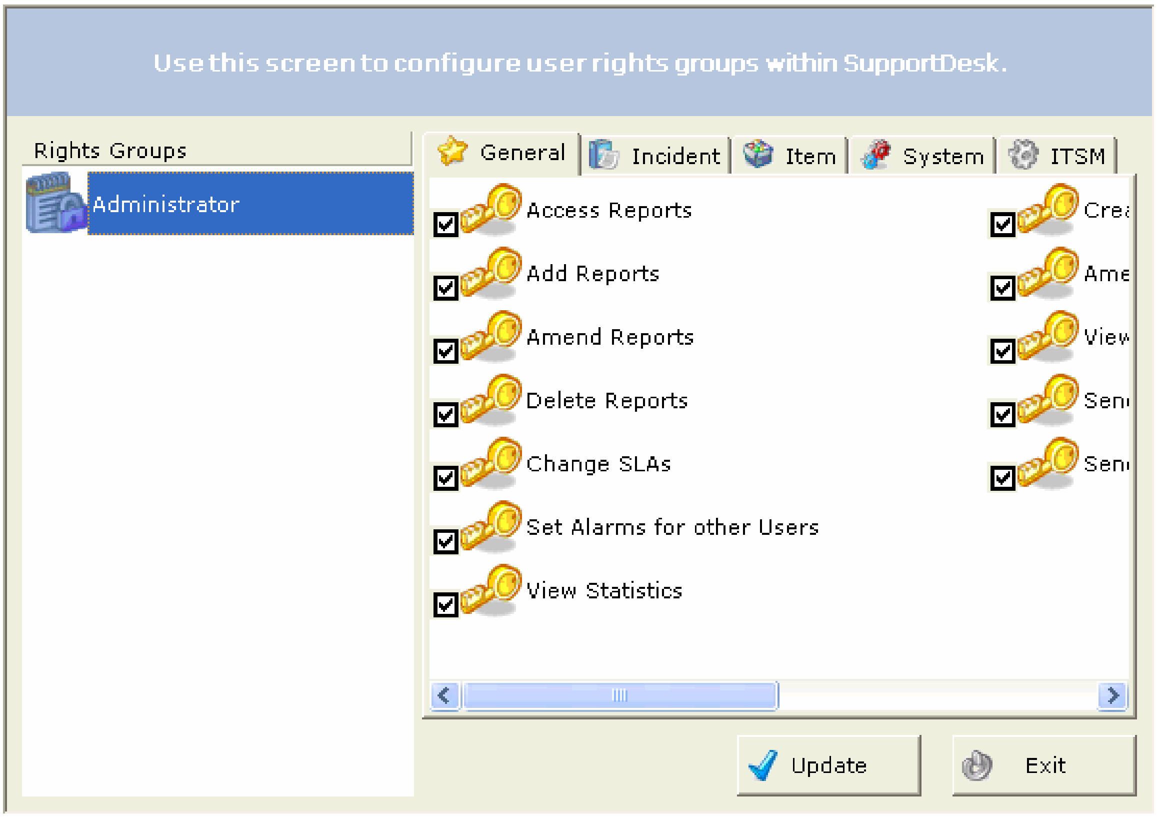
- The Group has Requests assigned against it.
- SupportDesk Users are members of the Group.
- The Group has been selected as a User's add request default.
- The Group is used as the default for E-mailed requests.
- The Group is used as the default for customers that log calls via the Web Interface.
- The Group is used as the default for NetOp Help Requests.

Rights Groups

Rights are configured to specifically allow and deny Users from performing certain functions within SupportDesk. By default an Administrator Rights Group exists. Members of this group have the rights to perform all tasks within SupportDesk.

The Setup Rights screen is used to:

- Add, delete and rename Rights Groups
- Configure the rights for each Rights Group



Adding a new Rights Group

- Right Click in the Rights Group section and select *Add New* from the context menu.
- Enter the name of the new Rights Group and click OK.

Rename a Rights Group

- Select the Rights Group to be renamed.
- Right Click on the Rights Group and select *Rename* to change the name of the Rights Group.

Deleting a Rights Group

- Select the Rights Group to be deleted.
- Right Click and select *Delete* from the context menu.
- You will then be asked to confirm the deletion.

***Note**:* You will not be able to delete a Rights Group if any specialists are members of the Rights Group.

General Rights

Each Rights Group can be assigned an individual set of rights

- Select the Rights Group from the list to gain access to the rights section.
- Configure the Rights as required.

- [ ] Access Reports
- [ ] Add Reports
- [ ] Amend external data information
- [ ] Amend Reports
- [ ] Change SLAs
- [ ] Create / Modify a KB Article
- [ ] Delete Reports
- [ ] Send an AdHoc SMS Message
- [ ] Send an SMS Message
- [ ] Set Alarms for other Users
- [ ] View external data
- [ ] View Statistics

Incident Rights

- [x] Amend Incident Details
- [x] Amend Incident Logged Date
- [x] Add an Incident
- [x] Delete an Incident
- [x] Add an Incident Action
- [x] Add an Incident Activity
- [x] Delete an Incident Action
- [x] Delete an Incident Activity
- [x] Reassign Incidents
- [x] Close an Incident Without Entering a Resolution
- [x] Select an Incidents SLA
- [x] Amend Other Users Actions
- [x] Amend Other Users Activities
- [x] Add Actions for Other People
- [x] Convert Activites in any order
- [x] Add a Quick Incident
- [x] Change a Quick Incident
- [x] Delete a Quick Incident
- [ ] Disallow the Closing of Incidents

Item Rights

- [ ] Add an Item
- [ ] Amend Item Details
- [ ] Copy / Move an Inventory Item
- [ ] Delete an Item

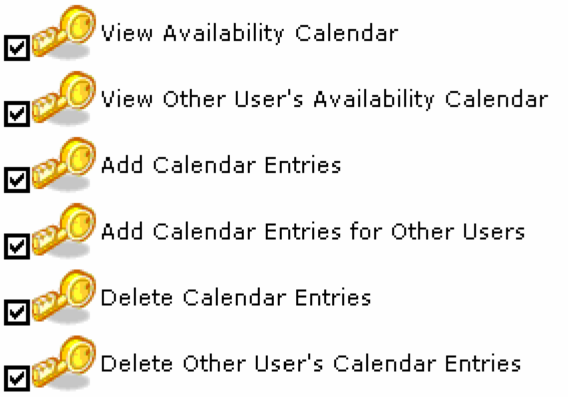
System Rights

- [ ] Access Database Admin
- [ ] Access Setup System Menu
- [ ] Amend Response and Resolution Times
- [ ] Amend View Restrictions
- [ ] Import Data
- [ ] Setup Actions
- [ ] Setup Categories
- [ ] Setup Email
- [ ] Setup Items
- [ ] Setup Rights
- [ ] Setup Styles
- [ ] Setup Users
- [ ] Setup View Restrictions
- [ ] Setup View Rights

ITSM Rights

- [x] Configure ITIL Settings
- [x] Add a New Problem
- [x] Delete a Problem
- [x] Add a Workaround
- [x] Delete a Workaround
- [x] View Problem Management Console
- [x] View Change Requests
- [x] Add New Change Requests
- [x] Modify Change Requests
- [x] Delete Change Requests
- [x] Add New CAB Notes
- [x] Delete CAB Notes
- [x] Add Change Tasks
- [x] Delete Change Tasks
- [x] Add New Task Type
- [x] Delete Task Types
- [x] View Change Management Console

Calendar Rights



Users

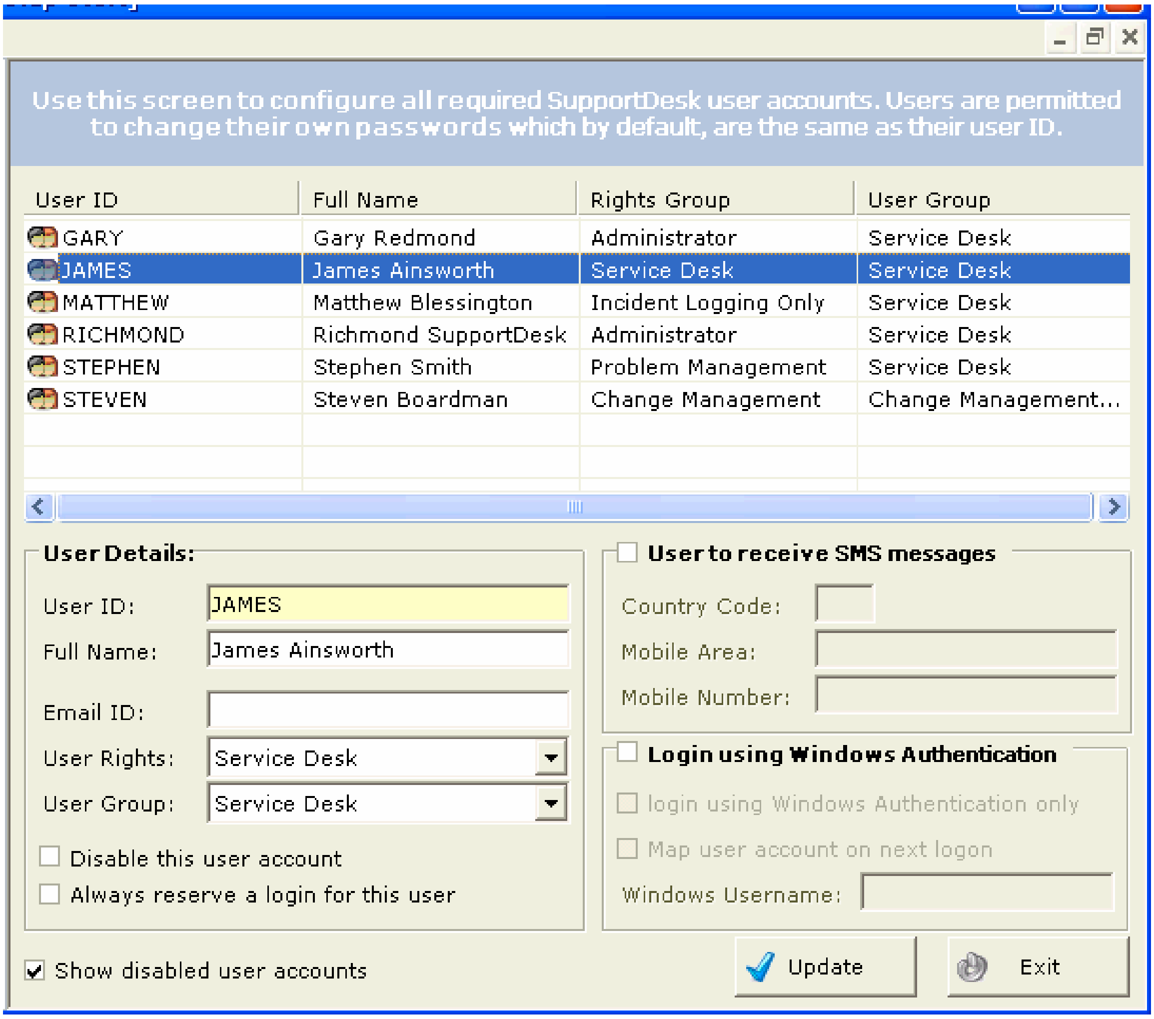
Users can be created for each individual that requires access to the SupportDesk Database as part of your support function. Users in SupportDesk are also referred to as Specialists.

A User logon is required to:

- Access the main Windows SupportDesk application
- Access the Specialist Web Interface
- Access the Management Console
- Receive alarms
- Assign Incident and Problem records against

The User Setup screen is used to:

- Add/Delete Users
- Provide User details
- Assign Users to User Groups and Rights Groups
- Configure SMS messaging
- Disable / enable User accounts
- Set reserved logons
- Configure Single Sign-on with Windows authentication



User Details

The following information can be added to a User account.

- **User ID**
  The ID used to logon to SupportDesk. Also referred to as a Specialist ID.
- **Full Name**
  The Users full name. Used for reporting.
- **Email ID**
  The Users' email address. Enables the User to be able to receive email alarms, and emails from other SupportDesk Users.
- **User Rights**
  Specify a Rights Group from the drop down list. This is a mandatory field.
- **User Group**
  Specify a User Group from the drop down list. This is a mandatory field.

User to receive SMS Messages

Enable the user to receive SMS Text Alarms.

- **Country Code**
  Country phone code
- **Area Code**
  Local phone area code

- **Mobile Number**
  Mobile phone number for the user.

Note: In order for SMS messages to work the SupportDesk SMS Module must be configured and running.

Adding a User

- Right Click in the User table and select Add User
- Complete the User Details Section.
- Complete the SMS Messaging section if required.
- Click on *Update* to save the new User.

Note: The Users' initial password will default to the same as their User ID.

Deleting a User

- Select the User to be deleted.
- Right Click on the selected User and select *Delete User* from the context menu.
- Confirm the deletion of the User.

Note: A User that has requests assigned to them can not be deleted. These requests can be reassigned to another User by selecting *Reassign User Requests* from the context menu. Reassigning requests can result in inaccurate history reporting so it is always recommended to disable the User account rather then deleting the User completely.

Reassign User Requests

Requests can be reassigned from one User to another User. This feature can be used when deleting an existing User from SupportDesk. The reassigning of Requests also includes Actions, Activities, and Alarms.

- Select the User whose requests are to be reassigned.
- Right Click on the selected User and select *Reassign User Requests* on the context menu.
- Click *OK* to confirm the instructions.
- Select the User who the requests will be reassigned to.
- Confirm the reassigning of request.

Reset Password

The Reset Password will reset the User's password to the default password. The default password is the same as the User ID. This can be used when a User has changed and then forgotten their password.

- Select the User whose password needs resetting.
- Right Click on the selected User and select *Reset Password* from the context menu.
- Confirm the resetting of the password.

Disable User Account

Disabling a User will prevent the User from logging into SupportDesk and prevent new Requests from being logged with that User as the Specialist.

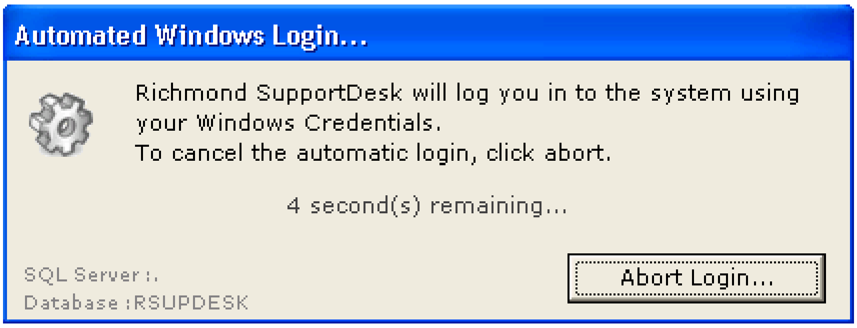
- Select the User that requires disabling.
- Right Click on the selected User and select *Disable User Account* from the context menu.

Always reserve a login for this user

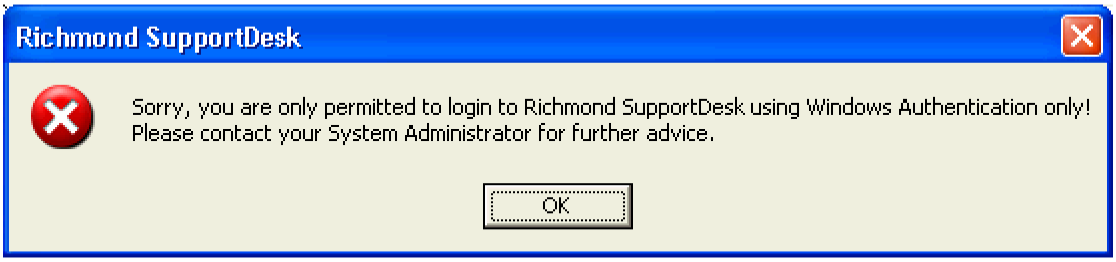
If there are more users of SupportDesk than concurrent connection licenses available selecting this option will reserve a license for this user. This allows for the creation of Named Users who are guaranteed a connection to SupportDesk. The remaining users will use a connection from the remaining pool of licenses.

Logon Using Windows Authentication

Selecting this option will provide pass through authentication into SupportDesk using the Windows User credentials. During the login process Users will be proved with an option to abort login using Windows credentials and the native SupportDesk Login Window will then be available.



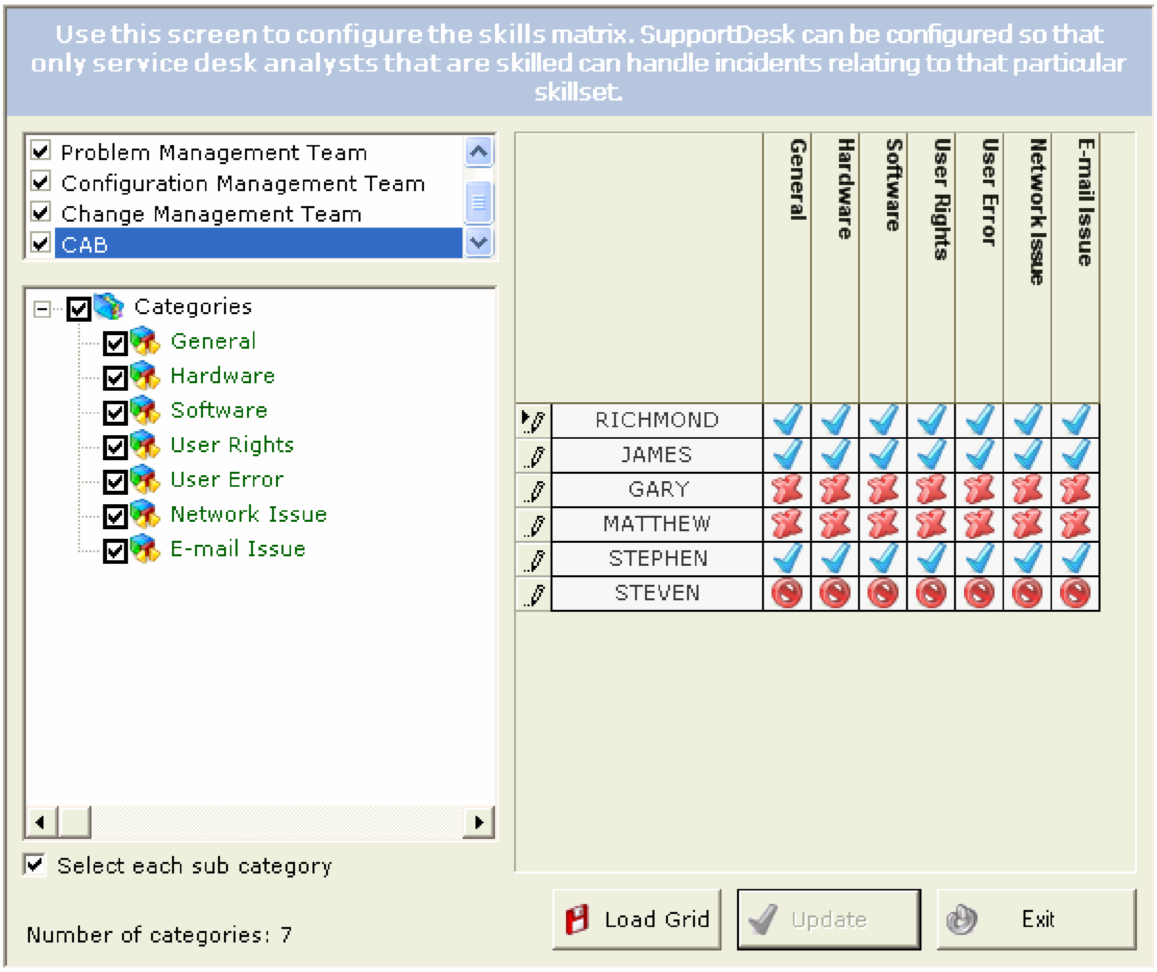
- **Logon Using Windows Authentication Only**
  This option will prevent Users from connecting to SupportDesk using the native SupportDesk logon. They must be on a computer with their Windows Credentials to be able to access SupportDesk. An attempt to use the native SupportDesk Logon will present the following message:



- **Map User account on next logon**
  The first time the User runs SupportDesk they will be prompted with the native SupportDesk logon window. At this point the users Windows Domain and name will be automatically recorded and subsequent logons will then use the Windows credentials.

Skills Matrix

The Skills Matrix is used to define which Users are skilled or unskilled in each Category. This will allow the routing of an Incident, Problem, or Known Error to only Users that are knowledgeable in the selected Category.



A User can be defined as one of three competencies.

Skilled – The User will be able to create or edit records against the category.

Unskilled – The User will not be able to create or edit records against the category.

Not Enforced – The User will be able to create, accept or edit Records against the category; however users will be notified that the User is not categorically skilled and will be prompted to confirm their actions whenever:

- An action or activity is logged for the User.
- When a new record is added with the User as the specialist.
- When a record is re-assigned to the User.

Configuring the Skills Matrix

The Skills Matrix screen is split into three sections. User Groups, Categories, and the Configuration Grid. By selecting a combination of User Groups and Categories the Configuration Grid will display the current Skills levels for each of the selected categories and the Users that are members of the selected User Groups.

- **User Groups**
  Select the User Groups to be viewed in the Grid.
- **Categories**
  Select the Categories to be viewed in the Grid. When the *Select each sub category* option is selected all sub Categories will automatically be selected.
- **Load Grid**
  Click on the *Load Grid* button to view the Matrix.

Clicking on each User name will change the competency level in the currently viewed categories for that particular User. Continue to click on the User name until the desired competency is display.

Configuration Management

Inventory Styles

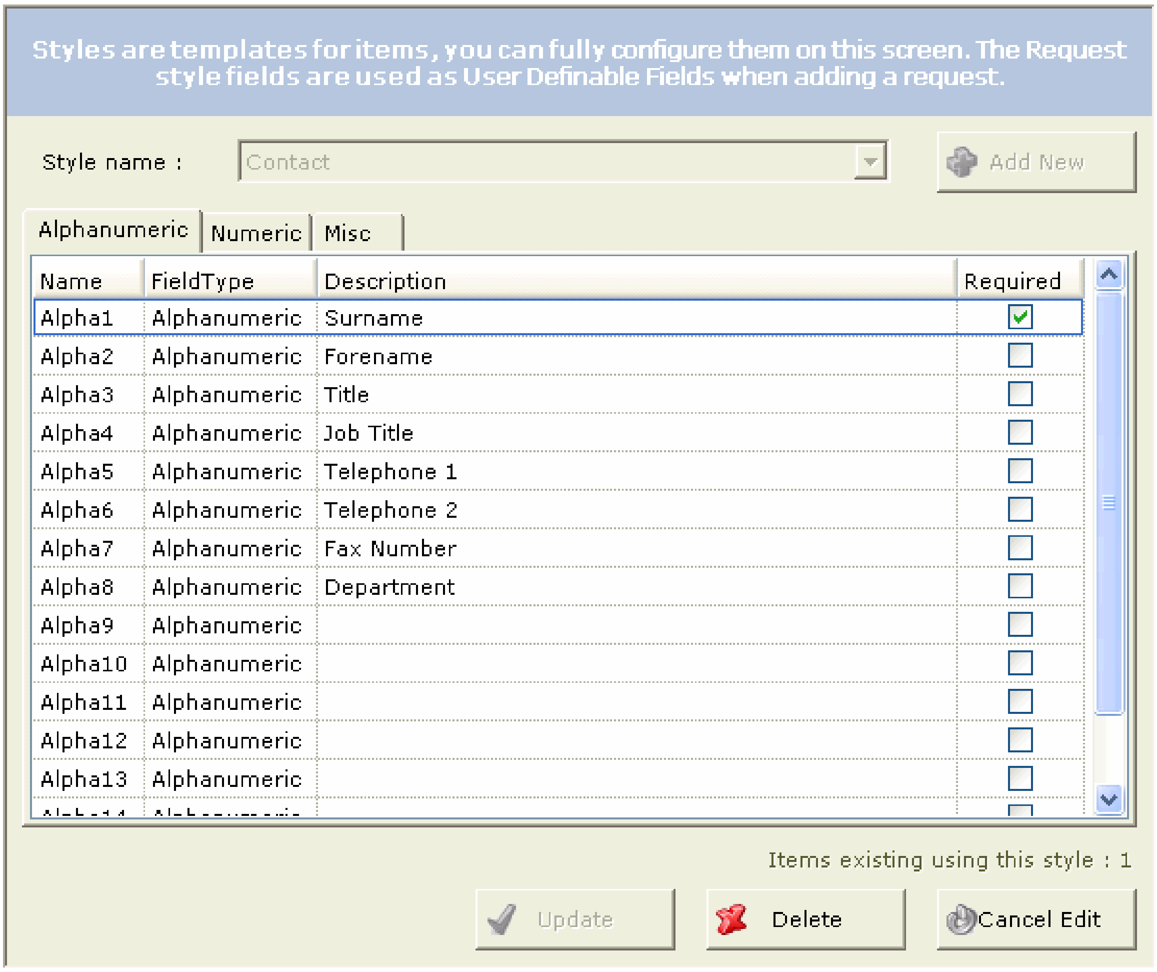
Inventory Styles are templates that define the format of any Item that becomes part of the Navigator Tree. Inventory Styles consist of a maximum of 25 definable fields (15 alphanumeric and 10 numeric).

A typical set of styles that would be useful in most situations are:

- Contact
- Company
- Department
- Computer
- Software

Alphanumeric Tab

An Inventory Style can contain up to 15 alphanumeric definable fields to hold attributes of an Item that is contained in the Navigator Tree.



In the Description column enter the names for the fields.

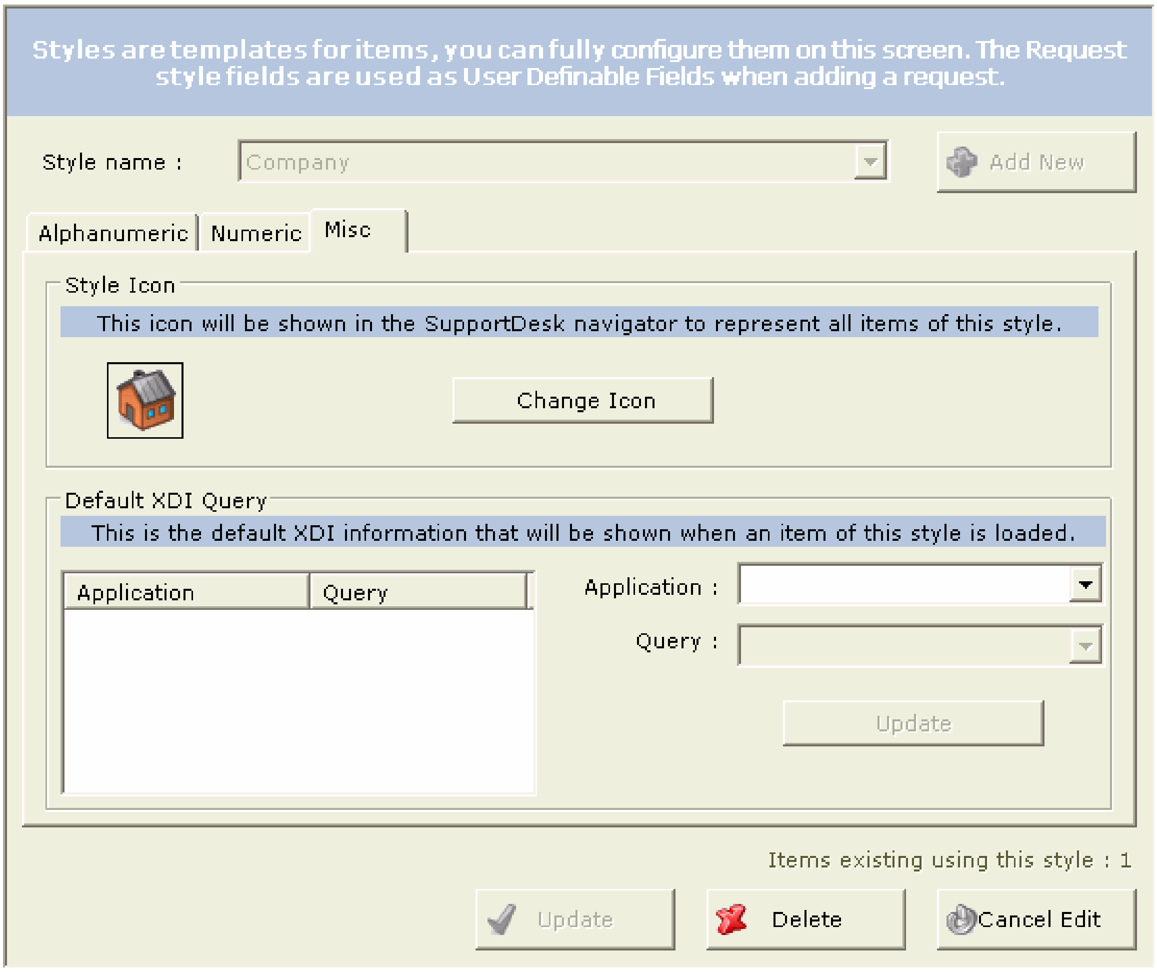
Check the *Required* box to make the field mandatory. Making fields 'Required' will force Users that create a new Item in SupportDesk to enter a value.

Numeric Tab

An Inventory Style can contain up to 10 numeric definable fields. These fields can only hold numeric values.

Misc Tab

The Misc Tab is used to assign an Icon to the Inventory Style and to define which XDI (eXternal Data Interface) is displayed by default on the details of an Item that uses this Inventory Style.

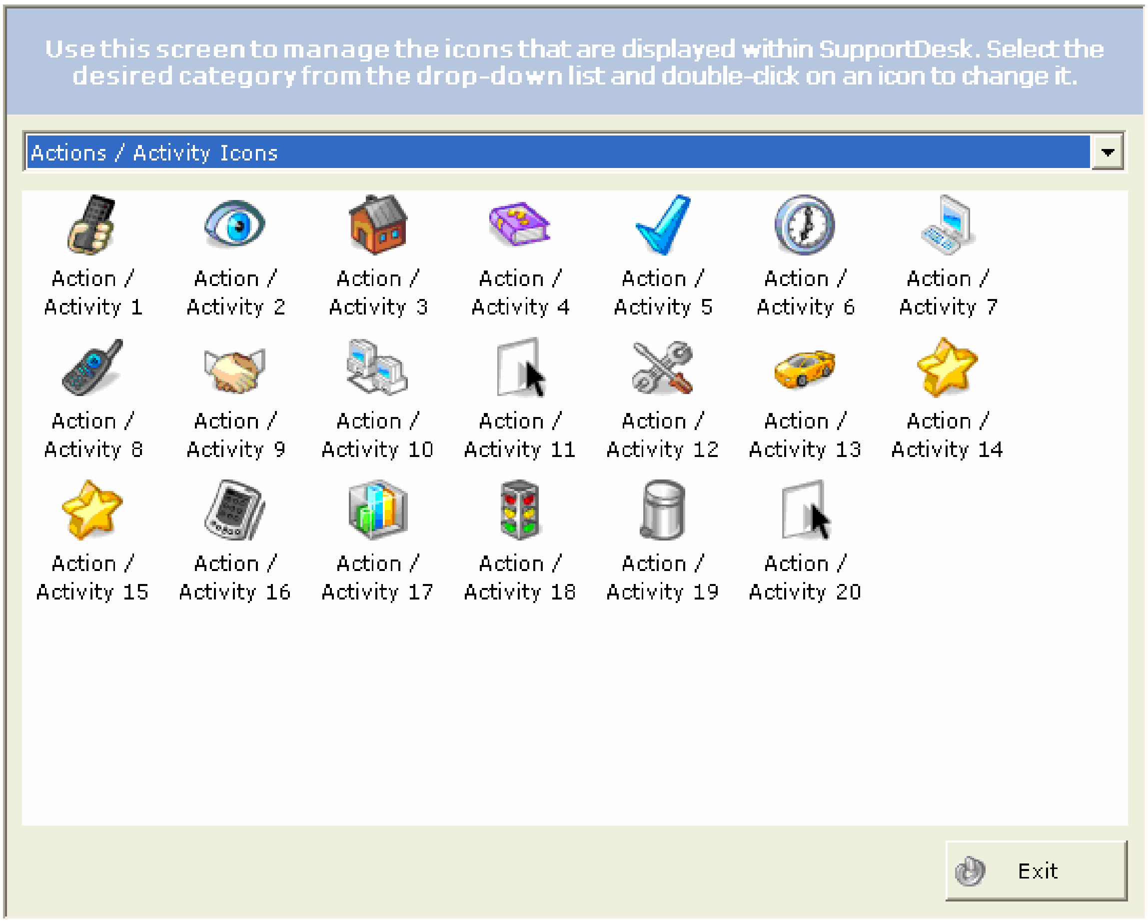


Inventory Icons

The Inventory Icons feature is used to change the default icons that are displayed in the root of the Navigator Tree and to select the available icons for Actions and Activities.

Action/Activity Icons

Up to twenty icons can be used to represent the different Actions and Activities. From the drop-down list select *Action/Activity Icons.*



To change the icon for an Action/Activity:

- Double click on the Activity/Action icon to be changed
- The Icon Library is displayed.
- Double click on the new icon that you wish to use.

External Database Integration

Introduction

SupportDesk allows users to connect to external databases from within the main application to interrogate other applications for information. For example, SupportDesk can be configured to query an accounting database to check for outstanding payments due from a customer. It is also possible to query inventory databases to display the hardware and/or software configuration of a computer. It is not possible to update data in the external database(s).

It is possible for an administrator to configure a database of their own choosing for this type of integration. Alternatively, Richmond Systems can provide consultancy for this purpose. Richmond Systems can also provide pre-configured 'Datapacks' which are available for a number of different database applications. Please contact your Richmond Systems account manager for more information on these services.

Prerequisites

The external database needs to meet the following criteria:

- Firstly, it is necessary to confirm that an ODBC or OLE DB database driver exists for the database in question. That driver also needs to support the adopenschema method, which means that it can describe its structure through the database driver. If you are unsure whether this is the case, please contact the manufacturer of the database system. Fortunately, almost all database drivers meet these criteria.
- Each record to be referenced needs to contain a unique identifier that SupportDesk can use. This identifier can contain any combination of alphanumeric characters.

- The external database needs to be capable of providing read only result sets to SupportDesk without disruption to the external databases application, and within a reasonable time (< 6 seconds).
- Users also need to check whether they need any additional database access licenses for the third party database they will be using.

Configuring an external database

PLEASE DO NOT ATTEMPT THE FOLLOWING UNLESS YOU ARE FAMILIAR WITH YOUR EXTERNAL DATABASE, SQL AND DATABASE DESIGN IN GENERAL. RICHMOND SYSTEMS CANNOT BE HELD RESPONSIBLE FOR DATA LOSS THROUGH INCORRECT USE OF THIS PRODUCT.

Richmond Systems cannot provide technical support for the use of external databases unless the connection parameters have been provided as part of a 'Datapack' or through consultancy from Richmond Systems.

Enabling an external database link through SupportDesk requires 2 steps. Firstly, SupportDesk needs to be configured with the connection string and query SQL strings to extract information from the database. This configuration is done in the database administration module.

For each application that SupportDesk links to, certain information has to be gathered in order to connect to the applications database.

- **Connection String**
  Stores the connection and security information needed to connect to the applications database.
- **External ID selection SQL**
  Stores an SQL statement to return a selection of Link Ids
- **Overall Query SQL**
  Stores either a standard SQL statement or an ADO SQL shape query to return hierarchical data. This query is used to provide data to the XDI list screen.
- **Item SQL Views**: Stores one or more SQL statements to run a query on a specific record in the applications database. The record has to be uniquely identified in a 'where' clause and identified by a replaceable marker. Examples of the SQL views can be found in the Data Connection Units.

Connection String

With each of the Data Connection Units that are installed with SupportDesk, you will notice that all of the fields are already filled in. The exception to this is the connection string, as each connection string will be unique to each user's site.

The connection string can be built up by clicking on the Get button and providing information to the 'data link properties' window. The user is prompted for the driver name, server location and authentication information.

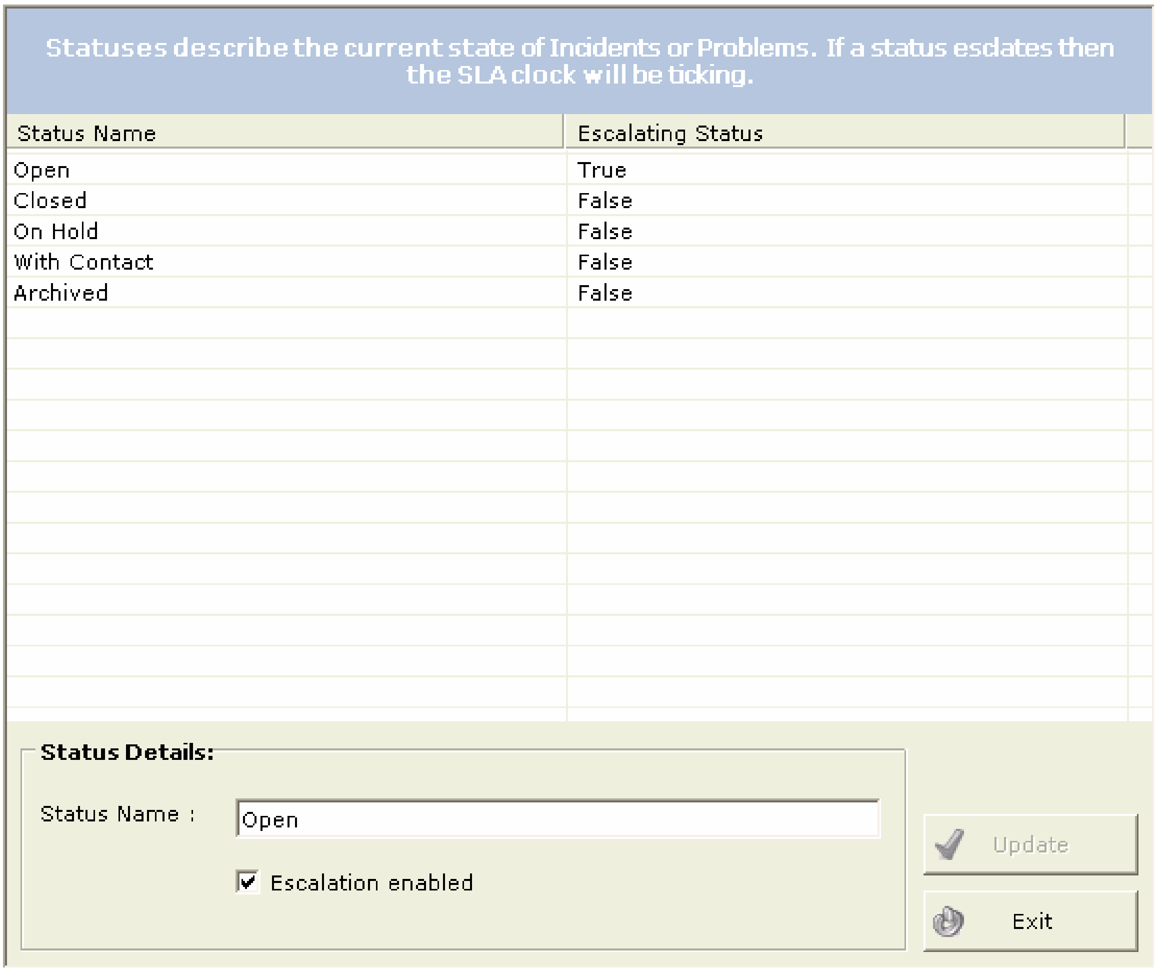
Incident Management

Statuses

Statuses are used to describe the current state of a Request. A status is applied to a Request when it is first logged. The status of a request can be changed throughout the life-cycle of the request. Statuses are used for statistical reporting in the Management Console.

The default Statuses include Open, Closed, On Hold, With Contact, and Archived.

A Status can be set to have escalation enabled or disabled. When the escalation is enabled the escalation clock will be active on any request using that Status. If the escalation is not enabled the escalation clock will not be active on any request using that Status.



Adding a New Status

- Right Click anywhere in the Status table.
- Select *Add New* Status from the context menu.
- In the Status Details box enter the name of the new Status.
- If the new Status will participate in escalations check the box *Escalation Enabled.*
- Click on *Update.*

Deleting a Status

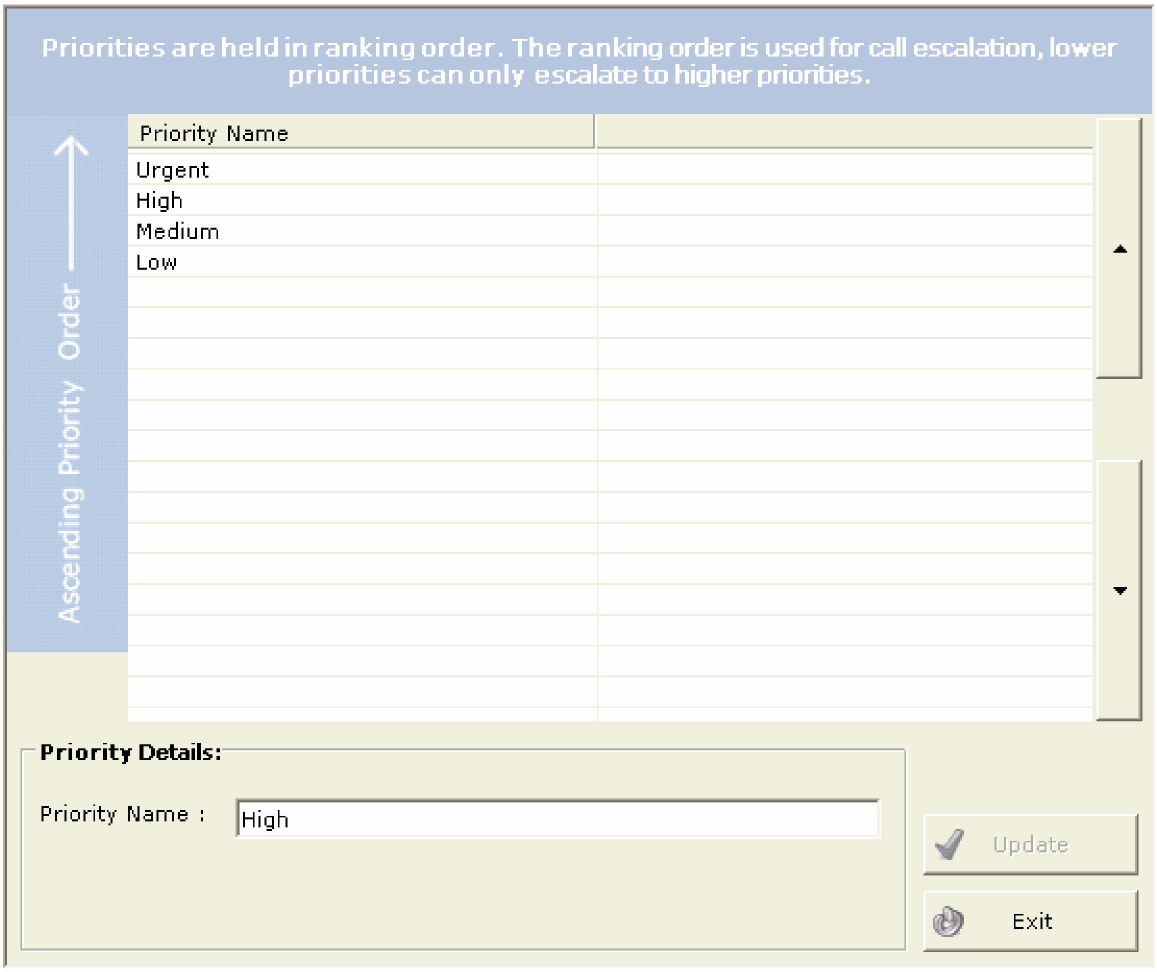
- Select the Status to be deleted.
- Right Click on the Status and select *Delete Status* from the context menu.
- Select *Yes* to confirm the deletion of the Status.

Note: It is not possible to delete a status that is in use by a Request.

Priorities

Priorities are used to describe the urgency of a Request. A priority is applied to a new Request either manually or when an SLA is selected for the Request. Priorities can be used to define the different escalation steps associated with a SLA. The Priority order is defined by the order that they appear in the Priority list.

The default Priorities include Urgent, High, Medium, and Low.



Adding a New Priority

- Right Click anywhere in the Priority table.
- Select *Add new* priority from the context menu.
- Enter the name of the new Priority in the *Priority Details* text box.
- Click on *Update*
- Use the *Up* and *Down* arrows to position the Priority.

Deleting a Priority

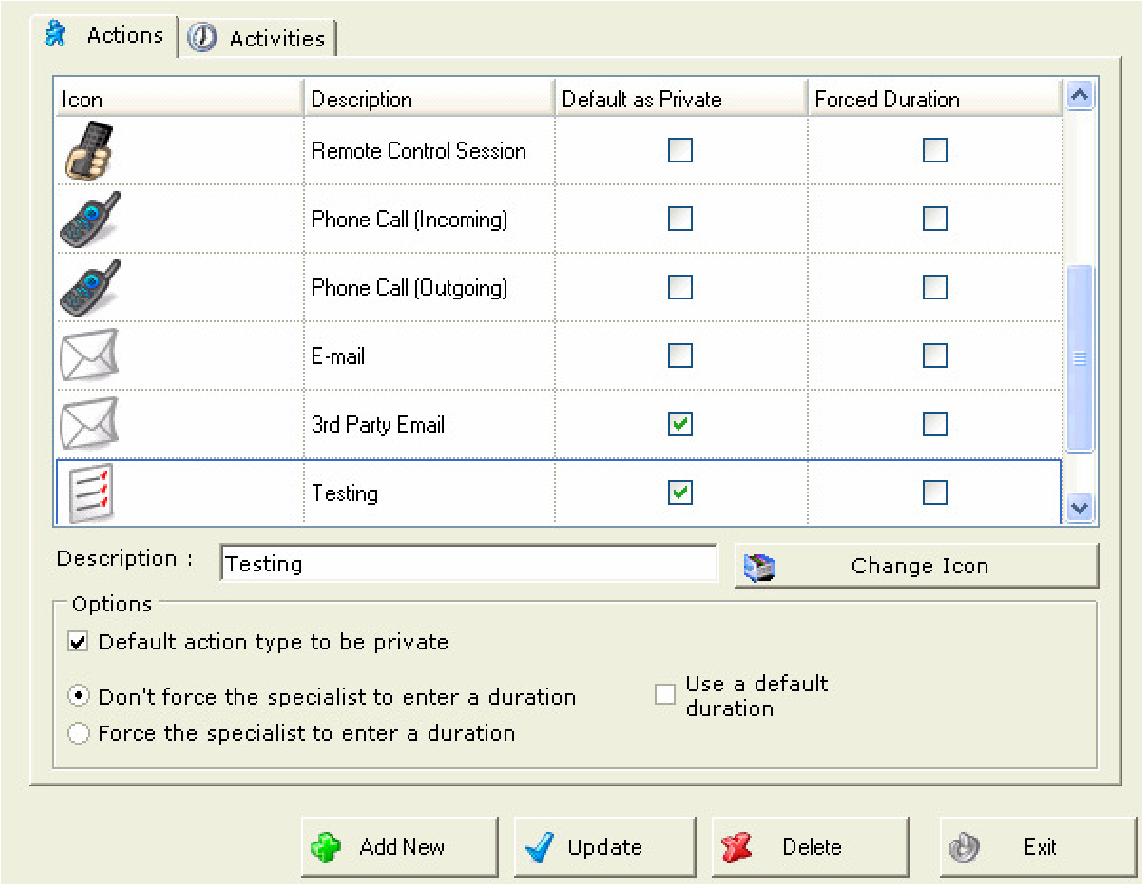
- Select the priority to be deleted.
- Right Click on the priority and select *Delete priority* from the context menu.
- Click on *Yes* to confirm the deletion.

Note: Priorities used as default in user profiles, for e-mailed requests, or in escalation types may not be deleted.

Action / Activity Setup

Actions

Actions are used within an Incident record to record events that have been completed or to record events as they are happening.



Adding new Action Types

- Click on the *Add New* button.
- Select the *New Action* from the Action List.
- Enter a new Description.
- Click on the *Change Icon* button to select an Icon for the Action.
- Click on Update.

A typical collection of Action Types may be:

- Phoned
- E-mailed
- Faxed
- Re-Installed
- Site Visit Completed

Action Options

- **Description**
  The Description identifies the type of Action. Descriptions should reflect completed or current events and not future events.
- **Change Icon**
  Click on the *Change Icon* button to open a window that displays 20 available icons to associate with the selected Action. Double click on the Icon to be associated with the selected Action. These icons will be displayed in the list of Actions within an Incident record.

  Note: The available list of Icons can be modified in the Configuration Management section of the Setup Console.
- **Default action type to be private**
  Actions can be set as *Private* to prevent them from being viewed by users of the Customer Web Interface. A Private Action will also not be available in any report.

- **Don't force the Specialist to enter a duration**
  If this option is selected the Specialist will not be required to enter a duration time in the Action.
- **Force the Specialist to enter a duration**
  The entry of the Action duration will be mandatory when adding a new Action to an Incident.
- **Use Default Duration**
  A default duration can be set for each Action. Enter the number of days, hours, and minutes that the selected action is expected to take.

Modify Actions

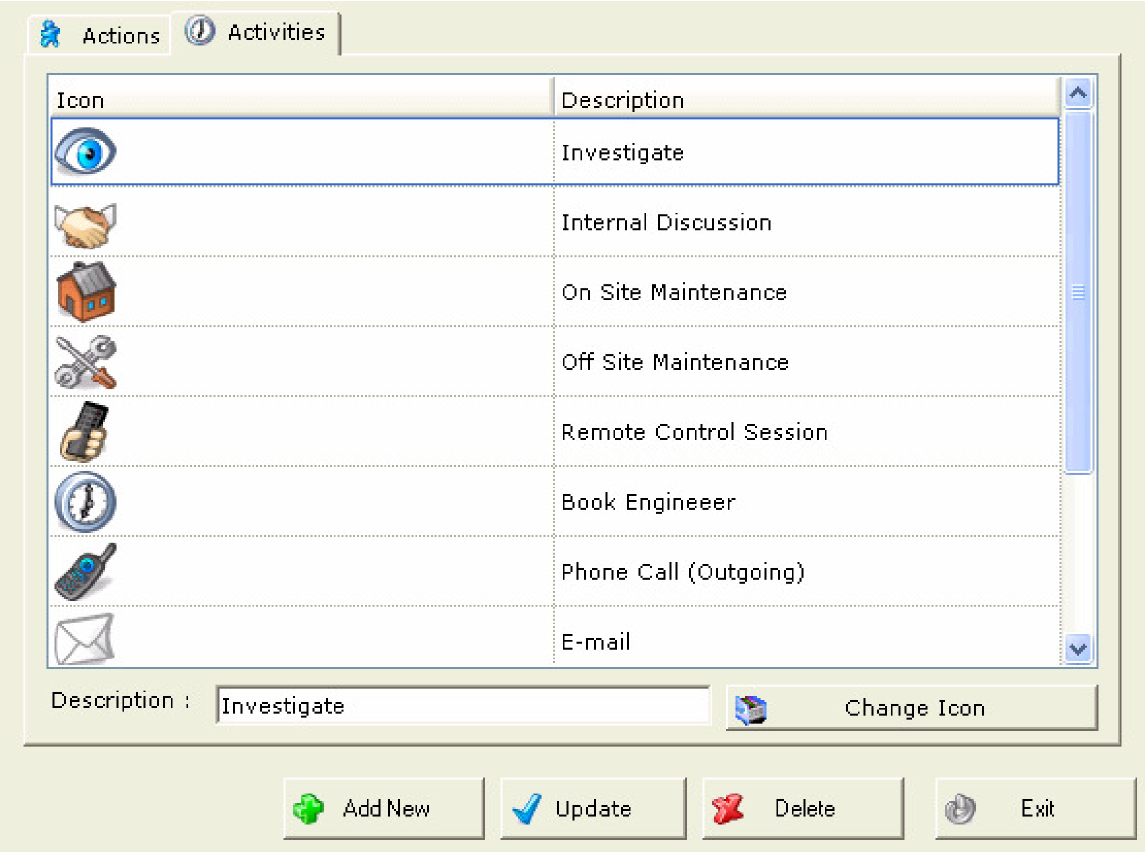
- Select the Action from the Action List
- Change the options for the Action
- Click on the *Update* button.

Delete Actions

- Select the Action from the Action List
- Click on the *Delete* button

Activities

Activities are used to record planned or future activities for an Incident. Activities can be assigned to any SupportDesk User and can be managed using the Activity List. Activity Types define the type of Activity that is to take place.



Adding new Activity Types

- Click on the *Add New* button.
- Select the *New Activity* from the Activity List.
- Next, enter a valid description for the activitity type.
- Click on the *Change Icon* to select an Icon for the Activity.
- Click on the *Update* button.

A typical collection of Activity Types may be:

- Phone
- E-mail
- Fax
- Re-Install
- Site Visit

Modify Activities

- Select the Action from the Action List
- Change the options for the Action
- Click on the *Update* button.

Delete Activities

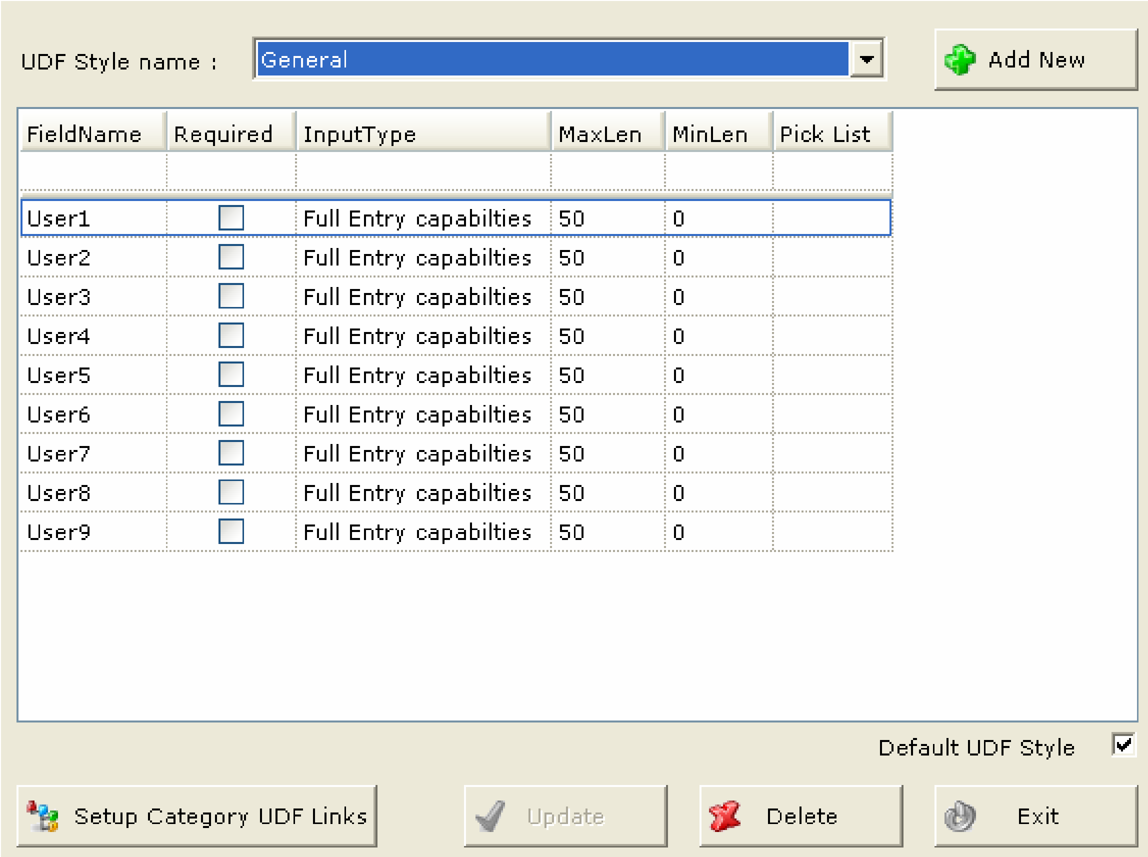
- Select the Action from the Action List
- Click on the *Delete* button

Note: Action and Activity Types can not be deleted if:

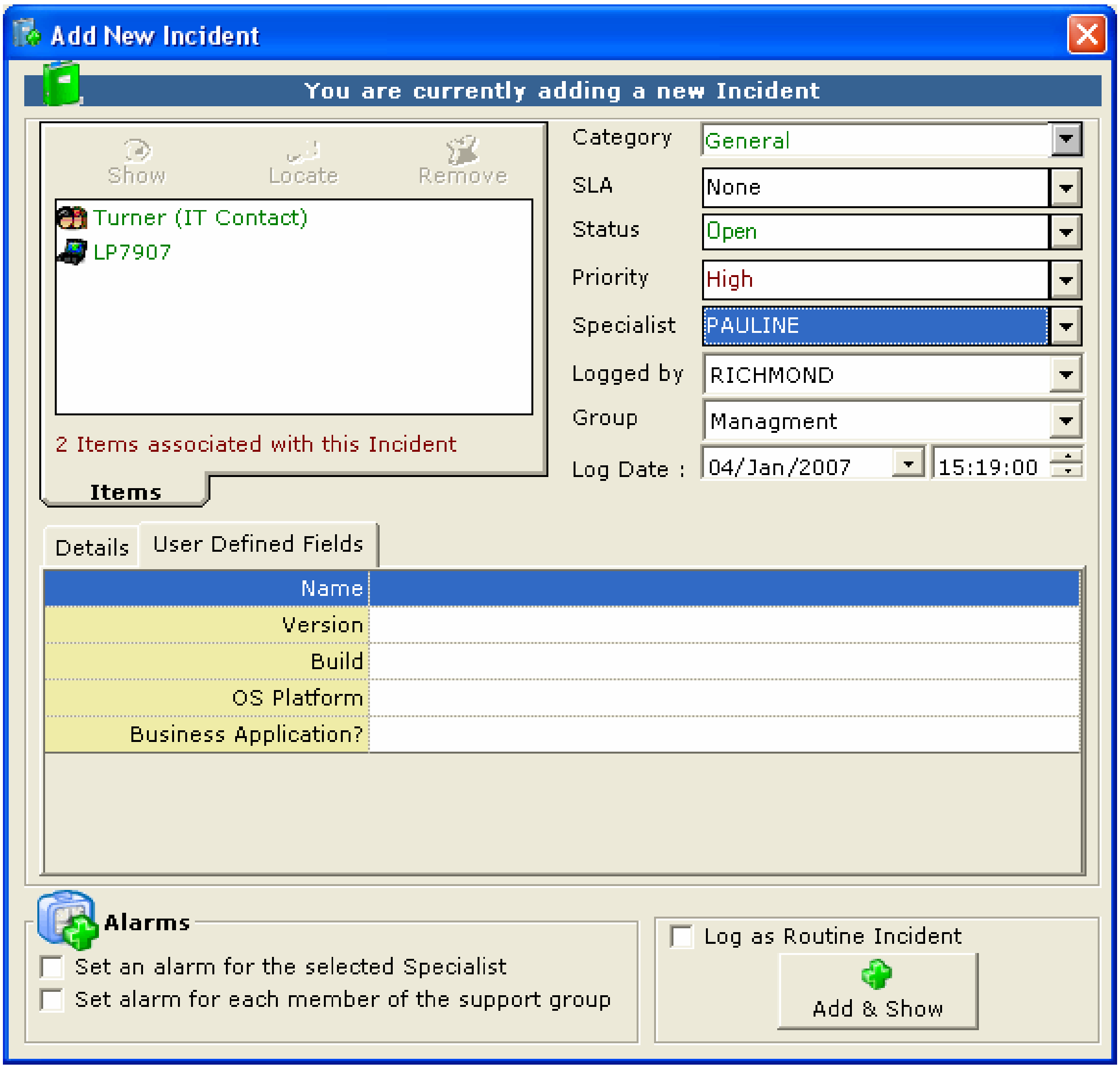
- There are any Incidents with the Action or Activity Type logged against it.
- Users have chosen the Action or Activity Type to be their default.

UDF Setup

User Definable Fields (UDF) are customisable fields used for the collection and recording of information relating to Incidents, Problems, and Known Errors. User Definable Fields can be used by SupportDesk Specialists and by end users logging Incidents through the Web Interface.



Multiple UDF Styles can be created, each containing custom defined fields that can relate to one or multiple categories. When a category is assigned to an Incident, the applied UDF Style will be available to the Incident record for the capture of data specific to the Category.



When adding an Incident the UDF tab will display the defined UDF fields associated with the selected Category.

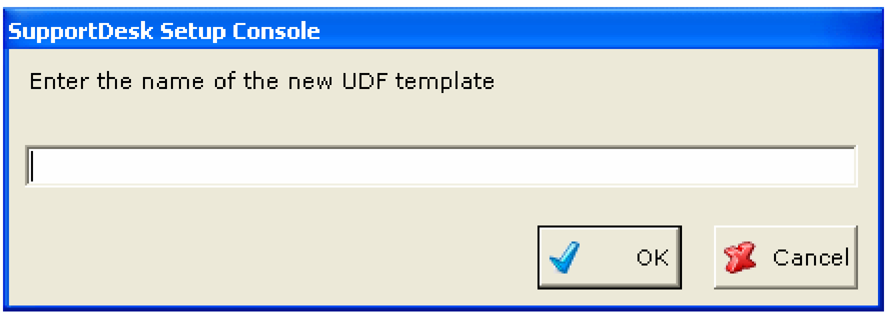
UDF Style Name

The *UDF Style Name* drop down box is used for the selection of existing UDF Styles to view or modify.

SupportDesk comes with one predefined UDF Style named *General*. . This is initially defined as the Default UDF Style and will be used for all Categories that have not been linked to a UDF style.

Add New

To add a new *UDF Style* click on the *Add New* button.



Enter the name of the Style that will be created.

> **Note:** When naming the Style it should reflect the information held within the style and the category that it will be assigned to as multiple categories can be assigned to a single Style

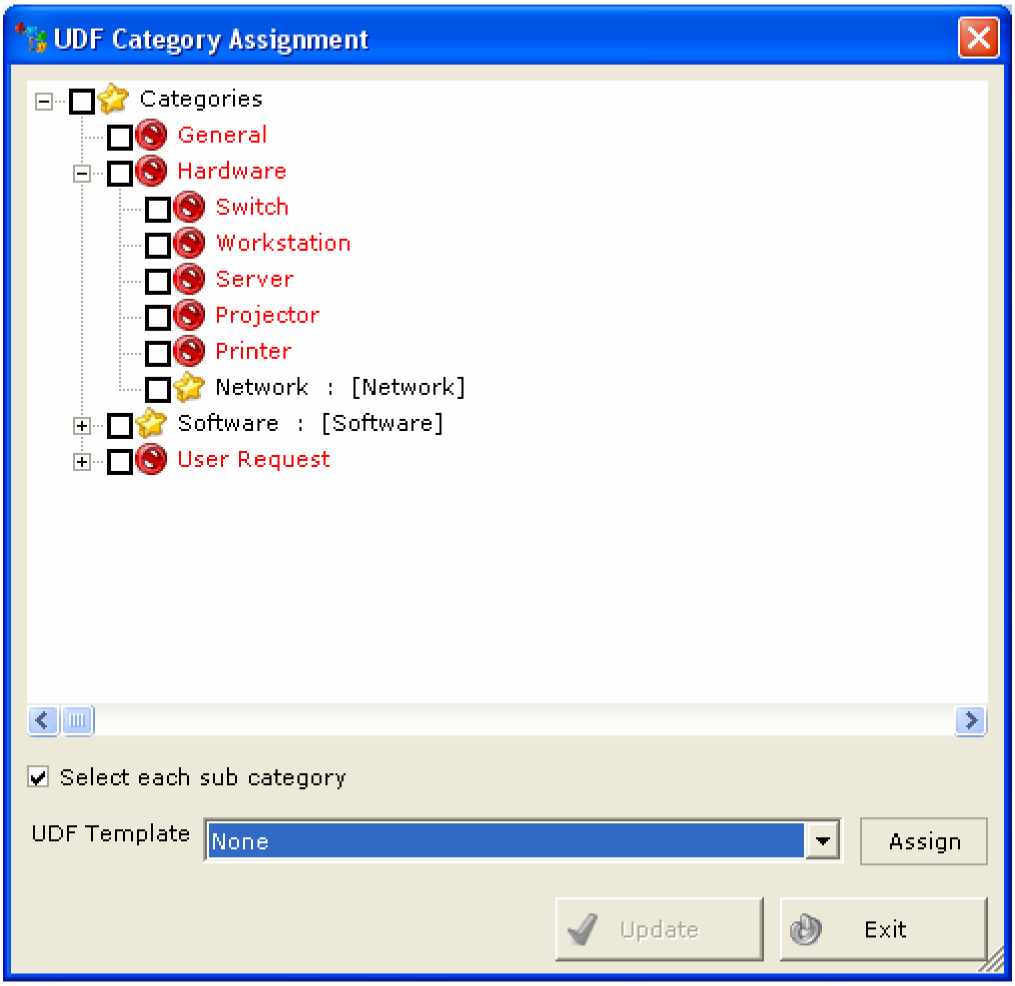
FieldName	Required	InputType	MaxLen	MinLen	Pick List
	☐		25	0	

Each UDF consists of five options:

- **Field Name**
  The Field Name contains the description of the field. This description is displayed to the Specialist or the End User when an Incident is being logged or when the UDFs are being updated. The description can be entered in the form of a question that can be directed at the Specialist or the End user.
- **Required**
  Selecting the Required check box will force this field to be populated at the time the Incident is being logged.
- **Input Type**
  Three methods of input can be defined for each field: Free text only, Pick List only, and Fully Entry Capabilities. Select from the drop down box which type of input will be used for this field.
- **MaxLen**
  Defines the maximum number of characters that can be entered into this field.
- **MinLen**
  Defines the minimum number of characters that can be entered into this field.
- **Pick List**
  The Pick List option lets you compile a list of items to populate the pick list. The Pick List can be imported from existing data either held within already entered data or from a CSV file.

Setup Category UDF links

The *Setup Category UDF links* is used to link one or multiple Categories with a single UDF Style. Click on the *Setup Category UDF links* button to perform this action.

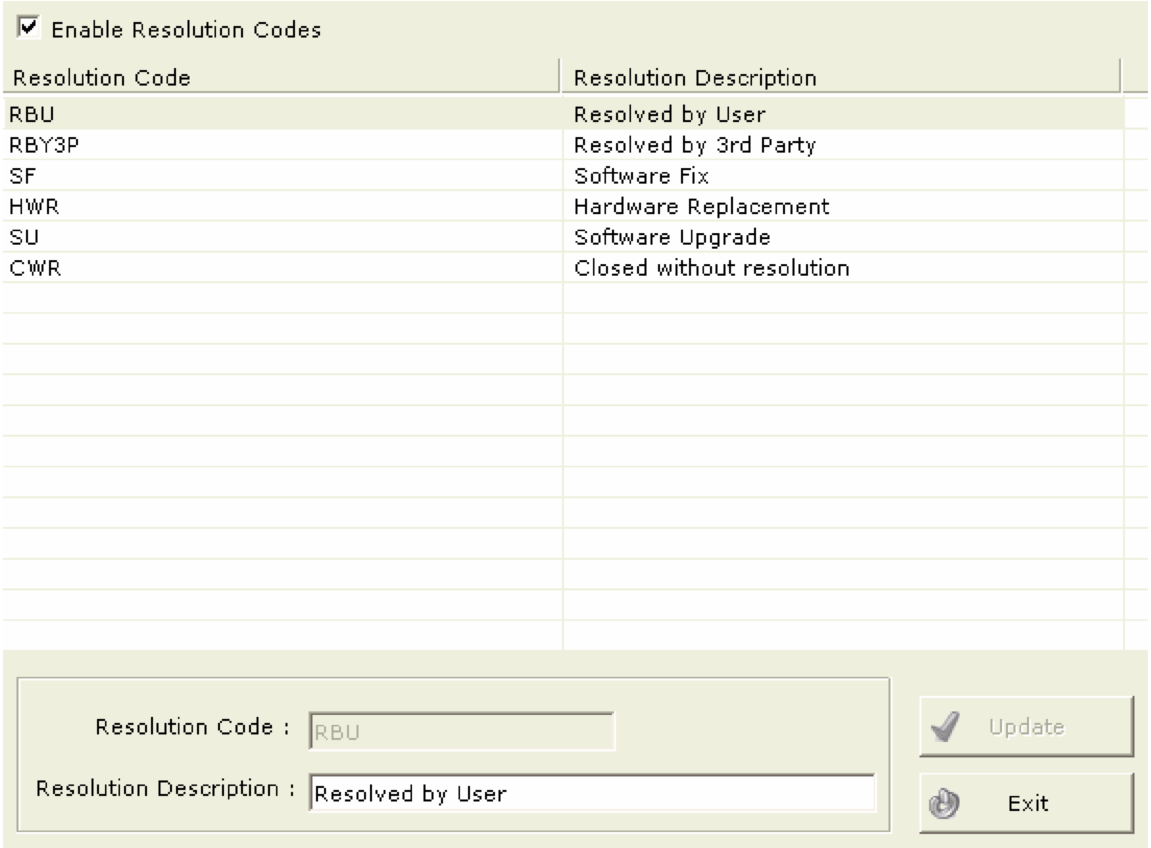


1. From the Category Tree select the Categories that you wish to link to an existing UDF Style.
2. From the UDF Style drop down box select the UDF Style that you wish to assign to the selections in the Category Tree.
3. Click on the *Assign* button.

Resolution Codes

Resolution Codes are used to help provide statistics of how Incident, Problems, and Known Errors were resolved. Resolution Codes are selectable from a drop down list on Incident Problem and Known Error forms.

Resolution Codes are not enabled by default. Select the *Enable Resolution Codes* check box to enable this feature.



Adding Resolution Codes

Before creating resolution codes define a system for your code. This may simply be a numbed system or abbreviation to match the description of the code.

- Right Click in the Resolution Code table.
- Select *Add New Resolution Code.*
- Enter a Resolution Code.
- Enter a Description.
- Click on the *Update* button.

Deleting Resolution Codes

- Select the Resolution Code to be deleted.
- Click on the *Delete* button.

Modifying Resolution Codes

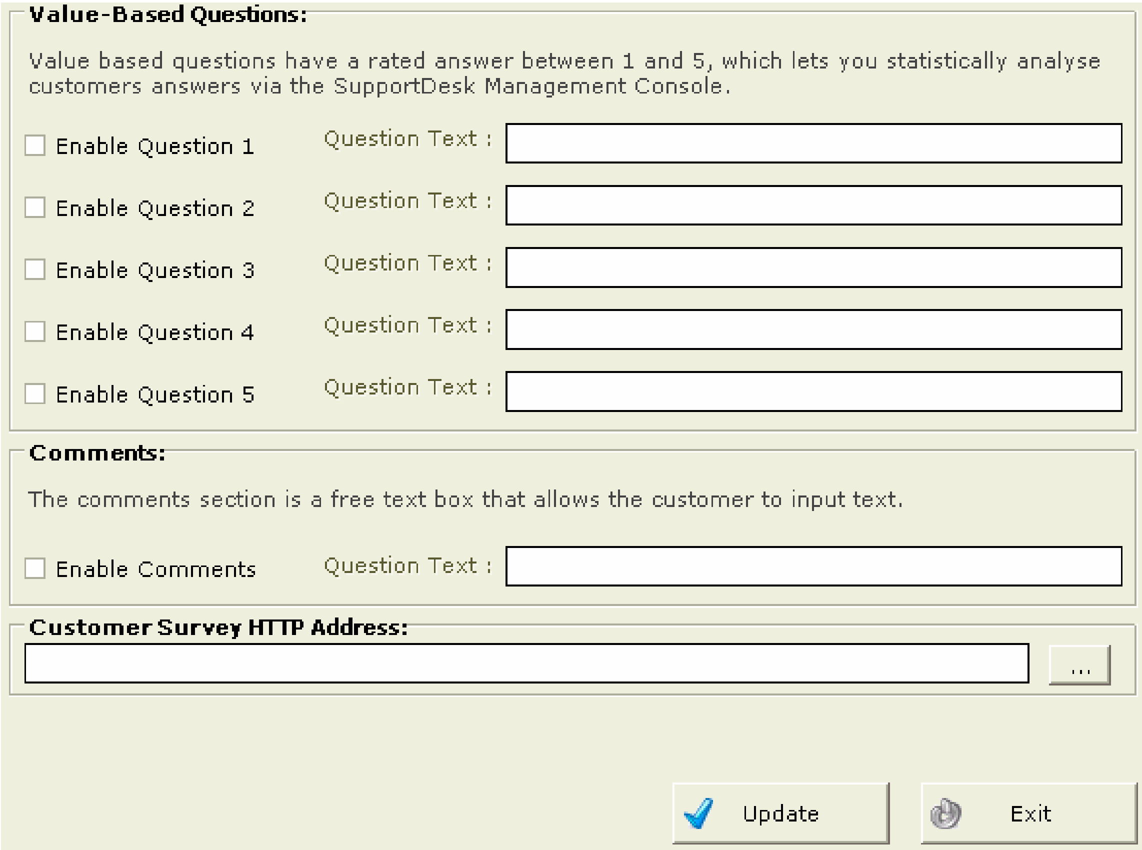
Once a Resolution Code has been created only the Description can be modified.

- Select the Resolution Code to be modified.
- Change the Description.
- Click on the *Update* button.

Satisfaction Survey

The Satisfaction Survey is used to collect feedback from users and customers about the level of service provided by the Service Desk.

The Web Interface is required to be installed to gain access to the Satisfaction Survey form.



Value-Based Questions

A total of 5 questions can be enabled and defined. Each question will have a selectable rating from 1 through 6.

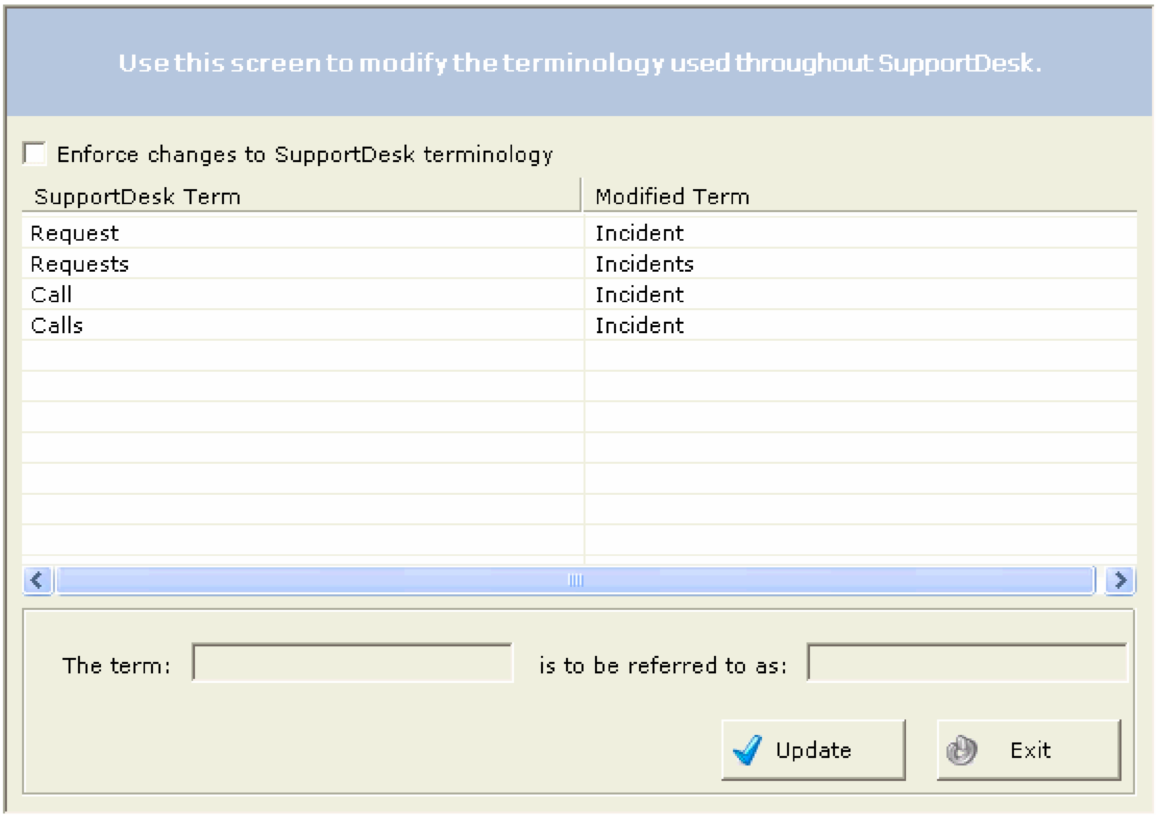
Comments

Customer Survey HTTP address

Terminology

SupportDesk has adopted the term "*Request"* for the name of a record containing a support call. ITIL® standards use the term "*Incident*."

Support Requests can also be known by other terms such as *Calls* and *Tickets.* This feature can be used to rename the term *Request* to a term to suit the environment. Incident is the recommended standard.



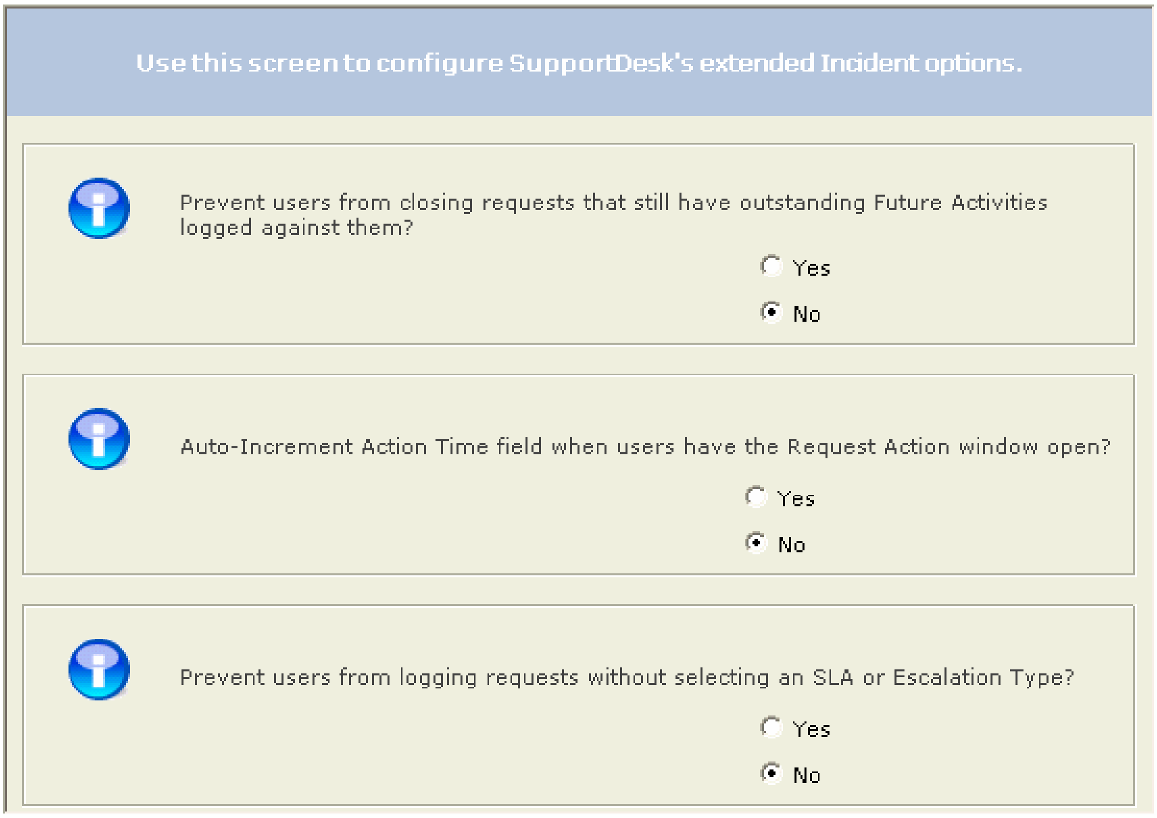
Any change here will be reflected throughout the entire product.

Changing a Term

- Select the term that needs changing.
- In the text box enter the new term.
- Click on the Update button.

Extended Incident Options

Enable or disable rules that enforce particular request behaviour.



These rules are described below:

- Prevent Users from closing requests that still have outstanding future activities logged against them.
    - If a Request has one or more future Activities logged against the call, the Status of the Request can not be set to Closed. An example Activity may be to contact the End User to confirm that the resolution has fixed the problem. Once this Activity has been completed the Request can be closed.
- Prevent users from logging requests without selecting an SLA or Escalation Type.
    - When a new Request is being created, this feature forces the selection of an SLA before the new Request can be saved. This can help enforce the assignment of SLAs to a Request to prevent Requests from missing SLA targets.
- Auto-Increment action time field when users have the Request Action window open. (Windows client only)
    - When a Request Action window is open, the length of time that the window is opened for will be tracked and recorded in the *Duration of Action* text box when the Action is saved. This can be used to automatically track the length of a phone call by creating the new Action at the time the call is made and closing the Action when the call is completed. Time is only calculated to the minute.

Enable or disable each setting as required and click on *Save*. The rules will be enforced when Users next login to SupportDesk.

Problem Management

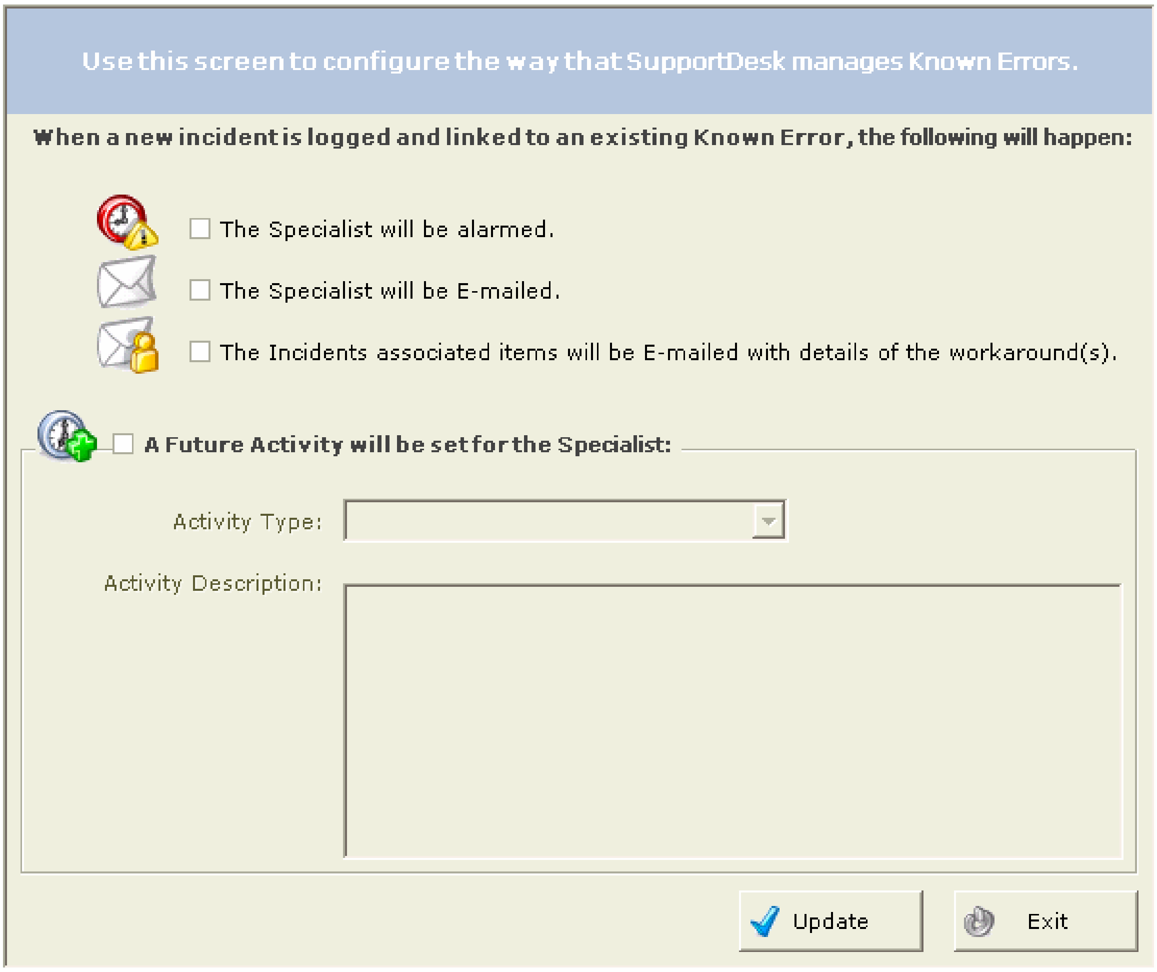
Disable/Enable Problem Management

Problem Management is a process for identifying and recording Problem records and Known Errors. Enabling the Problem Management introduces additional functionality:

- When new Incidents are logged it will automatically search for Problems and Known Errors that are logged under the same category.
- Problem records can be created against Items in the Navigator Tree.
- The Problem Management Console becomes available.
- Incidents can be linked to Problem and Known Error records.

Known Errors

A Known Error is an Incident or a Problem for which the cause is known and a temporary workaround or a permanent fix is available. When an Incident is linked to a Known Error selected events can occur automatically.

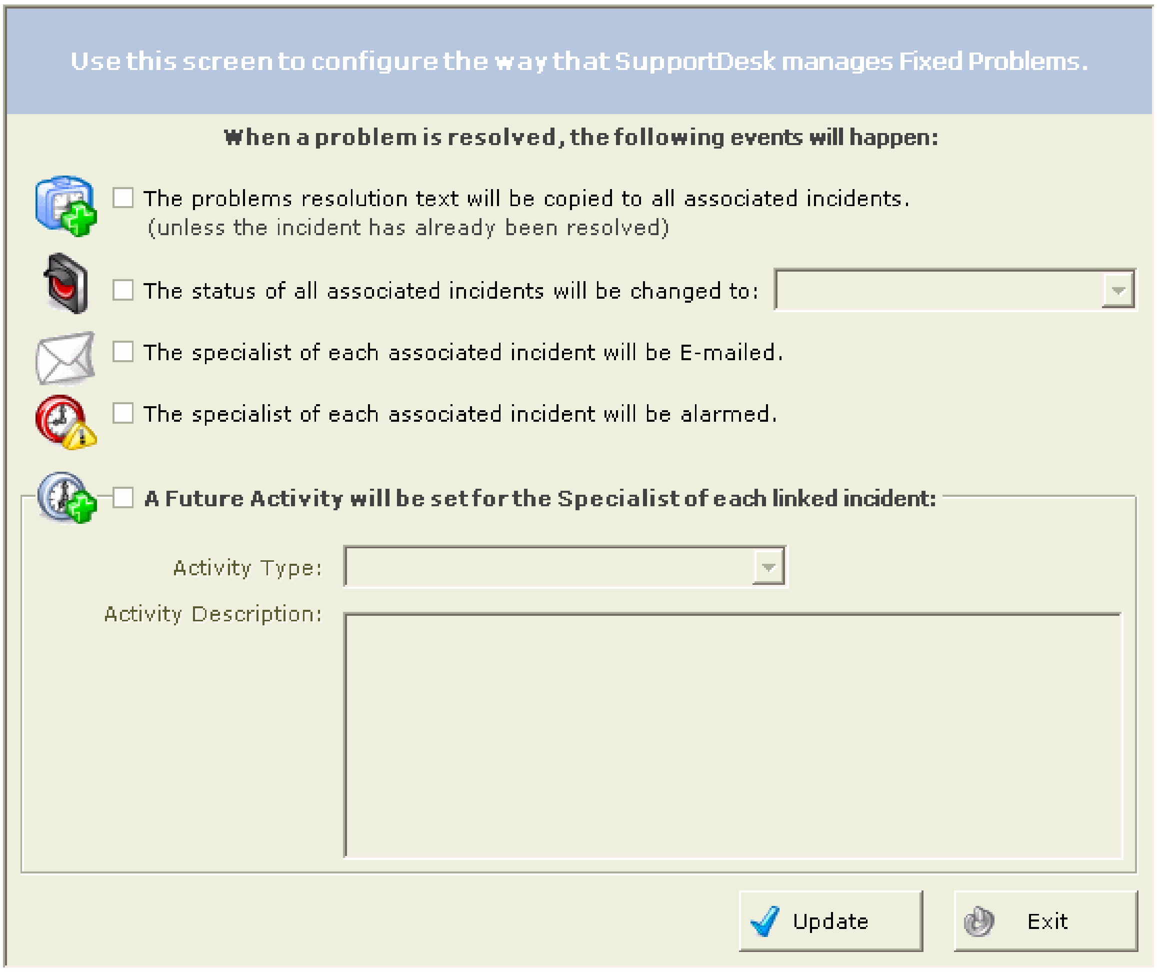


When an Incident is linked to a problem that has a workaround or the problem has been fixed the Specialist and any Item associated with the Incident can be notified of the workaround by SupportDesk Alarm or via email.

An Activity can be set for the Specialist to schedule contacting the customer, provide further instructions, or details of the workaround.

Fixed Problems

A Problem is an unknown underlying cause of one or more Incidents. When a Problem is resolved particular events can be configured to occur automatically.



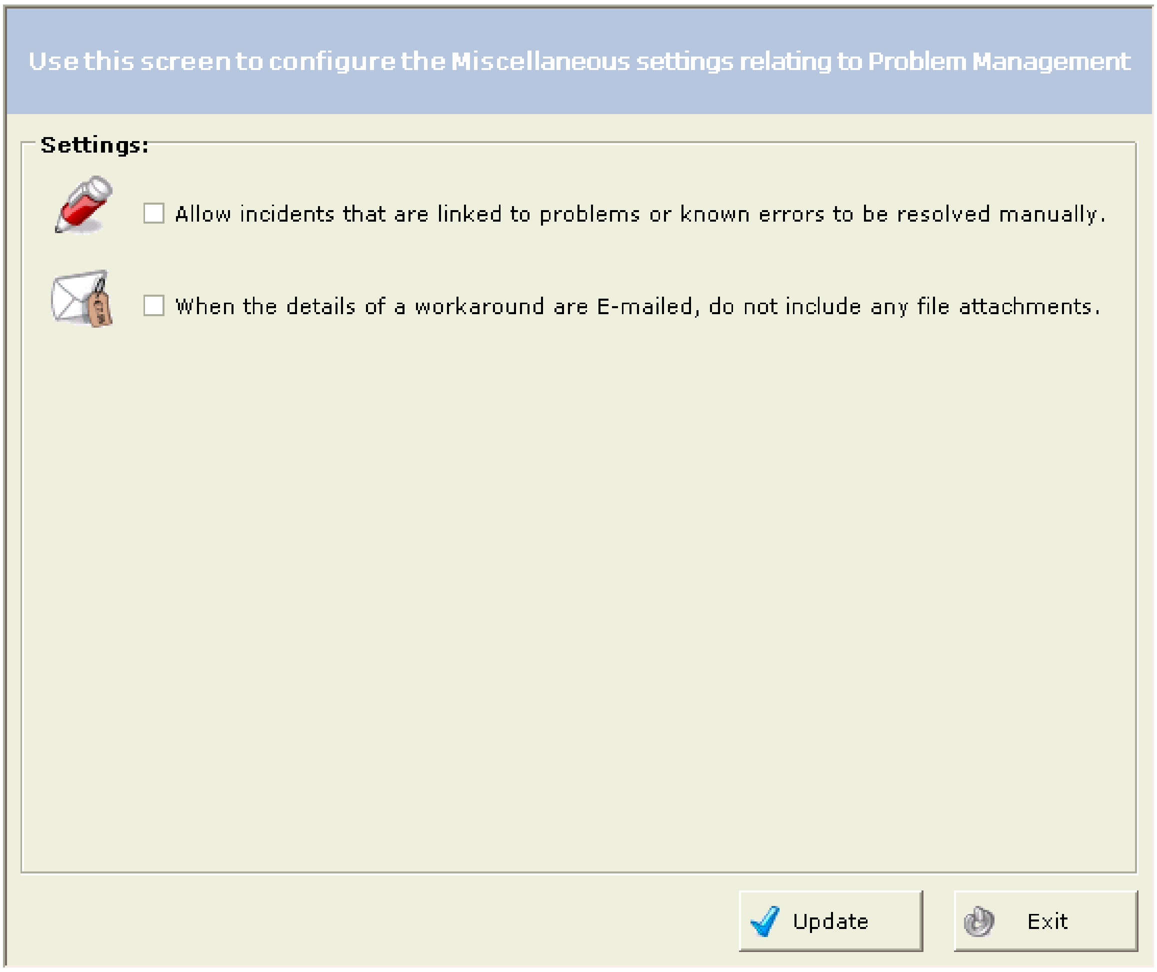
When a Problem has been resolved it can update and modify the status of any Incident that is linked to the Problem. You can also configure an alarm or email for the Specialists of the linked Incidents.

An Activity can be set for the Specialist to schedule contacting the customer, provide further instructions, or details of the workaround.

Misc

If an Incident is linked to a Problem, you can still give the Specialist the ability to manually add a resolution to the Incident.

You can also prevent the sending of Attachments when the details of a workaround are emailed.



Change Management

Change Management Configuration

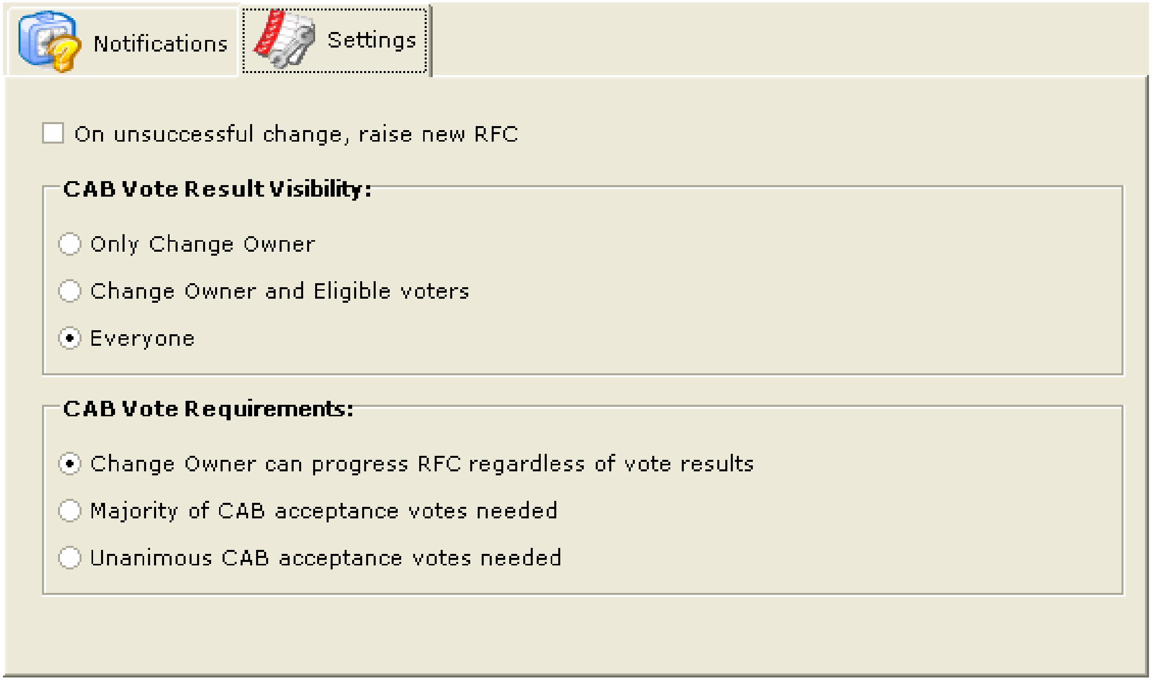
Change Management provides a standardized method of handling and recording any change to the infrastructure. A Change may be required as a result of an Incident or Problem. Requests for Changes can also come from proactively looking for ways to improve service such as updating software, hardware, documentation, network connectivity, and more.

Enable Change Management

Change Management is an optional component within SupportDesk that can be enabled at any point in time. Change Management can be enabled or disabled by selecting the *Enable Change Management* check box. Enabling Change Management will give you access to Request for Change (RFC) forms, RFC reporting, and the Change Console.

Settings

The Settings tab provides options for unsuccessful changes and voting requirements.



The check box labeled *On Unsuccessful change, raise new RFC* will enable the automatic creation of a new RFC when the Status of an RFC is changed to *Unsuccessful*. The new RFC will take Details, Links, and Costs from the unsuccessful RFC and insert a reference to the unsuccessful RFC.

CAB Vote Result Visibility

Each RFC can be put through an approval process by allowing members of the Change Advisory Board (CAB) to vote on the acceptance of the RFC. A RFC that requires voting will display a tab that contains the status and results of the voting. The visibility of this tab can be controlled using the selections below.

- **Only Change Owner**
  Only the Owner of the RFC can see the Change Approval
- **Change Owner and Eligible voters**
  The Owner of the RFC and the members of the CAB can see the Change Approval tab
- **Everyone**
  All Users of SupportDesk can see the Change Approval tab

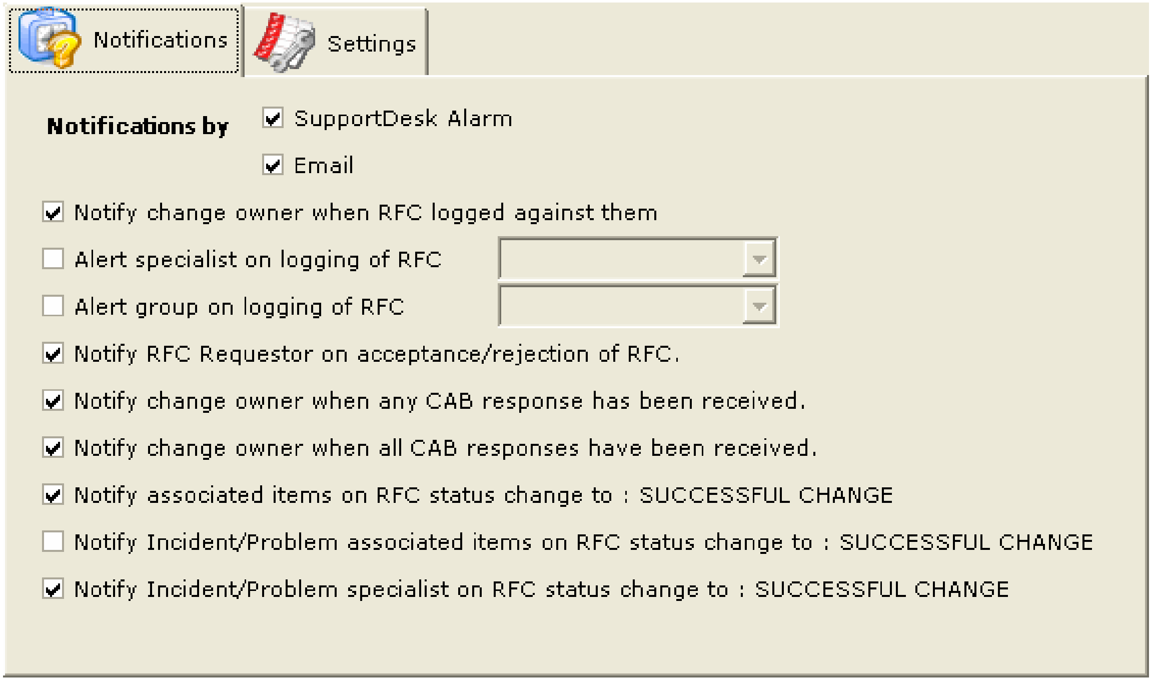
CAB Vote Requirements

Different levels of the number of votes required to accept a RFC can be selected here.

- **Change Owner can progress RFC regardless of vote results**
  The Change Owner can change the status of an RFC regardless of the vote results
- **Majority of CAB acceptance votes needed**
  Over 50% of voters must accept the RFC to proceed
- **Unanimous CAB acceptance votes needed**
  All CAB members must vote and accept the RFC

Notifications

Notification by email or SupportDesk Alarms Module can be configured to automatically alert users of changes or the status of a RFC.

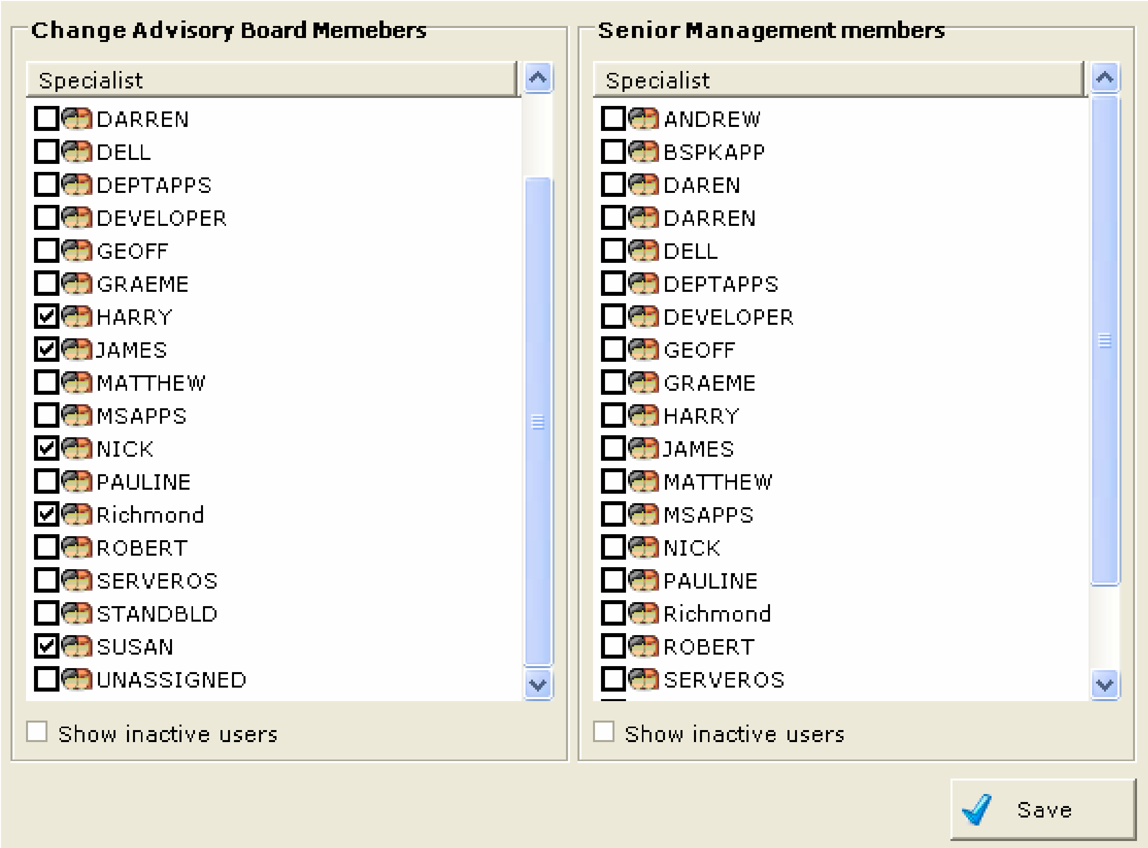


The *Notifications By* option allows you to select how the notification messages will be sent. Notifications can be sent by email or by the SupportDesk Alarms Module or both.

- **Notify Change Owner when RFC logged against them**
  When a RFC is added an owner must be selected. The Owner of the RFC is responsible for the Change through its life. This option will notify a SupportDesk User when a new RFC is created with them as the owner.
- **Alert Specialist on logging RFC**
  Any User set up as a Specialist in SupportDesk can be notified of the creation of any RFC. SupportDesk Specialists are selectable from a drop down list.
- **Alert Group on logging RFC**
  Any Group that has been configured in SupportDesk can be sent a notification of the new RFC. SupportDesk Groups can be selected from the drop down list.
- **Notify RFC Requestor on acceptance / rejection of RFC**
  When a RFC is either accepted or rejected the Requestor (the person who created the RFC) will be automatically notified.
- **Notify Change Owner when any CAB response has been received**
  The Change Owner will receive notification for each voting response by CAB members.
- **Notify Change Owner when all CAB responses have been received**
  The Change Owner will receive notification when all CAB members have voted on a RFC.
- **Notify Associated items on RFC Status change to: SUCCESSFUL CHANGE**
  Any item that has been linked to a RFC and contains an email address will be sent a notification when the RFC status has been changed to *Successful Change*.
- **Notify Incident/Problem associated items on RFC status change to: SUCCESSFUL CHANGE**
  If a RFC is linked to an Incident or a Problem, any item that is associated with either the linked Incident or Problem and contains an email address will be sent a notification that the status has been changed to *Successful Change*.
- **Notify Incident/Problem Specialist on RFC status change to: SUCCESSFUL CHANGE**
  If a RFC is linked to an Incident or a Problem, any Specialists of either the linked Incident or Problem will be sent a notification that the status has been changed to *Successful Change*.

CAB Setup

The CAB Setup lets you select who will be participating in the acceptance process of a RFC.



The CAB Setup is split into two groups – Change Advisory Board Members and Senior Management Members. When a RFC has an Impact level of *Significant* only the Change Advisory Board Members will be required to vote. When the Impact level has been selected as *Major*, both the Change Advisory Board and Senior Management will be required to vote.

Select each user that will participate in either the Change Advisory Board or the Senior Management.

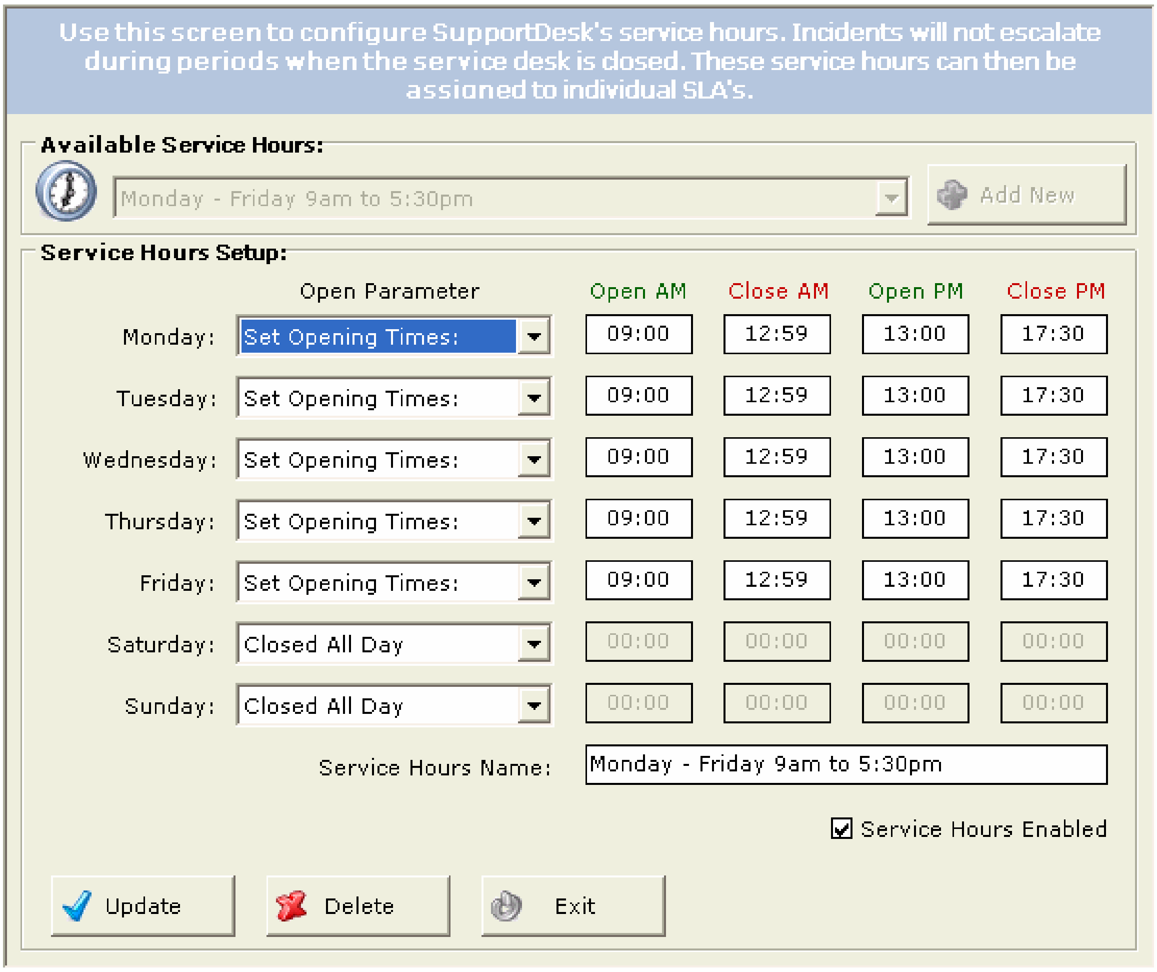
An option to display disabled users has been provided to allow for the removal of a SupportDesk User from either the CAB or Senior Management when the SupportDesk User account has been disabled.

Service Level Management

Service Hours

For each day of the week, the helpdesk can be set to be closed, open between definable hours (including lunchtimes) or open for all 24 hours. These settings should be for the regular working week only, and should not be used to reflect singular events, e.g., a holiday. Multiple Service Hours can be configured when there is a requirement to offer different opening hours for different SLAs

Service Hours are used to accurately calculate parameters such as when requests should escalate, and how long requests have been open for.



From the drop down boxes for each day, it is possible to select one of three options:

- Open all day: Helpdesk open 24 hrs
- Closed all day: Closed for all 24 hours
- Set opening times:

If the user selects the 'Set opening times' option, then the specific opening hours for that day must be entered. If the helpdesk does not close for lunch, then the 'Close AM' and 'Open PM' times must be set to zero (Specifically 00:00).

Adding new Service Hours

- Click on the *Add New* button.
- Select the *Open Parameter* for each day of the week.
- Enter the name of the Service Hours
- Click on *Update*

Deleting Service Hours

- From the available Service Hours drop down box and select the Service Hours to be deleted.
- Click on the Delete button.
- Click on *Yes* to confirm the deletion.

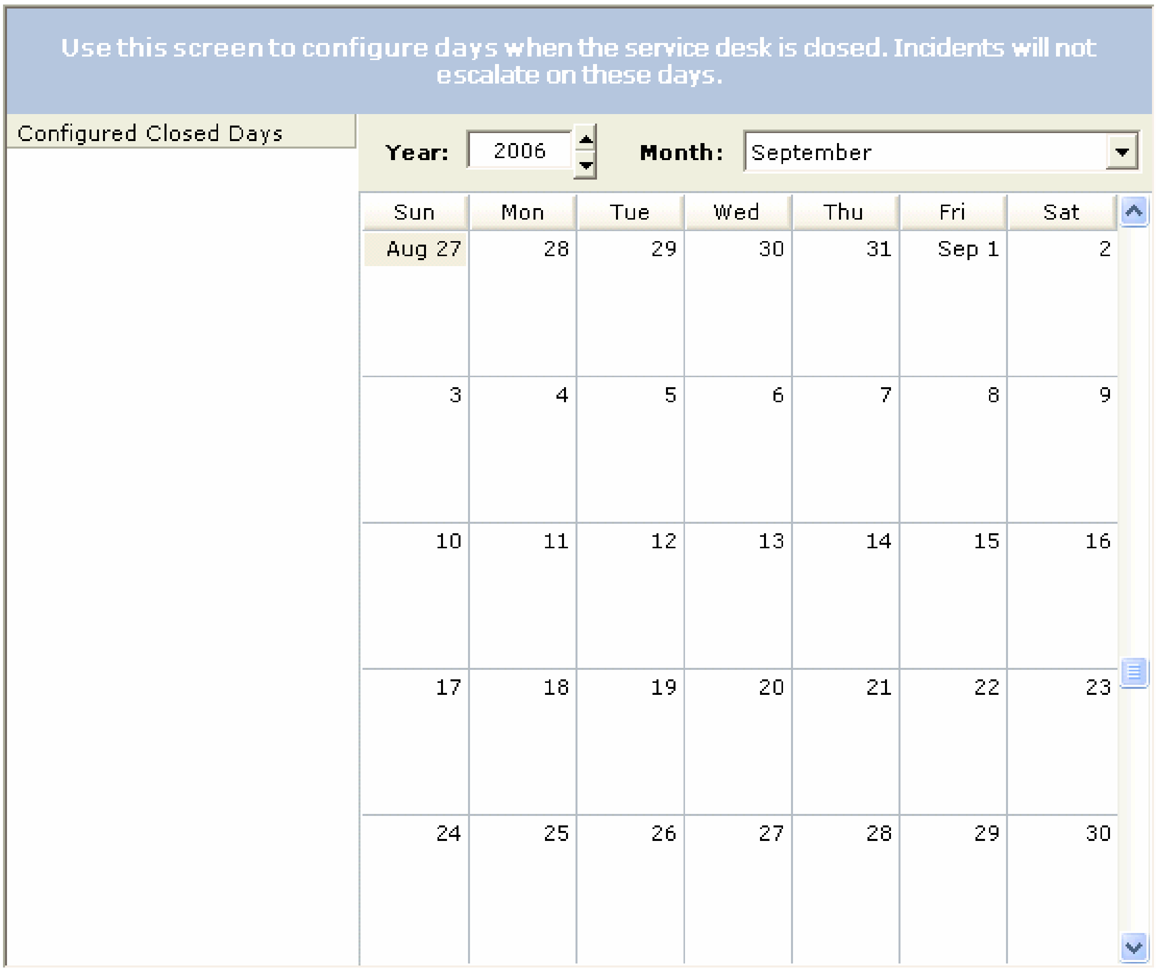
Disabling Service Hours

- From the available Service Hours drop down box and select the Service Hours to be disabled.
- De-select the check box labeled *Service Hours Enabled.*

Closed Days

Closed Days allows specific dates to be entered into SupportDesk to indicate when the helpdesk will be closed. Closed days are used to reflect singular events outside the normal working week such as holidays.

Closed days are calculated into the escalations, response times, and resolution times.



Add a Closed Day

- Select the day in the calendar to be configured as Closed.
- Right Click on that day and select *Add New* from the context menu.
- The new Closed Day is displayed in the Configured Closed Days list.

Note: Dates in the past may be entered to reflect days when the helpdesk was closed unexpectedly, and this may change the total open time displayed for some requests. However, this will not reverse escalations that have taken place, nor will it change the dates and times of escalations that are due to happen in the future.

Delete a Closed Day

- Select the Closed day.

- Right Click on the Closed Day.
- Select *Delete* from the context menu.

Escalation Types

An escalation type is a series of priorities and / or specialists that a request can be made to escalate through automatically (using the Escalation Module). It also constitutes a fixed response and resolution time, as well as series of definable alerts. These alerts will be triggered to warn users of escalation, or the passing of response and resolution times.

Escalation Types are applied to individual Incident Records by selecting the Escalation Types from the SLA drop down box on the *Add Incident* form.

Each escalation step can be configured to increase the priority, change the specialist and set alarms for any users of the helpdesk, as well as a specific alert for whoever the current specialist of a request is. A specific step does not have to increase the priority; however, any step cannot decrease the priority.

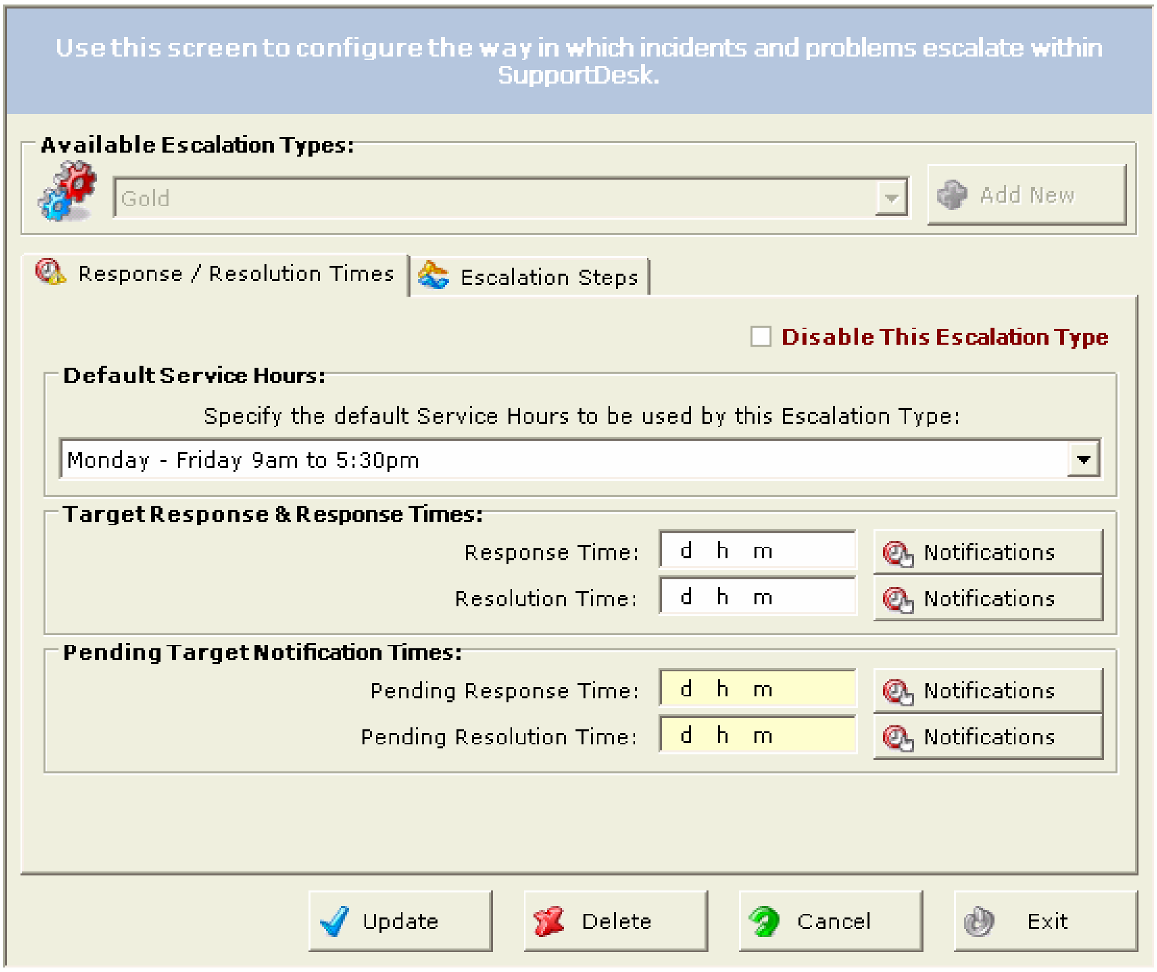
Existing escalation types can be modified by selecting one of the descriptions from the dropdown menu.

Adding an Escalation Type

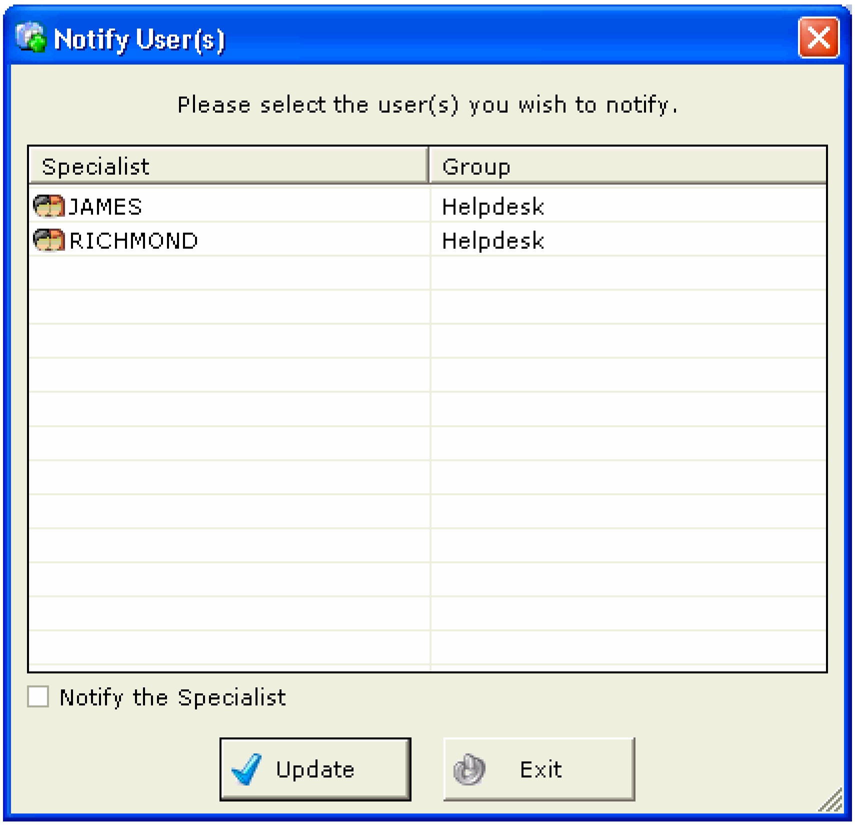
- Click on the *Add New* button.
- Enter the name of the Escalation type.
- Click *OK* to accept the new name.
- Select the Response/Resolution Times tab.
- Select the default Service Hours.
- Configure the Response and Resolution times.
- Configure the notifications.
- Select the Escalation Steps tab.
- Configure the Escalation steps.

Response and Resolution

The Response and Resolution tab lets you configure Target times for Response and Resolution and define notifications for each of the listed events.



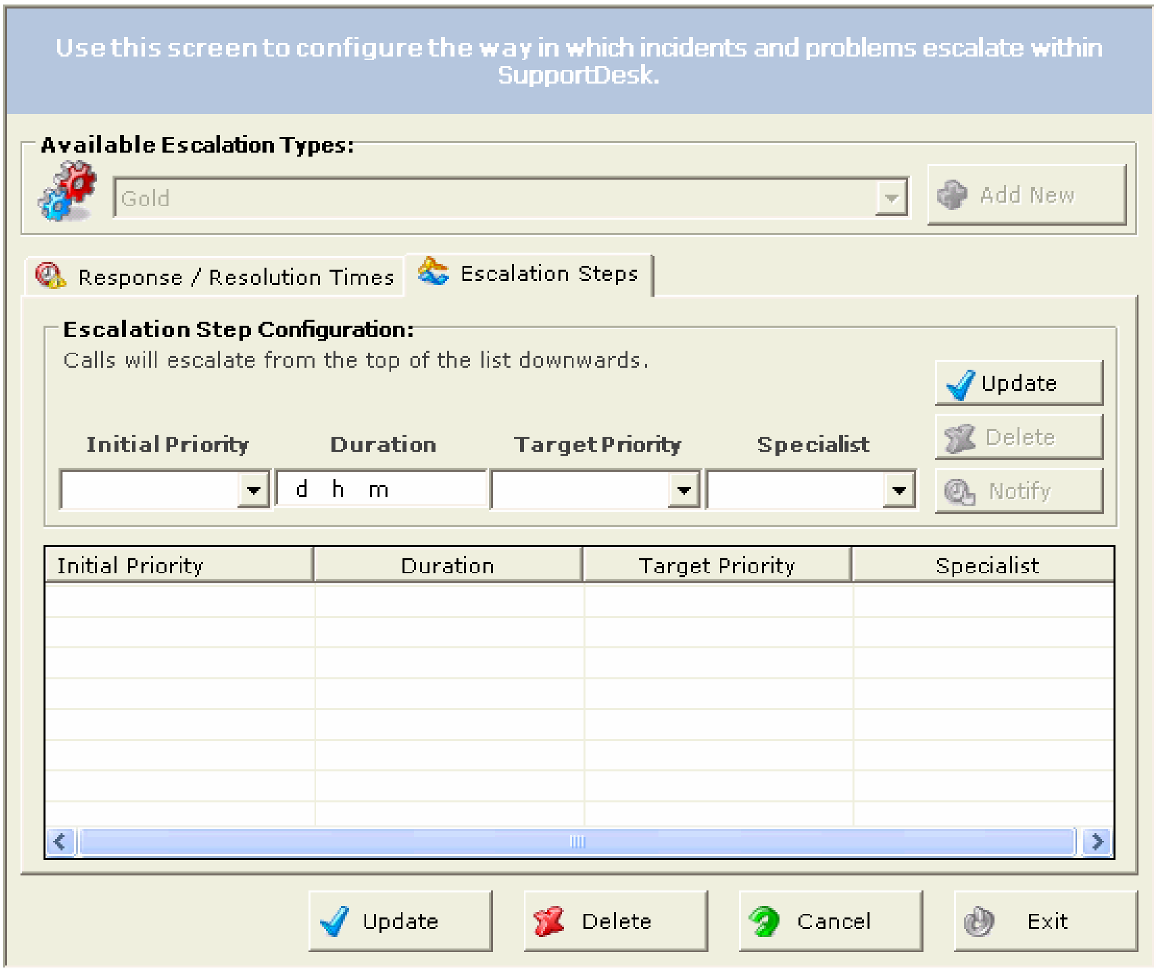
- **Default Service Hours**
  From the Default Service Hours drop down list select the Service Hours that will be used for this escalation series.
- **Response Times**
  Define how much time will pass before the Response target is reached.
- **Resolution Times**
  Define how much time will pass before the Resolution target is reached.
- **Pending Response Time**
  Define how much time prior to a Response target being reached that an alarm is sent to a specified user.
- **Pending Resolution Time**
  Define how much time prior to a Resolution target being reached that an alarm is sent to a specified user.
- **Notifications**
  The Response and Resolution Times and the Pending Response and Resolution Times each have an option to define one or more SupportDesk Users to be notified when that particular event happens. Clicking on the *Notification* button will bring up the following window:



Select each SupportDesk User that you wish to receive an alarm for that particular event. Select the check box *Notify the Specialist* to alert the User that has been assigned to the Request on which the event is occurring.

Escalation Steps

The Escalation Steps Tab lets you define how a Request increases its priority over a period of time. With each escalation Users of SupportDesk can be notified that an escalation has occurred. The Request can also be reassigned to different User when each escalation is reached.



Enter the Escalation Step starting with the lowest priority of all the steps.

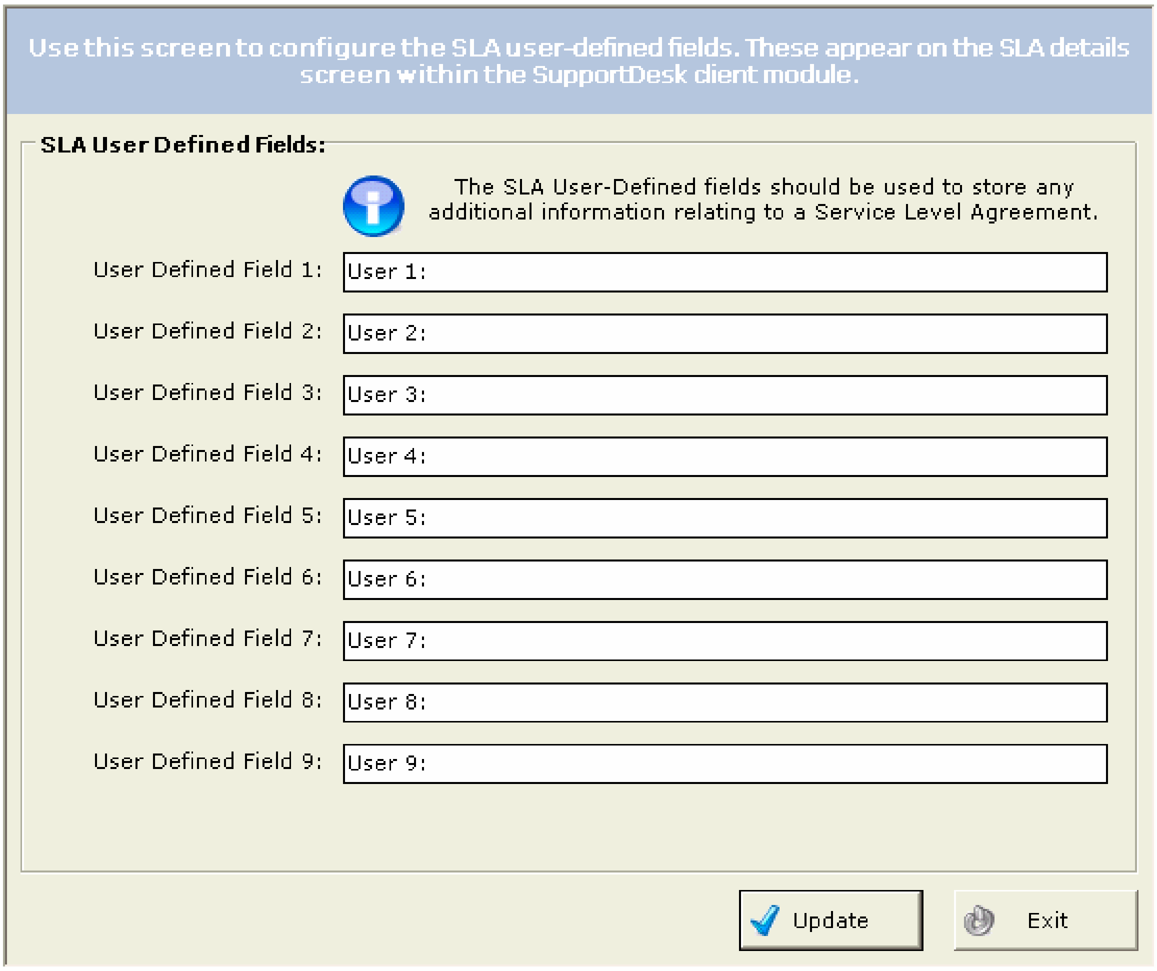
- Select the *Initial Priority* from the Drop down list.
- In the *Duration* box enter in the amount of time until escalation to the next priority. One day is equivalent to 24 hours. The duration time takes into consideration the Service Hours that are applied against the Escalation Type to calculate when the Request will escalate.
  - 01d04h30m is equivalent to 28 hours and 30 minutes.
  - Using 01d04h30m as the first escalation, if the Service Desk is open for 8 hours each day and a Request is logged at 9:00am on Monday, the escalation would occur on Wednesday at 13:30.
- Select the *Target Priority* from the Drop down list.
- Select a *Specialist* from the Drop down list to have the request reassigned when the Request escalates. This is not a required field and should only be used if a Request that escalates needs to be assigned to a different User.
- Click on the *Update* button.

Once an Escalation Step has been added the notification can be configured. This will send out an alarm when that escalation occurs.

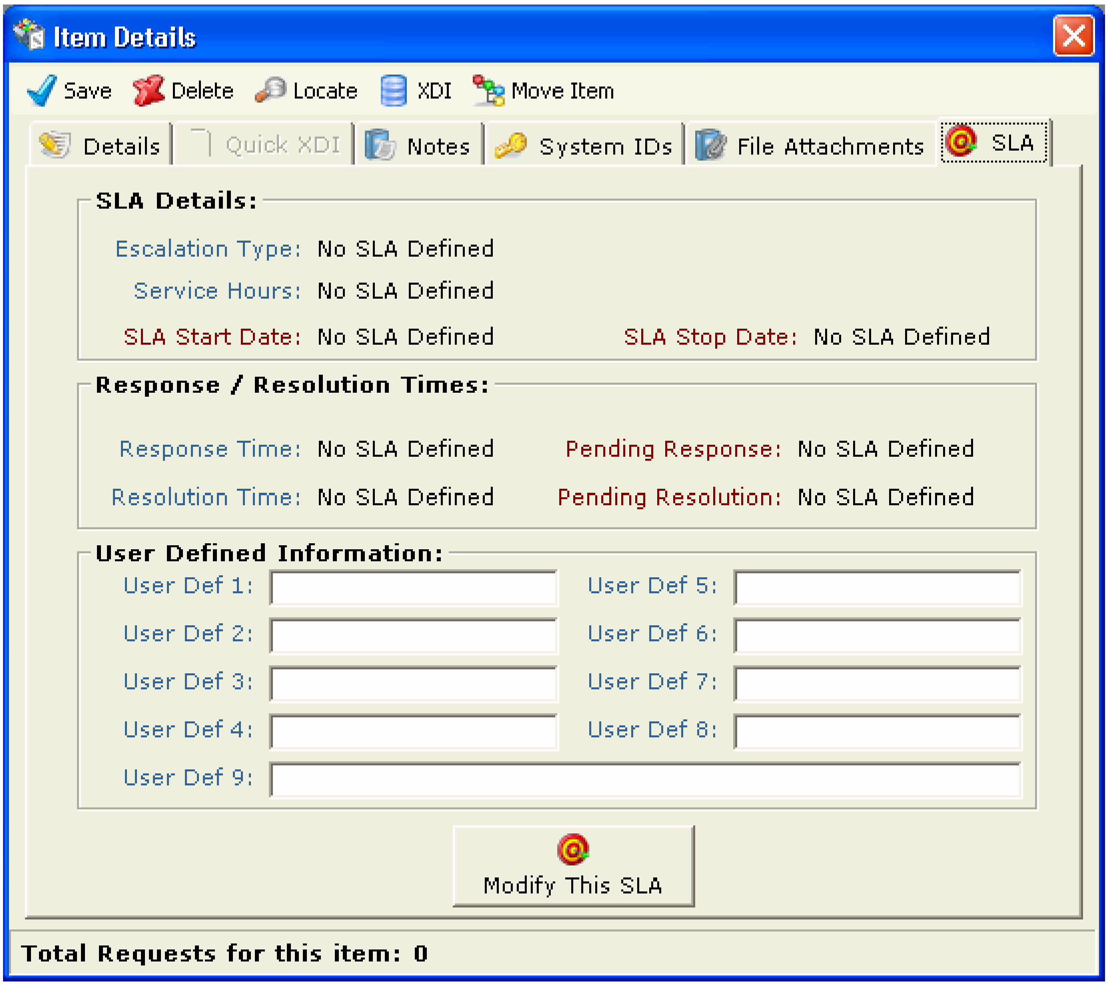
- Select the Escalation Step that requires Notification.
- Click on the *Notify* button.
- Select the User or Users that require notification of the escalation.
- Select the check box to notify the Specialist of the related Request.
- Click on *Update* to save the settings.

SLA User Defined Fields

The *SLA User Defined Fields* option lets you configure the labels for the user defined fields that are supplied with Category and Item SLAs. These allow for additional information about the Service Level Agreements that are configured against Categories and Navigator Items.



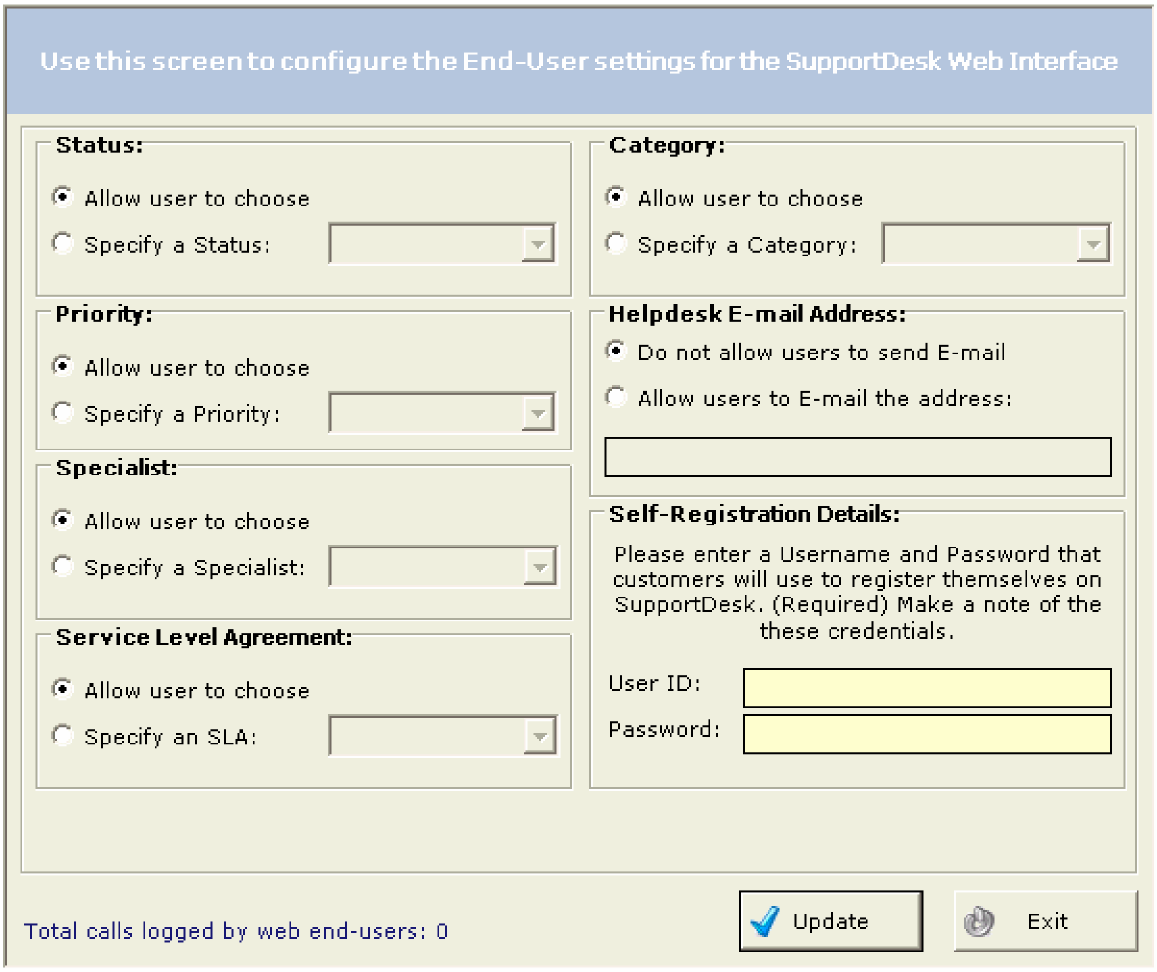
The user defined fields can be used for adding information such as reference numbers or coverage types. On the details window of an Item, this information can be viewed and modified on the SLA tab.



Miscellaneous

Web Interface Settings

The Web Interface Settings is used to configure how the Web Interface is used by customers.



- **Status**
  determines if Status is fixed or definable
- **Priority**
  determines if Priority is fixed or definable
- **Specialist**
  determines if the client may choose a specialist or is assigned one
- **Service Level Agreement**
  determines which SLA is applicable
- **Category**
  defines which categories of request are valid
- **Helpdesk E-mail Address**
  Show the SupportDesk email address on the Contact Us Web page.
- **Self Registration Details**
  Define a valid user ID and password details which customer must provide in order to register them self with the helpdesk.

Click on *Update* to save all changes.

Click on *Exit* to close the Web Interface Configuration Screen.

Icon Library

It is possible to customise all of the icons used within SupportDesk. SupportDesk can be used to support any type of device, hardware, software, furniture, equipment, etc. To represent the vast number of Items that can be added to the Navigator Tree, icons can be added to represent each type of Item.

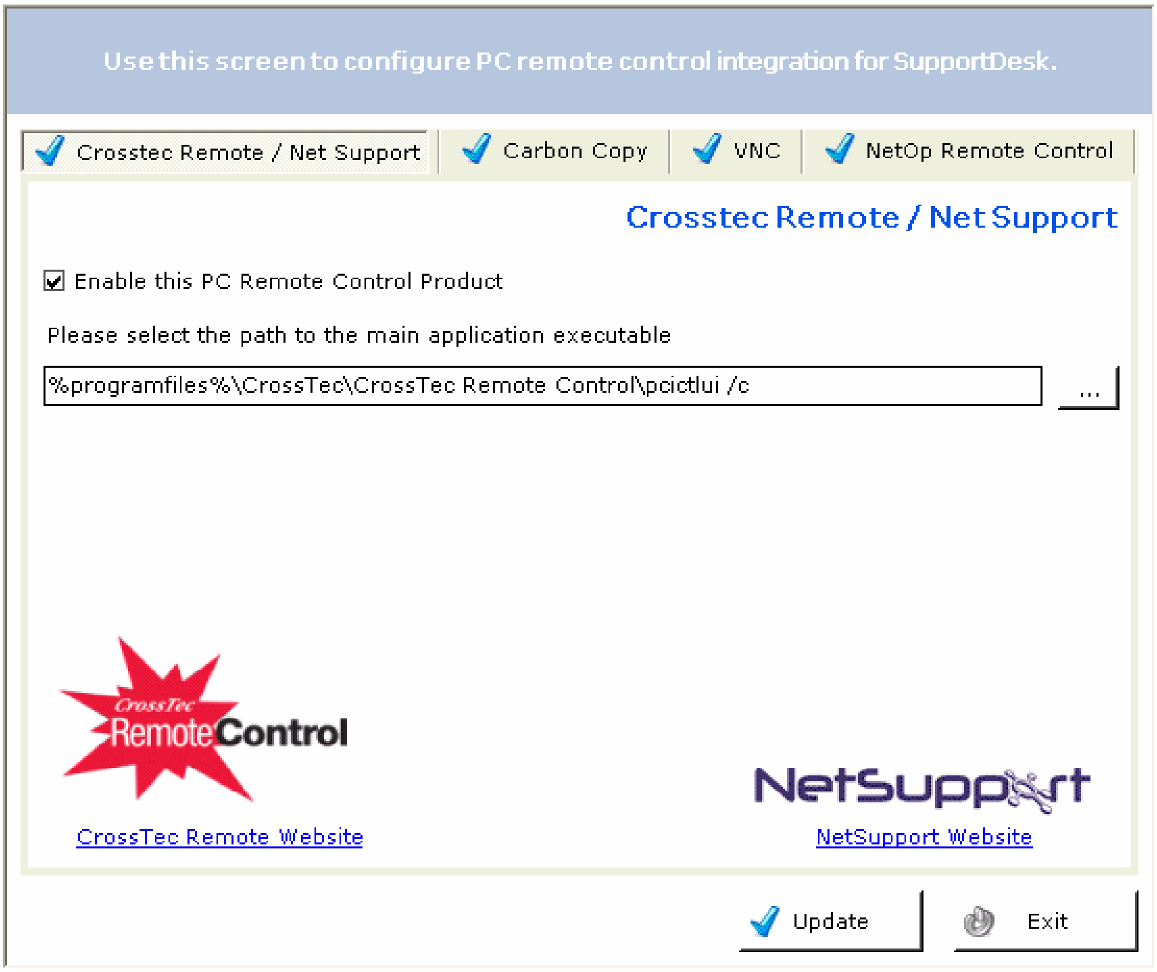
Adding new Icons

The Icon Library contains all of the Icons that can be used within SupportDesk. Additional Icons can be added to the Library.

- Right Click in the Icon Library window.
- Select *Add New Icon* from the context menu.
- Browse and select the Icon to be added.
- Click on *Open* to add the icon.

PC Remote Control

SupportDesk can integrate with market leading remote control solutions. The PC Remote Control section defines the parameters for launch a Remote Control session with a PC using Crosstec Remote Control, NetSupport Manager, Carbon Copy, VNC, and NetOp Remote Control.



Enable this PC Remote Control Product

A check box is supplied to Enable or Disable each available remote control solution. Deselecting the Enable check box will hide the product name from the System ID tab on the Item details.

Application Path

The path to the main application executable can be defined. This needs to reflect where the remote control software was installed.

- **Crosstec Remote Control / NetSupport**
  The main executable is named pcictlui.exe. The command line option /c is used to specify that the computer name will be passed to the program.
  - Example: %programfiles%\CrossTec\CrossTec Remote Control\pcictlui /c

- **Carbon Copy**
  The main executable is entered as a URL that hosted by a web server. The Name= option is used to pass the name of the computer to the application. An option for providing the timeout can also be configured.
  - Example: http://server/Altiris/CarbonCopy/CarbonCopyFull.aspx?Name=

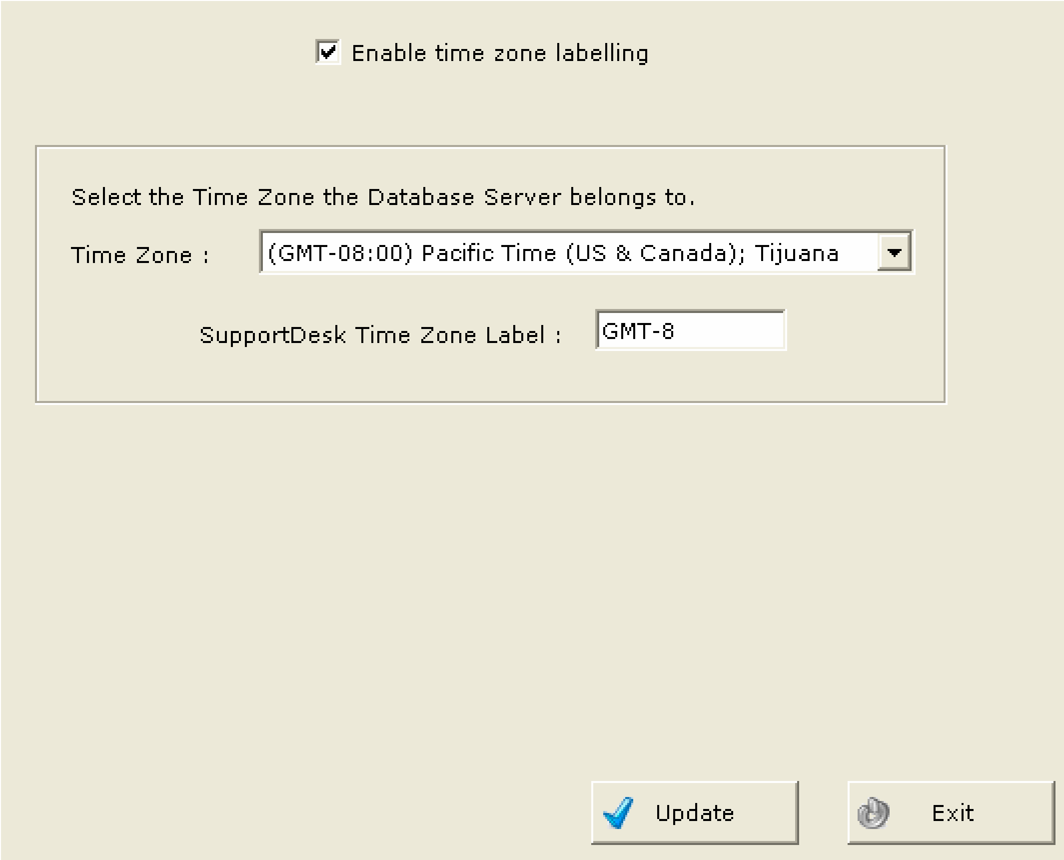
- **VNC**
  VNC has an option for the Windows version and the Web version. The main VNC application is called vncviewer.exe.
  - Windows Example: %programfiles%\RealVNC\VNC4\vncviewer.exe

  The VNC Web requires the URL for the VNC server.

- **NetOp Remote Control**
  NetOp Remote Control utilizes the NetOp phonebook for connectivity to computers. The path to the NetOp phonebook is required.

Time Zones

When SupportDesk is being used over multiple time zones the SupportDesk Windows Client and the Web Interface use the times and dates from the Server that hosts the SupportDesk database. Time Zone abbreviations can be configured to identify to the user what time zone is being used. When this is configured, all time fields in SupportDesk will display the time zone abbreviation.



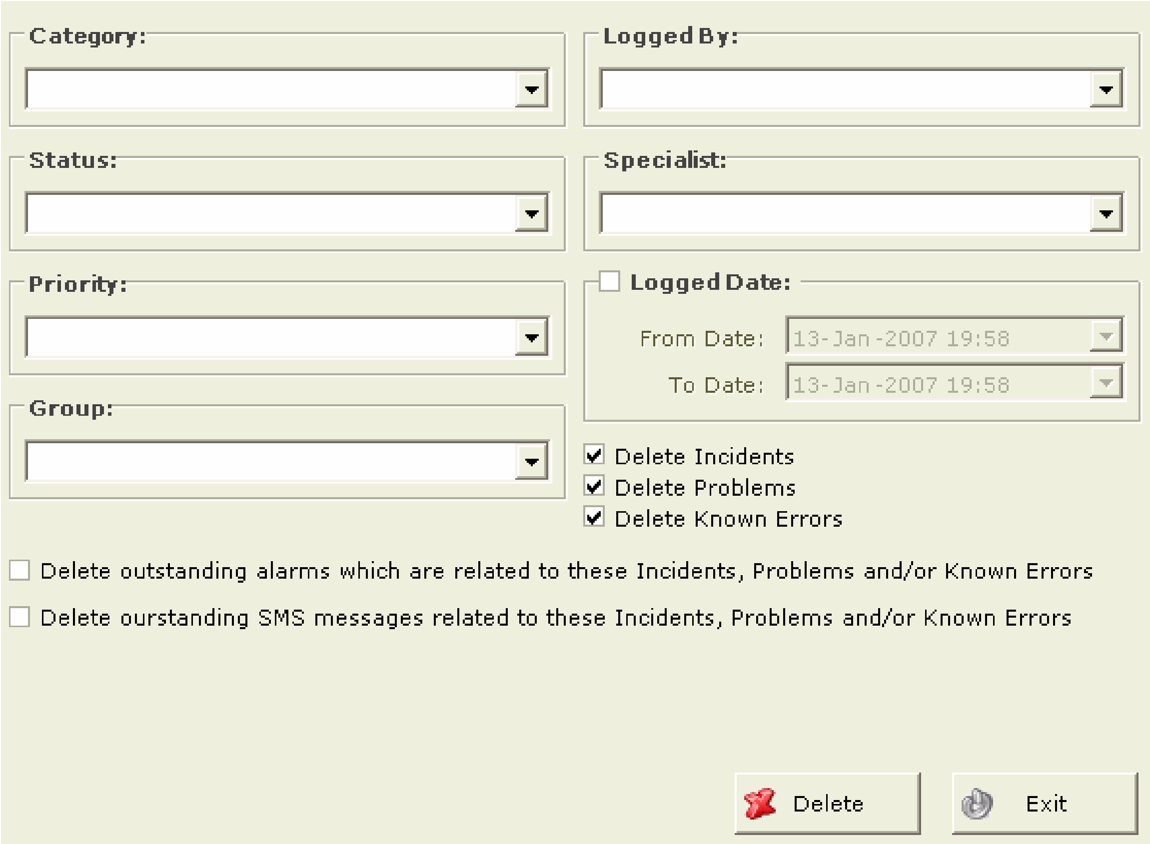
The *Enable Time Zone labelling* only needs to be selected if either SupportDesk Specialists or Users are accessing SupportDesk from a different time zone other than the one where the SupportDesk Database is installed.

The Time Zone drop down allows the selection of a time zone that is being used by the SupportDesk Database. Selecting a time zone will automatically populate the Time Zone Label with the GMT label +/- the number of hours offset from GMT.

The Time Zone Label can be manually added if you wish to display the abbreviation for the particular region. For example the time zone GMT -8 has the following regions: AKDT (Alaskan Daylight Time), PST (Pacific Standard Time, U (Uniform Standard Time).

Delete Records

The Delete Records option is used to permanently remove records on mass. Ensure that you perform a backup on the SupportDesk Database before using this feature. Once deleted the records can not be recovered.



The records to be deleted can be filtered by the following options:

- Category
- Status
- Priority
- Group
- Logged by
- Specialist
- Logged Date

The type of record to be deleted can be selected from the following options:

- Incident
- Problem
- Known Errors

Existing Alarms and SMS messages may still exist in the system for records that are to be deleted. Two options are available to remove outstanding Alarms and SMS messages that are associated with the records being deleted.

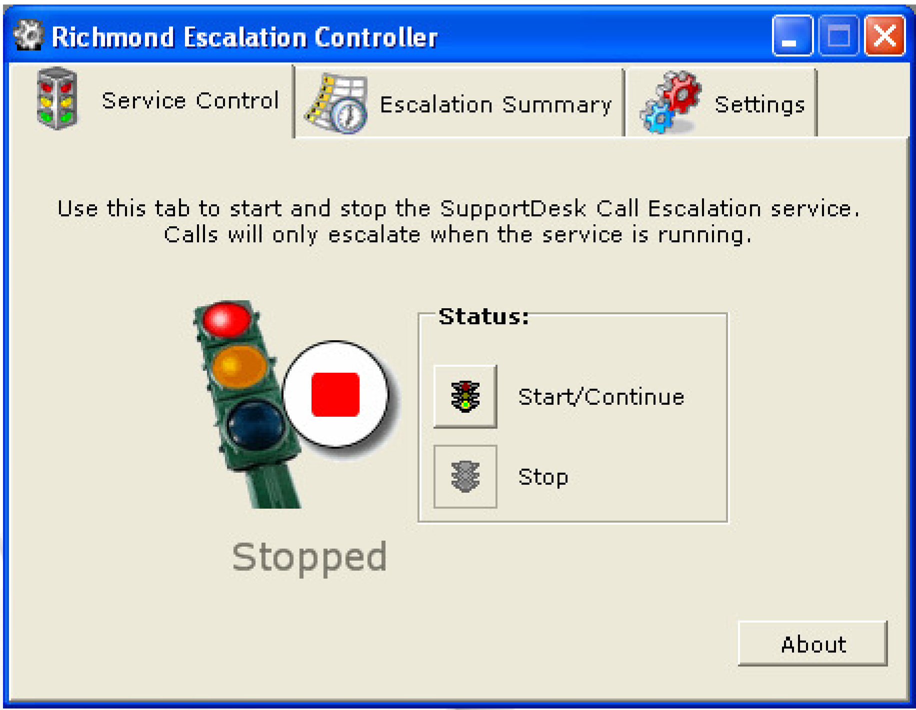
SupportDesk Escalation Module

Welcome

The SupportDesk Escalation comprises of two components, the Escalation Service and the Escalation Controller. The Richmond Escalation Service takes care of all the escalations within SupportDesk and the Richmond Escalation Controller is used to Start and Stop the Escalation Service, configure settings, and display a summary of escalations.

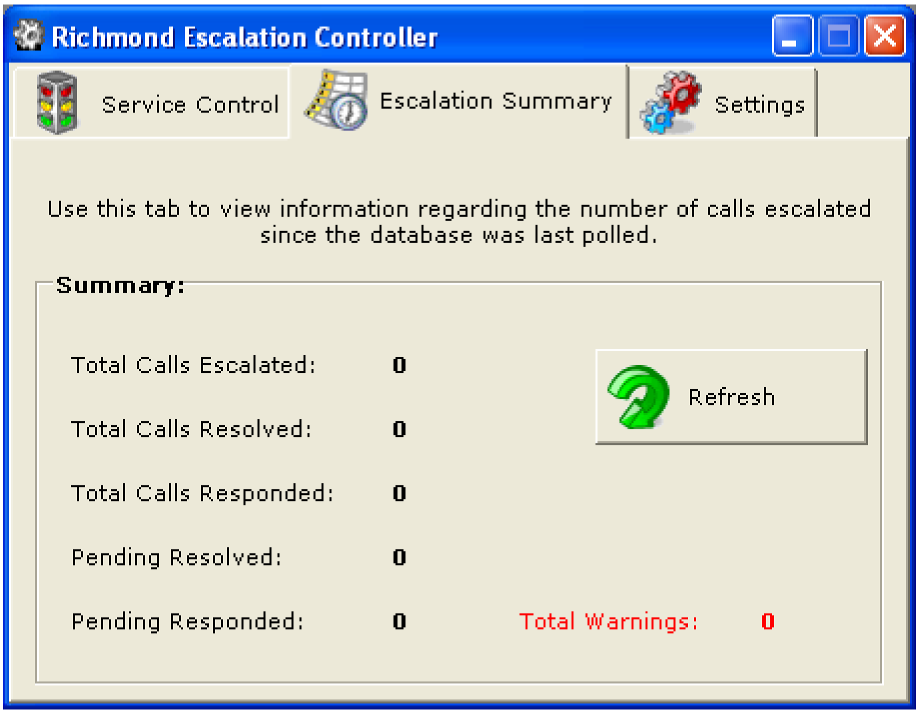
Service Control

The Service Control Tab displays the current status of the Escalation Service and allows you to stop and start the Escalation Service



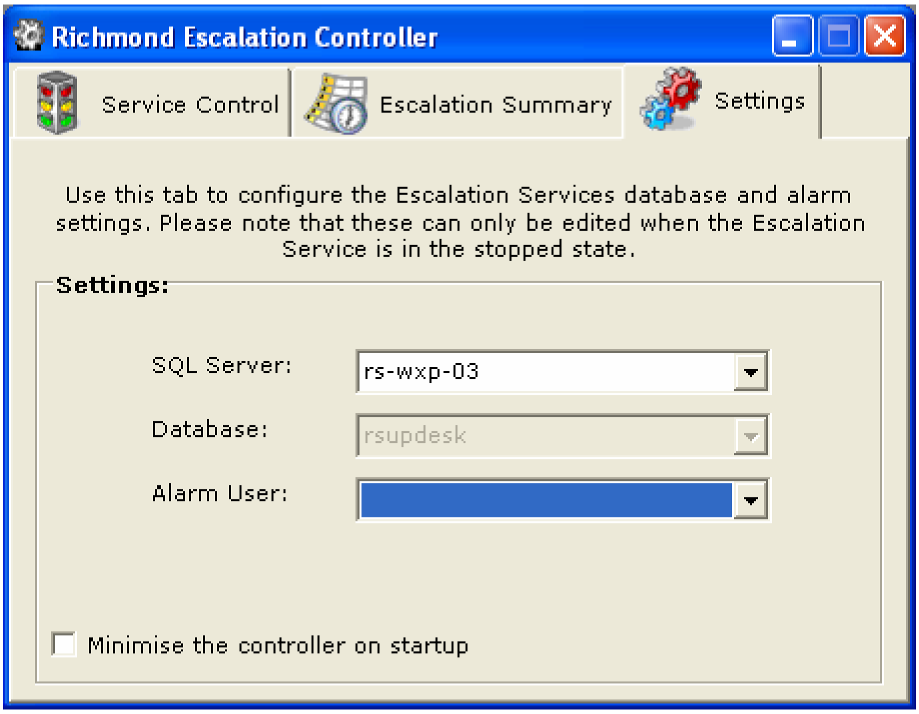
Escalation Summary

The Escalation Summary shows the numbers of Incidents that have escalated since the database was last polled. Database polling takes place once each minute.



Settings

The Settings tab is used to configure the Escalation Services database and alarm settings.



SQL Server: The name of the SQL server that hosts your SupportDesk database

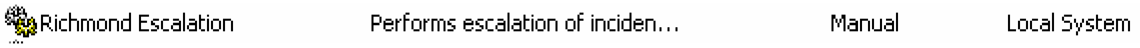
Database: The name of the SQL database

Alarm User: The name of a SupportDesk User who will receive alarms when errors occur on the Escalation Service

Selecting the Minimise the controller on startup check box will minimise the Escalation Controller to the System Tray.

Escalation Service

The Escalation Service can be viewed in the Windows Services console.

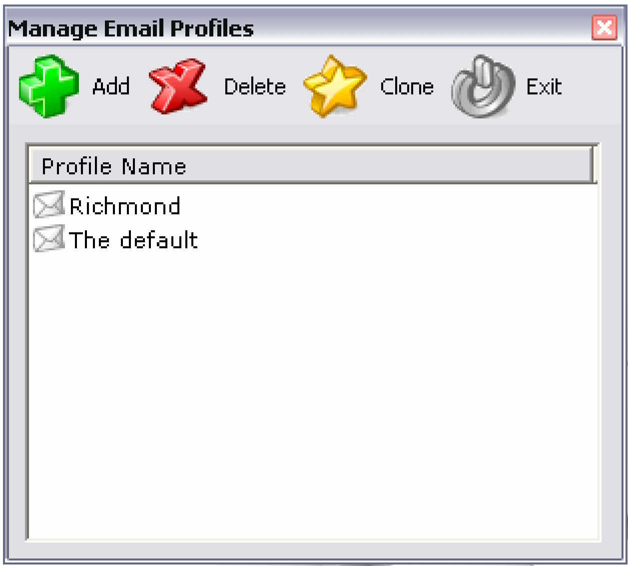


The default Startup Type is set to *manual*. When the computer is restarted the Escalation Service will not automatically start. If you wish to have the Escalation Service automatically start when the computer starts, the Startup Type needs to be changed to *Automatic.*

SupportDesk Email Service

Email Profile

SupportDesk 6.0 allows for the use of multiple *Email Profiles*.



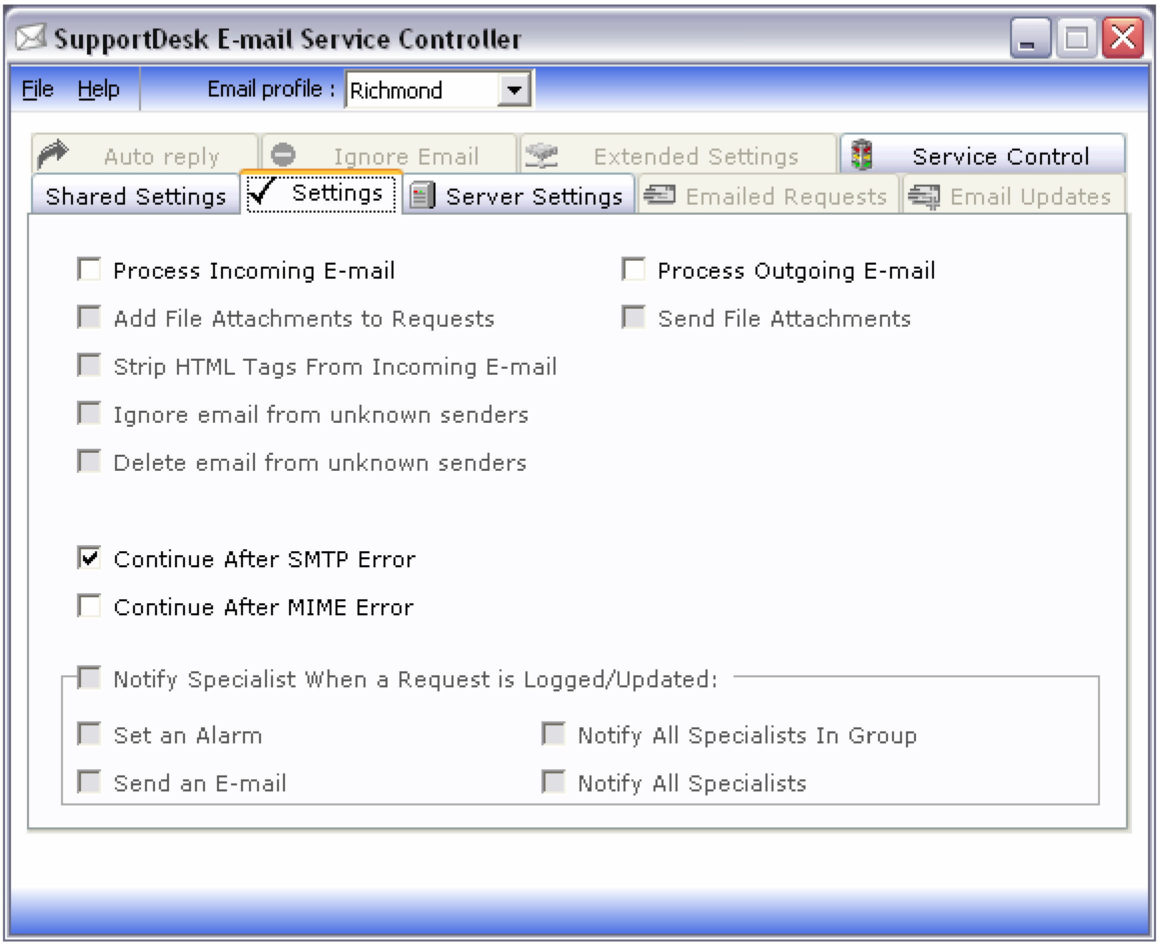
Each Profile represents a particular mailbox. Each email address used by the Support function can be configured to process emails in a unique way from the other profiles.

Click on *Add* to add a new profile name. Enter the name an click *OK*.

Each configured Email profile can be selected from the Email Profile drop down box on the main menu. Selecting an Email Profile will make available the settings for that profile.

Settings

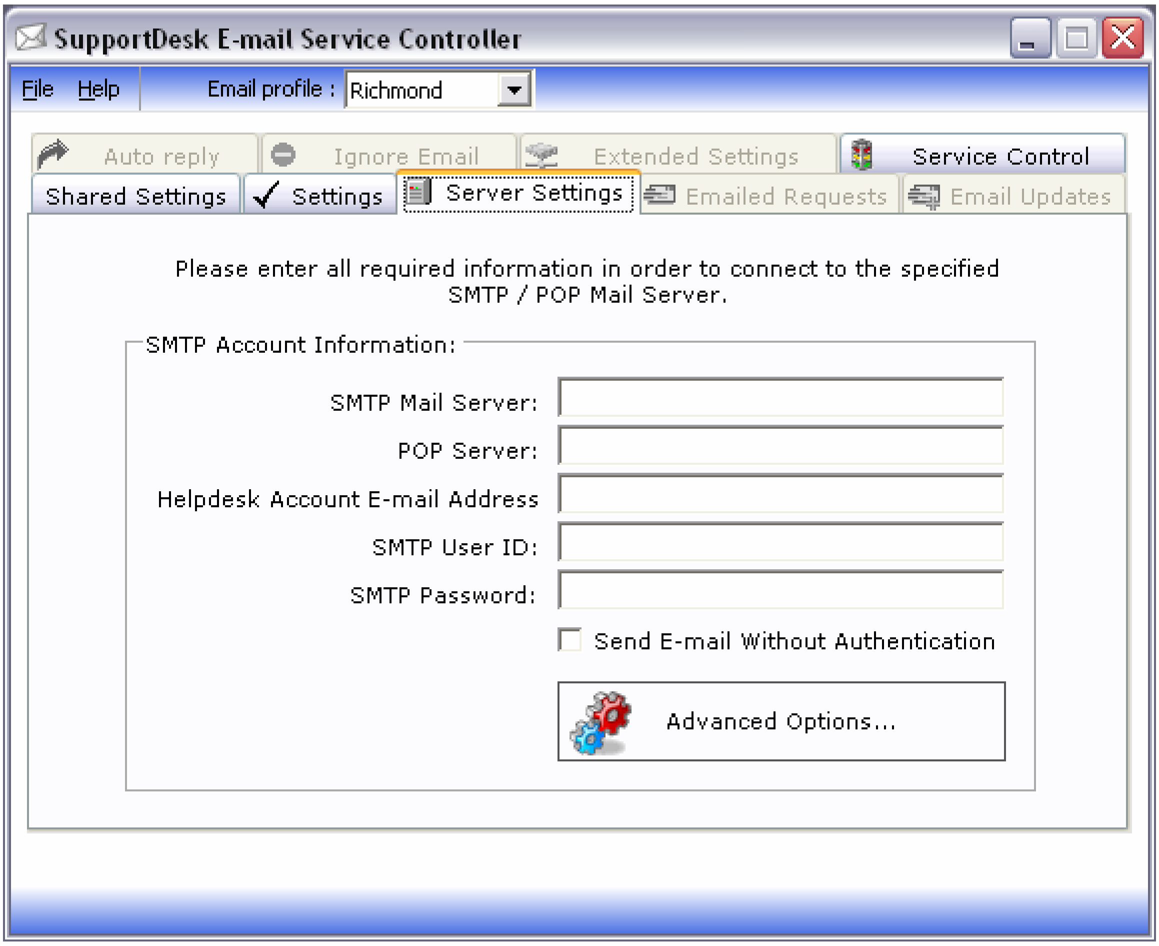
The Settings Tab contains general settings



- **Process Incoming E-mail**
  Enables the processing of e-mails that have been sent by customers. This will enable the *Ignore Email*, *Extended Settings*, *Email Requests*, and *Email Updates* tabs.
- **Process Outgoing E-mail**
  Enable the processing of e-mails that are being sent from SupportDesk.
- **Add File Attachments to Requests**
  When an email with an attachment arrives from a customer, the attachment will be added to the Request.
- **Send File Attachments**
  This will allow Specialist to send attachments when sending an email from within a Request.
- **Strip HTML Tags From Incoming E-mail**
  If an e-mail is received in HTML format all HTML tags will be removed from the e-mail. It is recommended that the e-mail account is configured to process e-mail as plain text at the server. Only use this option if you are unable to configure the e-mail account to use plain text.
- **Ignore email from unknown senders**
  Emails that arrive without a sender being listed in the e-mail header will be ignored.
- **Delete email from unknown senders**
  Emails that arrive without a sender being listed in the e-mail header will be deleted
- **Continue After SMTP Error**
  If a SMTP error is detected the Email Service will continue to process emails
- **Continue After MIME Error**
  If a MIME error is detected the Email Servcie will continue to process emails.
- **Notify Specialist When a Request is Logged/Updated**
  When the Email Service processes either a new Request or an updated Request an Alarm or email can be sent to the Specialist, a Group, or all Specialists.

Server Settings

The Server Settings Tab contains SMTP and POP account information

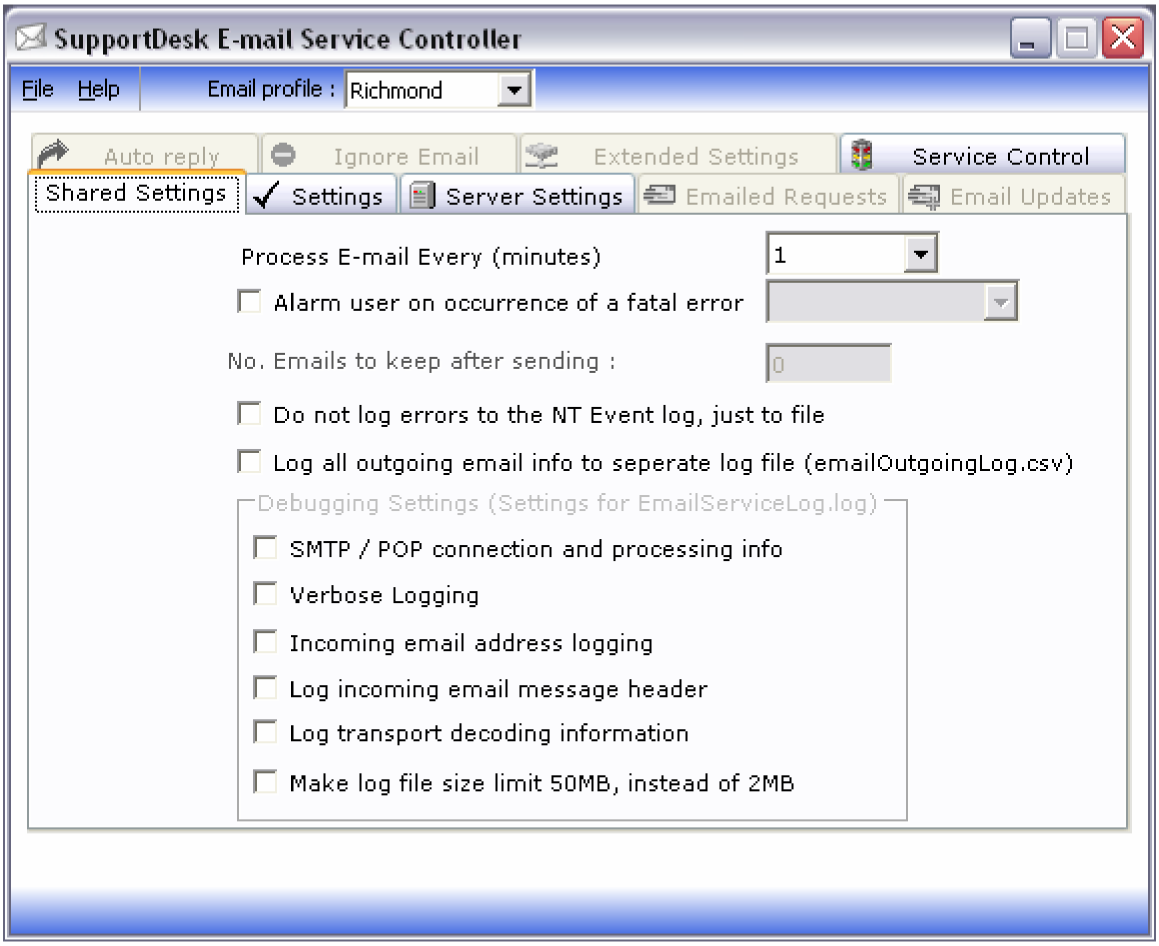


SMTP Account Information

- **SMTP Mail Server**
  The IP address or name of the Server that hosts your SMTP Email Server.
- **POP Server**
  The IP address or name of the Server that hosts your POP3 Email Server.
- **Helpdesk Account E-mail Address**
  The email address used by this email profile.
- **User ID**
  The user account to access the mailbox.
- **User Password**
  The password for the user.
- **Send E-mail Without Authentication**
  Select if the SMTP Server does not require authentication.
- **Advanced Options**
  Options for selecting encoding formats. The option *Automatically detect mail encoding format* is recommended when Microsoft Outlook is being used.

Shared Settings

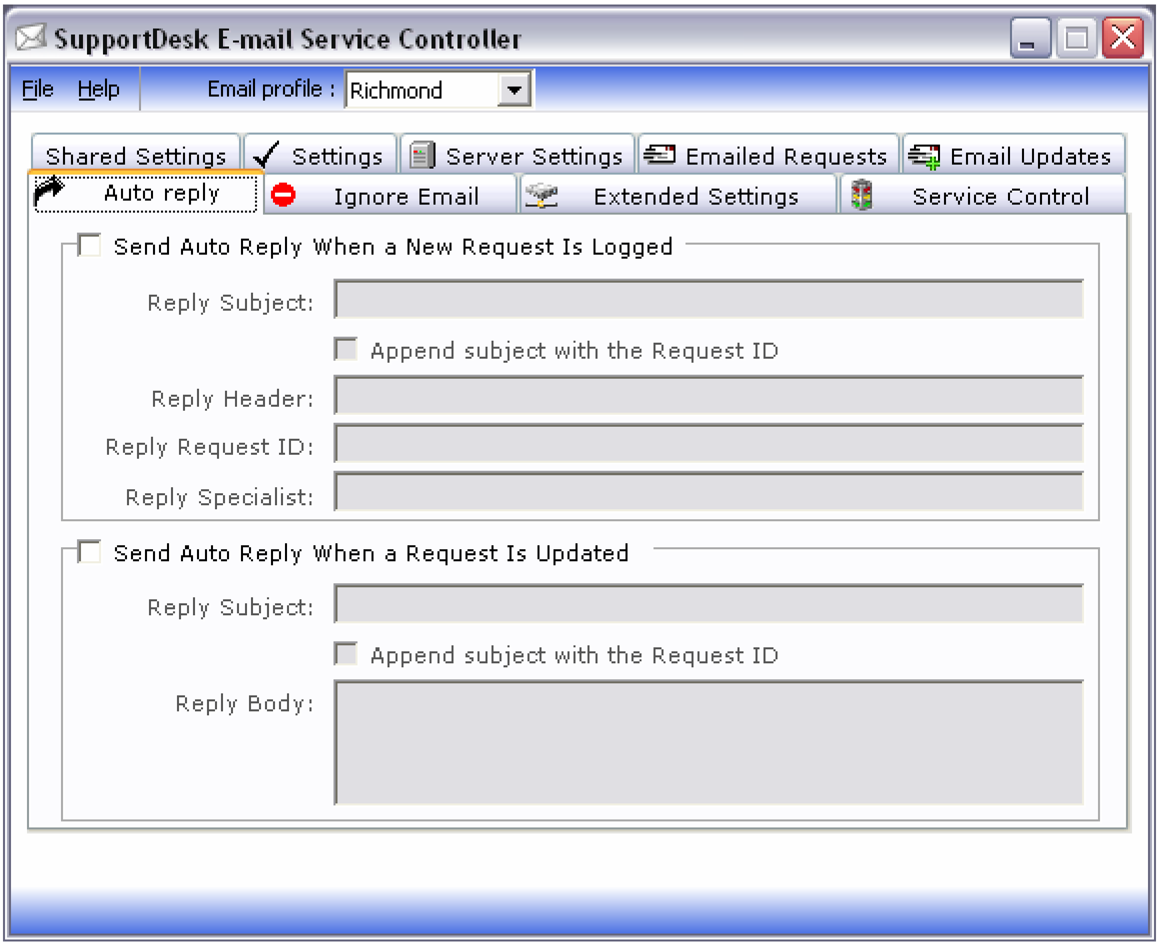
The Shared Settings Tab contains items that are common to all Email Profiles



- **Process E-mail Every (minutes)**
  Set the number of minutes that the E-mail Service will process emails
- **Alarm user on occurrence of a fatal error**
  Send an alarm to a selected Specialist when a fatal error occurs.
- **Do not log errors to the NT Event log, just to file**
  Prevent the logging of errors to the Windows Event Log.
- **Log all outgoing email info to separate log file (emailOutgoingLog.csv)**
  Keep track of all outgoing email.
- **Debugging Settings (Settings for EmailServiceLog.log)**
  The options listed under the Debugging Settings allows for configuration of information that will be logged to the EmailServiceLog.log.

Auto Reply

The Auto Reply Tab is used to configure auto responses when the Email Service logs a new Request or Updates an existing Request. You must have the *Process Outgoing Email* on the Settings Tab selected to enable this tab.

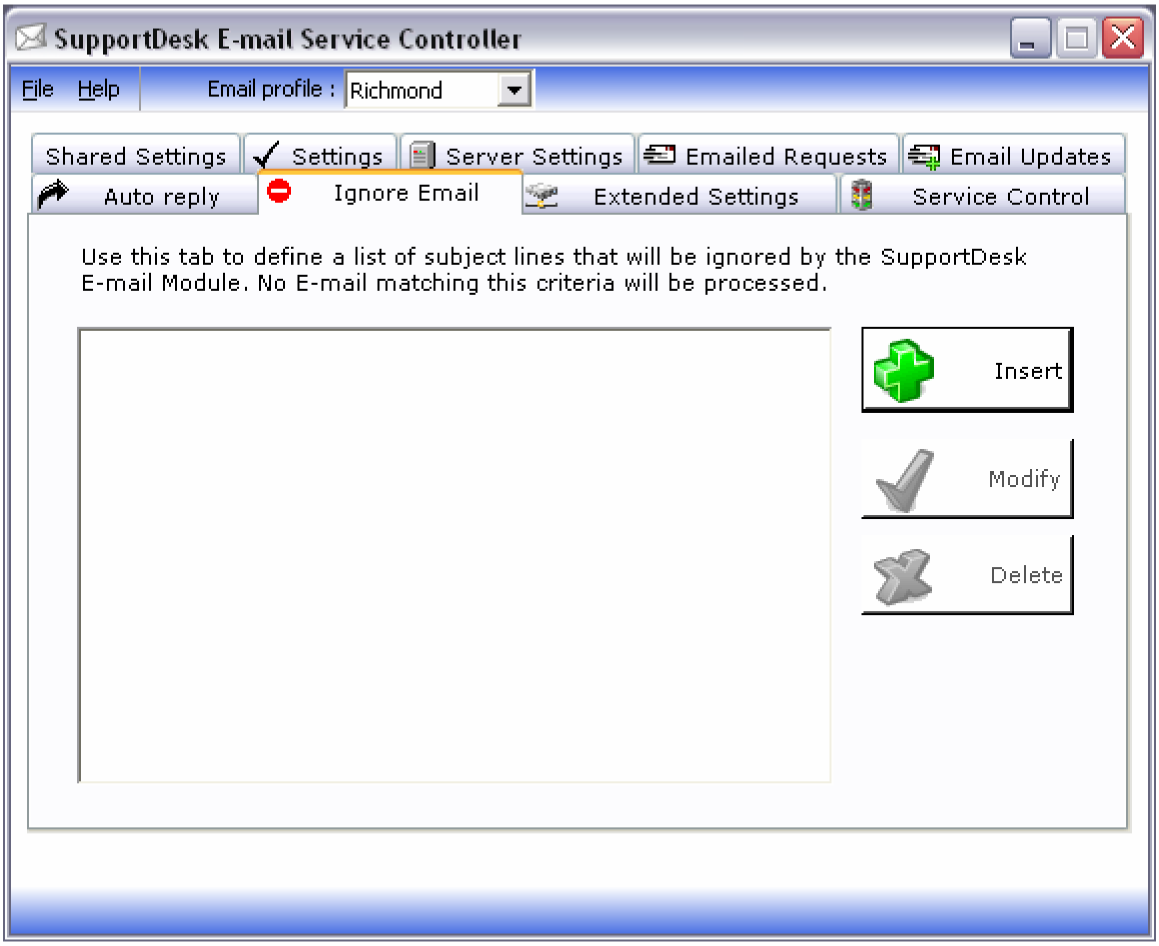


The *Send Auto Reply When a New Request Is Logged* option will automatically send a response email to the sender of the Request to notify them that the Request has been logged.

The *Send Auto Reply When a Request Is Updated* option will automatically send a response email to the sender of the Request Update when the Request has been updated.

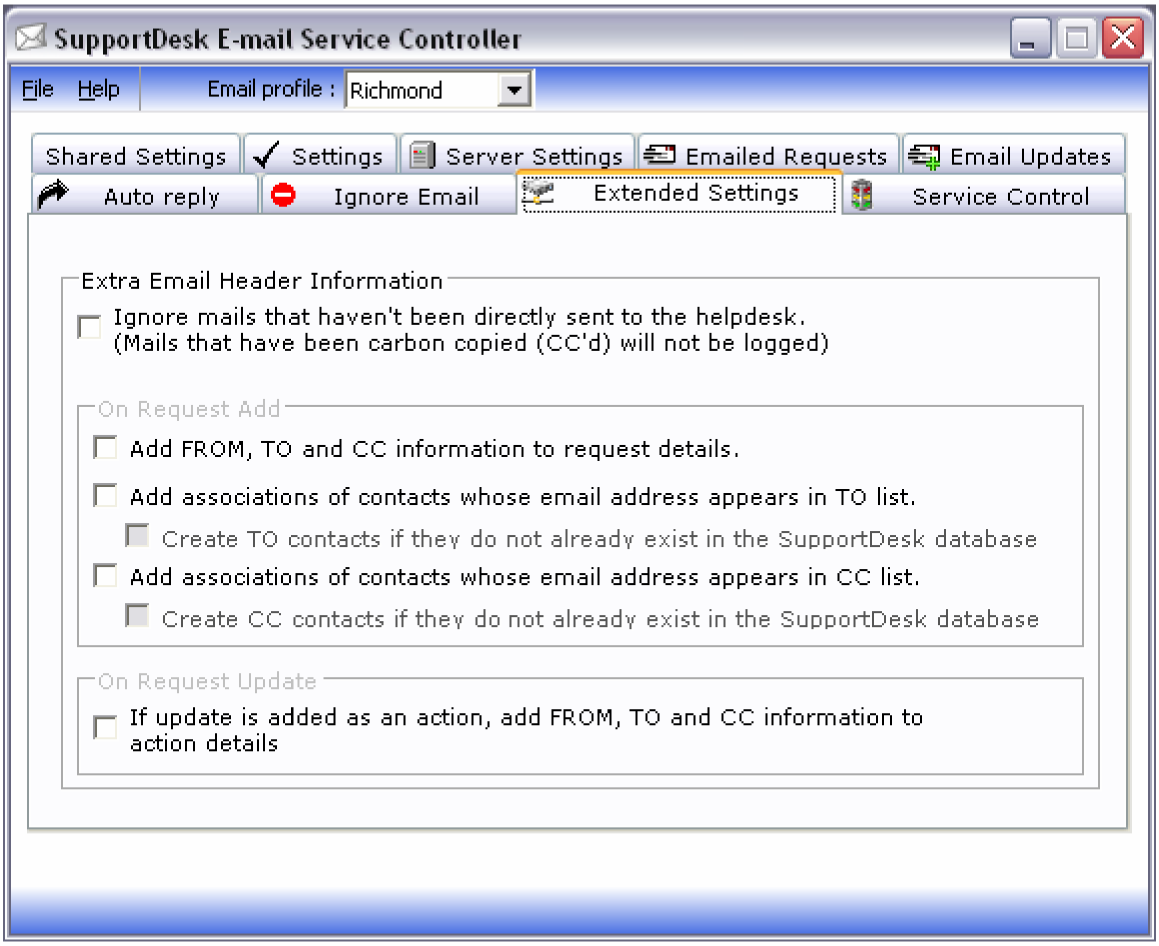
Ignore Email

The Ignore Email Tab lets you define strings of text that will cause an email to not be processed if the string is found in the subject line.



Extended Settings

The Extended Settings Tab lets you define further settings for processing emails.



You can ignore emails that have not been sent directly to the support mailbox.

On Request Add

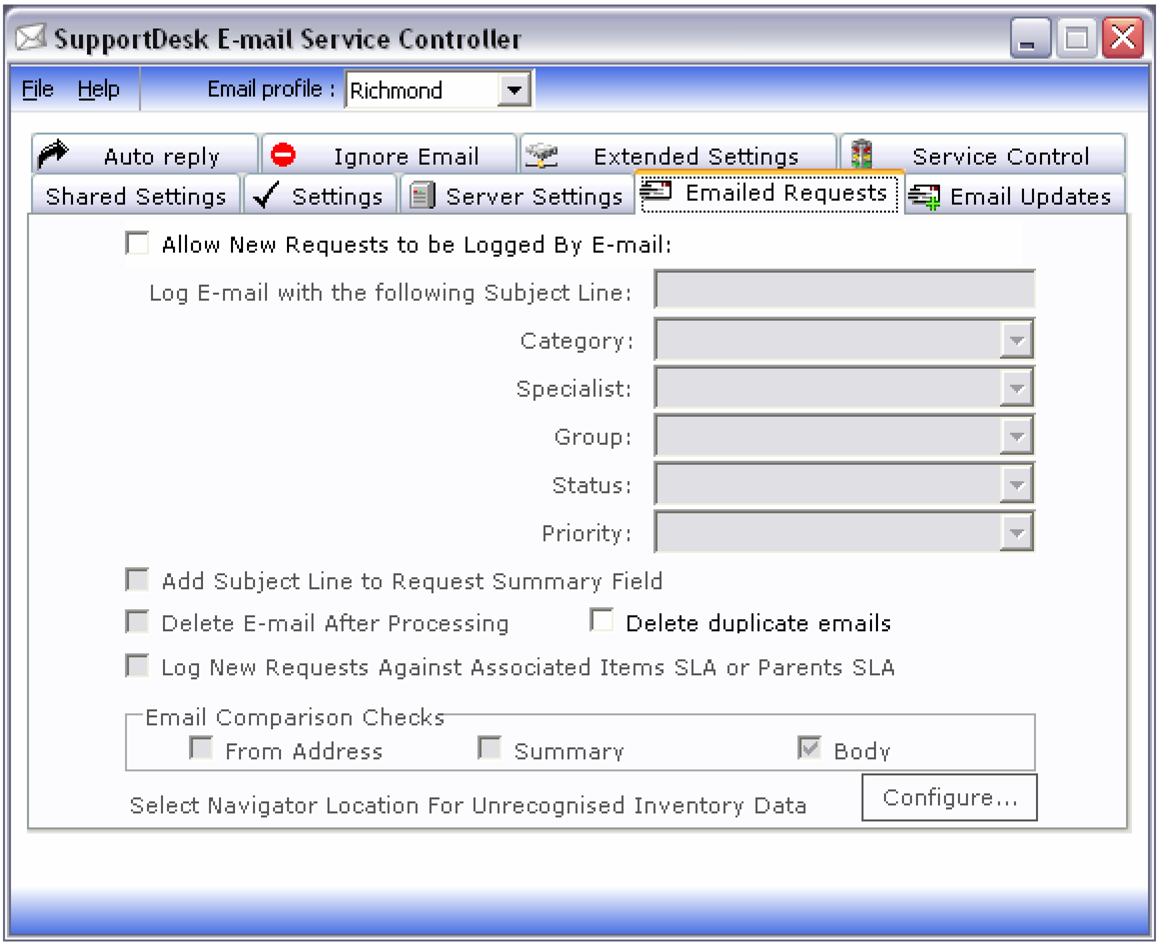
Define additional actions to take place when a Request is logged by email

On Request Details

Add the email addresses listed in the FROM, TO, and CC fields on an update are added to the Request Action.

Emailed Requests

The Emailed Requests Tab lets you define how Emailed Requests are entered into SupportDesk.



Select the *Allow New Requests to be logged by E-mail* to enable the logging of Requests by email.

Emails can be filtered so that only emails with a particular word or phrase found in the subject line will be able to be processed.

The Request details which include Category, Specialist, Group, Status, and Priority are mandatory fields. The Specialist could be a purpose added user, called for example EmailRequest, which all Requests logged by email are initially assigned to.

- **Add Subject Line to Request Summary Field**
  Make the subject line of the email be entered as the summary information for the Request
- **Delete E-mail After Processing**
  Once the email has been logged as a request the email is deleted from the mailbox. This will prevent an email from being re-entered into SupportDesk if original Request is deleted.
- **Delete duplicate emails**
  If the same email is received more than once into the Support Mailbox the duplicated will be deleted to prevent multiple logging of the same requests
- **Log New requests Against Associated Items SLA or Parent SLA**
  Select this option to apply an Item SLA against the Request

Email Comparisons

By default if an emailed request arrives and there is an existing Request that contains the identical text in the description as in the body of the email, the emailed request will be viewed as a duplicate and will not be logged.

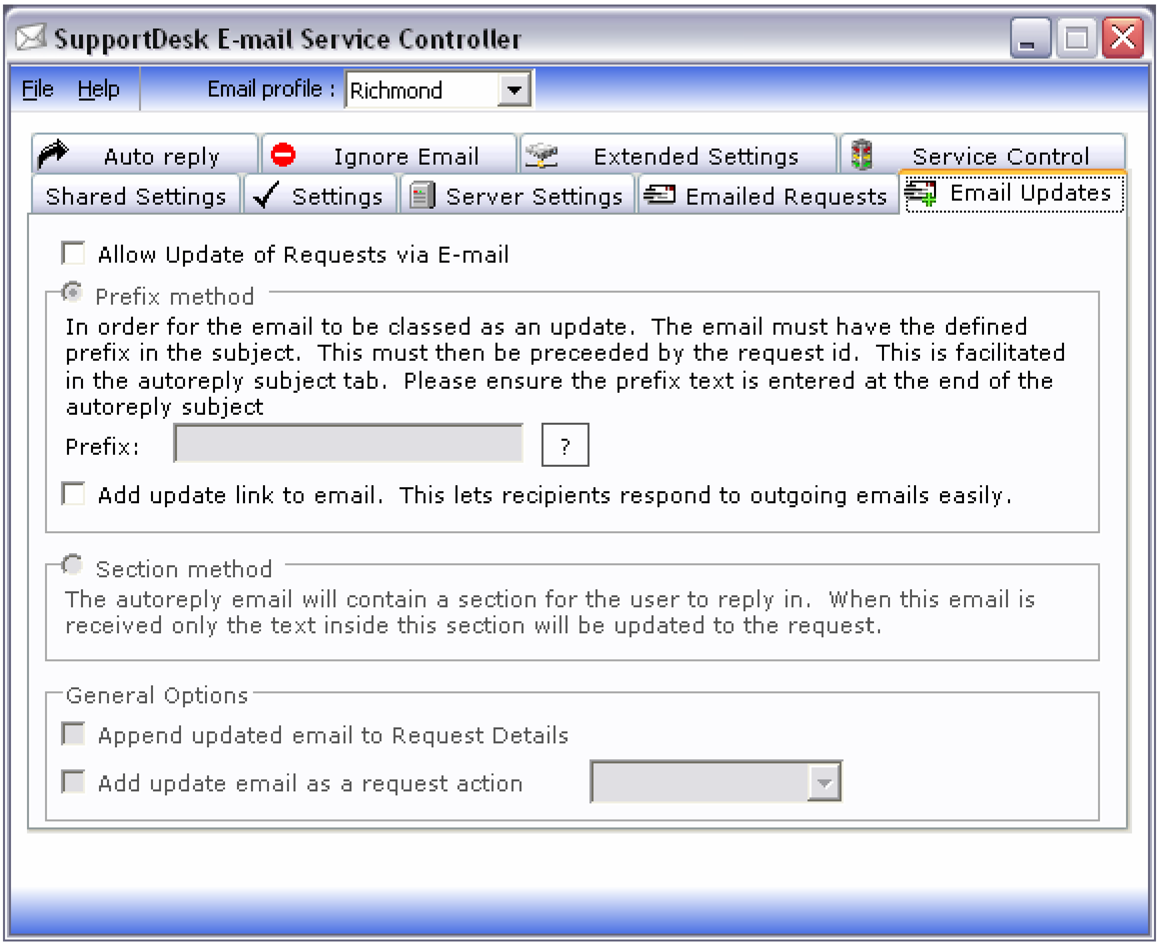
If you are receiving automatically generated emails that have identical text within the body of the email and it is required to have all of these requests logged you can select the *From Address* or the *Summary* check boxes.

- **From Address**
  Allow multiple emails with identical text in the body of the message be logged as long as the sender is different.

- **Summary**
  Allow multiple emails with identical text in the body of the message be logged as long as the subject line is different.

Email Updates

The Email Updates lets you define how existing Requests are updated by email.



Select the *Allow Update of Requests via E-mail* option to allow customers to update existing Request by email.

Prefix Method

In order for the email to be classed as an update, the email must have the defined prefix in the subject line. In the *Prefix* box enter in a prefix for example 'Update'.

Selecting the *Add update link to email* option will add a link within any auto response email to the customer. The customer can click on the link to open a new email message with the subject line automatically populated with the required prefix and Request number.

The Prefix Method is the recommended method of updating Requests.

Section method

The Section method creates a section within any auto response email to a customer with a section for adding update information. The customer will open a reply message to the auto response email and type in the update information in the space provided.

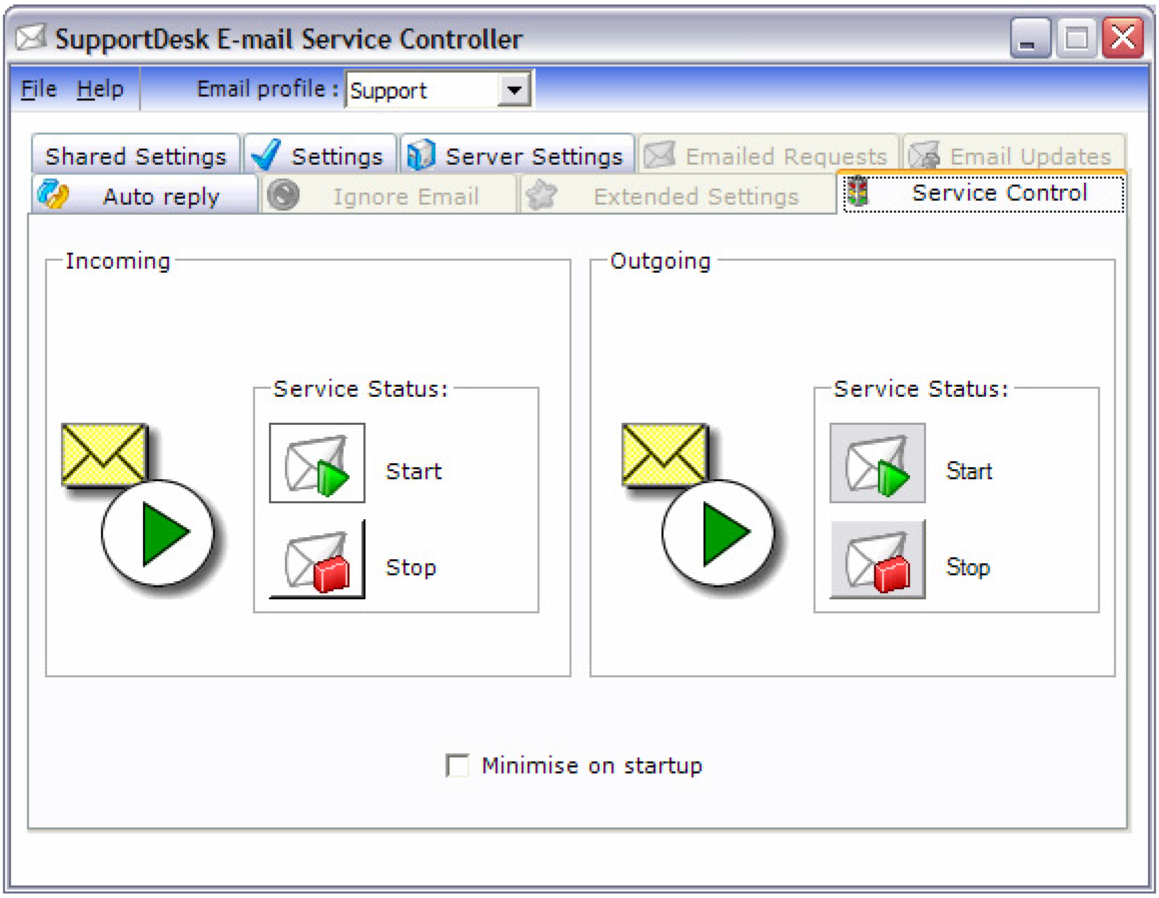
General Options

When an update by email is received you can select how you want the update to be added to the Request.

- **Append updated email to Request Details**
  The update information will be added to the Details section of the Request.
- **Add update email as a request action**
  Set the number of minutes that the E-mail Service will process emails

Service Control

The Service Control Tab shows the current status of the Email Service and lets you start and stop the services. There are separate Services for incoming email and outgoing email. Each has their own control to stop and start the service.



When the Email Service is in a Stopped state a red square will be displayed. When the Email Service is in a Started state a green arrow will be displayed.

Click on either the Start/Continue or Stop buttons to perform the desired action.

The Minimise on Startup will place the SupportDesk E-mail Service in the System Task Tray.

Options

Outgoing Mail Queue

The *Outgoing Mail Queue* has an option to Purge Queue. This will remove all emails that are being held in the SupportDesk Database that are waiting to be processed.

The *Purge Queue* option can be accessed from the *File→Options→Outgoing Mail Queue→Purge Queue.*

SupportDesk SMS Module

Welcome

The SupportDesk SMS Module allows Alarms to be sent to Users by SMS Text Messaging. Adhoc messages can also be sent from within SupportDesk.

Getting Started

SMS Login

Service Centre Settings

SMS Status Window

Getting Started

Installation

The SMS Module can be installed by running the Custom installation of SupportDesk. Please refer to the SupportDesk Installation Guide for further details.

Requirements

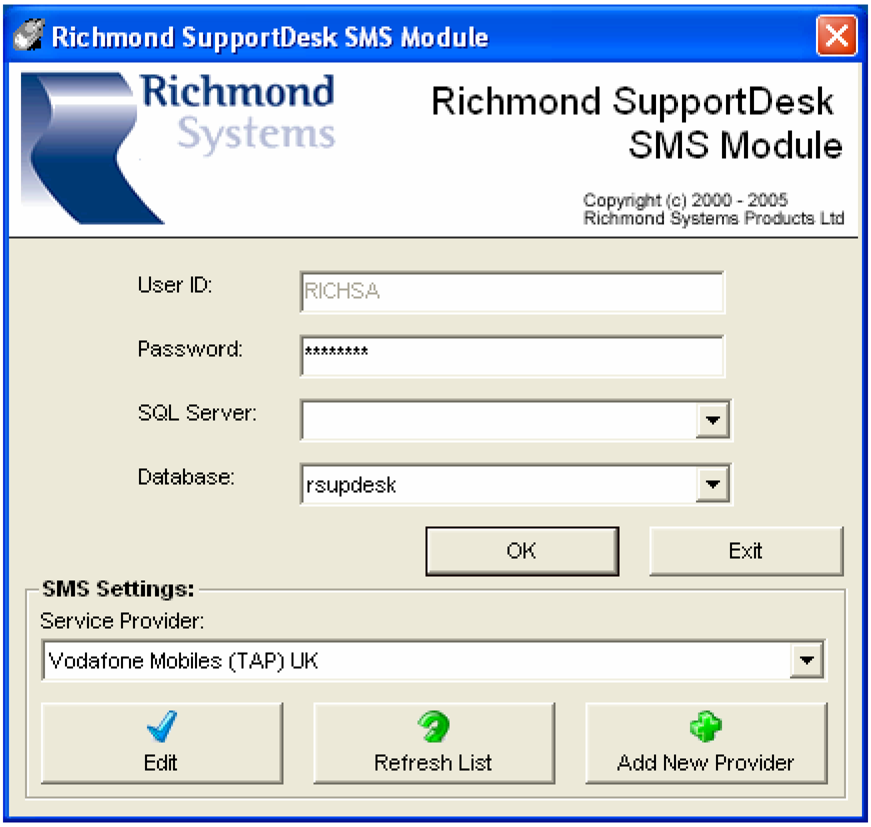
- The PC running the SMS Module needs to have a standard Windows TAPI complaint modem attached and connected to an external telephone line.
- The Microsoft .NET Framework is a requirement for all installation of SupportDesk Modules. During the installation of the SMS Module the install the Microsoft .NET Framework 1.1 will be installed if it is not already installed.
- The SMS Module runs as an application and therefore requires that the PC is logged in under a Windows account.
- The PC running the SMS Module should be available 24/7

SMS Charging

The SMS Services are provided by third party Service Providers and not Richmond Systems. Each Service Provider will have a cost per SMS message or connection. This will be billed directly to your phone that is being used for sending the SMS messages. For more information on costs please contact the Service Provider of your choice.

SMS Login

The SMS Login Window



The SMS Module requires authentication to the SupportDesk Database to be able to send SMS messages from a SupportDesk user.

The User ID is account used to login is the SupportDesk administration user RICHSA. The User ID can not be changed.

User ID: RICHSA

Password: the RICHSA password

SQL Server: Name of the SQL Server that hosts the SupportDesk Database

Database: Name of the SupportDesk Database

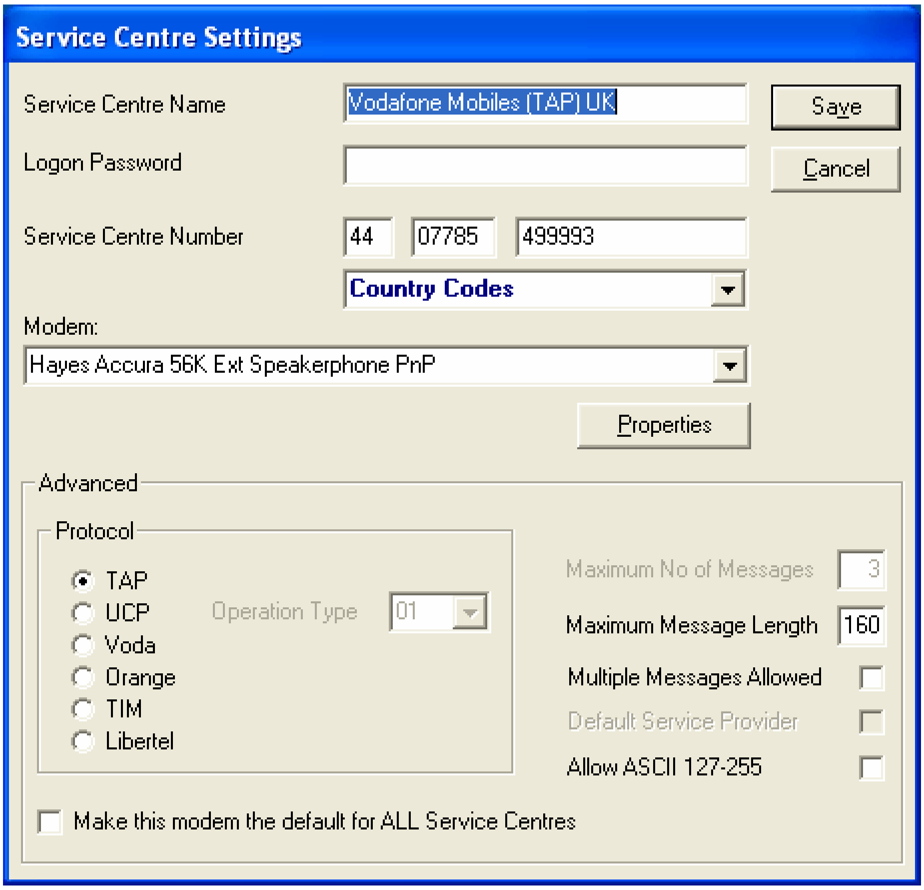
Service Provider: Name of the SMS provider

A selection of service providers is listed in the drop down box. Either select one of these, or choose the 'Add New Service Provider' button to enter details given to you by your service provider.

Click on the OK button to start the SMS Module

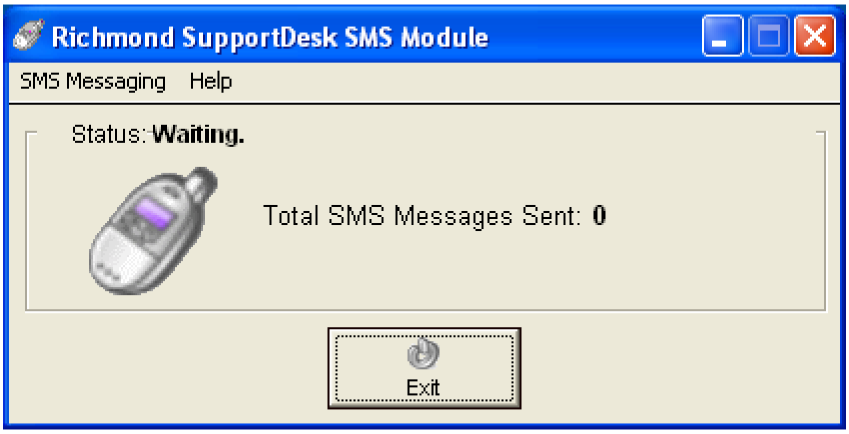
Service Centre Settings

The SupportDesk SMS Module comes with predefined Service Centres. It is not recommend to change these configurations unless instructed by your Service Provider.



SMS Status Window

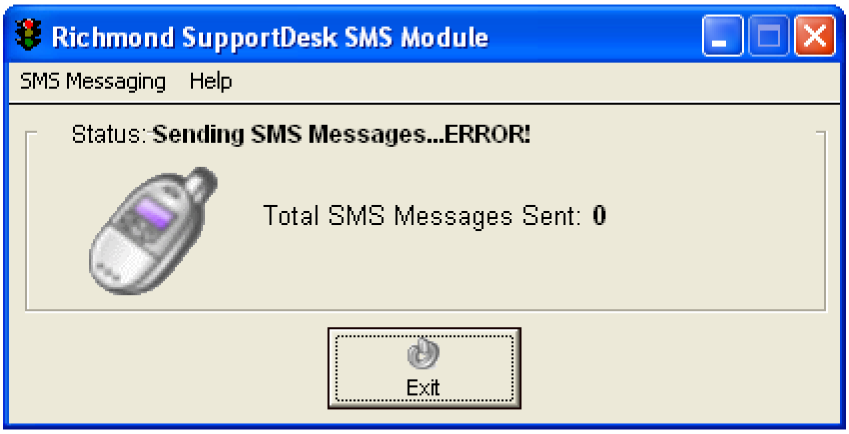
The SMS Status Window is displayed when the module is active.



Total SMS Messages Sent indicates the number of messages sent on each cycle. Once the message queue is cleared it will show 0

Click on Exit to close the SMS Module.

The Status Window will display an error message when detected.



Additional information about the error can be found in the RSSMS.txt file which is located in the SupportDesk program folder.

SupportDesk Data Transfer

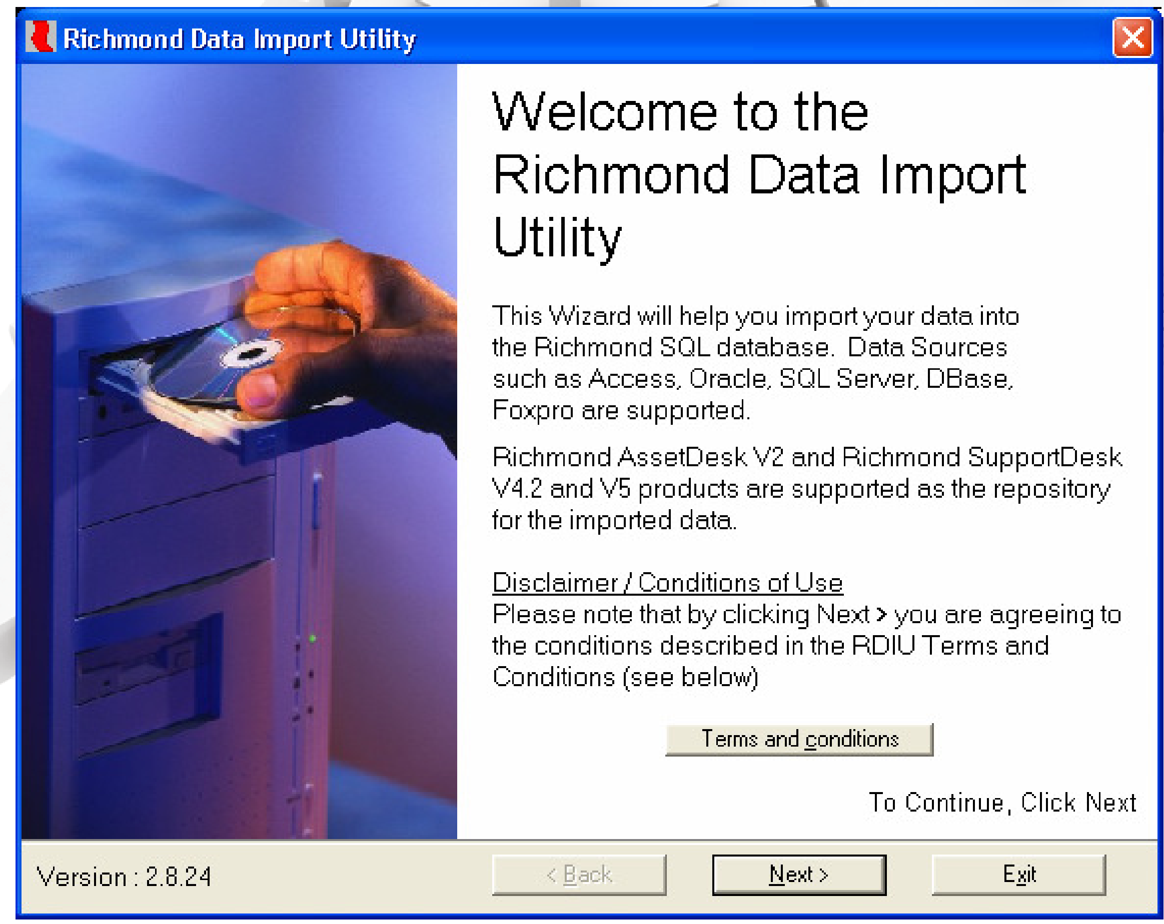
SupportDesk Data Transfer

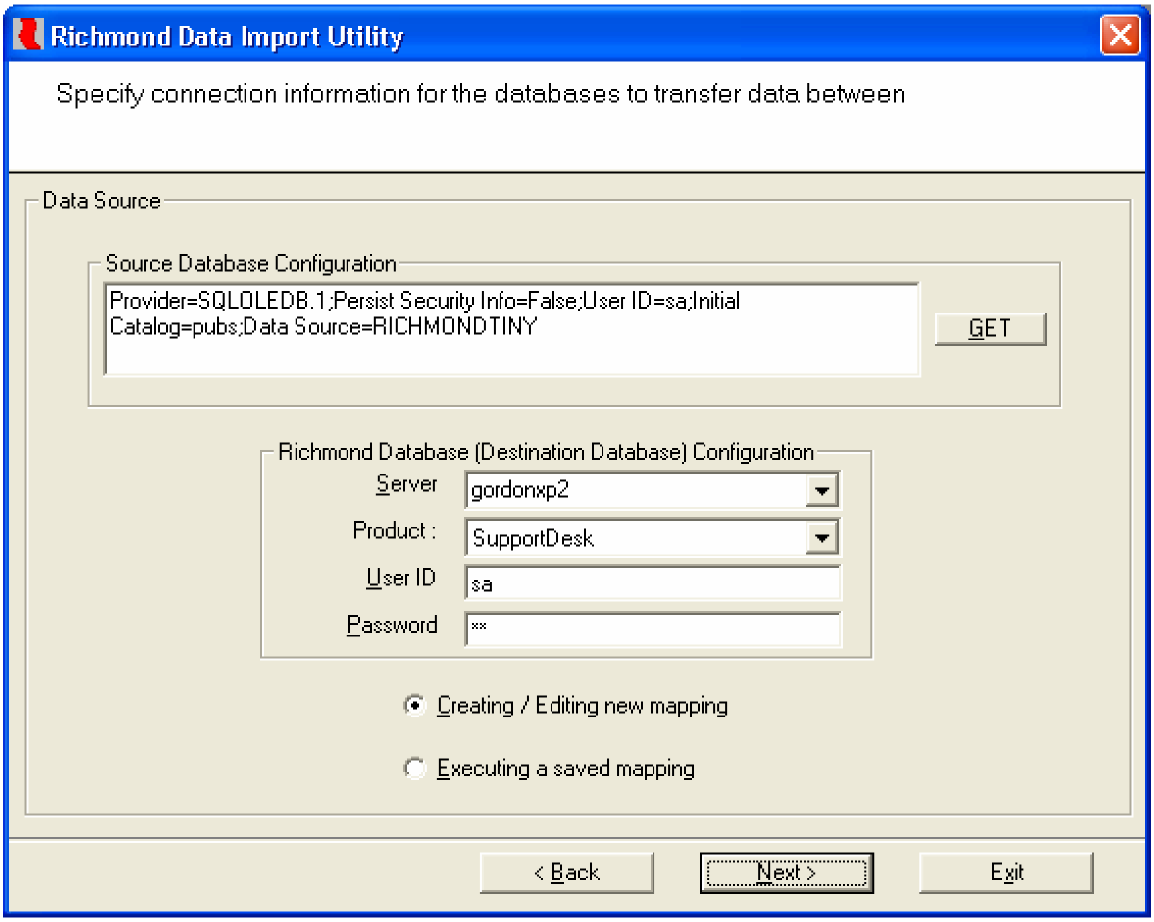
Sample data import – Step by Step

This article shows how to conduct a data import from a 3rd party database (Microsoft's sample Pubs database) to SupportDesk.

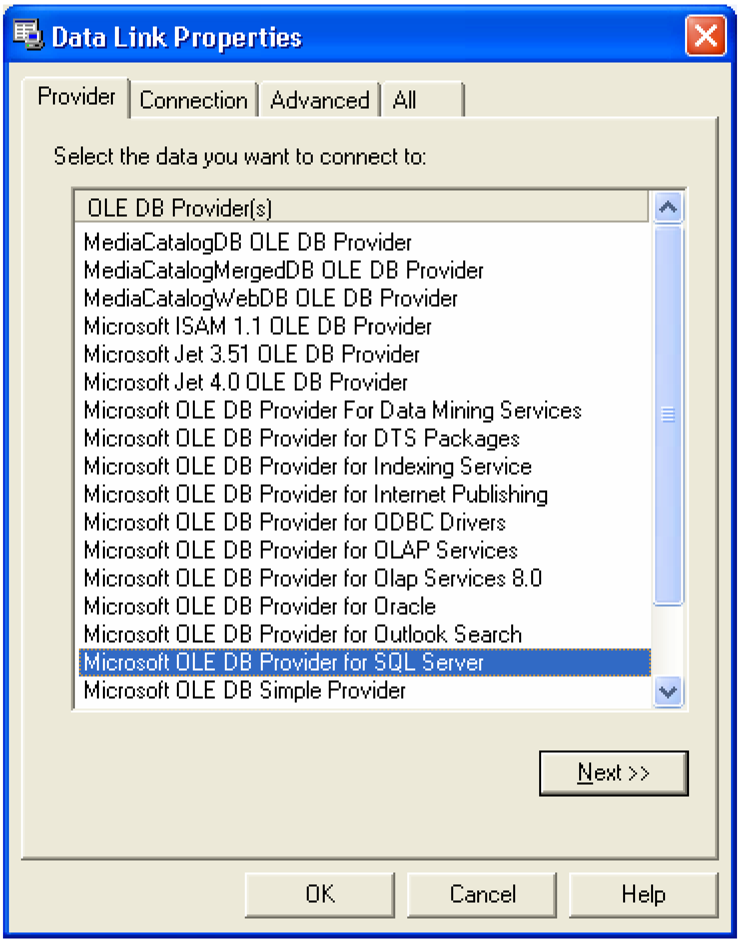
- Connection
- Structure
- Mapping
- Import
- Results in SupportDesk

Connection



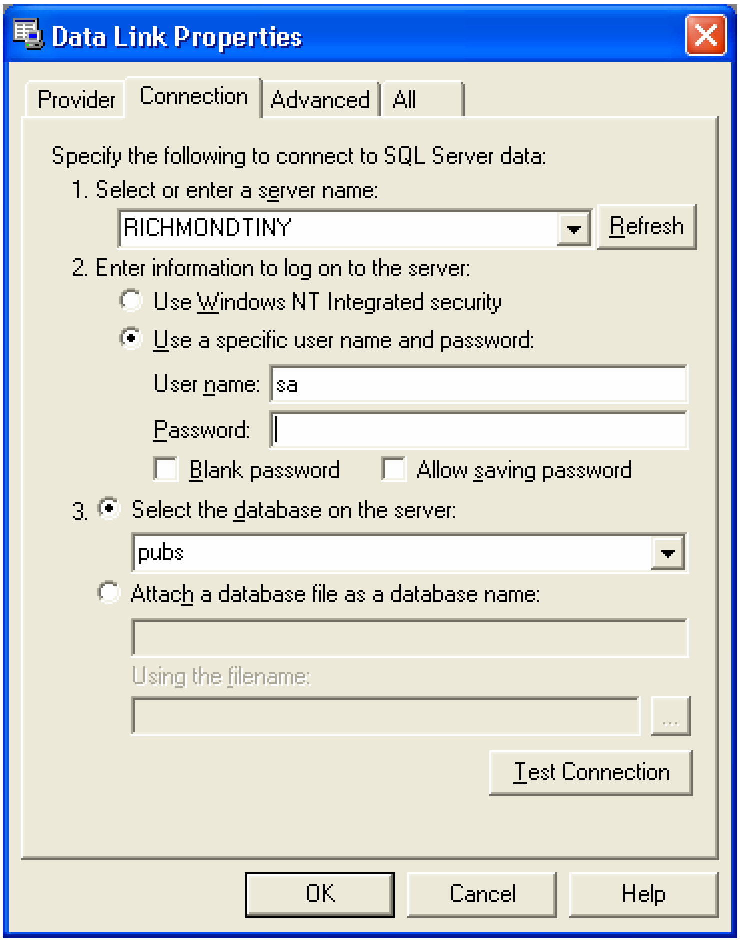


To initiate a data import, you must first connect to both the Pubs database and the SupportDesk database. To connect to the Pubs (source) database, click on the GET button in the source database configuration part of the screen. This will initiate a data connection wizard to help ensure your database connection is successful.



Select the appropriate data provider for your source database. In this example, we are connecting to a Microsoft SQL Server. Therefore the provider we have to use is 'Microsoft OLE DB Provider for SQL Server'.

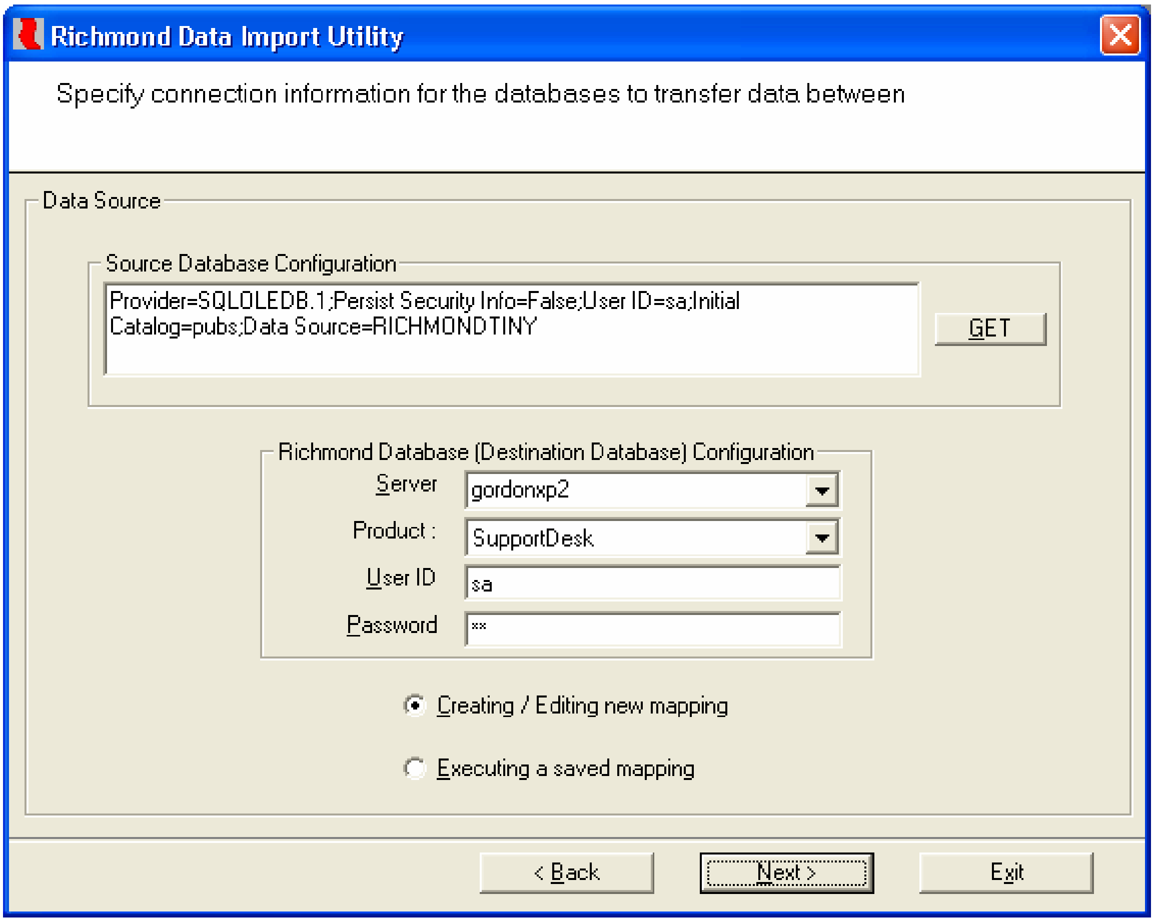
Note:
Another common data provider is the Microsoft Jet OLE DB Provider. This is the data provider to use if you are connecting to a Microsoft Access database.



The connection tab of the data link screen varies, depending on which data provider you have selected. To complete the connection to your selected database, just complete the connection fields to the database. If you are unsure on what information to use then ask your network/database administrator.

Note:
The preferred login to use is the system administrator (SA).

To ensure that a connection is successful, click the Test Connection' button. To use this connection, just click OK.



Complete the destination database configuration with the SQL server name of your SupportDesk database, User ID and Password. Please note that your SupportDesk login will not work. You can use the SQL server system administrator login (SA) or you can use the Richmond system administrators login (RichSA) to access the SQL server. By clicking next, connections to both databases will be established.

SupportDesk Directory Synchronisation

Welcome

The SupportDesk Active Directory Synchronisation provides the ability to populate the SupportDesk Navigator with User and Computer information from Active Directory. This can be accomplished by a single import from Active Directory or the RS Directory Extract Service can continually update SupportDesk as new Users and Computers are added to Active Directory or when details in Active Directory are updated.

The Active Directory Synchronisation contains three separate modules:

- **Quick Setup**

  The Quick Setup is a wizard driven application used to create an extraction template for creating Users and Organisational Units in the SupportDesk Navigator. This is the recommend method for setting up the synchronization of MS Active Directory with SupportDesk.

- **Directory Querier**

  The Directory Querier is a tool for advanced users that can be used to define additional object classes that you wish to extract from MS Active Directory. This should only be used when additional information is required that the Quick Setup does not provide.

- **RS Directory Extract Service**

  The RS Directory Extract Service is a Windows Service that can run on a server to automatically update Items in SupportDesk when changes are made to objects in MS Active Directory. The RS Directory Extract Service performs imports into SupportDesk using XML template files created by either the Quick Setup or the Directory Querier.

Installation

The Active Directory Synchronisation is part of the Richmond Server Extensions installation. Please refer to the installation instructions for the Server Extension for further information.

Quick Setup

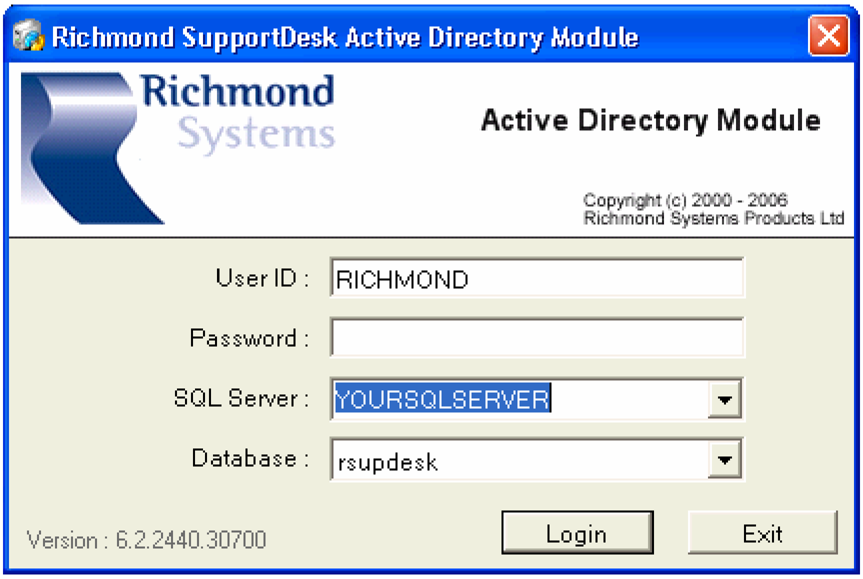
The Active Directory Quick Setup Wizard allows for the quick configuration of the import of Users and Computers from MS Active Directory into the SupportDesk Database. This is a quick and easy way to ensure that SupportDesk reflects your business. The Quick Setup Wizard will produce an xml template based on the selected Active Directory Organizational Units (OU).   A manual import can be run from the Quick Setup or the RS Directory Extract Service and be started to provide ongoing synchronization from MS Active Directory to SupportDesk.

Starting the Quick Setup

The Quick Setup can be started from the Windows Start Menu in the Programs→Richmond Systems→Active Directory Synchronisation program group. It is strongly recommended that all SupportDesk users are logged out of SupportDesk before using the Active Directory Quick Setup.

Logon to Quick Setup

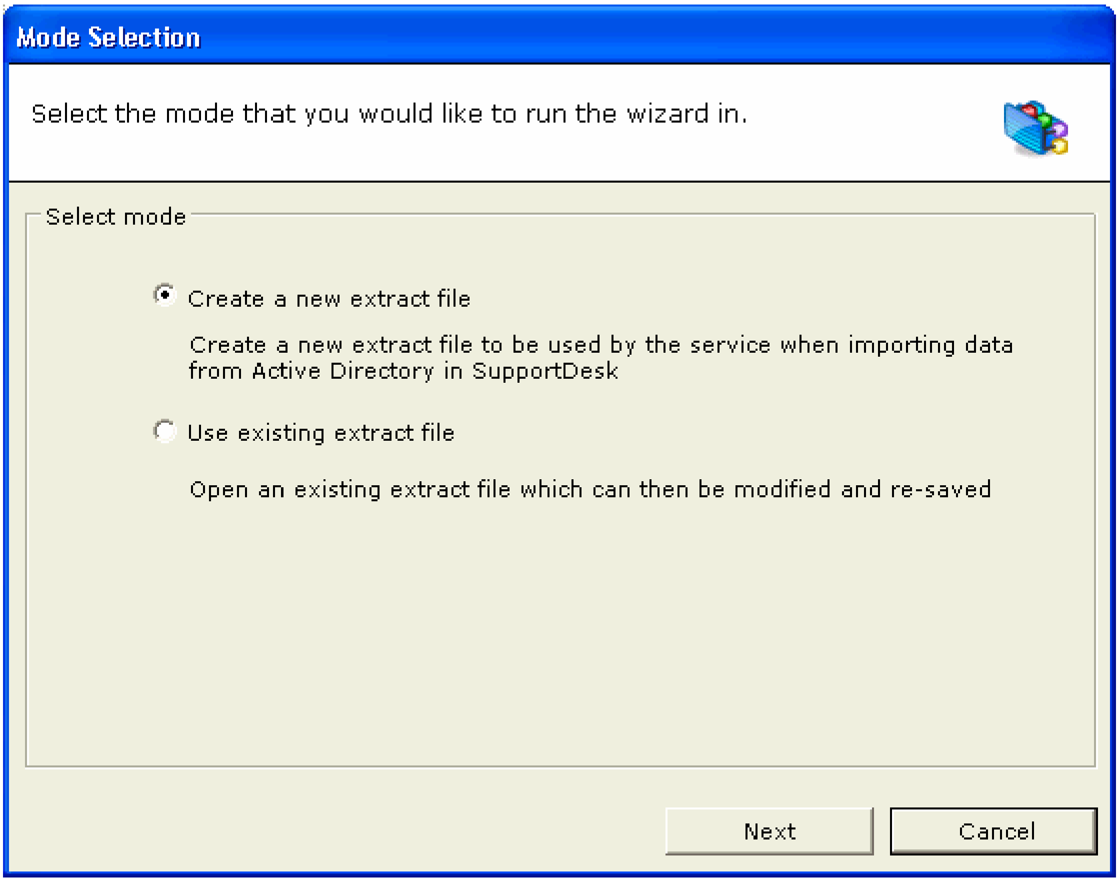
The Quick Setup Wizard requires authentication.



- **User ID**
  Unique user name provided by the SupportDesk Administrator
- **Password**
  user password
- **SQL Server**
  Name of the SQL Server that hosts the SupportDesk Database
- **Database**
  Name of the SupportDesk Database

Mode Selection

The Quick Setup Wizard has the option to create a new extract file or can open an existing extract file.

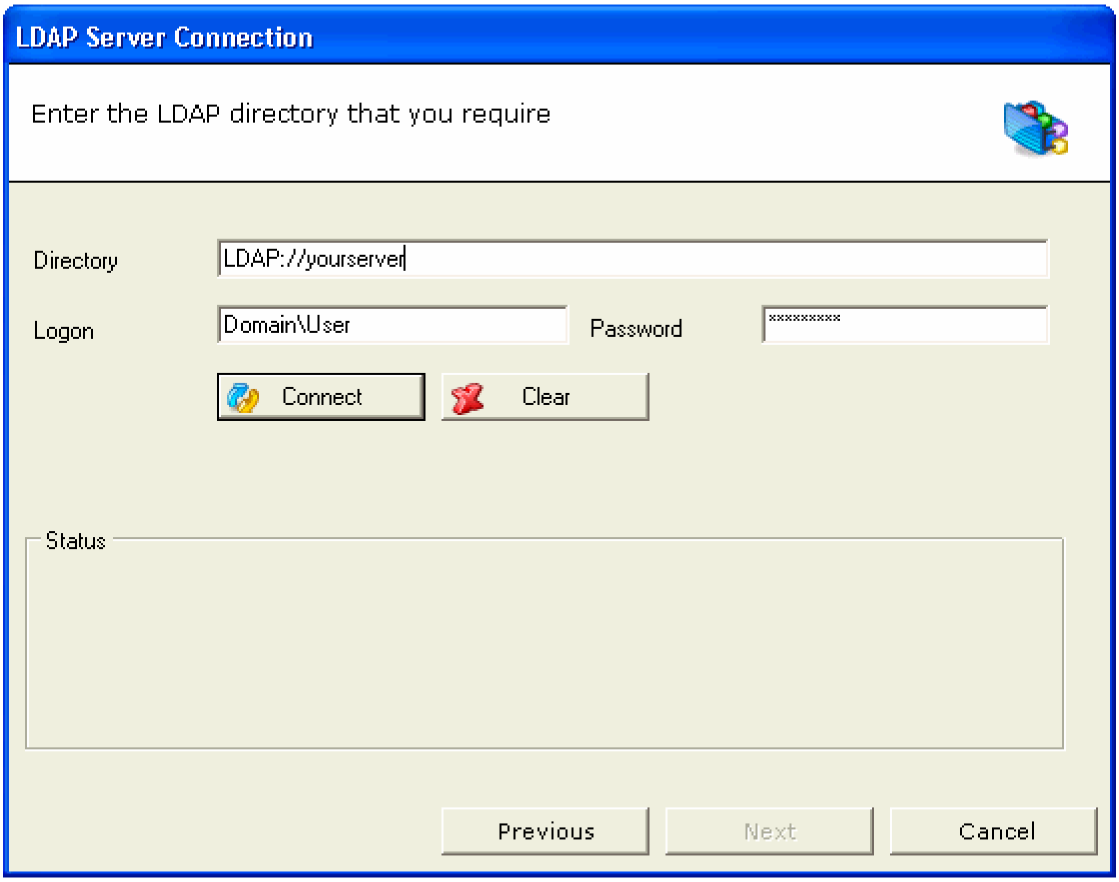


If this is the first time the Quick Setup has been used or if a new extract is going to be created select the option to *Create a new extract*.

If there is an existing configured extract file that needs to be changed select the option to *Use existing extract file.*

LDAP Server Connection

The Quick Setup wizard requires that you connect to your MS Active Directory using the LDAP (lightweight directory access protocol) protocol.



The *Directory* text box contains the LDAP connection details to your MS Active Directory. This requires a connection string in the format:

LDAP://<AD Server name or IP address>

Enter the name of the server that has Active Directory installed. This name must begin "LDAP://" and can then contain the physical machine name or IP address of the server. E.g. LDAP://ADServer1 or LDAP://192.168.0.1

If you do not know the connection details for your active directory then you should contact your System Administrator.

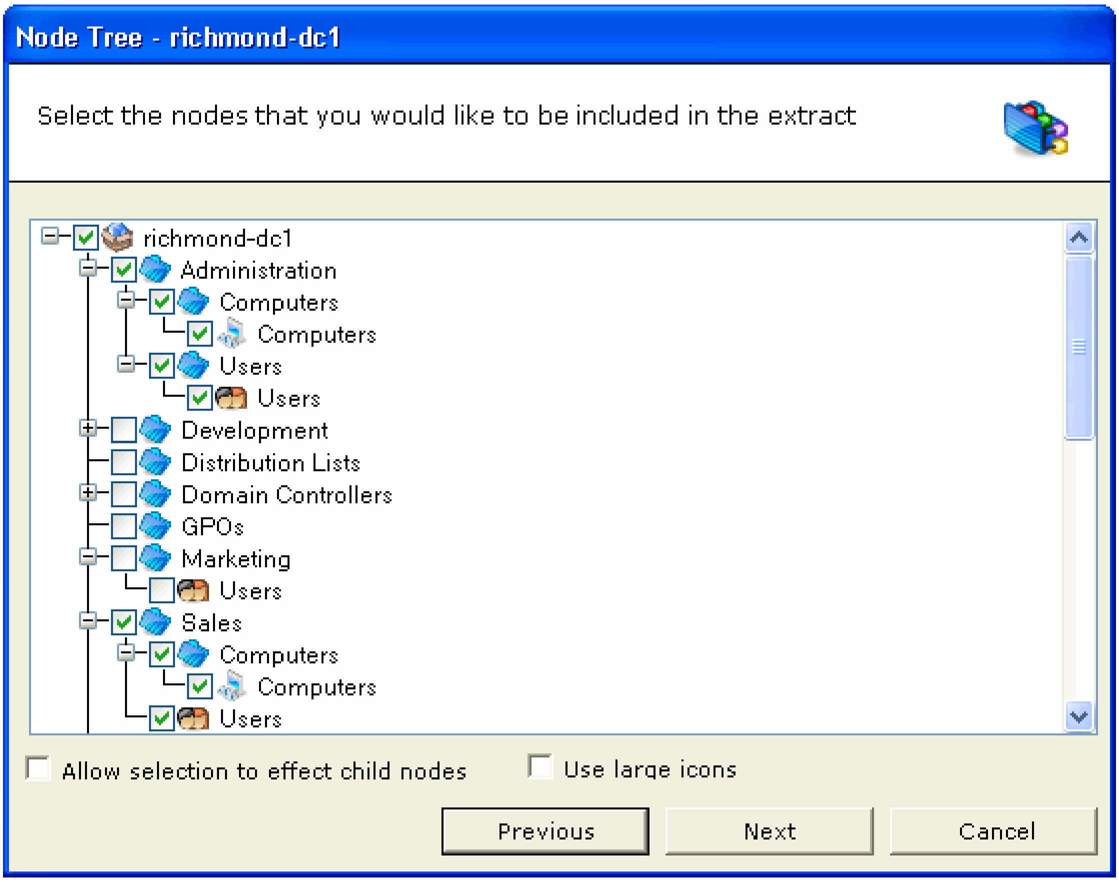
The *Logon* test box requires the name of a MS Active Directory User that has at least read rights to Active Directory. The user name should be entered in the format of **domain\user**.

The *Password* text box requires the password for the AD user that was entered in the *Logon* text box. Blank passwords are not accepted.

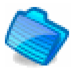
When all the connection information has been entered, click on the *Connect* button. The *Status* box should show "Connected to LDAP://YourDomainController"

Node Tree

The Node Tree is a representation of the Organizational Units (OUs) that exist in your MS Active Directory. Organizational Units that contain AD Users and Computers can be selected for import into SupportDesk. Only the selected OUs will be used during imports and synchronisation.



Organizational Units are represented by a folder icon:



Each selected OU will be created in the Navigator Tree in SupportDesk during imports and synchronization.

Any OU that contains AD Users will have a User container as a child item:

Each User container can represent any number of users that exist under that OU.

Any OU that contains AD Computers will have a Computer container as a child item:

Each Computer container can represent any number of computers that exist under that OU.

If a User or Computer container is selected the parent OUs will be automatically selected down to the root of the domain. This ensures that SupportDesk represents the hierarchy of the Active Directory structure correctly.

The "Allow selection to affect child nodes" checkbox is used to automatically select all child items of an OU when the OU is selected. This provides an easy way to deal with large structures that have many levels of hierarchy. If using this option make sure it is selected before selecting the nodes that you wish to import.

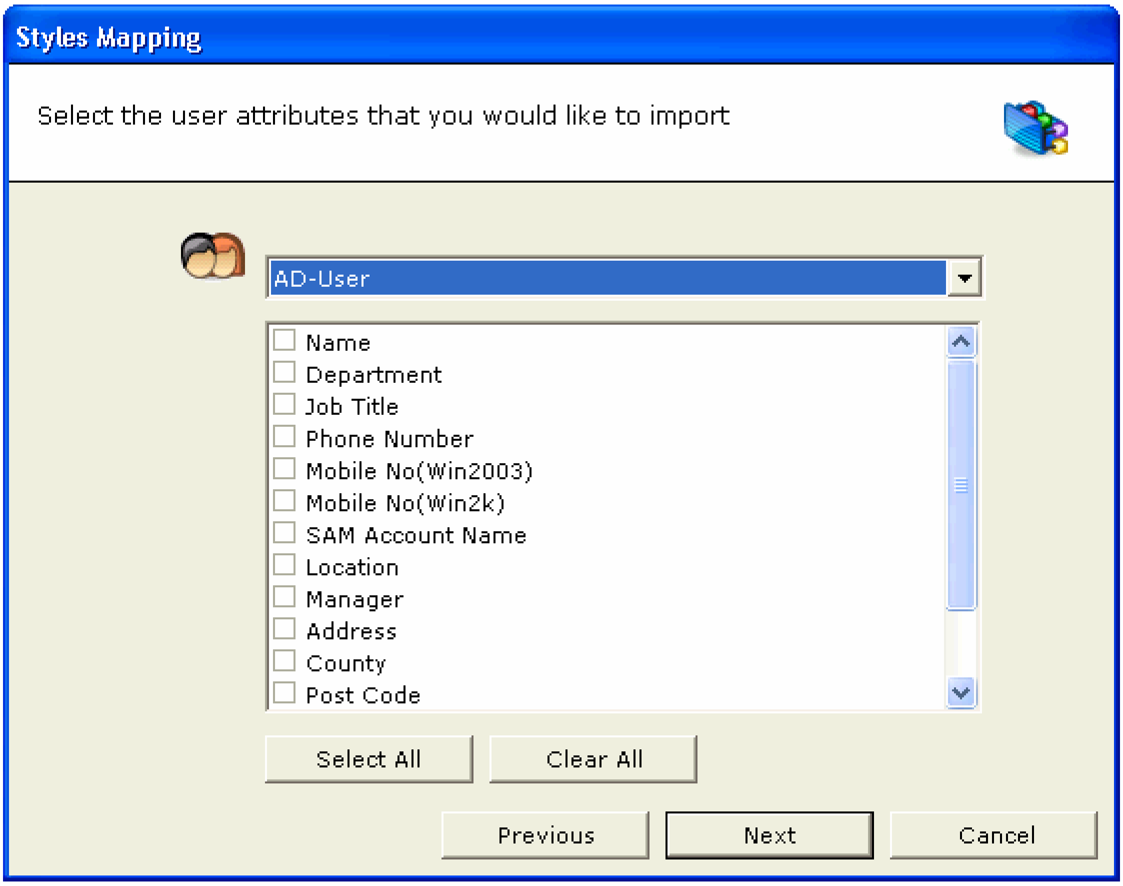
Style Mapping

A Style Mapping is used to create a list of attributes to be added to each AD-User Item and AD-Computer Item that gets created in the SupportDesk Navigator.

The AD-User style is a defined set of attributes for Active Directory Users to be stored in the SupportDesk Navigator. The AD-Computer style is used to create a list of attributes for Active Directory Computers to be stored in the SupportDesk Navigator.

Mapping information is created between the Active Directory containers and the SupportDesk Items so that when attributes in Active Directory are changed the affected SupportDesk Items are also updated when using the RS Directory Extract Service.

Selecting the AD-User style from the drop down will present you with the following options:



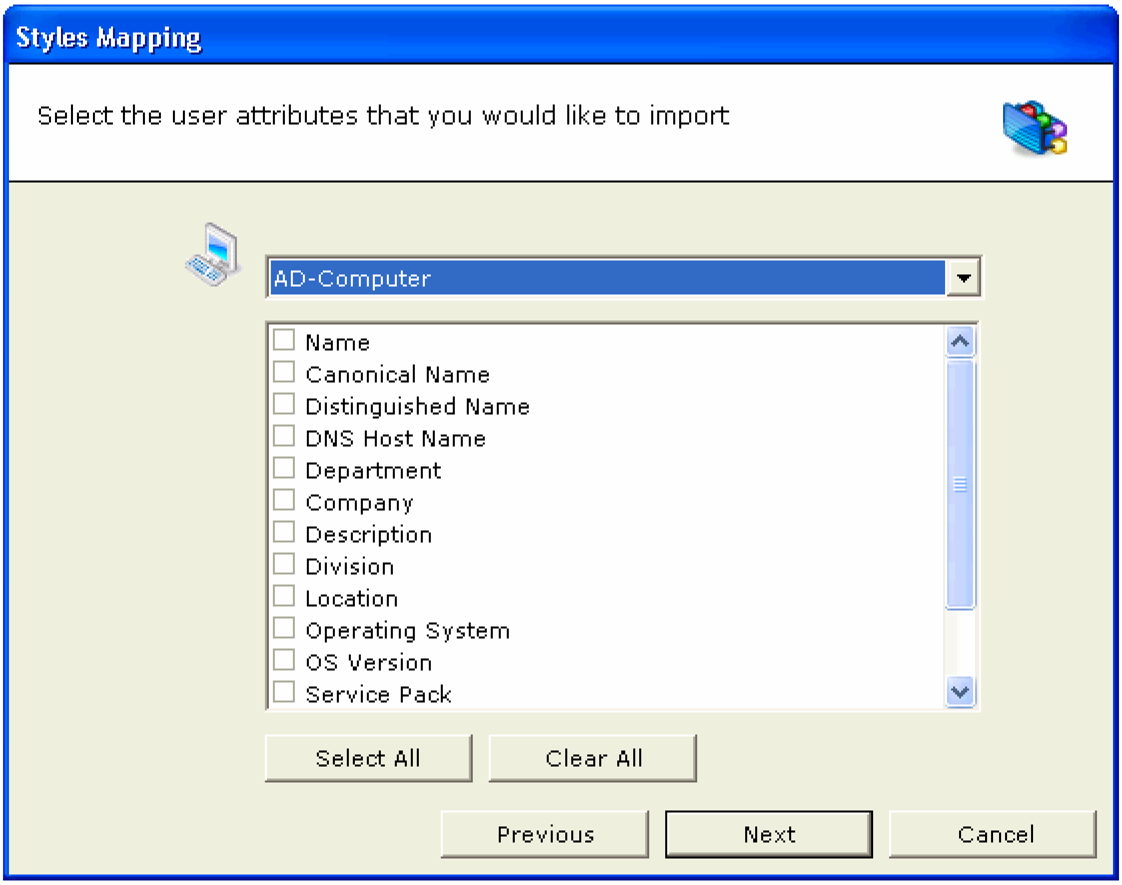
A list of available attributes from the MS AD User Class is displayed. Select the user attributes that you wish to import.

The full list of possible User attributes to choose from is as follows:

- Name
- Department
- Job Title
- Phone Number
- Mobile No(Win2003)
- Mobile No (Win2k)
- SAM Account Name
- Location
- Manager
- Address
- Country
- Post Code
- Company

- Login Count

Selecting the AD-Computer style from the drop down will present you with the following options:



The full list of possible User attributes to choose from is as follows:

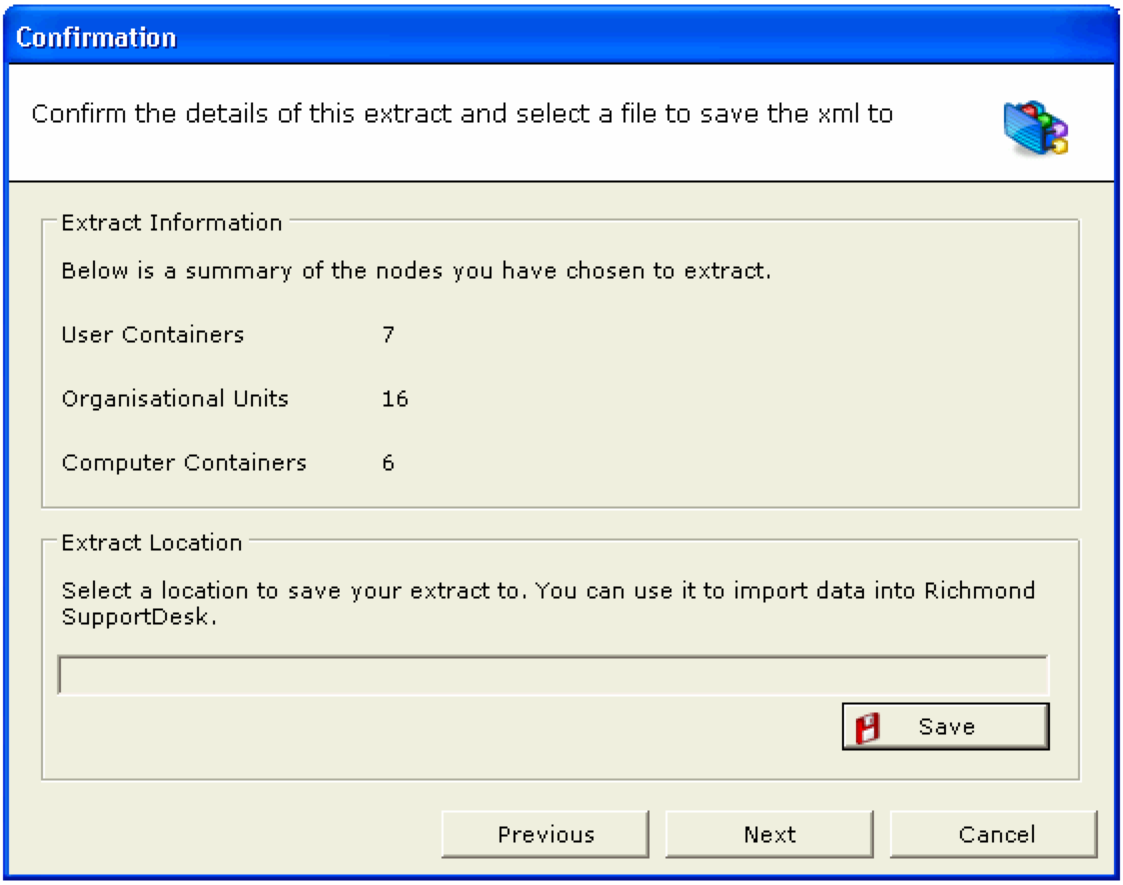
- Name (computername)
- Canonical Name (yourdomain.com/ou/computername)
- DNS Host Name (computer.domain.com)
- Department
- Company
- Description
- Division
- Location
- Operating System
- OS Version
- Service Pack
- Account Disabled
- When Changed
- When Created

***Note*:** The ability to define the AD-User style in this way is only available on the first import to SupportDesk. Once there are users in the SupportDesk database that use AD-User style it can no longer be modified. The Style Mapping screen will not be available the next time the AD Quick Setup is launched.

Note: Active Directory for Windows 2000 Server and Active Directory on Server 2003 store mobile phone numbers under different attribute names. Two options exist in the Style Mapping for Mobile phone numbers. Select only the Mobile Number for the version of Active Directory that you are running.

Confirmation

The Confirmation screen provides details on the number of nodes that will be extracted and requires the saving of the extraction XML template used for imports into SupportDesk.



The number of User Containers displays the number of User Containers selected on the Node Tree screen. This does not represent to total number of users being imported. Each container can hold any number of users.

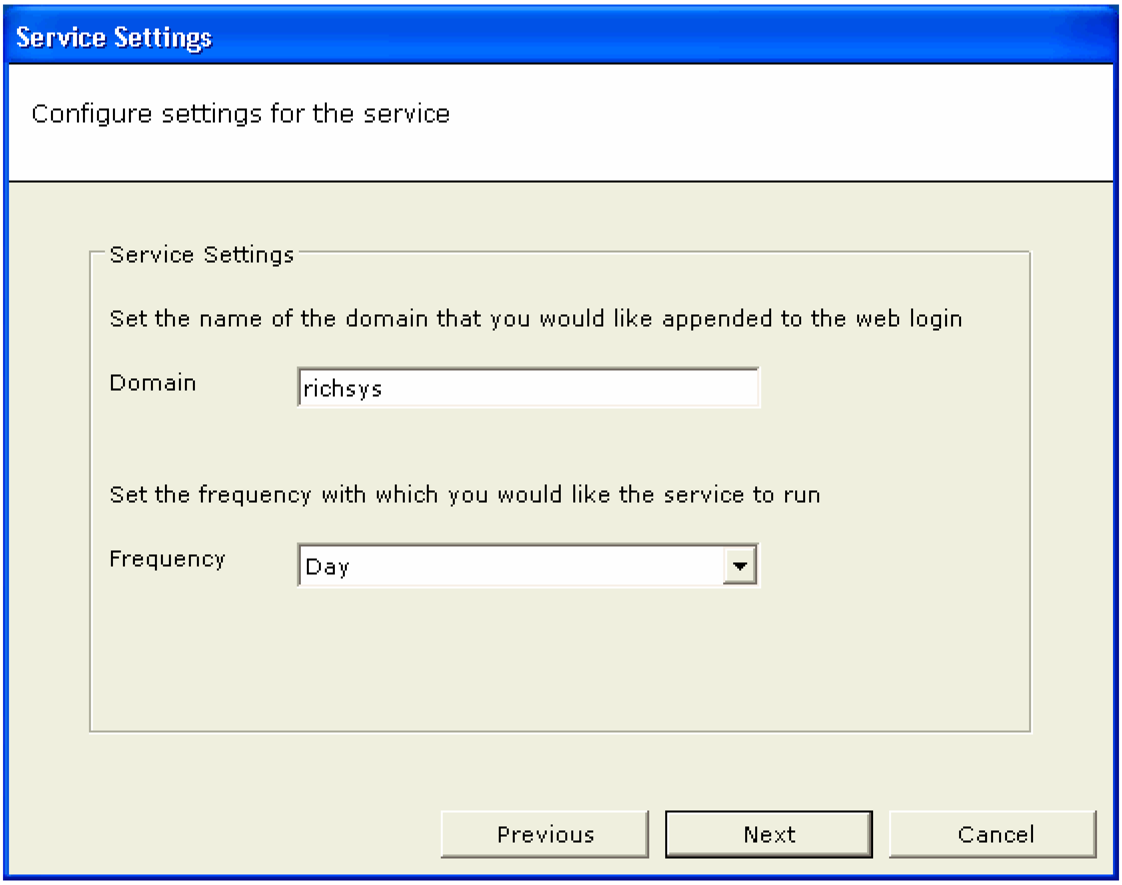
An XML file must be created and saved for the import or synchronization to work. The XML file contains information that has been selected in the Quick Setup.

Click on the *Save* button save the configured settings. The default directory for saving the XML extract is **C:\Program Files\Richmond Systems\SupportDesk\Extract.** It is important to store all extraction XML files in this default directory as the RS Directory Extract Service uses this default directory to read the XML files to perform imports and synchronisation.

Note: Even after you have saved the xml file you can return at any time to the node tree and make further selections. You then have the option of saving the extract to a new file or overriding the existing one. The RS Directory Extract Service will process all XML files that are located in the default extraction directory.

Service Settings

The Service Settings provides configuration options for the RS Directory Extract Service.



The *Domain* option lets you specify the prefix for Customer Web Interface login Web ID located on the AD-User Items. If NT Authentication is enabled for the Customer Web Interface this is required.

The Frequency option lets you specify how often you would like the Service to perform synchronization from AD to SupportDesk.

Minute – The service runs every minute, on the minute.

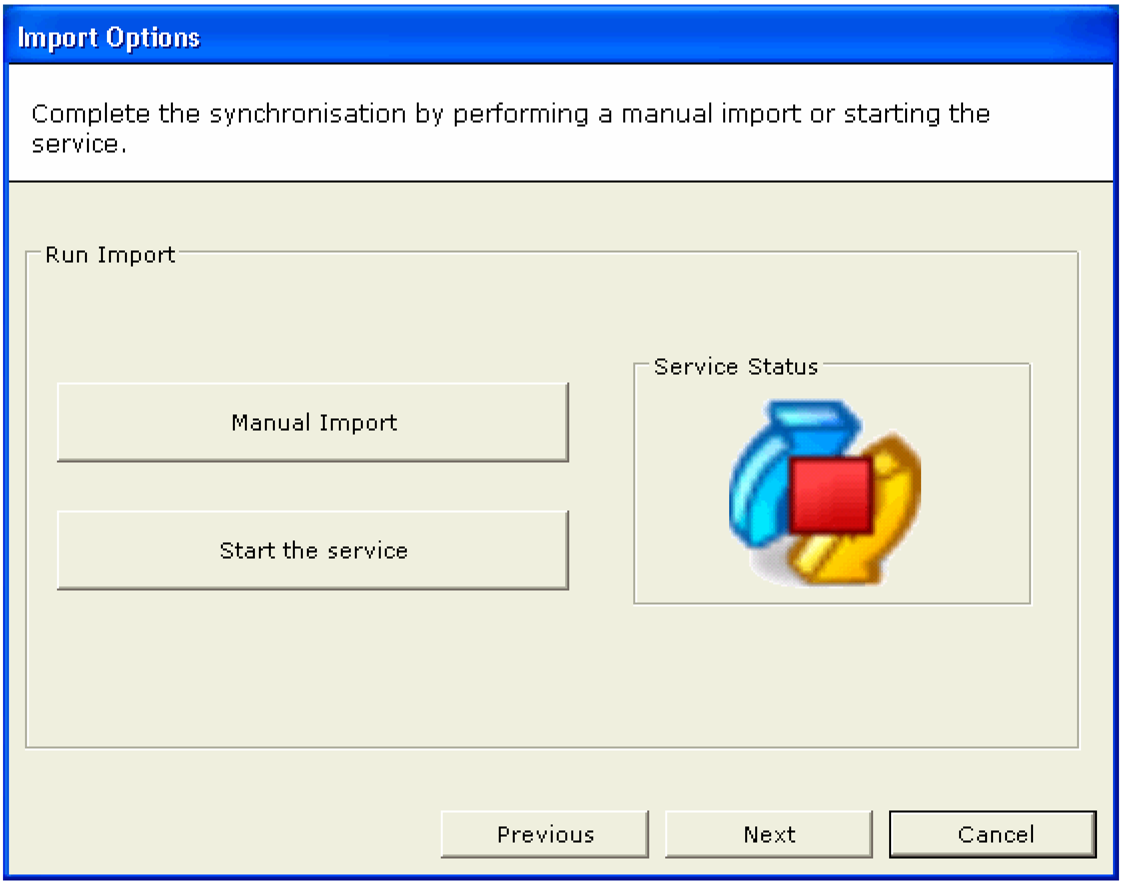
Hour – The service runs every hour, on the hour.

Day – The service runs every day at 23:00

Note: The default time 23:00 can be changed by modifying the C:\Program Files\Richmond Systems SupportDesk\directories.xml file. Modify the entry <extStartDate>2004/03/20 23:00</extStartDate> to reflect the time that you wish the RS Directory Extract Service to perform an import into SupportDesk.

Import Options

The Import Options gives the option to perform a manual import of Active Directory Users into SupportDesk or to start the RS Directory Extract Service to perform scheduled imports.



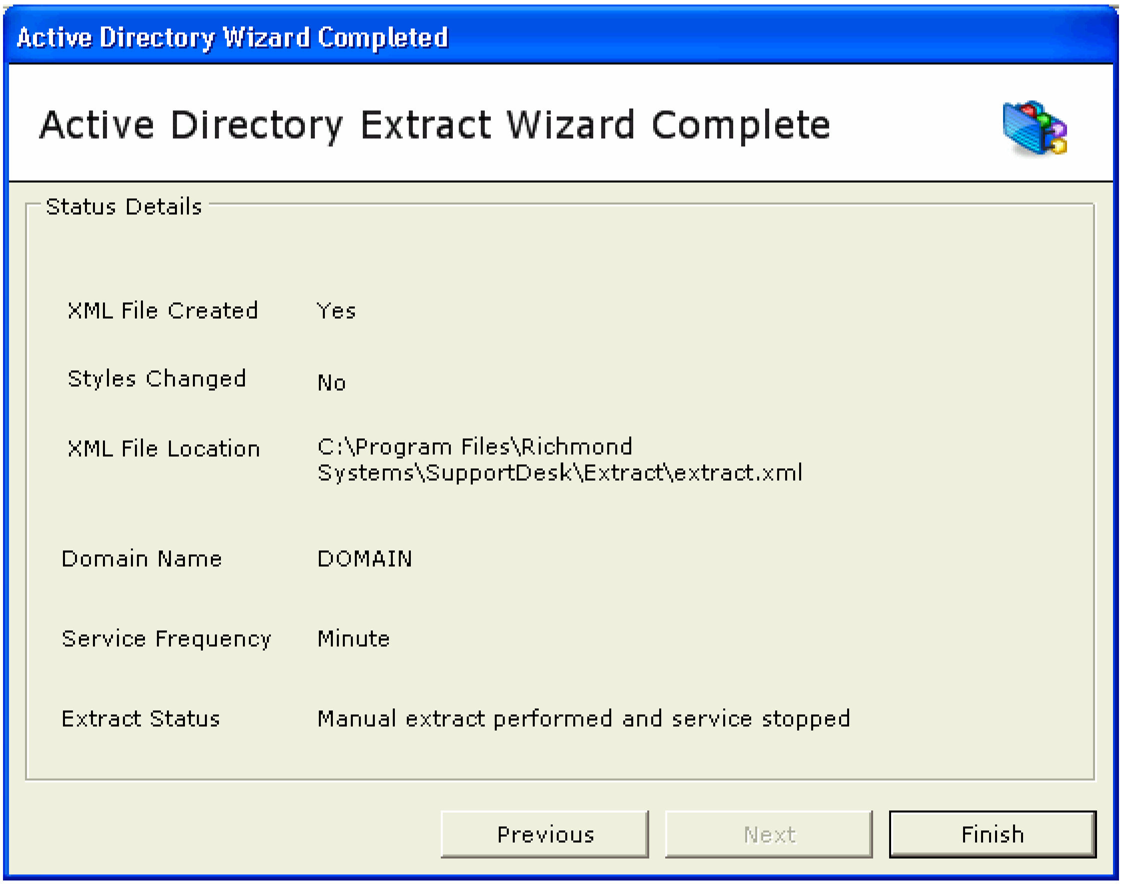
The *Manual Import* button will perform a single import into SupportDesk. This should be used when you only want a one time import and you do not wish to have continued synchronisation.

The *Start the Service* button starts the RS Directory Extract Service. Running the service will allow continued synchronisation to occur between Active Directory and the SupportDesk database. If a new user is added to Active Directory in one of the selected AD Node it will automatically be added to SupportDesk at the next scheduled import.

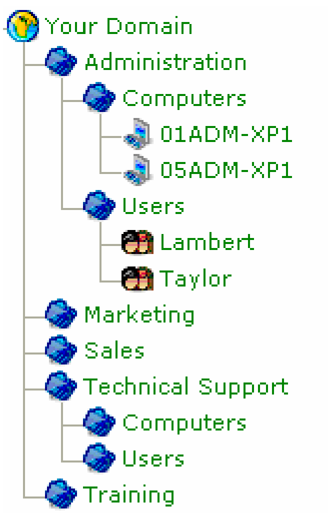
Note: The RS Directory Extract Service **Startup Type** is set to **Manual**. If the computer where the RS Directory Extract Service is installed is rebooted the RS Directory Extract Service will return to a stopped state. The Startup Type can be set to Automatic so that the service is started each time the computer is started. For more details please see the section on the RS Directory Extract Service.

AD Wizard Extract Completed

The final window displays a summary of the settings that were configured. Click on Finish to exit the AD Quick Setup.



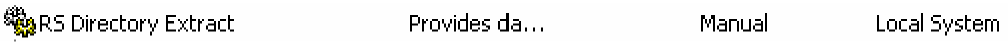
If a manual import was run, the imported Users will be immediately available in the SupportDesk Navigator Tree. If the RS Directory Extract Service is being used for importing Users, the SupportDesk Navigator Tree will be populated according to the schedule that was selected.



RS Directory Extract Service

The RS Directory Extract service is an unattended program that runs on one machine to keep the data between MS Active Directory and Richmond SupportDesk synchronised. Only start the Extract Service if you intend to synchronise Active Directory with SupportDesk.

The RS Directory Extract Service is installed with the Active Directory Synchronisation module.



Before the RS Directory Extract Service can import Active Directory information into SupportDesk an Extract XML file must be created using the AD Quick Setup or the Directory Querier.

The following operations are performed by the Extract Service

- Perform queries of Active Directory to look for changes
- If an Object's attributes change value in Active Directory the associated Item in SupportDesk will be updated with the change.
- If a new Object is added to Active Directory it will automatically be added to SupportDesk.
- If an Object is moved to a different Organisational Unit, the move will be reflected in SupportDesk.
- Items that are deleted in the directory will not be deleted from SupportDesk.
- All extract templates that exist in the extract folder will be processed in alphabetical order.
- Windows Event logs are created for the status of each extract and for any errors if they occur.

Note: The above actions will only apply to Organizational Units that have been selected in the Quick Setup or the Querier. Only selected OUs will be monitored for changes and moves.

By default the RS Directory Service start up option is set to Manual. In the case that the computer where the RS Directory Extract Service is installed is rebooted the RS Directory Extract Service will need restarting. To have the RS Directory Extract Service start automatically when the computer is rebooted, change the settings of the RS Directory Extract Service to Automatic.

Directories XML Settings

The Directories XML file is used to configure settings for the importing of information from Active Directory. The directories.xml file is located in the SupportDesk program folder.

The Directories.xml file can be opened and modified using Notepad. XML tags are held between angled brackets (<>). Tags must not be modified or deleted.

Between an opening tag and a closing tag

- **DomainName**

  The DomainName entry is added as a prefix to the webID. The DomainName and webID are used for Web Interface Credentials on the Customer Web Interface. Replace DomainName with the name of your domain.

  <DomainName>**YourDomainName**</DomainName>

  Note: If you do not wish to prefix the webID with the DomainName, remove the DomainName text from between the two tags. This is only recommended if you are not using NT Authentication for the Customer Web Interface.

  <DomainName></DomainName>

- **webID**

  The webID entry is used to populate the Web Interface Credentials on the Customer Web Interface. The default entry uses the **sameaccountname** attribute held in Active Directory. Other Active Directory attributes can be used. For example:

  givenname – The first name of the Active Directory User

  sn – The Surname of the Active Directory User

  samaccountname – The login name of the Active Directory User. Required for NT Authentication.

- **extPeriodAmount**

  This indicates the period amount used by the extPeriodType. The extPeriodAmount and the extPeriod Type together represents how often the Active Directory is polled.

- **extPeriodType**

  This indicates the period type. This can be set to minute, hour, or day. The extPeriodAmount and the extPeriod Type together represents how often the Active Directory is polled.

- **extStartDate**

  The date and time for the first extract to start. This is in the format YYYY/MM/DD HH:MM

Rsupdesk XML Settings

The RSUPDESK.xml can be found in the SupportDesk program folder.

Active Directory related entries in the RSUPDESK.xml file are grouped under the <RSDIRECTORIES> section:

<RSDIRECTORIES>

<ExtractFilePath>C:\PROGRAM FILES\RICHMOND SYSTEMS\SUPPORTDESK\DIREXTRACT</ExtractFilePath>

<DirectoriesFile>C:\PROGRAM FILES\RICHMOND SYSTEMS\SUPPORTDESK\Directories.xml</DirectoriesFile>

ExtractfilePath – Defines the path for storing the extract profile files. The Directory Viewer uses this path for loading and saving extract profile files. The Extract Service processes all files in this path.

DirectoriesFile – Defines the path and name of the DIRECTORIES.XML file which contains details of each type of directory service that the Directory Viewer and Extract process can work with.

Additional Active Directory Settings can be found in the SETTINGS section:

<SETTINGS>

<ActiveDirPeplicateMove>Y</ActiveDirPeplicateMove>

<ADDelCIID/>

ActiveDirReplicateMove – When an Object is moved from one Organisational Unit to another, this move can be automatically replicated in the SupportDesk Navigator Tree. This must be set to =Y

ADDelCIID – When an Active Directory User is deleted from Active Directory the related SupportDesk user can be moved to a specified location in the SupportDesk Navigator. The numeric ID of this location must be added to the ADDelCIID setting. Example: <ADDelCIID>128</ADDelCIID>

To find the CIID id of an item in SupportDesk run the following from a command window on the SQL Server:

1.) OSQL -E
2.) Use rsupdesk
3.) go
4.) Select id FROM CIID WHERE alpha1 = '<The name of Navigator Item where you want deleted users to be stored>'
5.) Go
6.) Exit

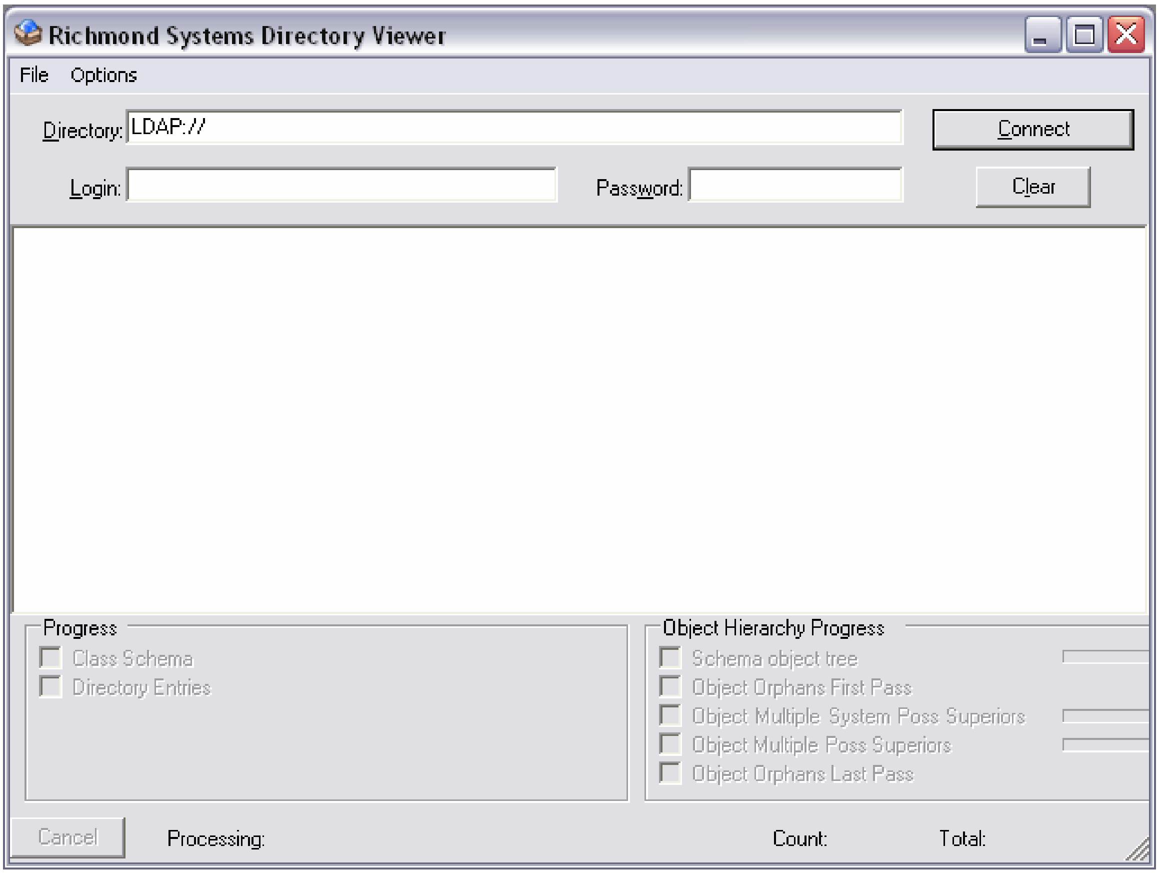
Directory Querier

Directory Querier

The Directory Querier is an advanced tool for creating customised Active Directory Extracts or modifying extracts created by the Quick Setup wizard. The Directory Querier should only be used if there are custom requirements that the Quick Setup can not provide.

The Directory Querier consists of two elements – The Directory Viewer and the Extract Configuration.

Directory Viewer



Directory Entry Field – Enter the name of the server that has Active Directory installed. This name must begin "LDAP://" and can then contain the physical machine name of the server or the domain name of the domain the server manages. e.g. LDAP://servername or LDAP://domainname

Login Entry Field – This is a username in the form that is known to the directory e.g. for the Windows Guest user account CN=Guest,CN=Users,DC=richmondsys,DC=co,DC=uk. A login is not required if you are using an existing XML extraction file.

Password Entry Field – This is the Windows Logon password for the username entered above. A password is required for both the Object Hierarchy and Class Schema. If a user account has a blank password then that user account cannot be used to read the Object Hierarchy or Class Schema.

Connect Button – Pressing the Connect button attempts to read the directory on the server specified. The information to be retrieved is determined by the Options menu items selected.

Clear Button – Pressing the Clear button clears the Directory, Login, and Password entry fields

Status Pane - The small pane at the bottom of the window is a status pane showing processing information when connecting to a directory.

Cancel Button – Whilst reading information from a directory this button is enabled. Pressing it allows the process to be paused or cancelled. If the process is cancelled then the directory tree will still be displayed with the information loaded so far.

Menu Items

File

- **Open Extract Form -** Opens the Extract Configuration Window.
- **Exit** - Closes the Directory Viewer application.

Options

- **Directory Type** – This sub menu allows the selection of the type of directory that the Directory Viewer will connect to the next time the Connect button is pressed. Currently, MS Active Directory is the only option available.
- **Display** – This sub menu provides a list of options for the types of information to be read from the directory the next time the Connect button is pressed. At least one must be selected. Directory Entries is selected by default. The first three options show the configuration details of the directory. The fourth option shows the actual data.
- **RootDSE** – Each directory maintains information about its own service within a special entry called RootDSE. This information is made available by the Viewer but is not required for extracting data. It is displayed under the "rootDSE" node.
- **Class Schema** – This option will read the complete schema contents of the directory and display the details under the "schema" node. There are two child nodes created. The first is "attributeSchema" which simply lists all the attribute names in alphabetical order. The second is "classSchema" which displays all the classes available in a hierarchical structure.
- **Object Hierarchy** – A directory defines which objects can contain which other objects. This is represented by a tree structure under the child node "objectSchema" within the "schema" node when this option selected.
- **Directory Entries** – This option must be selected to view the actual data stored in a directory.

Tree Context Menu Clicking with the right mouse button on a selected item in the tree will display the following context menu:

- **Extract** Opens the Extract Configuration window. The highlighted directory item will be added to the extract tree at the relative position.

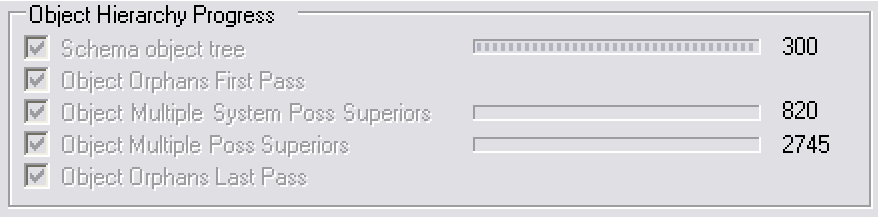
- **Find Text** electing this item will display the Find Window detailed in the following section.

- **Remove Node** Selecting this item removes the node and all sub nodes.

Connecting to the Directory

Connecting to the Directory initiates the processing of the entire Directory Services. Depending on the size and complexity of the Directory Services this process can take a considerable amount of time.

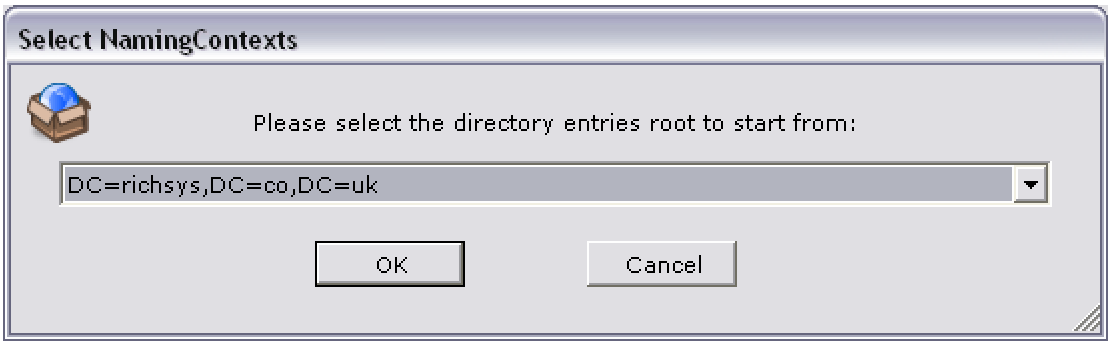
The progress can be monitored from the Progress area.



Retrieving the Directory Entries

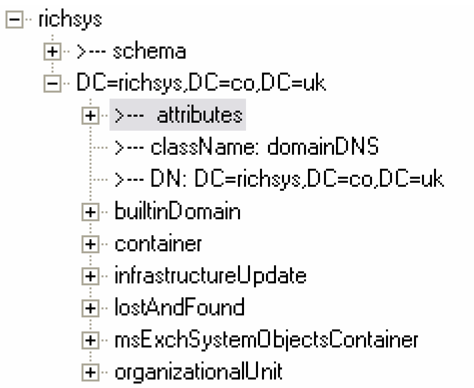
Enter the name of the server or the domain name into the Directory entry field and press the Connect button

When the query has completed a drop down option will be displayed to select the Naming Context for the directory.



The drop down list consists of three options. The "CN=Configuration,…" and "CN=Schema,CN=Configuration, and "DC=…". Select the "DC=…".

A typical directory structure would look similar to the following:



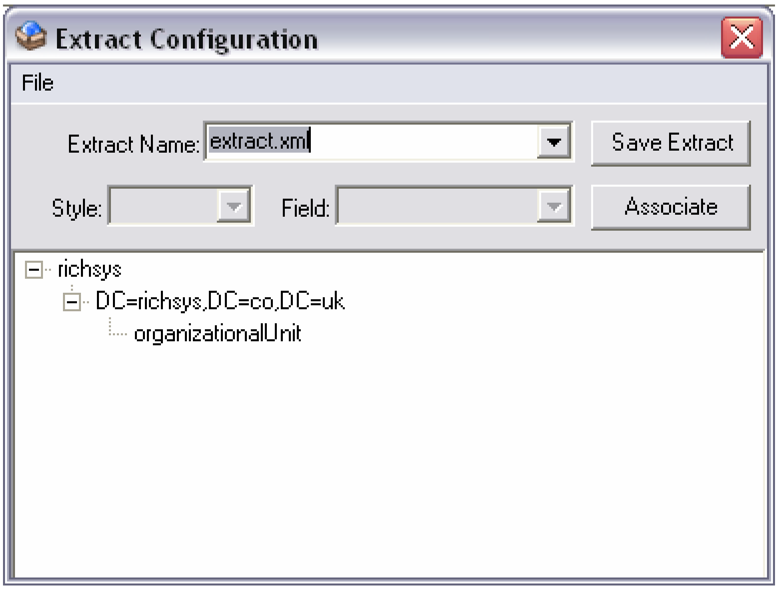
Extract Configuration

Creating an Extract template

Extract templates are xml files that contain the Directory structure that will be imported into SupportDesk. To be able to create an extract template, or amend an existing one, the directory must first be loaded in the viewer.

An extract template is edited in the Extract Configuration window, which can be opened in two ways.

- Select the main menu option File – Open Extract Form … to open the window without any contents.
- Right Click on a class, object or attribute in the Directory Viewer and select Extract from the context menu. The Extract Configuration window will appear with a tree structure based on the item selected.



Drag and drop classes, objects and attributes onto the extract profile tree to define which items of information are to be extracted from the directory. The structure of the extract profile tree defines what information is extracted. The order in which the items are added to the extract profile tree does not affect the extract process.

A class in the extract tree will correspond to all objects in the directory of that class. This will create as many items in the Supportdesk Navigator as there are objects in the directory of that class at the level specified.

Attributes define what actual data is taken from the directory. Each object and class in the extract tree must have at least one associated attribute.

Associating Navigator Items with the Extract

Each object, class and attribute in the extract tree needs to be associated to a Navigator style and field. The Style and Field combo boxes in the Extract Window are used for this. Selecting an object or class in the tree will enable the Style combo box. Selecting an attribute in the tree will enable the Field combo box but only if a style has been associated with the related object or class. The Style and Field combo boxes are populated with the relevant values from the SupportDesk database. Once the desired value has been selected in the Style or Field combo boxes, the Associate button should be pressed to create the association. The next time the node on the tree is selected the associated value will be displayed in these fields.

Saving the Extract Template

- In the *Extract Name* field enter a name to save the template as. The file name requires the extension .xml.
- Click on the *Save Extract* button to save the template. Before the file is saved a check is made to ensure that all objects, classes and attributes have been associated with Navigator styles and fields.

Note: Extract files are saved in a sub folder of the SupportDesk program folder called Extract.

Extract to SupportDesk

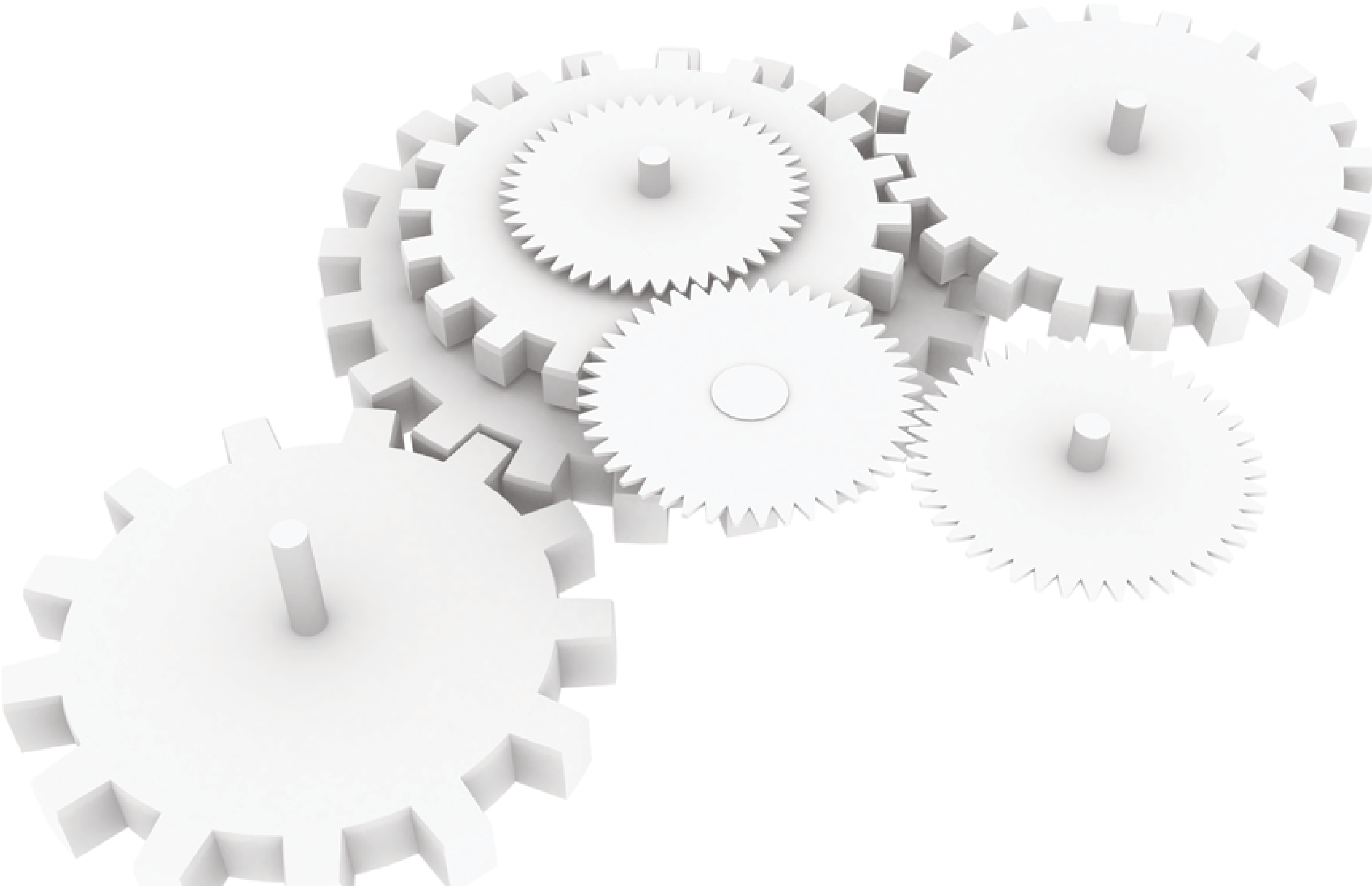
Once an Extract Template is saved an Extract to SupportDesk can be performed.

- Select the Extract Template from the Extract Name drop down box.
- From the File menu select the *Extract Now* menu item.

Note: The extract process runs in the background and processes the extract template file, not the contents of the Extract Configuration window. Therefore, if changes are made to the template in the window they must be saved before running the extract. Details about the extract are written to the Application event log.

Index

RICHMOND SupportDesk



RICHMOND
SupportDesk