

Polar Help Desk 4.1

Administration Guide

Copyright (legal information)

Copyright Polar 1995-2005. All rights reserved.

The information contained in this document is proprietary to Polar and may not be used or disseminated inappropriately. This document, or any part of it, may not be reproduced without the written permission of Polar.

TRADEMARKS

Microsoft, Windows, Windows NT, Windows 2000, Windows XP, Windows 2003, .NET, SQL Server, Office logo and BackOffice are either trademarks or registered trademarks of Microsoft Corporation.

Other product and company names mentioned herein may be trademarks and/or service marks of their respective owners.

DISCLAIMER

SOFTWARE DOCUMENTATION IS PROVIDED AND LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Contents

POLAR HELP DESK ADMINISTRATION GUIDE OVERVIEW.....	5
GENERAL ADMINISTRATION.....	6
View Settings	6
Language Management.....	6
SMTP Server Settings.....	8
POP3 Server Settings	8
Scheduler Settings	10
File Automation	10
GROUP MANAGEMENT	12
Overview	12
Creating New Group.....	12
Modifying Group Information.....	13
BUSINESS UNIT MANAGEMENT.....	13
Overview	13
Creating New Business Unit.....	13
Modifying Business Unit Information.....	14
USER MANAGEMENT	15
Overview	15
Creating New User	15
Modifying User Information.....	16
Importing Users.....	16
ROLE MANAGEMENT	18
Overview	18
Creating New Role	18
Modifying Role Information	19
SERVICE MANAGEMENT	20
Overview	20
Creating New Service.....	20
Modifying SL Information.....	20
SERVICE LEVEL MANAGEMENT.....	21
Overview	21
Creating New SL	21
Modifying SL Information	23
SERVICE LEVEL AGREEMENT MANAGEMENT	24
Overview	24
Creating New SLA.....	24
Modifying SLA Information.....	24
INCIDENT TEMPLATE MANAGEMENT	25
Overview	25

Resolution	25
Creating New Incident Templates	25
Modifying Incident Template Information.....	26

WORK ORDER TEMPLATE MANAGEMENT 26

Overview	26
Description	26
Creating New Work Order Templates	26
Modifying Work Order Template Information.....	27

INCIDENT DATA 28

Administering Incident Category	28
Administering Incident Origin	28
Administering Incident Closure Classification	29

Polar Help Desk Administration Guide Overview

This guide provides information on Polar Help Desk administration tasks. These tasks include general settings, staff management, roles and permissions management, service level management, incident data management, incident templates management and reports management. Only a user who has permissions on viewing Polar Help Desk Administration Desktop can perform these tasks. Such user is called Polar Help Desk Administrator.

General Administration

In tab "General" on Administration Desktop you can change general Polar Help Desk settings.

View Settings

View settings define the size of different web popups and the number of rows in the grids. Settings can be changed on:

- Desktop
- Web popup (when viewing item data, like groups, users etc.)
- Web find popup (when searching for existing items, for example when adding existing users to a group)

You can change the following view settings:

- number of rows in the grid on the desktop
- number of rows in the grid in the popup web form
- number of rows in the grid in the find popup web form
- size of the popup web form
- size of the popup find web form

Welcome message which appears on the login screen can also be changed in view settings.

Language Management

Polar Help Desk allows it's users to choose among different languages while accessing the web interface. Every user can choose a language for their profile. The languages available are numbered in a combo box on the My Profile form for every user.

Additionally, Help Desk Administrator can set up default languages for every business unit available. On the Business Unit form there is the combo box with available languages listed. After the default language is set up, all the users in that business unit will see web interface in that particular language until they choose their own language from available languages list on My Profile form. If they do not set the particular language, the changing of the Default Business Unit language will affect their web interface language.

On the Language Management popup on the Administration Desktop you can set up the Default Language for Help Desk. This language is set to English (United States) by default, and has the following functions:

- The Login Page is the same for all the users and is in Default language.
- All business units use this language until the specific language is chosen for them.
- All users that are not members of any business unit use this language until they choose specific language to use.

Only Enabled languages can be default for Help Desk, default for business unit or used by particular user. To activate language:

- Choose "Disabled" from the Language Filter combo box.
- Choose the languages you want to enable by checking the check box in the grid.
- Press "Enable Languages" in the toolbar to enable chosen languages.

Please note!

There are currently 159 languages which are available by default in Help Desk. These languages are subjected to automatic updates every time you install a new version of the Polar Help Desk product. Although most of the languages are not defined and are on the Disabled list, you should not update them on your own. The reason for this is that any of these languages might be available in some future versions of Polar Help Desk as Enabled and fully defined languages. Then, when the upgrade of the product is performed all the translations you have made to that particular language, will be overwritten.

It is also recommended to export the custom languages you actively use to an XML file each time you perform the upgrade of the product. This way you will backup all the work.

In order to create a new, custom language which will not be subjected to upgrade changes, do the following steps:

1. Export English (United States) language from the list of all languages by checking the check box in the grid and pressing Export Languages button in the toolbar.
2. Downloaded the XML file to the disk
3. Open it in notepad or some XML editor.
4. Change this tag (on the top):
<language name="English (United States)" description="English Language">
In order to define new language name, like this:
<language name="My Language" description="My Custom Language">

The step above is not necessary, because you can set the language name latter. However, if you forget to set the language name latter, you can update the English (United States) by accident. It is recommended to change this tag information as soon as possible.

5. Translate all the strings in the XML file by changing all the strings between <value> and </value> tags. Translate the English (United States) strings, for example:

Change

```
<data id="Administration_Users" type="System.String">  
  <value>Users</value>  
</data>
```

to

```
<data id="Administration_Users" type="System.String">  
  <value> Utilisateurs</value>  
</data>
```

6. Translate all the strings.
7. Save the XML.
8. On Administration Desktop > General > Language Management press Import Language button in the toolbar.
9. Find the XML file with new language on the disk using the Browse button.
10. Enter the new name for the Language in the New Language Name textbox. If you have defined language name in the XML file in the step 3, you can leave this field empty.

If the import is completed successfully, the new language is in the list of Enabled languages and it is ready for use.

Please note!

When upgrading Polar Help Desk product, always have in mind that new strings may have appeared since the last version you installed it. Until you translate these new strings for the languages your users use, they will be displayed in English (United States).

In order to upgrade or change an existing language, do the following steps:

1. Export the language you want to upgrade (or change) to an XML file.

2. Edit the XML file by changing the strings available. It is very important NOT to change the tag `<language name="My Language" description="My Custom Language">` because it contains information of the language which will be updated later.
3. Scroll to the bottom of the XML language file and find if there are any new strings for translation available. The new strings, if there are any, are always added on the bottom of the XML language file when the language is exported.
4. Import changed XML file the same way you would create a new language. The language with name specified within the tag `<language name="My Language" description="My Custom Language">` will be updated.

Importing Language from RESX file

From version 4.1.0 Polar Help Desk does not require RESX file in order to work properly. This file was used for language settings storing. In order not to lose your work and language translations, import the RESX file into Help Desk. To import language from a RESX file which was used in earlier versions of Polar Help Desk, do the following steps:

1. On Administration Desktop > General > Language Management press Import Language button in the toolbar.
2. Find the RESX file with language on the disk using the Browse button.
3. Enter the new name for the Language in the New Language Name textbox.
4. If the import is completed successfully, the new language is in the list of Disabled languages because it does not contain all the necessary strings.
5. Find the language on the Disabled list using the Language Filter.
6. Export the language. The export format is XML.
7. Find XML file on the disk and translate all the new strings available. The new strings are always available on the bottom of the XML file.
8. On Administration Desktop > General > Language Management press Import Language button in the toolbar.
9. Find the XML file you have just edited on the disk but do NOT fill the New Language Name textbox.
10. If the import process is successfully finished, the language has been upgraded.

SMTP Server Settings

You can modify the following settings for E-mail sending:

Outgoing E-mail server and port number
Sender E-mail address that you want to be displayed when users receive E-mail notifications

Example:

Outgoing E-mail Server:	mail.polarsoftware.com
Outgoing E-mail Server Port Number:	25
Sender E-mail Address:	<u>support@polarsoftware.com</u>

E-mail is by default disabled. In order to allow you staff to receive any email notifications you have to enter valid SMTP server data and to enable email sending.

POP3 Server Settings

Polar Help Desk allows you to open new incident or to update an existing one by sending a simple E-mail to a defined E-mail address.

To enable this feature you must do the following:

enter an E-mail server and a port number to read received E-mails from

specific E-mail account username and password

Example:

Incoming E-mail Server: pop.polarsoftware.com
Incoming E-mail Server Port Number: 110
Server Username: support@polarsoftware.com
Server Password: password

POP3 Delivery Settings

After receiving E-mail from POP3 server you can either choose to delete it immediately or leave it on server for a number of days (or indefinitely).

E-mail Automation Modes

You can choose different modes of work when opening incidents from E-mails.

- *Automation Disabled* – Polar Help Desk does not perform any E-mail automation, in other words the E-mail is not received at all.
- *All E-mails are being moved to waiting list* – any E-mail received from POP3 server is sent to the waiting list. The staff must perform E-mail publishing manually from the waiting list.
- *Smart Mode: E-mails from Existing users are being registered as Incidents* – if the email from which the email is sent is found in the database a new incident is opened, if it isn't, the E-mail goes to the waiting list.
- *Smart Mode with User Registration: All E-mails are being registered as Incidents* – Any E-mail received from POP3 server is opened as incident. Please note that using this mode you risk opening incidents from junk E-mail and spam because no authentication is performed.

Updating Incidents

The following two E-mail smart modes allow you to update incidents that are already opened in Help Desk:

- Smart Mode: E-mails from Existing users are being registered as Incidents
- Smart Mode With User Registration: All E-mails are being registered as Incidents

If one of these modes is on and a service user replies to an E-mail notification from Help Desk (see chapter "Service Level Management") the corresponding incident will be updated.

Please note that any incident which receives update in this way it automatically changes status to "New" in order for the staff to detect and control this change.

Use case:

- Administrator configures SMTP and POP3 settings of the Polar Help Desk in such way that the "Sender E-mail Address" and the "Server Username" are the same – pointing to the same email account.
- Service User received E-mail notification that the his incident has changed it's status to resolved (E-mail Title: "Incident status for incident [ID: 3] has been changed to Resolved")
- Service User sends the reply to the E-mail notification. The title must be left unchanged with eventual prefixes ("RE: Incident status for incident [ID: 3] has been changed to Resolved") and the E-mail address of the service user must be the same one he or she received notification to.
- When the Polar Help Desk Scheduler reads the emails from the POP3 server, Polar Help Desk recognizes the ID of the incident and the E-mail of that particular service user. If these two conditions are fulfilled, the incident with ID: 3 can be updated.

- If the service user replies using some other email account, the incident will be treated as a new one and processed accordingly.
- If the service user replies and changes E-mail notification title, the incident will be treated as a new one and processed accordingly.

Please note!

In order to update incident, the E-mail received has to fulfil both of the following conditions:

- unchanged title of the notification email with eventual prefixes
- E-mail sending account must be the same as the E-mail account of the service user (this incident owner) in the Polar Help Desk database

This way it is assured that service users can update only their own incidents.

How to Start Receiving E-mails from POP3 Server

In order for Polar Help Desk to receive E-mail you can either wait for the scheduler or force the scheduler manually (see the chapter below: Scheduler Settings). Either way, Help Desk will start to receive E-mails unless the "Automation Disabled Mode" is on.

Scheduler Settings

If enabled, scheduler periodically escalates incidents' priority. If disabled, eventual escalations and E-mail receiving are not performed. As the scheduler performs actions after specific period of time, incident priority can sometimes be incorrect. If so, the scheduler can be forced to perform escalation. After this action, incidents' priorities will be accurate.

File Automation

Polar Help Desk allows you to open a new incident simply by copying an xml file in the directory defined in this tab (XML File Automation Directory filed). The scheduler periodically checks if there are new files in the XML File Automation Directory and creates new incidents or edits existing incidents according to the content of that file. When a new incident is open or edited, the xml file is deleted if possible. If the file can not be deleted, the scheduler "remembers" which files it has processed.

The XML file has to be in the following format:

```
<Incident>
  <IncidentID></IncidentID>
  <IncidentTemplate></IncidentTemplate>
  <IncidentTemplateID></IncidentTemplateID>
  <IncidentData>
    <IncidentField1></IncidentField1>
    <IncidentField2></IncidentField2>
    ...
  </IncidentData>
</Incident>
```

By copying xml file to the XML File Automation Directory you can perform the following actions:

1. Register New Incident. To do this you must specify <IncidentTemplateID> or <IncidentTemplateName>. <IncidentID> field must be left empty.
2. Edit Existing Incident. To do this you must specify <IncidentID>. In this case incident templates will not be used but the incident fields will be changed.

<Incident Data> nod can contain the following incident fields:

- Title
- ServiceUserID
- ServiceUser
- IncidentStatusID
- IncidentStatusName
- PriorityID
- PriorityName
- GroupID
- GroupName
- AssigneeID
- Assignee
- ClosureClassificationID
- ClosureClassificationName
- ServiceLevelID
- ServiceLevelName
- IncidentCategoryID
- IncidentCategoryName
- IncidentOriginID
- IncidentOriginName

If for example both GroupID and GroupName are specified in the xml, GroupID has priority over GroupName. This rule applies to all incident fields available, including Incident Templates.

Example:

Create an xml file (the name on the actual file on the disk is not important but the extension of the file must be *.xml) containing xml content below:

```
<?xml version="1.0" encoding="utf-8" ?>
<Incident>
  <IncidentTemplate>Default Incident Template</IncidentTemplate>
  <IncidentData>
    <Title>Incident Number 1</Title>
    <ServiceUserID>2</ServiceUserID>
  </IncidentData>
</Incident>
```

To test this Polar Help Desk feature, copy an xml file to the XML File Automation Directory and then force scheduler (see section Scheduler Settings). After this action is performed, the new incident should be registered in Help Desk and the xml file should be deleted from the XML File Automation Directory.

To edit the incident you have just registered, copy a new xml file containing IncidentID (let us say the IncidentID for the incident we have just created is 35) in the XML File Automation Directory:

```
<?xml version="1.0" encoding="utf-8" ?>
<Incident>
  <IncidentID>35</IncidentID>
  <IncidentData>
    <Title>Incident Number Changed</Title>
    <ServiceUserID>2</ServiceUserID>
  </IncidentData>
</Incident>
```

Force the scheduler and the Incident Title for that particular incident will be changed.

Group Management

Overview

Groups are used to organize users. Users are organized into groups to ease the user management and incident management.

Everyone who uses Help Desk in any way, must be assigned to a group. When a new user is created, he is assigned to "All" group by default and can never be excluded from that group. Thus, the "All" group contains all users at all times. To find out more about users read chapter 4. User Management.

In the "Groups" tab on the Administration Desktop the list of all the existing groups is displayed. There are two columns named "Group Name" and "Description". By clicking the header of each column you can sort the groups. For example, if you click on "Group Name" column the groups will be sorted by their name in ascending order. If you click twice, the groups will be sorted by their name in descending order.

Groups differ in their name which is required and unique. You can never have two groups with the same name or a group with no name. You can also enter description of the group which is optional.

Creating New Group

You can create a new group by clicking "New Group" button.

General Information

When you click "New Group" button, "New Group" form is displayed.

Fill in group data.

The group's name is required and has to be different from existing ones.

Group's description receives any text describing the group. You can enter any information you consider valuable and helpful. The field is optional.

Managing Group's Members

To manage group's users, click the "Members" tab of the "New Group" form.

The groups have their members – users. When a new group is created it is empty, with no users.

One user can be added to multiple groups.

Adding Group Members

If you want to add new members, click "Add Users" button. A new dialog box form is opened.

Filter groups for users or use "Find". Select users from "Available Users" list and add them to "Selected Users".

After clicking "OK" only users in "Selected User" list will be added to the group.

Users added to a group are now listed in “Members” tab of the “New Group” form.

Removing Group Members

Users can be removed from group if you select the users you want to remove and click “Remove” button.

Saving the Group

If you want to save the current data, but continue editing or viewing the data, click “Save” button.

If you want to save and close the form, click “Save&Close” button.

Modifying Group Information

In order to view or modify a group’s data fields and the group’s assignments to different users, click on the particular group. A dialog box will be opened in which you can change the data.

Business Unit Management

Overview

Service Level Agreements are used to assign a particular level of service to particular business units. The first step is to create a SLA which associates a Service to a Service Level. Then, you can add business units which use this SLA. This in fact means that a business unit has certain level of service for a particular service.

If the business unit does not have a SLA defined for a certain service, it is always assigned the default level of service (which is set to a lowest level of service).

Creating New Business Unit

You can create a new business unit by clicking “New Business Unit” button under “Business Unit” tab on Administration Desktop.

To create new Business Unit you must define a Business Unit Name (which is a required field) and other fields you find necessary.

In “Members” tab you can add service users to this business unit. If the chosen user already has a business unit defined, he will no longer be a member of that business unit, but a new one to which we just assigned him to.

Business Units have tree structure, which means they can have their child business units. Under “Child Business Units” tab you can add a business unit a child business unit.

Under “SLA” tab you can add this particular business unit an SLA for a particular service. If the business unit does not have a SLA defined for certain Service, service users who are members of this business unit can only get support using default level of service (which is by default set to a lowest level of service).

Modifying Business Unit Information

In order to view or modify Business Unit's data fields and settings, click on the particular Business Unit. A dialog box will be opened in which you can change the data.

User Management

Overview

Everyone who uses Help Desk has to have his account in “Users” tab on Administration Desktop.

In “Users” tab the list of all the existing users is displayed. There are four columns named “User Name”, “First Name”, “Last Name “ and “E-mail”. By clicking the header of each column you can sort the users. For example, if you click on “Last Name” the users will be sorted by their last name in ascending order. If you click twice, the users will be sorted by their last name in descending order.

When a new user is created, he is assigned to “All” group by default and can never be excluded from that group. Thus, any user is in the “All” group at any time. User can be assigned to multiple groups.

User can also be assigned to multiple roles.

Creating New User

You can create a new user by clicking “New User” button.

The following user fields are required:

- User Name
- Password
- First Name
- Last Name
- E-mail

General Information

When you click “New User” button, “New User” form is displayed.

Fill in the required user data and optional, if you find them useful.

Users and Groups

Every user has groups he is assigned to.

To manage groups the user is assigned to, click the “Groups” tab of the “New User” form. A user can be assigned to one or more groups or just assigned to “All”.

Assigning Users to Groups

If you want to assign user to new groups, click “Add Groups” button. A new dialog box form is opened.

Find groups to which you want to assign the user to. Select groups from “Available Groups” list and add them to “Selected Groups”.

After clicking “OK” only groups in “Selected Groups” list are the ones the user is assigned to.

Groups the user is assigned to are now listed in “Groups” tab of the “New User” form.

Removing User from Groups

User can be unassigned from groups if you select the groups you want to remove and click “Remove” button.

Users and Roles

You can assign single user to multiple roles. To find out more about roles, read chapter 5. Role Management

To manage roles of the user, click the “Roles” tab of the “New User” form.

Assigning Users to Roles

If you want to assign user to new roles, click “Add Role” button. A new dialog box form is opened.

Find roles you want to the user to be assigned to. Select roles from “Available Roles” list and add them to “Selected Roles”.

After clicking “OK” only roles in “Selected Roles” list are the ones the user is assigned to.

Roles the user is assigned to are now listed in “Roles” tab of the “New User” form.

Removing User from Roles

User can be removed from roles if you select the roles you want to remove and click “Remove” button.

Saving the User

If you want to save the current data, but continue editing or viewing the data, click “Save” button.

If you want to save and close the form, click “Save&Close” button.

Modifying User Information

When you click “New User” button, “New User” form is displayed.

Fill in the required user data and optional, if you find them useful.

Importing Users

Users can be imported from:

- a file
- Active Directory

Importing from the File

When importing form a file you must specify the following fields:

- Source File – path to the source file on the disk. The file is uploaded to the server before import takes place.
- Destination Group – group to which the users will be added to (since every user in Help Desk must have at least one group defined)
- Default Role – role to which the users will be added to (since every user in Help Desk must have at least one role defined)

- Column Delimiter. If the field is left blank then column delimiter is the default: tab (t)
- Translation Table, for example:

```
<translation version="1">
  <translate from="FIRSTNAME" to="FirstName"/>
  <translate from="LASTNAME" to="LastName"/>
  <translate from="USERNAME" to="UserName"/>
  <translate from="PASSWORD" to="Password"/>
  <translate from="TITLE" to="Title"/>
  <translate from="EMAIL" to="Email"/>
  <translate from="WEBPAGE" to="WebPage"/>
  <translate from="TELEPHONENUMBER" to="TelephoneNumber"/>
</translation>
```

Importing from Active Directory

When importing from Active Directory you must specify the following fields:

- Active Directory Path (LDAP://server_name/dc=domain_name)
- Active Directory Username and Password (if needed to access Active Directory)
- Active Directory Filter – you can use this filter to get user data:
((&(objectCategory=person)(objectClass=User)(givenname=*)(sn=*)(mail=*)(sAMAccountname=*))
- Destination Group – group to which the users will be added to (since every user in Help Desk must have at least one group defined)
- Default Role – role to which the users will be added to (since every user in Help Desk must have at least one role defined)
- Translation Table – rules to convert data from Active Directory. For example:

```
<translation version="1">
  <translate method="AddDomainPrefix" from="sAMAccountname"
  to="UserName"/>
  <translate from="sn" to="LastName"/>
  <translate from="givenname" to="FirstName"/>
  <translate from="mail" to="Email"/>
</translation>
```

If the “AddDomainPrefix” attribute is present then the DOMAIN_NAME\ prefix will be added in front of the column strings, in this case: UserName. So every UserName will be imported in this form: DOMAIN_NAME\UserName. The DOMAIN_NAME needs not to be defined but is detected automatically.

Enabling NTLM

To enable the NTLM, you need to go to the Control Panel - Administration Tools - Internet Information Services.

Find the virtual folder where Service Desk is installed and browse for the HTTPRequestNTLMLogin.aspx. It should be on this path: PolarHelpDesk – CommonDialogs – HTTPRequestNTLMLogin.aspx.

Right click on this file and select properties. Once the dialog has opened, go to tab File Security and click on the Edit button in the Anonymous access and authentication control. Once the dialog opens deselect all the check boxes you see except the “Integrated windows authentication” check box. Apply the changes and close the Internet Information Services window.

Now, when you go to the Login page, you will notice that your windows login name is already set as the username. Provided that this username also exists in the Help Desk database, all you need to do is click the login button.

Role Management

Overview

Roles are used to define a set of permissions. After a set of permissions for a certain role has been defined, specific users can be assigned to a group. To find out more about users, read the chapter 4. User Management.

In "Roles" tab the list of all the existing roles is displayed. One role field is displayed as column: "Role Name". By clicking the header of the column you can sort the roles by their name. If you click on "Roles Name" column the roles will be sorted by their name in ascending order. If you click twice, the roles will be sorted by their name in descending order.

Roles differ in their name which is a required field and the role permission set. You can also enter description of the role which is optional.

Creating New Role

You can create a new role by clicking "New Role" button.

General Information

When you click "New Role" button, "New Role" form is displayed.

Fill in role data.

Role's description receives any text describing the role. You can enter any information you consider valuable and helpful.

Setting Items Permissions

The most important part of creating a role is defining a set of its permissions. Before you assign any users to a role, you have to define a set of permissions on items in Polar Help Desk.

You can set permissions on items in Item tab of the "New Role" form.

Polar Help Desk Items

The items you can set permissions on are the following:

- Help Desk Desktop
- Incident Management Desktop
- Reports Desktop
- Administrator Desktop
- Incident Form
- User Form
- Work Order Form

The items above have their child entities you can also set permission to.

Items Permissions

Items in Polar Help Desk have the following set of four permissions:

- Create Item Permission - permission to create new item,
- Read Item Permission - permission to view the contents of an existing item,
- Update Item Permission - permission to update an existing item,
- Delete Item Permission - permission to delete item.

However, you cannot set all of these permissions on every item. For example, the only permission you can set on "Administration Desktop" item is the "Read" permission. Therefore, no user can create, delete, or update this item; it can only be allowed to be seen.

In "New Role" form, you can not set permissions whose check boxes are grey coloured.

Roles and Users

You can assign multiple users to single role. To find out more about users, read chapter 4. User Management

To manage users that are assigned to a role, click the "User" tab of the "New Role" form.

Assigning Users to Roles

If you want to assign new users to a role you have just defined permissions for, click "Add Users" button. A new dialog box form is opened.

Find users you want to assign to the role. Select users from "Available Users" list and add them to "Selected Users".

After clicking "OK" only user in "Selected Users" list are the ones assigned to the role.

Users that are assigned to the role are now listed in "Users" tab of the "New Role" form.

Removing User from Roles

User can be removed from a role if you select the users you want to remove and click "Remove" button.

Assigning Templates to Roles

A different set of templates can be assigned to a certain role, both Incident Templates and Work Orders. Users in certain role can only use templates they have permissions on. They cannot see other templates. Any new template created is automatically assigned to the Administrator role. They can however later be removed.

Saving the Role

If you want to save the current data, but continue editing or viewing the data, click "Save" button.

If you want to save and close the form, click "Save&Close" button.

Modifying Role Information

In order to view or modify a role's data fields, permissions and the users assigned to this role, click on the particular role. A dialog box will be opened in which you can change the data.

Service Management

Overview

Support on your Help Desk can be provided for different services. Based on available services you can define different Service Level Agreements for your internal and external customers, for a particular service.

You can manage Services on the Administration Desktop. Choose “SLM” tab in left menu and then choose “Services” tab in content panel.

Creating New Service

You can create a new Service by clicking “New” button – the “New Service” form is displayed.

Service Name should be defined and the Description is an optional field. Service can be blocked by unchecking the Active check box on the form. A blocked Service will not appear in other forms in Polar Help Desk.

Modifying SL Information

In order to view or modify Service’s data fields and Service’s settings, click on the particular Service. A dialog box will be opened in which you can change the data.

Service Level Management

Overview

Service Level (SL) Management in Polar Help Desk allows defining different Service Levels which are associated with incidents when incidents are registered.

Service Level encapsulates:

- Levels of service based on days and hours of service availability.
- E-mail notifications. These are notifications to specific users which can be sent throughout the life-cycle of the incidents the SL is associated with (in other words, certain users are being notified about incident status).
- Priority Escalation Time Limits. It is necessary to define a set of rules for the escalation of the priority of the incidents the SL is associated with. These rules are defined in terms of the SL time limit necessary for the incident to increment its priority (for example the time necessary for the incident to change its priority from low to medium).
- Set of notifications to specific users which are sent when the priority of the incident associated with the SL changes.

You can manage Service Levels on the Administration Desktop. Choose "SLM" tab in left menu and then choose "Service Levels" tab in content panel.

The default SL must be defined.

Creating New SL

You can create a new SL by clicking "New" button.

General Information

When you click "New" button, "New Service Level" form is displayed.

Fill in Service Level data.

The SL's name is required field.

SL's description receives any text describing the SL. You can enter any information you consider valuable and helpful. The field is optional.

Operation Time Settings

Click the "Operation Time" tab to define operation time settings.

Settings in this tab allow you to set the days and hours when the incident escalation should apply, and to set the specific days on which the escalation does not apply. Blocked dates are typically used to designate holidays. These settings should be updated every year.

Setting hours of operation

By checking the days in the week you can decide to which days the incident escalation applies. Working hours are the hours between "Starts At" and "Ends At".

Adding a blocked date

To add a blocked date click "Choose Blocked Date" button and a calendar is displayed. Select a date and click OK. Selected date is in the blocked date list below.

Removing a blocked date

Select the date in the blocked date list you want to remove and click "Delete" button. The deleted date will disappear from the list.

Notification Settings

Click the "Notifications" tab to define notifications that are sent throughout the life-cycle of the incidents the SL is associated with. Notifications are sent by email.

Use this form to determine who will receive the notification e-mail message on the following events:

- When the incident is created.
- When the incident is reassigned to a different support representative.
- When the incident is reassigned to a different support group.
- When the incident is updated.
- When the incident status changed (any status can be chosen).

Selecting individuals/groups to be notified

All the individuals who can receive notification message on a particular event are displayed in the list.

Click on the individual you want to select. In order to select more persons, use Ctrl key. To select more individuals in a range hold down Shift key.

All the selected individuals will be displayed in blue colour.

Notifications can be sent to the following users (which are enumerated in the list boxes):

- *Service User* (user who created the incident)
- *Current Assignee* (a support representative who currently works on the incident)
- *New Assignee* (This notification is only sent when reassignment is performed. The notification is sent to the support representative who will be working on the incident when the reassignment takes place)
- *Old Assignee* (This notification is only sent when reassignment is performed. The notification is sent to the support representative who was previously working on the incident)
- *All Assigned Group Members* (The notification is sent to all support representatives in the group of the currently assigned support group)
- *All New Assigned Group Members* (This notification is only sent when group reassignment is performed. The notification is sent to all support representatives in the support group which will be assigned to the incident when the reassignment takes place.)
- *All Old Assigned Group Members* (This notification is only sent when group reassignment is performed. The notification is sent to all support representatives in the previously assigned support group.)

Incident Priority Escalation Settings

Click the "Priority Escalation" tab to define SL time limits for each priority escalation the notifications that are sent when a priority changes for the incidents the SL is associated with. Notifications are sent by email.

Every incident is created from an incident template. A starting priority of the incident is defined by that incident template.

Priority escalation takes place every time the SL escalation period for a certain priority exceeds. Therefore, for every available incident priority an SL time limit must be defined. After that period, incident priority is incremented. When the incident priority has reached "High" priority, there is no further escalation is performed. Thus, incident maintains in "High" priority until resolved.

You enter the time in hours how long incident can be in a particular priority level before it is escalated to the next. You have to enter the SL time limit value for all the priority levels.

Selecting individuals/groups to be notified

You can also define notification rules for every priority escalation. When incident changes its priority, the notification is sent.

All the individuals who can receive notification message on a particular event are displayed in the list.

Click on the individual you want to select. In order to select more persons, use Ctrl key. To select more individuals in a range hold down Shift key.

All the selected individuals will be displayed in blue colour.

Notifications can be sent to the following users (which are enumerated in the list boxes):

- Service User (who created the incident)
- Current Assignee (a support representative who currently works on the incident)
- All Assigned Group Members (the notification is sent to all support representatives in the group of the current assignee)

Saving SL

If you want to save the current data, but continue editing or viewing the data, click "Save" button.

If you want to save and close the form, click "Save&Close" button.

Modifying SL Information

In order to view or modify SL's data fields and SL's settings, click on the particular SL. A dialog box will be opened in which you can change the data.

Service Level Agreement Management

Overview

Service Level Agreements are used to assign a particular level of service to particular business units. The first step is to create a SLA which associates a Service to a Service Level. Then, you can add business units which use this SLA. This in fact means that a business unit has certain level of service for a particular service.

If the business unit does not have a SLA defined for a certain service, it is always assigned the default level of service (which is by default set to a lowest level of service).

Creating New SLA

To create new SLA you must define the following fields in the "New SLA Form":

- SLA Name
- Service
- Service Level

Now you can add business units which use this SLA in the "Business Units" tab.

Modifying SLA Information

In order to view or modify SLA's data fields and SLA's settings, click on the particular SLA. A dialog box will be opened in which you can change the data.

Incident Template Management

Overview

Incident templates are used by Help Desk personnel while creating new incidents. When registering an incident, a member of Help Desk staff may use existing incident templates with predefined fields:

- Incident Title (defining title for the new incident)
- Service User (person who raises an incident)
- Incident Status (defining initial status of the incident)
- Incident Priority (defining initial priority of the incident)
- SL (which is associated with the incident)
- Incident Category (defining status of the incident)
- Incident Origin (defining origin of the incident)
- Incident Closure Classification (defining closure classification of the incident)
- Assignment to Group (to which incident will be assigned to)
- Assignment to User (to which incident will be assigned to)

You can also add attachments to a template. The attachment will be added to any incident created from that template.

Resolution

Benefits of incident templates:

- Providing resolutions to common incidents. Creating a number of incident templates, you can shorten the time the Help Desk personnel need to resolve incidents which occurs more often than the others.
- Setting desired data fields for certain incidents. For example, incidents from certain service user should always have a specific SLA. Therefore, using incident template with the "Service User" and "SLA" fields well defined, you can assure a specific SLA for that service user.
- Assigning incidents to a specific group of support representatives.
- Assigning incidents to a specific support representative (specific user).

In the Templates tab the list of all the existing incident templates is displayed. One Incident Template field is displayed as column: "Template Name". By clicking the header of the column you can sort the incident templates by their name. If you click on "Template Name" column the incident templates will be sorted by their name in ascending order. If you click twice, the incident templates will be sorted by their name in descending order.

Creating New Incident Templates

You can create a new incident template by clicking "New Incident Template" button. "New Incident Template" form is displayed.

A new dialog box is opened.

The incident template's name is required field.

Saving the Incident Template

If you want to save the current data, but continue editing or viewing the data, click "Save" button.

If you want to save and close the form, click "Save&Close" button.

Modifying Incident Template Information

In order to view or modify an incident template's data fields, click on the particular incident template and a dialog box will be opened with all the data for you to update it.

Work Order Template Management

Overview

Work order templates are used by Help Desk personnel while creating new work orders. When creating a work order, a member of Help Desk staff may use existing work order templates with predefined fields:

- Work Order Title (defining title for the new work order)
- Work Order Status (defining initial status of the work order)
- Work Order Priority (defining initial priority of the work order)
- Assignment to Group (to which work order will be assigned to)
- Assignment to User (to which work order be assigned to)

In the Templates tab the list of all the existing incident templates is displayed. One Incident Template field is displayed as column: "Template Name". By clicking the header of the column you can sort the incident templates by their name. If you click on "Template Name" column the incident templates will be sorted by their name in ascending order. If you click twice, the incident templates will be sorted by their name in descending order.

Description

In the description field you can enter the description for the amount of work the work order requires.

Use case:

If the work orders are often repeated in you company, you might consider creating a number of work order templates containing information for the particular amount of work. Thus, the repeated work descriptions are avoided when a new work order is created from that template.

Creating New Work Order Templates

You can create a new work order template by clicking "New Work Order Template" button. "New Work Order Template" form is displayed.

A new dialog box is opened.

The work order template's name is required field.

Saving the Work Order Template

If you want to save the current data, but continue editing or viewing the data, click "Save" button.

If you want to save and close the form, click "Save&Close" button.

Modifying Work Order Template Information

In order to view or modify an work order template's data fields, click on the particular work order template and a dialog box will be opened with all the data for you to update it.

Incident Data

Administering Incident Category

Overview

In “Incident Data” tab you can administer Incident Categories. You are allowed to define multiple incident categories which will be used by customers or Help Desk personnel to categorize incidents.

There are no Incident Categories defined by default.

In “Incident Data” tab the list of all existing incident categories is displayed. It consists of two columns: “Incident Category” and “Blocked”. In the first column the names of all existing incident categories are listed.

The “Blocked” column determines whether incident category is disabled (not available) for Service User or Help Desk personnel when new incident is created.

Creating New Incident Category

You can create a new incident category by clicking the “New Incident Category” button.

A “New Incident Category” form is displayed.

The incident category’s name is required and has to be different from existing ones.

To block this incident category check the “Blocked” check box. When blocked, incident category is not displayed to any customers or Help Desk personnel. Administrator can at any time unblock any incident category and make it available for customers or Help Desk personnel.

Saving Incident Category

If you want to save the current data, but continue editing or viewing the data, click “Save” button.

If you want to save and close the form, click “Save&Close” button.

Modifying Incident Category

In order to view or modify an incident category’ data fields, click on the particular incident category and a dialog box will be opened with incident category data for you to update it.

Administering Incident Origin

Overview

When creating new incidents, Incident Origin field defines how incidents are registered.

In “Incident Data” tab you can administer incident origins. You are allowed to define multiple incident origins which will be used by Help Desk personnel when registering incidents or when incidents are being registered automatically.

By default, the following incident origins are defined:

- Unknown
- Web
- Phone
- Automatic Registration

In "Incident Data" tab the list of all existing incident origins is displayed. It consists of two columns: "Incident Origin" and "Blocked". In the first column the names of all existing incident origins are listed.

The "Blocked" column determines whether incident origin is disabled (not available) for Service User or Help Desk personnel when new incident is created.

Creating New Incident Origin

You can create a new incident origin by clicking the "New Incident Origin" button.

A "New Incident Origin" form is displayed.

The incident origin's name is required and has to be different from existing ones.

To block this incident origin, check the "Blocked" check box. When blocked, incident origin is not displayed to any customers or Help Desk personnel. Administrator can at any time unblock any incident origin and make it available for customers or Help Desk personnel.

Saving Incident Origin

If you want to save the current data, but continue editing or viewing the data, click "Save" button.

If you want to save and close the form, click "Save&Close" button.

Modifying Incident Origin

In order to view or modify an incident origin click on the particular incident origin. A dialog box will be opened in which you can change the incident origin data.

Administering Incident Closure Classification

Overview

When closing incidents, Incident Closure Classification field can be defined.

In "Incident Data" tab you can administer incident closure classifications. You are allowed to define multiple incident closure classifications which will be used by Help Desk personnel to classify incidents when closing them.

By default, the following incident origins are defined:

- (None)
- Advice Given
- Bug Reported
- Documentation needs reviewing
- Follow up
- Monitoring Required
- No fault found
- Unknown

In "Incident Data" tab the list of all existing incident closure classifications is displayed. It consists of two columns: "Incident Closure Classification" and "Blocked". In the first column the names of all existing incident closure classifications are listed. The "Blocked" column determines whether incident closure classification is disabled (not available) for Service User or Help Desk personnel when new incident is being closed.

Creating New Incident Closure Classification

You can create a new incident closure classification by clicking the "New Incident Closure Classification" button.

A "New Incident Closure Classifications" form is displayed.

The incident closure classification's name is required and has to be different from existing ones.

To block this incident closure classification check, the "Blocked" check box. When blocked, incident closure classification is not displayed to any customers or Help Desk personnel. Administrator can at any time unblock any incident closure classification and make it available for customers or Help Desk personnel.

Saving Incident Closure Classification

If you want to save the current data, but continue editing or viewing the data, click "Save" button.

If you want to save and close the form, click "Save&Close" button.

Modifying Incident Closure Classification

In order to view or modify an incident closure classification click on the particular incident closure classification. A dialog box will be opened in which you can change the incident closure classification data.