



Configuring Support Representative Functionality

Support Representative functionality controls the features available to support representatives throughout the iSupport application.

Configuration Overview

Basic Configuration

- The iSupport **Setup Wizard** appears when the Desktop is initially accessed by the System Administrator profile; it includes options for creating groups, creating support representative profiles, and assigning support representatives to groups. Those assigned to the Administrators group via the wizard will be available for routing and have access to configuration options, knowledge approvals, and incident data override. Those assigned to the Support group and any other group created by the wizard will only be available for routing.
- In iSupport, **support representative groups** are used in routing, reporting, restricting access to functionality. Support representatives must be assigned to a primary group; when a support representative logs in, the permissions of their primary group will apply. Use the Core Settings | Groups screen to create a support representative group and assign members, roles/permissions, Desktop components, the work items/features involved in global search, work item UI settings, and mySupport chat settings. See [“Configuring Support Representative Groups” on page 3](#) for more information.

You can utilize configured groups and roles with **Active Directory** and **LDAP integration**. See [“Using the Data Source Integration Feature” on page 50](#).

- Use the Core Settings | **Support Representatives** screen to set up a profile and access options for support representatives that will be using iSupport. See [“Configuring Support Representative Profiles” on page 11](#) for more information. In that screen you can:
 - Create **roles with associated permissions** to restrict access to iSupport functionality. You can assign roles/permissions to individual support representatives or support representative groups. Note that if multiple roles are added, all permissions associated with those roles will be in effect for a group. See [“Configuring Roles and Permissions” on page 21](#).
 - Create **locations** for reporting, location-based routing, and setting the display time zone for multiple support representatives. See [“Configuring Locations” on page 44](#) for more information.
 - Create **support centers** to assign support representatives to different areas within a single iSupport installation. For support representatives assigned to a support center, the support center’s time zone will be used for time/date display. See [“Setting Up Support Centers” on page 45](#) for more information.
 - Use the **Active Sessions** screen to display the support representatives currently logged into iSupport. You also can log off a support representative. See [“Monitoring Active and Exceeded Sessions” on page 46](#).

Optional Customization

- Configured roles and permissions will determine whether a support representative can create, edit, and delete a personal or shared dashboard; use the **Dashboards** tab in the Content Manager (accessed via the Desktop Content icon) to add, delete, and rename dashboards and specify dashboard access. You can also use the Save and Push option to automatically add a dashboard to all support representative desktops. See [“Managing Dashboards for Support Representatives” on page 47](#).
- Use the Options and Tools | Customize | **Desktop Settings** screen to set the colors of dashboard elements and Desktop header text, the components that all support representatives can add to dashboards, and the records/features involved in global searches performed by all support representatives. Note that you can use the Support

Representative Group screen to override these settings for members of a support representative group. See [“Managing Components, Colors, Header Text, and Global Search” on page 48](#).

Optional Integration

- Use the **Data Source Integration** screen to utilize Active Directory and LDAP integration as a source for iSupport's Support Representative Profile information. See [“Using the Data Source Integration Feature” on page 50](#) for more information.

Administration

- Utilize **Microsoft® Windows-based authentication** in order for support representatives to bypass the Login prompt for the Desktop. See [“Setting Up Microsoft Windows-Based Authentication for the Desktop” on page 60](#) for more information.
- If you are not using Microsoft® Windows-based authentication with iSupport, use the Options and Tools | Administer | **Security** screen to enable password security options, enter text for the login screen, and configure locks. See [“Configuring Password Complexity, Expiration, and Login Locks” on page 61](#) for more information.

Configuring Support Representative Groups

Use the Core Settings | Groups screen to create support representative groups for functionality such as routing, reporting, and restricting access to iSupport functionality. The Administrators group and the Support group are included by default in iSupport. You can enable Desktop components, the work items/features involved in global search, work item UI settings, and mySupport chat settings for group members.

Note that if a support representative is a member of multiple groups, the settings for the primary group will take effect when the representative logs in; if a support representative is assigned to a group other than their primary group for a work item, the primary group permissions will still take effect for work item functions. If the logged in representative's primary group has a layout as does the selected category for a work item, the Order of Precedence specified for the work item type in the Layouts configuration screen will determine the layout that appears.

Use the Details section to enter a name and description of the group, enable chat, and associate roles.

Details	Group Name	Tier I
Membership	Group Type	IT
Desktop	Enable Customer Chat	On Off
Work Item UI	Description	Reps with first customer contact
Chat		
Associated Roles Effective Permissions		
Add Remove		
<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Applications	Permissions for IT applications

Group Name - Enter the name of the group. This name will appear for selection in views and group-based routing dialogs.

Group Type - Enter a label that can be assigned to multiple groups for reporting.

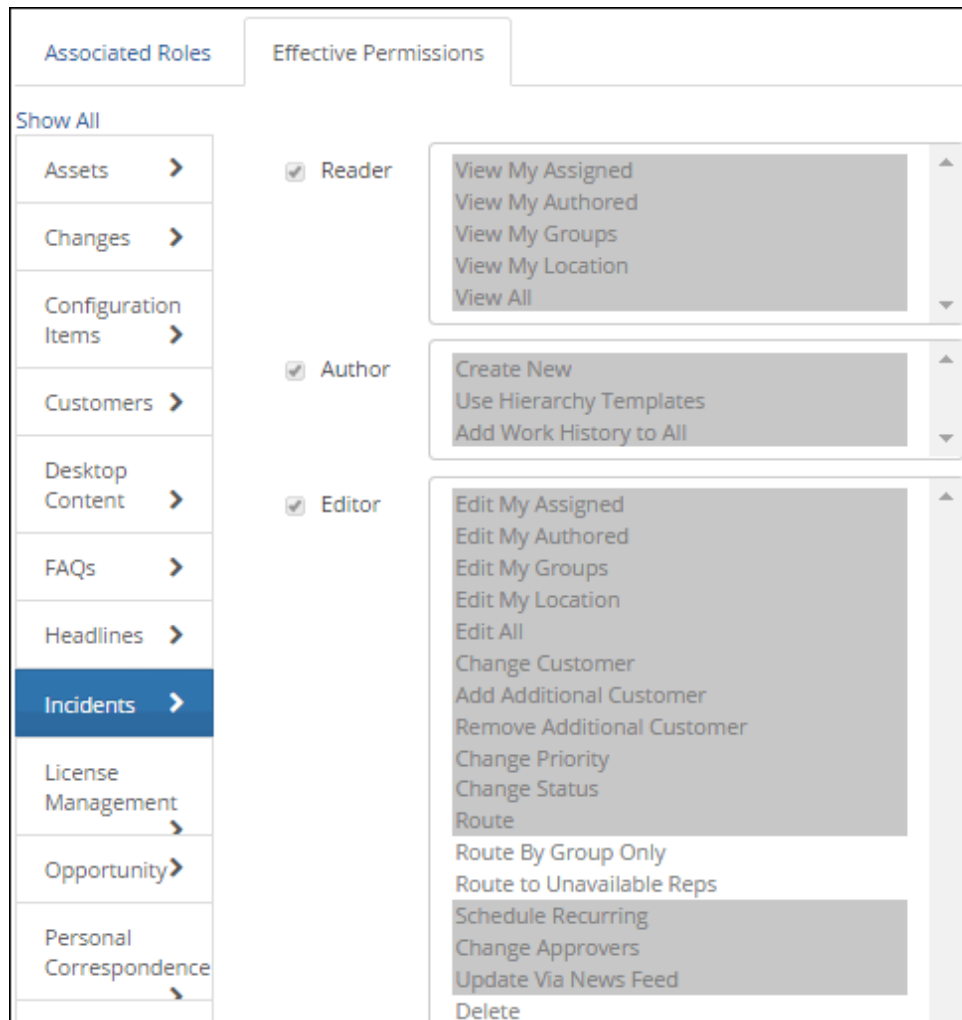
Enable Customer Chat - Select Yes to enable the mySupport Chat section for configuring options for the mySupport Chat feature which enables support representatives to chat with customers using the mySupport portal. See ["Setting Customer Chat Options" on page 9](#).

Description - Enter a description of the group. This description will display in the Group view in the Configuration database.



Associating Roles and Viewing Permissions

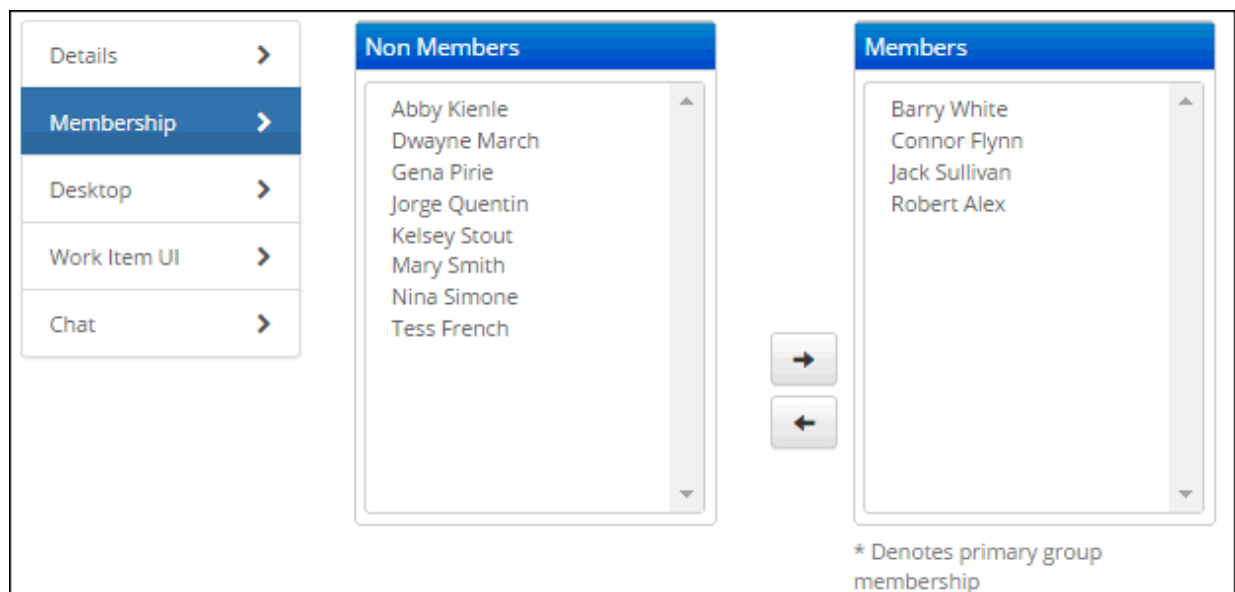
Click the Add link on the Associated Roles section to assign one or more predefined roles to the group. Roles are created with associated permissions via the Roles screen; you can assign roles via that screen, the Rep Profile screen, and the Support Representative Group screen. **Note that if multiple roles are added, all permissions associated with those roles will be in effect for the group.** See ["Configuring Roles and Permissions" on page 21](#) for information on configuring roles.

You can view all of the permissions configured for the associated roles via the Effective Permissions section.



Adding Support Representatives to a Group

Use the Membership section to add support representatives to and remove support representatives from a group via right arrow  icon and left arrow  icons. You can also add support representatives to a group via the Rep Profile screen; an asterisk indicates that the group has been designated as the support representative's primary group in that screen. When a support representative logs in, the permissions of their primary group will apply.



Viewing Desktop Item Access/Specifying Access to Components and Global Search

Use the Desktop section to:

- View the Desktop items (dashboards, views, charts, calendars, and discussion feeds) that the group has access to.

Name ▲	Author	Globally Shared
	System	Yes
All Active Headlines	System	Yes

A Yes in the Globally Shared column indicates that there are no group access restrictions for an item; a No in that column indicates that the item has been restricted via one of the following methods:

- Desktop dashboards: Access option on right-click dashboard menu
- Views: Access field in the View Designer
- Charts: Access field in the Chart Designer
- Event calendars: Rep Groups with Access and Rep Groups with Edit Access fields in the Event Calendars screen
- Specify the available Desktop components and records/features that will be involved when members of the group perform a global search.

Override Allowed Components - Select Yes to override the settings in the Dashboard Settings screen (which designates the components available to all representatives) and use the Allowed Components section to specify available components for members of the group.

Details >

Membership >

Desktop >

Work Item UI >

Chat >

Override Allowed Components

OnOff

Override Allowed in Global Search

OnOff

DashboardsViewsChartsCalendarsEdit Calendars

Allowed Components

Allowed in Global Search

Don't Include:

Cloud Monitor

Twitter Monitor

Twitter

Facebook Monitor

Rep Map

Facebook

CI Relationship Viewer

Embedded Content

Leaderboard

Include:

Global Search ✕

RSS Feed ✕

Pin Board ✕

Calendar ✕

Chart ✕


Asset Monitor ✕

View ✕

Badges ✕

Rep Manager ✕

News Feed ✕

Override Allowed in Global Search - A Global search can be performed via the Global Search component on the Desktop as well as the View |  Search feature in the Incident screen. The types of records and features that are involved in a global search are specified in the Dashboard Settings screen; select Yes to override those settings and

iSupport Software
Page 6

use the Allowed in Global Search section to specify the types of records and features involved in searches for members of the group.

Details >

Membership >

Desktop >

Work Item UI >

Chat >

Override Allowed Components

OnOff

Override Allowed in Global Search

OnOff

DashboardsViewsChartsCalendarsEdit Calendars

Allowed Components

Allowed in Global Search

Don't Include:

Archived Problem

Configuration Item

Archived Purchase

Purchase

Archived Change

Archived Incident

Opportunity

Product

Service Contract

Include:

FAQ

Problem

Knowledge Entry

Change

Customer

Incident

Asset

Google



Discussion Posts







Company

Headline


iSupport Software
Page 7

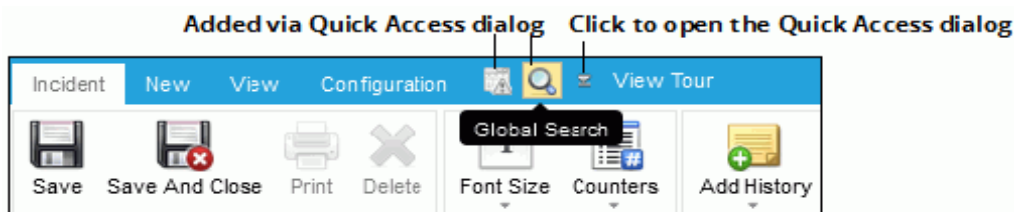
Associating Layouts and Quick Access Icons

Use the Work Item UI tab to assign a layout with fields and tabs as well as a default quick access icon menu that will display when support representatives in the group access the applicable work item entry screen. You can use the Create New  and View/Edit  icons to access the Layouts configuration screen.

Details >	Incident Layout	Tier I Layout ▾	 
Membership >	Incident Default Quick Access Items	Edit	
Desktop >	Change Layout	Default ▾	 
Work Item UI >	Change Default Quick Access Items	Edit	
Chat >	Problem Layout	None ▾	 
	Problem Default Quick Access Items	Edit	
	Purchase Default Quick Access Items	Edit	
	Customer Default Quick Access Items	Edit	
	Company Default Quick Access Items	Edit	
	Asset Default Quick Access Items	Edit	
	Knowledge Entry Default Quick Access Items	Edit	

Depending on the type of work item, a layout can also be associated with a category, customer group, or template; the Order of Precedence link on a section in the Layouts list screen determines which layout to use when more than one reference is applicable (for example, if the logged in rep's primary group has a layout as does the selected category).

Use the <work item> Default Quick Access Items fields to configure a set of quick access icons for commonly-used functions to display in the menu bar at the top of the applicable work item screen by default; this set will be replaced once a user adds icons in those screens via the Open Quick Access Dialog  icon as shown in the example below.



Setting Customer Chat Options

Use the mySupport Chat section to set options for support representatives in the group using the mySupport Chat feature. Note that these options do not apply to the Rep to Rep Chat feature.

Details

Membership

Desktop

Work Item UI

Chat

Auto Create Incident for Accepted Chats **On** **Off**

Incident Template for Chats Incident Created Via Ch: + edit

Max Number of Chats Per Rep 5

Chat Accepted Response Here to Help + edit

Chat Ended by Rep Message The support representative has left the chat.

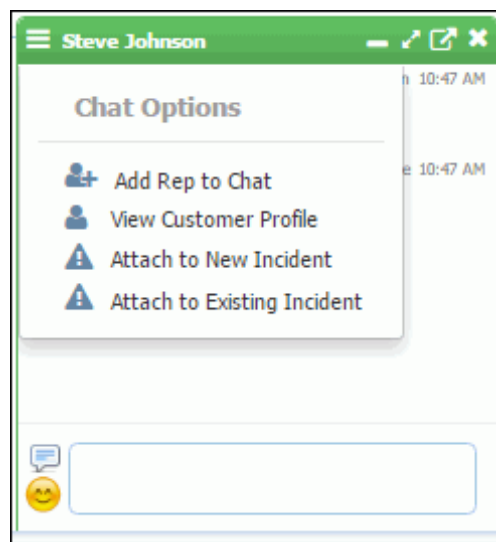
In order for chat requests to appear, double-click in the calendar below to schedule chat availability for each support representative.

today 11/13/2016 - 11/19/2016 Day Week Month

	Sun, 13	Mon, 14	Tue, 15	Wed, 16	Thu, 17	Fri, 18	Sat, 19
all day							
8:00 AM							


Auto Create Incident for Accepted Chats - Select On to automatically create an incident when a support representative in the group accepts a customer chat. If you select Off, the following options will appear in the chat window Options menu:

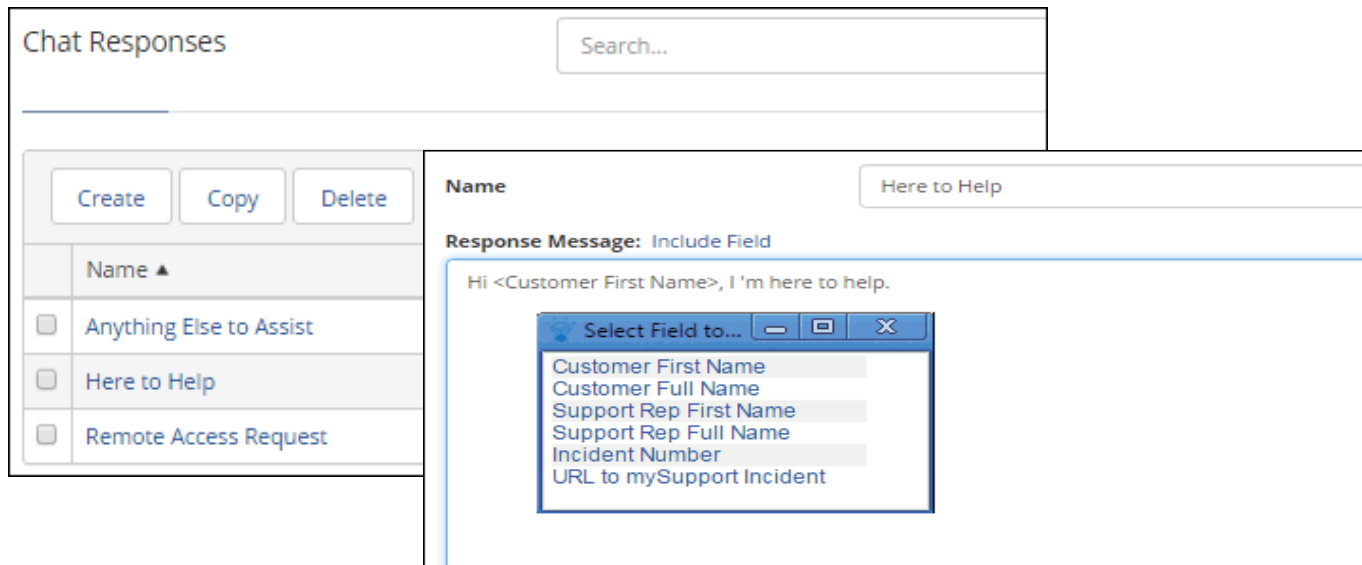
- Attach to New Incident to create a new incident
- Attach to Existing Incident to append the chat history to an existing incident
- View Customer Profile to open the customer's Profile record



Incident Template for Chats - Select or create (via the Create New icon) the incident template to apply to the incident created when a support representative in the group accepts a chat. Note that the template must be made available on the mySupport portal via the Advanced section in the Incident Template screen, and the person who accepts the chat will be assigned to the created incident (not the assignee on the template).

Max Number of Chats Per Rep - Enter the maximum number of accepted chat dialogs that can be open at one time for a support representative.

Chat Accepted Response - Select or create (via the Create New  icon) a mySupport chat response that will appear after the customer's question once you accept the chat. In the mySupport | mySupport Chat Responses screen, enter responses for selection in the customer chat dialog. You can use the Include Field link to add first and full name from the customer and accepting support representative's Profile record, as well as the number and URL of the incident created when the chat is accepted in the Response Message field.



Name ▲	
<input type="checkbox"/> Anything Else to Assist	
<input type="checkbox"/> Here to Help	
<input type="checkbox"/> Remote Access Request	

Response Message: Include Field

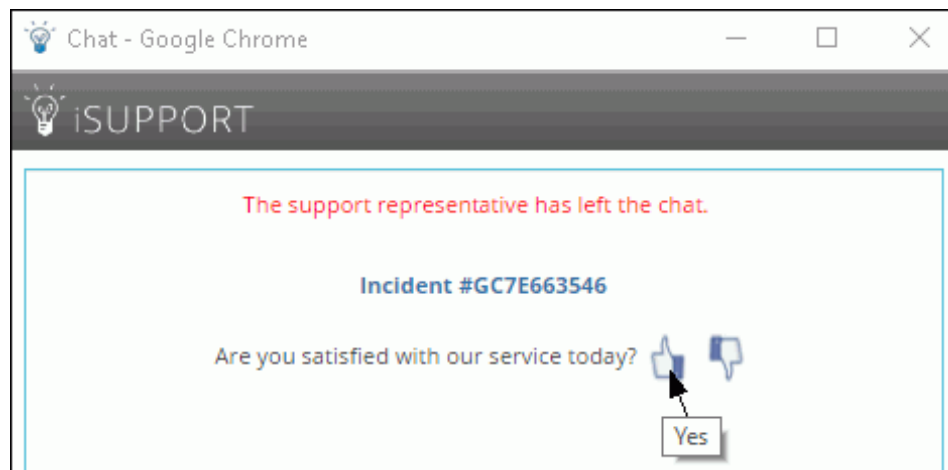
Hi <Customer First Name>, I'm here to help.

Select Field to...

- Customer First Name
- Customer Full Name
- Support Rep First Name
- Support Rep Full Name
- Incident Number
- URL to mySupport Incident

Chat Ended by Rep Message - Enter the message to appear to the customer when the support representative ends the chat.

Request Incident Feedback at End of Chat - Select On to enable display of an incident feedback question (configured via the Feedback tab in the Incident Feature Basics screen) and Comments field at the end of the chat.



Chat - Google Chrome

iSUPPORT

The support representative has left the chat.

Incident #GC7E663546

Are you satisfied with our service today?

Yes

The Comments field will appear after selecting a feedback option.



iSUPPORT

Thanks for your input!


Additional Comment:

Thanks for the prompt attention!

Submit

Configuring Support Representative Profiles

Use the Support Representative Profile screen to set up every person in your organization that will be using iSupport.

Details >	First Name	<input type="text" value="Barry"/>
Advanced	Last Name	<input type="text" value="White"/>
Groups	Email Address	<input type="text" value="bw@example.com"/>
Roles	Pager Email Address	<input type="text"/>
Skills	Phone	<input type="text" value="360-397-1000"/>
Vendor Products	Fax	<input type="text"/>
Calendar	Cellular	<input type="text"/>
Rep Manager Groups	Login	<input type="text" value="BW"/>
	Password	<input type="password"/> Reset
	First Rep to Notify	<input type="text" value="Abby Kienle"/> ▼
	Second Rep to Notify	<input type="text" value="Connor Flynn"/> ▼
	Available for Routing	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Available for Load Balanced Routing	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Available for Round Robin Routing	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Location	<input type="text" value="Headquarters"/> ▼ <input type="button" value="+"/> <input type="button" value="✎"/>
	Support Center	<input type="text" value="External Support"/> ▼ <input type="button" value="+"/> <input type="button" value="✎"/>
	Avatar	 <input type="button" value="New"/> <input type="button" value="Remove"/>

Completing Rep Details

First Name/Last Name - Enter the name of the support representative.

Email Address - Enter the support representative's email address. This address will be used with

Pager Email Address - Enter a secondary address for the support representative.

Phone - Enter the phone number for the support representative.

Fax - Enter the fax number for the support representative.

Cellular - Enter the support representative's cellular phone number.

Login - Enter the support representative's user name for logging into the Desktop. If using Microsoft® Windows-based authentication with iSupport to bypass the iSupport Login prompt, enter the support representative's

Microsoft® Windows user name as follows: *DOMAINNAME\username*. See [“Setting Up Microsoft Windows-Based Authentication for the Desktop” on page 60](#) for more information.

Password - If you are *not* using Microsoft® Windows-based authentication with iSupport, enter the temporary password for logging into the Desktop. (The support representative will be forced to enter a new password after entering his/her username and the temporary password.) The typed characters are masked after a few seconds, but you can copy the masked characters in the field. Password requirements configured via the Administer | Security screen will be enforced; you can use the Generate New link to create a new temporary password that meets the requirements. See [“Configuring Password Complexity, Expiration, and Login Locks” on page 61](#) for more information on configuring password requirements and expiration as well as including a Forgot Password link and formatted text and images in the login dialog.

Note that support representatives can change their password via the Preferences screen (accessed via the Desktop menu).

First Rep to Notify - Select first person to which notifications should be sent regarding iSupport events. "First Rep to Notify" is included in recipient lists used for configuring notifications.

Second Rep to Notify - Select second person to which notifications should be sent regarding iSupport events. "Second Rep to Notify" is included in recipient lists used for configuring notifications.

Available For Routing - Select:

- On to designate the support representative as available for routing incidents, changes, and problems (if enabled).
- Off to designate the support representative as unavailable for routing. (The support representative will not be included in the selection dialog.) Note: Selecting No will exclude (for routing purposes) the support representative from all of the groups in which the support representative is assigned. It will not prevent assignment if a support representative is the default owner of incidents and changes submitted via the mySupport portal, an incident or change template, and email-submitted incidents.
- **Available for Load Balanced Routing** - Select Off to exclude the support representative from those considered for load-balanced routing.
- **Available for Round Robin Routing** - Select Off to exclude the support representative from those considered for round robin routing.

Note that support representatives can change availability via the In/Out link next to their name on the Desktop menu.


Location - Enter locations via the Location tab in the list view that appears. Select the location for the support representative. Locations are used for location-based routing and setting the display time zone for multiple support representatives.

Support Center - If applicable, select the support center for the support representative or leave Default selected to use the support center specified as default in the Support Center screen. The support center's time zone will be used for time/date display.

Avatar - Click the Browse button to select an image to display in news feeds, as well as on the Approvals section in the Incident, Change, or Purchase Request screens if the support representative is an approver in an approval cycle for the record.

Completing Advanced Settings

Details	iSupport Administrator	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Advanced >	iSupport Maintenance Administrator	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Groups	Discussion Feed Administrator	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Roles	Allow Approver Override	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Skills	Allow Data Override	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Vendor Products	Allow Mobile Access Inside Firewall	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Calendar	Mobile Display Option	HTML5 Only ▾
Rep Manager Groups	Allow Mobile Access Outside Firewall	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Available Rep Broadcast	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Display In Awareness	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Display Time Zone	(GMT-08:00) Pacific Time (US & Canada) ▾
	The Display Time Zone is for display purposes only. Business hours escalation and statistics are based on the assignee's support center time zone.	
	Knowledge Approver	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Opportunity Rule Group	None ▾ + ✎
	Vendor	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
	Work Day Hours	Start 8:00 ⌚ End 5:00 ⌚

iSupport Administrator - Select On to enable the Configuration option to appear on the Desktop  menu and in the Preferences dialog for the support representative to use to configure all functionality via the Configuration module. The support representative will also be able to view applicable configuration options in work item screens.

iSupport Maintenance Administrator - Select On to enable the support representative to receive notifications regarding new versions of iSupport, and display the Check for New Versions and Updates option on the Desktop Help menu for the support representative.

Discussion Feed Administrator - Select On to enable the support representative to create a shared feed, change configuration options for any shared feed, and delete or remove discussion feed entries (posts and replies) in the News Feed component on the Desktop. Support representatives without Discussion Feed Administrator access cannot create discussion only feeds; they can only create private feeds with a combination of discussion posts and work items.

Allow Approver Override - Select On to allow the support representative (who may or may not be an approver) to specify a verdict for incidents, changes, and purchases that are pending approval.

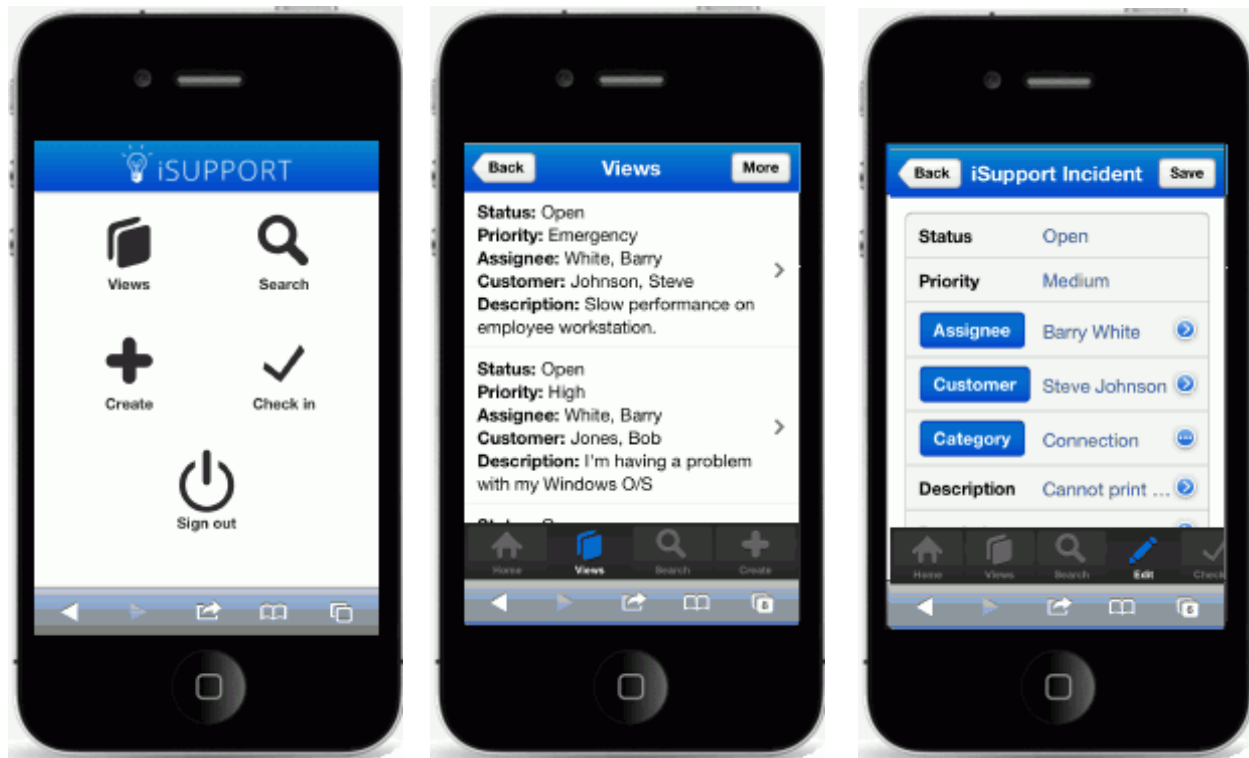
Allow Data Override - Select On to enable the support representative to overwrite fields on any saved or closed incident, problem, change, or service contract. When a change is made using this feature, it will be logged in the Audit History field and notifications will be suppressed. If an approval cycle is in effect and the status is changed to Closed via data override, the cycle will be canceled and notifications will not be sent.

Allow Mobile Access Inside Firewall - Select On to enable the support representative to access iSupport inside the firewall via the iSupport application URL (<http://<server>/Rep/> by default). If accessing iSupport inside the firewall, it must be done via a smart phone or tablet. You can enable a rich work item interface in addition to the HTML5 interface if using a tablet.

Mobile Display Option - If accessing iSupport inside the firewall via a smart phone or tablet, select HTML5 to display the HTML5 interface via a phone or tablet. Select HTML5 & Rich Work Items (Tablet Only) to enable work items to appear in an interface when accessed via a tablet.

Allow Mobile Access Outside Firewall - Select On to enable the support representative to use the Mobile Desktop URL to access iSupport outside the firewall. Note that the Mobile Desktop must be installed via the iSupport setup.exe file.

HTML5 Interface




HTML5 & Rich Work Items (Tablet Only)



Note that only HTML5 layouts configured via the Mobile Settings screen apply to smart phones; other layouts configured via the Layout screen in each module will not apply.

Available Rep Broadcast - If the Rep Broadcast feature is enabled, select On to enable the support representative to display a message to all support representatives or to support representatives in selected groups via the Send Broadcast option on the Desktop menu. Support representatives will need to individually close the message window.

Display in Awareness - The Awareness feature displays an icon  if two or more support representatives have the same record (Incident, Problem, Change, Customer Profile, Company, Asset, and/or Purchase Request record) open. The support representatives can click the icon to display a popup with the names of the support representatives involved, and click on a name to initiate a chat. Select On in this field to enable the support representative to be included in the popup and count on the icon. Note that a support representative without Display in Awareness enabled will still see the popup if other support representatives are in the record.

Display Time Zone - Select the time zone to use for date/time stamps that will display for the support representative. This is for display purposes on the support representative's Desktop client only. If a support representative changes his/her display time zone in the Preferences screen, it will be updated in their Support Representative record.

Knowledge Approver - Select On to allow the support representative to approve or decline knowledge entries and add, change, or delete feedback comments. If No is selected, knowledge approval functionality will not display.

Opportunity Rule Group - If you have the Service Edition and Opportunity Management functionality is enabled, select the opportunity rule group to be applied when the support representative is assigned to an opportunity.

Vendor - Select On to designate the support representative as a vendor, which enables association of Product records for use in purchase requests. This also enables the Vendor Products section to appear in the Rep Profile screen for associating the support representative with Product records.

Work Day Hours - This field appears if Microsoft Office Outlook Calendar and/or Google Calendar integration is enabled. Select the time frame during which you are available to have meetings scheduled via iSupport. (Dates/times outside of work day hours will be designated as "Unavailable" in the calendars displayed via iSupport.) Note that work day hours can also be set in the Desktop Preferences dialog.

Assigning Groups

Use the Groups section to designate the support representative as a member of groups for reporting, group-based routing, and permissions. Support representatives must be assigned to a primary group; when a support representative logs in, the permissions of their primary group will apply. To designate the support representative's primary group, select the group in the No Membership field and click the right arrow ➡ icon next to the Primary field.

The screenshot shows a user interface for assigning groups. On the left, under the 'No Membership' header, there is a list with 'Quality Control' selected. In the center, there are three arrow buttons: a right-pointing arrow at the top, and left and right-pointing arrows at the bottom. On the right, under the 'Membership' header, the 'Primary' field is set to 'Administrators'. Below this, a list contains 'Support (IT)', 'Hardware Repair', 'Tier I (IT)', and 'Trainers'.

When you save the record, you will have the option to push the dashboards associated with the group specified as primary to the support representative's Desktop.

Changing the Primary Group for Multiple Support Representatives

To change the primary group for more than one support representative at one time, select Rep Profiles, use the checkboxes on the left in the Support Reps list screen to select the support representatives, and then click the Change Primary Group link.

The screenshot shows the 'Support Representative' management screen. On the left is a sidebar with 'Profiles' selected. At the top right is a search bar. Below the sidebar, there are buttons for 'Create', 'Export to Excel', 'Change Primary Group', and 'Delete'. A table below these buttons lists support representatives with columns for selection checkboxes, first name, last name, availability, primary group, and locked status.

	First Name ▲	Last Name	Available	Primary Group	Locked
<input checked="" type="checkbox"/>	Abby	Kienle	No	Administrators	No
<input checked="" type="checkbox"/>	Barry	White	Yes	Administrators	No

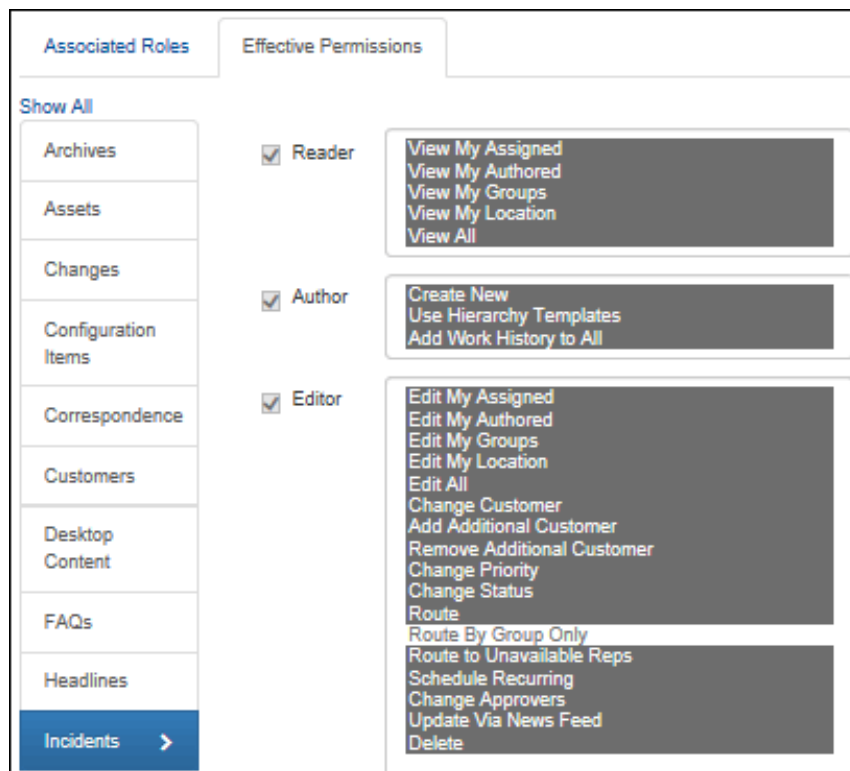
Associating Roles

Click the Add link on the Associated Roles section to assign one or more predefined roles to the support representative. Each role has a set of permissions; you can assign roles to individual support representatives or groups of support representatives. If multiple roles are added, **all** permissions associated with those roles will be in

effect for the support representative. See [“Configuring Roles and Permissions” on page 21](#) for more information on configuring roles.



You can view all of the permissions that will take effect for a support representative via the Effective Permissions section. This will include an aggregate of permissions for roles added to groups in which the support representative is a member as well as permissions for roles added for the individual support representative.

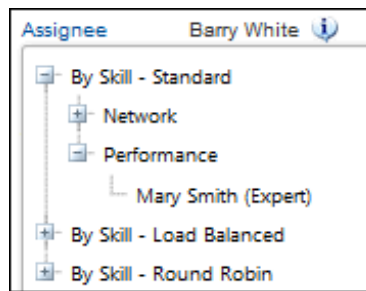


Designating Skills

Use the Skills section to set up skills for skill-based routing of incidents, problems, and changes (if enabled). Skill levels (such as Beginner, Intermediate, Advanced, and Expert for skill levels one through four) are associated with the categories you set up for routing. Enable skill-based routing and label skill levels in the Incident Basics screen. You can also associate support representative skill levels with categories in the Categories screen.

How Skills are Used in Skill-Based Routing

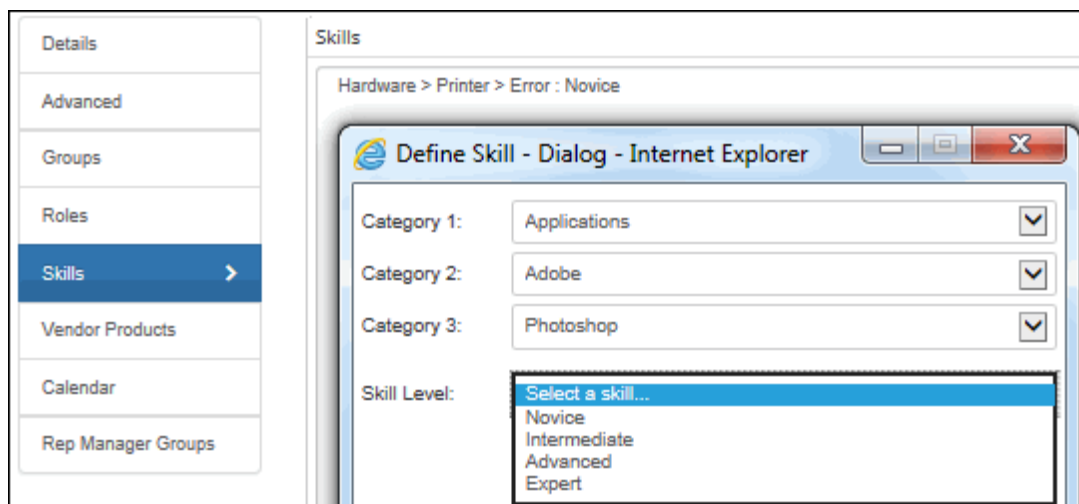
After a support representative classifies the incident, problem, or change (if enabled) and selects skill-based routing, the selected category levels will appear along with the support representative(s) that have those skills configured in their profile.



If using the skill-based/load balanced routing method, after the categorization level is selected, a support representative is selected based on the workload of the support representatives who have the exact match of the selected categorization in their Support Representative record. After a support representative is automatically selected, a dialog displays their name; a Back button is included on that dialog in case the selected assignee is not appropriate. If a support representative has worked with an incident and the incident is reassigned, he/she will be bypassed until all available support representatives with the skill or in the group or location (depending on the method selected) have worked with the incident.

Specifying Skills

Use the Skills section to specify the support representative's skills for skill-based routing feature. To designate a skill, click the Add button on the Skills section. In the Define Skill dialog, select the category set in the Category fields and then select the support representative's skill level for the categories in the Skill Level field. (Skill levels are labeled in the Incident Basics screen.) Click OK. The categorizations and skills appear on the Skills section.



Assigning Vendor Products

After a support representative is designated as a vendor on the Details section, you can associate products with the support representative and make the support representative/associated product combination available for selection on purchase requests. Products that are associated with support representative vendors in the Product screen will appear on this section.

Select an existing asset type and product record, and enter a rate to appear by default in the Purchase Request screen; the rate will be multiplied by the quantity entered in that screen.

The screenshot shows a sidebar with navigation options: Details, Advanced, Groups, Roles, Skills, and Vendor Products (selected). The main area has 'Add' and 'Delete' buttons above a table.

		Asset Type	Name	Rate
<input type="checkbox"/>		Laptop	Documentation	\$ 50.00

Accessing a Support Representative's Calendar

If Microsoft Outlook Calendar and Google Calendar integration is configured, use the Calendar tab to display appointments on a support representative's calendar.

The screenshot shows a sidebar with navigation options: Details, Advanced, Groups, Roles, Skills, Vendor Products, Calendar (selected), and Rep Manager Groups. The main area is titled 'Calendar to add new appointments to:' and has tabs for Google Calendar™, Microsoft® Outlook®, and Both. The calendar view is set to 'WEEK' for '5/29/2016'. A pop-up window shows details for an appointment on Friday, 5/29/2016 at 8am.

Subject:
Working on Incident E8SD686A77

Body:
Working on Incident E8SD686A77. Rep link: <http://csdoc/rep/Incident/Default.aspx?ID=44>
Customer link: <http://csdoc/user/Incident/View/44>
Working on Incident E8SD686A77

Designating Rep Manager Groups

Use the Rep Manager Groups tab to designate the support representative groups that will appear to the support representative in the Desktop Rep Manager component which enables a support representative or administrator to control routing availability. Enable component availability via the Desktop Settings screen.

Select Yes in the Rep Manager Administrator field to enable the support representative to display the Rep Manager and Leaderboard components on the Desktop, and then select the support representative groups that will appear in the Rep Manager component.

The screenshot shows the 'Rep Manager Administrator' configuration window. On the left is a sidebar with a list of menu items: Details, Advanced, Groups, Roles, Skills, Vendor Products, Calendar, and 'Rep Manager Groups' (which is highlighted in blue with a right-pointing arrow). The main area is titled 'Rep Manager Administrator' and features a toggle switch at the top right set to 'On' (green) with an 'Off' button next to it. Below the title are two columns: 'Exclude' and 'Include'. The 'Exclude' column contains a list with 'Tier I (IT)' and 'Trainers'. The 'Include' column contains a list with 'Administrators', 'Support (IT)', 'Quality Control', and 'Hardware Repair'. Between these two columns are two buttons: a right-pointing arrow (→) and a left-pointing arrow (←).

Configuring Roles and Permissions

iSupport's permissions allow or disallow certain types of access to functionality; enable roles to select and assign a set of permissions to individual support representatives or groups of support representatives. This functionality is completely configurable; for example, you could create functionality-related roles, title-related roles (with minimal sets of permissions for beginners and a more advanced set of permissions for managers), etc. If multiple roles are associated with a support representative or group, **all** permissions associated with those roles will be in effect.

After enabling Role functionality in the Core Settings | Global Settings screen, use the Details section in the Roles screen to enter a role name and description and select the permissions for the role. You can assign the role to individual support representatives via the Support Reps section in this screen or the Rep Profile screen. You can assign the role to groups of support representatives via the Groups section in this screen or the Rep Groups screen.

Details	Permissions	Support Reps	Groups
Name	Applications		
Description	Permissions for IT applications		

Assigning Permissions to a Role

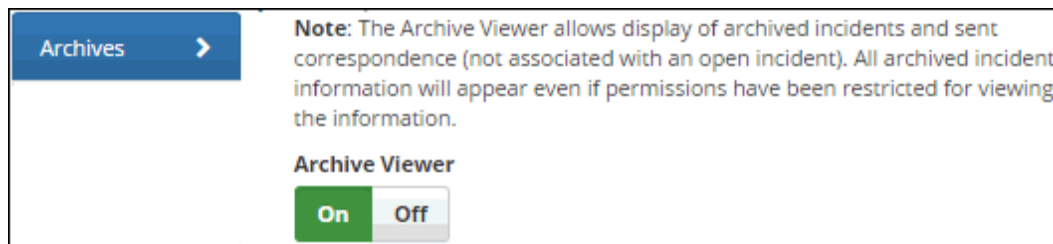
Use the iSupport Permissions section to assign permissions to a role. When you select an option on the left, the applicable fields will display. Use the Select All link to select all permissions, or the Clear All link to deselect all permissions for each option.

With the Reader permissions, functionality will only be allowed for selected permissions. For example, if the View My Assigned permission is selected and the View All permission is not, a support representative will only be able to view his/her assigned incidents. With Author and Editor permissions, if a permission is *not* selected, the function will not display for the support representative. For example, if the Create New option is not selected for incidents, the Create Incident option will not be included on the Desktop menu.

Details	Permissions	Support Reps	Groups
Hide sections without any selected permissions			
Archives >	<input checked="" type="checkbox"/> Reader	<div>View My Assigned</div> <div>View My Authored</div> <div>View My Groups</div> <div>View My Location</div> <div>View All</div>	<div>Select All Incident Permissions</div> <div>Clear All Incident Permissions</div>
Assets >			
Changes >			
Configuration Items >	<input checked="" type="checkbox"/> Author	<div>Create New</div> <div>Use Hierarchy Templates</div> <div>Add Work History to All</div>	
Customers >			
Desktop Content >	<input checked="" type="checkbox"/> Editor	<div>Edit My Assigned</div> <div>Edit My Authored</div> <div>Edit My Groups</div> <div>Edit My Location</div> <div>Edit All</div> <div>Change Customer</div> <div>Add Additional Customer</div>	
FAQs >			
Headlines >			
Incidents >			

Assigning Permissions for Archive Functionality

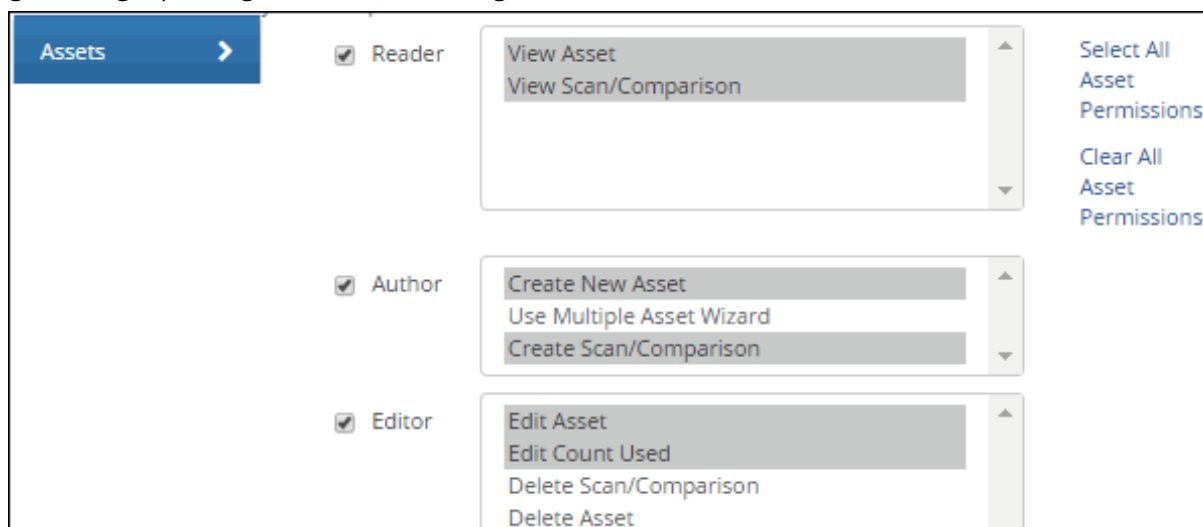
iSupport's Archive feature moves items that are not marked for deletion, with a specified Closed status, to an archive database. In order for an item to be archived, a specified number of days must have elapsed past the close date. Archived items cannot be edited. Select Archives to allow or disallow access to iSupport's Archive Viewer.



Archive Viewer - Select On to include archive views in the list of views available to the support representative for display on the Desktop. Note: the support representative will be able to view all customer and incident information using the Archive option, even if incident permissions have been restricted. This includes archived incidents (with a Closed status that have been moved to an archive data set), archived correspondence (displays archived sent correspondence that was not associated with open incidents), etc.

Assigning Asset Permissions

This option appears if Asset functionality is enabled; select Assets to allow or disallow access to asset functions such as creating, viewing, updating fields, and scanning.



Reader - Click the Reader checkbox to select both permissions or select:

- **View Asset** to allow the support representative to view any Asset record. If this option is *not* selected, all views of Asset records will not be included on the Desktop, and the View Asset option will not be included in the Incident screen. If configured, Asset fields may still be included in the Incident screen with information on an asset associated with an incident.
- **View Scan/Comparison:** Select to allow the support representative to view any Asset Scan Comparison record. If this option is *not* selected, all views of Asset Scan Comparison records will not be included on the Desktop.

Author - Click the Author checkbox to select all Author permissions, or select one or all of the following:

- **Create New:** Select to allow the support representative to create Asset records. If this option is not selected, the Create Asset option will not be included on the Desktop, and the New Asset option will not be included in the Incident screen.
- **Use Multiple Asset Wizard:** Select to include the Asset Creation Wizard on the Create menu on the Desktop Home page for the support representative. The Asset Creation Wizard enables automatic creation of multiple Asset records; you can enter data to populate asset fields in all records created, display prompts for entering data unique to a record, and save your settings in a profile for use later.

- **Create Scan/Comparison:** Select to allow the support representative to perform a scan on non-Windows SNMP-enabled devices in your network, computers with Windows 98 and above, or any other WMI-compliant machine (WMI must be installed and active). You can also perform a scan comparison. If this option is not selected and the support representative has the View permission, he/she can view Asset records but the Scan fields will be disabled.

Editor - Click the Editor checkbox to select all Editor permissions, or select one or all of the following. Note: the View permission is required for these permissions.

- **Edit Asset:** Select to allow the support representative to update Asset records.
- **Edit Count Used:** Select to display the Update Unit Counts link when an asset with count tracking enabled is selected in the Incident, Problem, or Change screen. If this permission is enabled, the support representative can click the Update Unit Counts link, make an entry in the Used Count field, and decrement the unit count.
- **Delete Scan/Comparison:** Select to allow the support representative to delete scan comparisons. If this option is not selected, the Delete option will not be included in the Asset Scan Comparison screen and on the Desktop.
- **Delete Asset:** Select to allow the support representative to delete Asset records. If this option is not selected, the Delete option will not be included in the Asset screen and on the Desktop.

Assigning Change Permissions

This option appears if Change functionality is enabled; select Changes to allow or disallow access to Change functions such as creating, viewing, updating fields, and routing.

The screenshot displays the 'Changes' permissions configuration interface. It features a 'Changes' tab with a right-pointing arrow. Below the tab, there are three roles: Reader, Author, and Editor, each with a checkbox and a list of permissions. The Reader role has a checked checkbox and a list containing 'View My Assigned', 'View My Authored', 'View My Groups', 'View My Location', and 'View All'. The Author role has a checked checkbox and a list containing 'Create New', 'Use Hierarchy Templates', and 'Add Work History to All'. The Editor role has a checked checkbox and a list containing 'Edit My Assigned', 'Edit My Authored', 'Edit My Groups', 'Edit My Location', 'Edit All', 'Change Priority', 'Change Status', 'Change Impact', 'Change Urgency', 'Route', 'Route By Group Only', 'Route to Unavailable Reps', 'Schedule Recurring', 'Change Approvers', 'Update Via News Feed', and 'Delete'. On the right side of the interface, there are two links: 'Select All Change Permissions' and 'Clear All Change Permissions'.

Reader - Click the Reader checkbox to select all Reader permissions, or select one or more of the following:

- **View My Assigned:** Select to allow the support representative to view the Change records to which they are assigned.
- **View My Authored:** Select to allow the support representative to view the Change records they create.

- **View My Groups:** Select to allow the support representative to view those Change records assigned to any member of any group to which the support representative is assigned. Note: the View My Assigned permission is required for this permission.
- **View My Location:** Select to allow the support representative to view those Change records assigned to support representatives in the support representative's location. Note: the View My Assigned permission is required for this permission.
- **View All:** Select to allow the support representative to view any Change record in the iSupport application. Note: All View permissions are required for this permission.

Author - Click the Author checkbox to select all Author permissions, or select one or more of the following:

- **Create New:** Select to allow the support representative to create new Change records. If this option is *not* selected, the Create Change option will not be included on the Desktop menu and the New menu in the Change screen.
- **Use Hierarchy Templates:** Select to allow the support representative to select a hierarchy template for a Change record. If this option is *not* selected, the Use Hierarchy Template icon and menu option will not be included in the Change screen. Note: one of the View permissions and the Create New or Edit permission is required for this permission.
- **Add Work History to All:** Select to allow the support representative to update the Work History field on any Change record that the support representative can view in the iSupport application. This option is not affected by the Editor options; its purpose is to allow you to restrict updates to only the Work History field if needed.

Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note: if a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after the change is initially saved.

- **Edit My Assigned:** Select to allow the support representative to update any Change record to which they are assigned. If this option is not selected, the support representative will not be able to update their assigned Change records. Note: the View My Assigned permission is required for this permission.
- **Edit My Authored:** Select to allow the support representative to update any Change record they create. Note: the View My Authored permission is required for this permission.
- **Edit My Groups:** Select to allow the support representative to update Change records assigned to any member of any group to which the support representative is assigned. Note: the Edit My Assigned, View My Groups, and View My Assigned permissions are required for this permission.
- **Edit My Location:** Select to allow the support representative to update Change records assigned to support representatives in their location. Note: the Edit My Assigned, View My Locations, and View My Assigned permissions are required for this permission.
- **Edit All:** Select to allow the support representative to update any Change record in the iSupport application. Note: The View All permission is required for this permission.
- **Change Priority:** Select to allow the support representative to select a priority for a saved Change record. If this option is not selected, the Priority field will display in the Change screen but the drop-down list will be disabled. Note: one of the View permissions is required for this permission.
- **Change Status:** Select to allow the support representative to select a status for a saved Change record. If this option is not selected, the Status field will display in the Change screen but the drop-down list will be disabled. Note: one of the View permissions is required for this permission.
- **Change Impact:** Select to allow the support representative to make a selection in the Impact field for a saved Change record. If this option is not selected, the Impact field will display in the Change screen but the drop-down list will be disabled. Note: the Impact and Urgency fields cannot be enabled or disabled individually; either enable both or disable both. One of the View permissions is required for this permission.
- **Change Urgency:** Select to allow the support representative to make a selection in the Urgency field for a saved Change record. If this option is not selected, the Urgency field will display in the Change screen but the drop-down list will be disabled. Note: the Impact and Urgency fields cannot be enabled or disabled individually; either enable both or disable both. One of the View permissions is required for this permission.

- **Route:** Select to allow the support representative to assign a Change record to another support representative. If this option is not selected, the Route icon and menu option will not be included in the Change screen and the Assignee link will be disabled. Note: one of the View permissions is required for this permission.
- **Route by Group Only:** Select to restrict the support representative to routing only to other support representatives in his/her assigned group(s). Note: one of the View permissions is required for this permission.
- **Route to Unavailable Reps:** Select to enable the support representative to route to support representatives who are unavailable for routing. Support representatives who are unavailable for routing will be designated as "Out". This only affects manual routing functionality; automated routing initiated from an email, mySupport submission, or by rule using load balancing or round robin methods still includes available reps.
- **Schedule Recurring:** Select to allow the support representative to schedule tickets on a recurring basis for a specified time frame. Note: one of the View permissions is required for this permission.
- **Change Approvers:** Select to allow the support representative to change approvers when an ad hoc approval cycle is initiated.
- **Update Via News Feed:** Select to include the Update link next to changes in the News Feed dashboard component for the support representative.
- **Delete:** Select to allow the support representative to delete Change records. If this option is not selected, the Delete option will not be included in the Change screen. Note: one of the View permissions is required for this permission.

Assigning Configuration Item Permissions

This option appears if Configuration Management (CMDB) functionality is enabled. Select Configuration Items to allow or disallow access to configuration item functions such as creating, viewing, and updating Configuration Item records.

The screenshot displays the 'Configuration Items' permissions configuration screen. On the left, there is a blue header with the text 'Configuration Items' and a right-pointing arrow. Below this, there are three rows, each with a checkbox and a dropdown menu. The first row has a checked 'Reader' checkbox and a dropdown menu showing 'View'. The second row has a checked 'Author' checkbox and a dropdown menu showing 'Create New'. The third row has a checked 'Editor' checkbox and a dropdown menu showing 'Edit' and 'Delete'. To the right of these rows, there are two links: 'Select All Configuration Item Permissions' and 'Clear All Configuration Item Permissions'.

Reader - Click the Reader checkbox or select **View** to allow the support representative to view any Configuration Item record. If this option is *not* selected, views of Configuration Item records will not be included on the Desktop for the support representative.

Author - Click the Author checkbox or select **Create New** to allow the support representative to create new Configuration Item records. If this option is *not* selected, the Create option will not be available to the support representative for Configuration Item records on the Desktop and in the Configuration Item screen.

Editor - Click the Editor checkbox to select both Editor permissions, or select one or both of the following. Note: the View permission is required for these permissions.

- **Edit:** Select to allow the support representative to update Configuration Item records. If this option is *not* selected, the support representative can view Configuration Item records but the fields will be disabled.

- **Delete:** Select to allow the support representative to delete Configuration Item records. If this option is *not* selected, the Delete option will not be included on the Desktop and in the Configuration Item screen for the support representative.

Assigning Customer/Company Permissions

Select Customers to allow or disallow access to customer functions such as creating, viewing, updating fields, and changing mySupport access. Company permissions are tied to these settings; if a support representative has permission to delete a Customer Profile record, he/she also has permission to delete a Company record.

The screenshot displays the 'Customers' permissions configuration interface. It features a blue header with the word 'Customers' and a right-pointing arrow. Below this, there are three sections, each with a checkbox and a dropdown menu:

- Reader:** The checkbox is checked. The dropdown menu is open, showing the option 'View'.
- Author:** The checkbox is checked. The dropdown menu is open, showing the options 'Create New', 'Create New from Change', and 'Create New from Incident'.
- Editor:** The checkbox is checked. The dropdown menu is open, showing the options 'Edit', 'Change mySupport Password', 'Change mySupport Access', 'Unlock mySupport Access', 'Change Unsubscribe Status', 'Merge', and 'Delete'.

On the right side of the interface, there are two links: 'Select All Customer Permissions' and 'Clear All Customer Permissions'.

Reader - Click the Reader checkbox or select **View** to allow the support representative to view any Customer Profile or Company record. If this option is *not* selected, all views of Customer Profile and Company records will not be included on the Desktop, and the View Customer Profile and View Company Profile options will not be included in the Incident screen.


Author - Click the Author checkbox to select all Author permissions, or select one or all of the following.

- Select **Create New** to allow the support representative to create Customer Profile and Company records. If this option is *not* selected, the Create Customer and Create Company options will not be included on the Desktop. The Create Customer option will not be included on the New menu in the Incident screen. Only basic customer information can be entered for a new customer or company in the Select Customer dialog.
- Select **Create New from Change** to allow the support representative to create Customer Profile and Company records only from the Change screen.
- Select **Create New from Incident** to allow the support representative to create Customer Profile and Company records only from the Incident screen.

If the Create New, Create New from Change, and Create New from Incident options are *not* selected, the Create Customer and Create Company options will not be included on the Desktop. The Create Customer option will not be included on the New menu in the Incident and Change screens, and only basic customer information can be entered for a new customer or company in the Select Customer dialog.

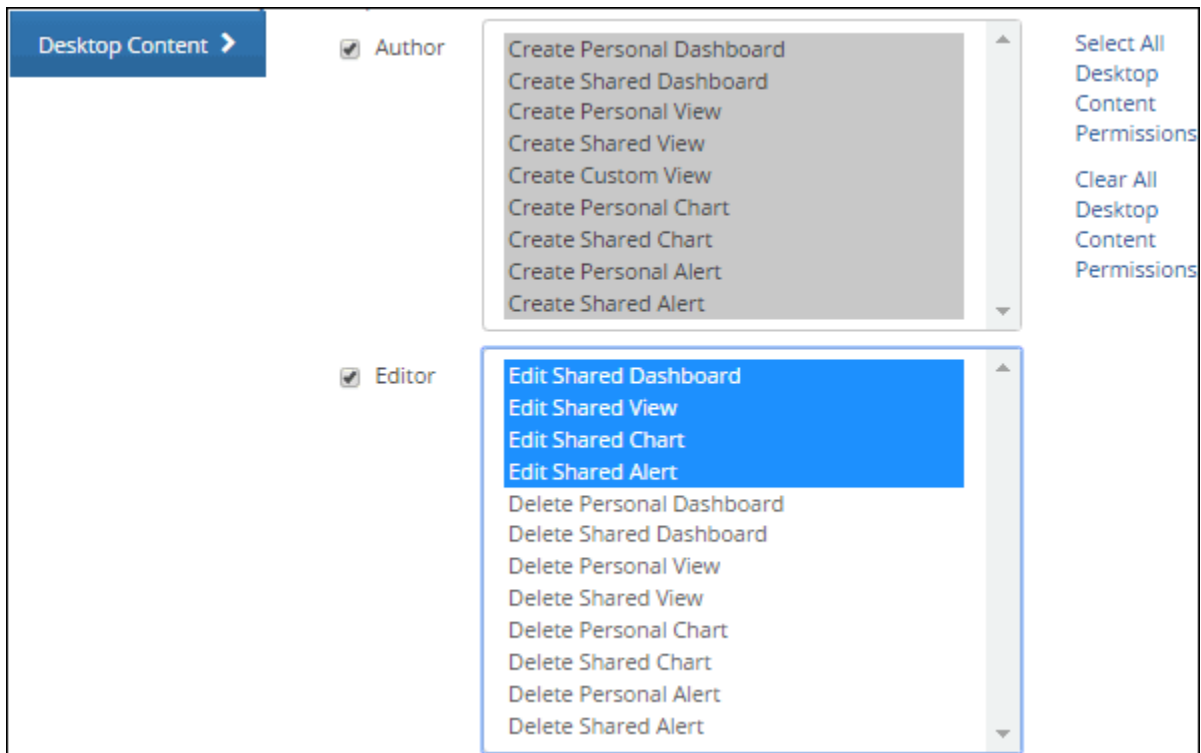
Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note: the View permission is required in order to select any of these permissions. If a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after a Customer Profile or Company Record is initially saved.

- **Edit:** Select to allow the support representative to update Customer Profile and Company records.
- **Change mySupport Password:** Select to allow the support representative to update the mySupport Password field in Customer Profile records. If this option is *not* selected, the mySupport Password field in Customer Profile records will be disabled for the support representative.

- **Change mySupport Access:** Select to allow the support representative to update the mySupport Access field in Customer Profile records. If this option is *not* selected, the mySupport Access field in Customer Profile records will be disabled for the support representative.
- **Unlock mySupport Access:** Support rep locks (configured in the Customer Security screen) prevent a customer from logging in until a support representative unlocks their customer profile. Select this permission to enable the support representative to set the failed login attempt count to zero by clicking the Unlock link that appears in the banner in the Customer Profile screen when a profile is locked, or by selecting the Unlock Access option on the Actions menu in the Locked Customers view.
- **Change Unsubscribe Status:** Select to allow the support representative to change the status in the Unsubscribe Status field in the Customer Profile screen and if the customer has an unsubscribed status the prompt "Customer has unsubscribed from correspondence. Click Continue to proceed." will appear when a correspondence is initiated, and the Include Unsubscribe Text option will be included in the Correspondence screen. If this option is not selected, the Correspondence menu option will be disabled in the Customer Profile and Opportunity screens and the support representative will not be able to send correspondence via the Desktop to a customer with an Unsubscribed status. See ["Configuring Unsubscribe Settings" on page 61](#) for more information.
- **Merge:** Select to display the Merge  icon on the support representative's Desktop company and customer views for using the Customer/Company Merge feature.
- **Delete:** Select to allow the support representative to delete Customer Profile and Company records. If this option is *not* selected, the Delete option will not be included in the Customer Profile and Company screen.

Assigning Desktop Content Permissions

Select Desktop Content to allow or disallow display of the dashboard, view, chart, and alert functionality on the Desktop.



Desktop Content >

☒ Author

- Create Personal Dashboard
- Create Shared Dashboard
- Create Personal View
- Create Shared View
- Create Custom View
- Create Personal Chart
- Create Shared Chart
- Create Personal Alert
- Create Shared Alert


☒ Editor


- Edit Shared Dashboard
- Edit Shared View
- Edit Shared Chart
- Edit Shared Alert
- Delete Personal Dashboard
- Delete Shared Dashboard
- Delete Personal View
- Delete Shared View
- Delete Personal Chart
- Delete Shared Chart
- Delete Personal Alert
- Delete Shared Alert

Select All Desktop Content Permissions

Clear All Desktop Content Permissions

Author -

- **Create Personal Dashboard:** Select to enable the support representative to create dashboards for display on their own Desktop. If this option is not enabled, the Add Personal option will not appear on the dashboard  menu.
- **Create Shared Dashboard:** Select to enable the support representative to create dashboards that are designated as Shared (dashboards that other support representatives can access via the Add Existing option on

the dashboard menu). If this option is not enabled, the Add Shared option will not appear on the dashboard  menu.

- **Create Personal View:** Select to enable the View Designer to appear on the Desktop menu for the support representative.
- **Create Shared View:** This permission requires the Create Personal View permission. Select this option to include the Access field in the View Designer for the support representative. Group members will be able to create personal views that cannot be accessed by other representatives, as well as shared views that can be accessed by other representatives.
- **Create Custom View:** This permission requires the Create Personal View permission. Select this option to include the Design Custom View link in the View Designer for the support representative. The Design Custom View link enables users to access existing custom SQL queries within an iSupport SQL table.
- **Create Personal Chart:** Select to enable the Chart Designer option to appear on the Desktop menu for the support representative.
- **Create Shared Chart:** This permission requires the Create Personal Chart permission. Select this option to include the Access field in the Chart Designer for the support representative. The support representative will be able to create personal charts that cannot be accessed by other representatives, as well as shared charts that can be accessed by other representatives.
- **Create Personal Alert:** Select to, for the support representative, enable the Alert icon to appear in content frames, and the Alert button to appear in the View Designer and Chart Designer.
- **Create Shared Alert:** Select to include the Send To field in the Alert creation screen for the support representative.

Editor -

- **Edit Shared Dashboard:** Select to allow the support representative to change the content of a dashboard that is designated as Shared via the dashboard Access option. Other support representatives can add dashboards designated as Shared to their own Desktops.
- **Edit Shared View:** Select to allow the support representative to change the content of a view that is designated as Shared via the Access field in the View Designer.
- **Edit Shared Chart:** Select to allow the support representative to change the content of a chart that is designated as Shared via the Access field in the Chart Designer.
- **Edit Shared Alert:** Select to allow the support representative to change the settings of an alert configured with specified support representatives in the Send To field.
- **Delete Personal Dashboard:** Select to allow the support representative to delete dashboards designated as personal via the dashboard Access option. Personal dashboards are not available to other support representatives.
- **Delete Shared Dashboard:** Select to allow the support representative to delete a dashboard that is designated as Shared via the dashboard Access option.
- **Delete Personal View:** Select to allow the support representative to delete a view that is designated as Myself via the Access field in the View Designer.
- **Delete Shared View:** Select to allow the support representative to delete a view that is designated as Myself via the Access field in the View Designer.
- **Delete Personal Chart:** Select to allow the support representative to delete a chart designated as Myself via the Access field in the Chart Designer.
- **Delete Shared Chart:** Select to allow the support representative to delete a chart designated as Shared via the Access field in the Chart Designer.
- **Delete Private Alert:** Select to allow the support representative to delete an alert that they have created.
- **Delete Shared Alert:** Select to allow the support representative to delete an alert that is configured to display to support representatives and/or support representative groups (via the Send To field).

Assigning FAQ Permissions

Select FAQs to allow or disallow access to functions such as creating, viewing, deleting for frequently asked questions and the topics by which frequently asked questions are sorted on the Desktop and mySupport portal.

The screenshot shows a web interface for assigning permissions. On the left, there is a blue header with the text 'FAQs' and a right-pointing arrow. To the right of this header are three rows, each with a checkbox and a label: 'Reader', 'Author', and 'Editor'. Each row has a corresponding dropdown menu. The 'Reader' dropdown shows 'View Topic/FAQ'. The 'Author' dropdown shows 'Create New Topic' and 'Create New FAQ'. The 'Editor' dropdown shows 'Edit Topic', 'Edit FAQ', 'Delete Topic', and 'Delete FAQ'. On the far right, there are two links: 'Select All FAQ Permissions' and 'Clear All FAQ Permissions'.

Reader - Click the Reader checkbox or select **View Topic/FAQ** to allow the support representative to view frequently asked questions on the Desktop. If this option is *not* selected, no frequently asked questions will be available to the support representative in predefined views, the View Designer, and the Chart Designer on the Desktop.

Author - Click the Author checkbox to select both Author permissions, or select:

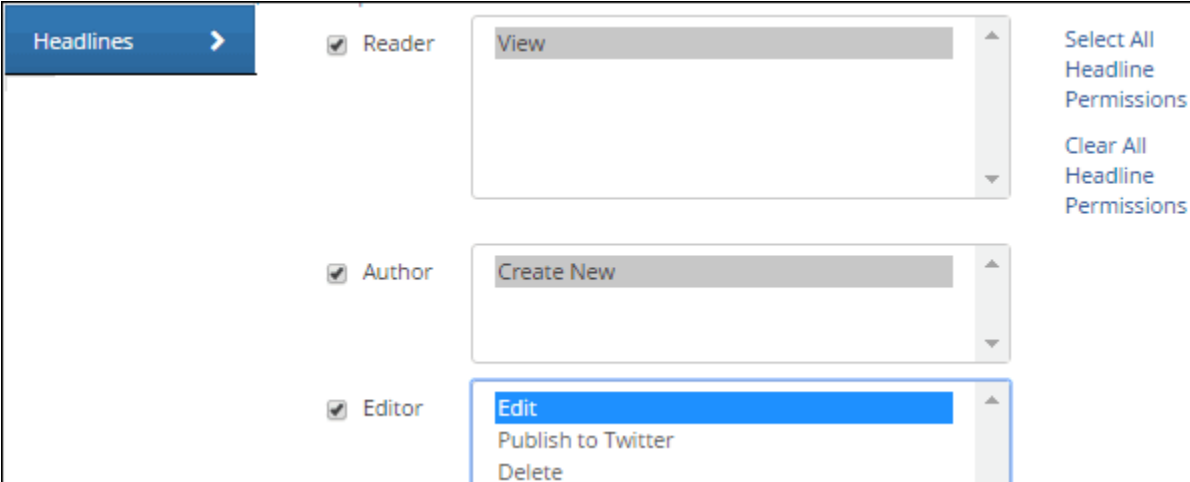
- **Create New Topic** to allow the support representative to create topics for sorting frequently asked questions on the Desktop and mySupport portal. If this option is *not* selected, the Topic field label will not be a link in the FAQ entry screen.
- **Create New FAQ** to allow the support representative to create frequently asked questions. If this option is *not* selected, the FAQ option will not be included on the Desktop menu.

Editor - Click the Editor checkbox to select all Editor permissions, or select one the following. Note: the View permission is required in order to select any of these permissions. If a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after a FAQ is initially saved.

- **Edit Topic:** Select to allow the support representative to update topics (via the Topic link in the FAQ entry screen).
- **Edit FAQ:** Select to allow the support representative to update Frequently Asked Question records.
- **Delete Topic:** Select to allow the support representative to delete topics. If this option is *not* selected, the Delete option will not be included in the Manage FAQ Topics dialog (accessed via the Topic link in the FAQ entry screen).
- **Delete FAQ:** Select to allow the support representative to delete frequently asked question records. If this option is *not* selected, the Delete option will not be included in FAQ views on the Desktop.

Assigning Headline Permissions

Select Headlines to allow or disallow access to functions such as creating, viewing, and deleting headlines.



The screenshot shows a configuration window for 'Headlines' permissions. On the left, a blue header bar contains the word 'Headlines' and a right-pointing arrow. Below this, there are three rows of permissions, each with a checkbox and a dropdown menu. The first row is for 'Reader' (checkbox checked), with a dropdown menu showing 'View'. The second row is for 'Author' (checkbox checked), with a dropdown menu showing 'Create New'. The third row is for 'Editor' (checkbox checked), with a dropdown menu showing 'Edit', 'Publish to Twitter', and 'Delete'. To the right of these dropdowns, there are two links: 'Select All Headline Permissions' and 'Clear All Headline Permissions'.

Reader - Click the Reader checkbox or select **View** to allow the support representative to view headlines on the Desktop. If this option is *not* selected, no headlines will be available in predefined views, the View Designer, and the Chart Designer on the Desktop.

Author - Click the Author checkbox or select **Create New** to allow the support representative to create headlines. If this option is *not* selected, the Create Headline option will not be included on the Desktop menu.

Editor - Click the Editor checkbox to select both Editor permissions, or select one or both of the following. Note: the View permission is required in order to select any of these permissions. If the support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after a headline is initially saved.

- **Edit:** Select to allow the support representative to update Headline records.
- **Publish to Twitter:** Select to allow the support representative to publish headlines to Twitter (if configured via the Social Media Integration screen).
- **Delete:** Select to allow the support representative to delete Headline records. If this option is *not* selected, the Delete option will not be included in the Headline screen.

Assigning Incident Permissions

Select Incidents to allow or disallow access to incident functions such as creating, viewing, updating fields, and routing.

The screenshot displays the 'Incidents' permissions configuration page. It features a sidebar with the 'Incidents' menu item. The main area is divided into three sections for different roles: Reader, Author, and Editor. Each role has a checkbox to select all permissions for that role, followed by a list of specific permissions. The Reader role permissions include 'View My Assigned', 'View My Authored', 'View My Groups', 'View My Location', and 'View All'. The Author role permissions include 'Create New', 'Use Hierarchy Templates', and 'Add Work History to All'. The Editor role permissions include 'Edit My Assigned', 'Edit My Authored', 'Edit My Groups', 'Edit My Location', 'Edit All', 'Change Customer', 'Add Additional Customer', 'Remove Additional Customer', 'Change Priority', 'Change Status', 'Change Impact', 'Change Urgency', 'Route', 'Route By Group Only', 'Route to Unavailable Reps', 'Schedule Recurring', 'Change Approvers', 'Update Via News Feed', and 'Delete'. On the right side, there are two buttons: 'Select All Incident Permissions' and 'Clear All Incident Permissions'.

Reader - Click the Reader checkbox to select all Reader permissions, or select one or more of the following:

- **View My Assigned:** Select to allow the support representative to view incidents assigned to the support representative.
- **View My Authored:** Select to allow the support representative to view incidents created by the support representative.
- **View My Groups:** Select to allow the support representative to view incidents assigned to any member of any group to which the support representative is assigned. Note: the View My Assigned permission is required for this permission.
- **View My Location:** Select to allow the support representative to view incidents assigned to support representatives in their location. Note: the View My Assigned permission is required for this permission.
- **View All:** Select to allow the support representative to view any incident in the iSupport application. Note: All view permissions are required for this permission.

Author - Click the Author checkbox to select all Author permissions, or select one or more of the following:

- **Create New:** Select to allow the support representative to create a new incident. If this option is *not* selected, the Create Incident option will not be included in the Desktop menu and the New menu in the Incident screen.
- **Use Hierarchy Templates:** Select to allow the support representative to select a hierarchy template for an incident. If this option is *not* selected, the Use Hierarchy Template icon and menu option will not be included in

the Incident screen. Note: one of the View permissions and an Edit permission or the Create New permission is required for this permission. This permission does not apply to auto-fill and auto-close templates.

- **Add Work History to All:** Select to allow the support representative to update the Work History field on any incident that the support representative can view in the iSupport application. This option is not affected by the Editor options; its purpose is to allow you to restrict updates to only the Work History field if needed. Note: In the Customer Work History fields in the Incident Basics screen, work history notes can be configured to display when customers view their incidents on the mySupport portal.

Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note that selecting an Edit permission will restrict the support representative's access to only that permission. If a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after an incident is initially saved.

- **Edit My Assigned:** Select to allow the support representative to update any incident assigned to the support representative. Note: the View My Assigned permission is required for this permission.
- **Edit My Authored:** Select to allow the support representative to update any incident he/she creates. Note: the View My Authored permission is required for this permission.
- **Edit My Groups:** Select to allow the support representative to update incidents assigned to any member of *any* group to which the support representative is assigned. Note: the Edit My Assigned, View My Groups, and View My Assigned permissions are required for this permission.
- **Edit My Location:** Select to allow the support representative to update incidents assigned to any support representative in their location. Note: the Edit My Assigned, View My Locations, and View My Assigned permissions are required for this permission.
- **Edit All:** Select to allow the support representative to update any incident in the iSupport application. Note: All view and all edit permissions are required for this permission.
- **Change Customer:** Select to allow the support representative to assign a customer to a saved incident. If this option is *not* selected, the Select Customer option will not be included in the Incident screen and the Name link will be disabled. Note: one of the View permissions is required for this permission.
- **Add Additional Customers:** Select to allow the support representative to add customers to an incident. If this option is *not* selected, the Add Additional Customer option will not be included in the Incident screen. Note: One of the View permissions is required for this permission.
- **Remove Additional Customer:** Select to allow the support representative to remove an additional customer from a saved incident. If this option is *not* selected, the Remove Customer option will not be included in the Incident screen. Note: one of the View permissions is required for this permission.
- **Change Priority:** Select to allow the support representative to change a priority for a saved incident. If this option is *not* selected, the Priority field will display in the Incident screen but the drop-down list will be disabled. Note: one of the View permissions is required for this permission.
- **Change Status:** Select to allow the support representative to change a status for a saved incident. If this option is *not* selected, the Status field will display in the Incident screen but the drop-down list will be disabled. Note: one of the View permissions is required for this permission.
- **Change Impact:** Select to allow the support representative to change the Impact field for a saved incident. If this option is *not* selected, for all members of the group, the Impact field will display in the Incident screen but the drop-down list will be disabled. Note: the Impact and Urgency fields cannot be enabled or disabled individually; you either enable both or disable both. One of the View permissions is required for this permission.
- **Change Urgency:** Select to allow the support representative to change the Urgency field for a saved incident. If this option is *not* selected, for all members of the group, the Urgency field will display in the Incident screen but the drop-down list will be disabled. Note: the Impact and Urgency fields cannot be enabled or disabled individually; you either enable both or disable both. One of the View permissions is required for this permission.
- **Route:** Select to allow the support representative to assign an incident to another support representative. If this option is *not* selected, the Route icon and menu option will not be included in the Incident screen and the Assignee link will be disabled. Note: one of the View permissions is required for this permission.

- **Route by Group Only:** Select to restrict the support representative to routing only to other support representatives in his/her assigned group(s). Note: one of the View permissions is required for this permission.
- **Route to Unavailable Reps:** Select to enable the support representative to route to support representatives who are unavailable for routing via the following methods: No is selected in the Available for Routing field in the support representative's Profile record or in the Rep Manager Desktop component, or the support representative selected Out next to their name on the Desktop menu. Note that this permission only affects manual routing functionality; automated routing initiated from an email, mySupport submission, or by rule using load balancing or round robin methods only includes available support representatives.
- **Schedule Recurring:** Select to allow the support representative to schedule tickets on a recurring basis for a specified time frame.
- **Change Approvers:** Select to allow the support representative to change approvers when an ad hoc approval cycle is initiated.
- **Update Via News Feed:** Select to include the Update link next to incidents in the News Feed dashboard component for the support representative.
- **Delete:** Select to allow the support representative to delete incidents. If this option is *not* selected, the Delete option will not be included in the Incident screen. Note: one of the View permissions is required for this permission.

Assigning License Management Permissions

The License Management feature enables you to track instances of one or more software titles against a specified condition and quantity. The License Management agent scans all existing scheduled scans and searches for instances of the software titles specified in Software License Profile records. It compares the actual quantities found against the conditions, flags the profiles that meet the conditions, and updates the profiles with the actual quantities. See the online help for more information.

Select License Management to allow or disallow access to License Management functions such as viewing, creating, editing, and deleting Software License Profile records.

Reader - Click the Reader checkbox or select **View** to allow the support representative to view any Software License Profile record. If this option is *not* selected, views of Software License Profile records will not be included on the Desktop for the support representative.

Author - Click the Author checkbox or select **Create New** to allow the support representative to create new Software License Profile records. If this option is *not* selected, the Create option will not be available to the support representative for Software License Profile records on the Desktop and in the Software License Profile screen.

Editor - Click the Editor checkbox to select both Editor permissions, or select one or both of the following. Note: the View permission is required for these permissions.

- **Edit:** Select to allow the support representative to update Software License Profile records. If this option is *not* selected, the support representative can view Software License Profile records but the fields will be disabled.

- **Delete:** Select to allow the support representative to delete Software License Profile records. If this option is *not* selected, the Delete option will not be included on the Desktop and in the Software License Profile screen for the support representative.

Assigning Permissions for Opportunity Functionality



This option will appear if Opportunity functionality is enabled; select Opportunity to allow or disallow access to iSupport's Opportunity functionality.

The screenshot shows the 'Opportunity' permissions configuration interface. On the left, there is a sidebar with 'Opportunity' selected. Below it, there are three checkboxes: 'Reader', 'Author', and 'Editor'. The 'Reader' checkbox is checked, and next to it is a dropdown menu showing 'View'. The 'Author' checkbox is checked, and next to it is a dropdown menu showing 'Create New'. The 'Editor' checkbox is checked, and next to it is a list of permissions: 'Edit', 'Edit Closed', 'Change Description', 'Change Invoice', and 'Delete'. On the right side of the interface, there are two links: 'Select All Opportunity Permissions' and 'Clear All Opportunity Permissions'.

Reader - Click the Reader checkbox or select **View Opportunities** to allow the support representative to view any Opportunity record. If this option is *not* selected, views of Opportunity records will not be included on the Desktop for the support representative.

Author - Click the Author checkbox to select all Author permissions, or select **Create New Opportunity** to allow the support representative to create new Opportunity records. If this option is *not* selected, the Opportunity option will not be included on the Desktop menu and the New menu in the Opportunity screen for the support representative.

Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note: the View permission is required for these permissions.

- **Edit:** Select to allow the support representative to update Opportunity records.
- **Edit Closed:** Select to enable modification to allow the support representative to modify the Assignee, Stage, Type, Estimated Close Date, Purchase Order, and Probability fields after a stage requiring a win/loss reason is selected in the Opportunity screen and the opportunity is saved.
- **Change Description:** Select to allow the support representative to make an entry in the Description field in the Opportunity screen.
- **Change Invoice:** Select to display the Add button in the Invoice field in the Opportunity screen for adding a PDF file, as well as an Invoice Unpaid  icon if a file is added. A support representative can click this icon to flag the invoice as Paid . If this permission is *not* selected, the Add button will not appear.
- **Export to QuickBooks:** This option is included if QuickBooks integration is enabled; select to display the Export to QuickBooks icon in the Opportunity screen for the support representative to export the customer, company, and selected products and prices to QuickBooks.
- **Delete:** Select to allow the support representative to delete Opportunity records. If this option is *not* selected, the Delete option will not be included in the Opportunity screen.

Assigning Personal Correspondence Template Permission

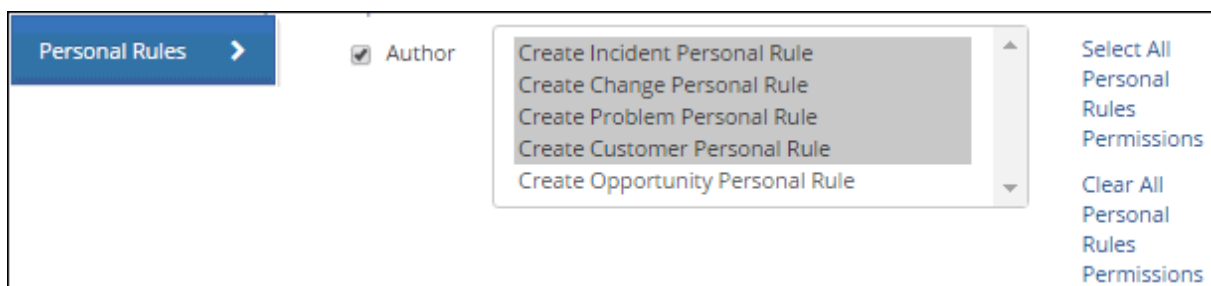
A personal correspondence template appears only to the support representative who created it in the list of correspondence templates available in iSupport. Select Personal Correspondence to allow or disallow creation of personal correspondence templates.



Author - Click the Author checkbox allow the support representative to create personal correspondence templates.

Assigning Personal Rule Permissions

Personal rules evaluate specified conditions when any record of a certain module type (incident, change, problem, or customer profile) is saved and send a notification to the email address in the support representative's profile if those conditions are met. The notification will contain a specified subject, the text "Click the following link to review this (*incident/change/problem/customer profile/opportunity*)", a link to the saved record. Support representatives access the Personal Rule configuration screen via the Personal Rules section in Desktop Preferences. Note that notifications sent by personal rules are logged in Configuration Audit History. Select Personal Rules to allow or disallow creation of personal rules.



Author - Click the Author checkbox or select one of the **Create** options to allow the support representative to create new personal rules for incidents, problems, changes, opportunities, and/or customer profiles via the Preferences screen.

Assigning Problem Permissions

This option will appear if Problem functionality is enabled in the Enable Features screen. Select Problems to allow or disallow access to problem functions such as creating, viewing, updating fields, and routing.

The screenshot shows the 'Problems' permissions configuration interface. It features a blue header bar with the text 'Problems' and a right arrow. Below the header, there are three sections: 'Reader', 'Author', and 'Editor', each with a checked checkbox. To the right of these sections are three scrollable lists of permissions. The 'Reader' list includes 'View My Assigned', 'View My Authored', 'View My Groups', 'View My Location', and 'View All'. The 'Author' list includes 'Create New' and 'Add Work History to All'. The 'Editor' list includes 'Edit My Assigned', 'Edit My Authored', 'Edit My Groups', 'Edit My Location', 'Edit All', 'Change Priority', 'Change Status', 'Change Impact', 'Change Urgency', 'Publish', 'Publish to Twitter', 'Route', 'Route By Group Only', 'Route to Unavailable Reps', 'Update Via News Feed', and 'Delete'. On the far right, there are two links: 'Select All Problem Permissions' and 'Clear All Problem Permissions'.

Reader - Click the Reader checkbox to select all Reader permissions, or select one or more of the following:

- **View My Assigned:** Select to allow the support representative to view the Problem records to which they are assigned.
- **View My Authored:** Select to allow the support representative to view the Problem records they create.
- **View My Groups:** Select to allow the support representative to view the Problem records assigned to any member of any group to which the support representative is assigned. Note: the View My Assigned permission is required for this permission.
- **View My Location:** Select to allow the support representative to view those Problem records assigned to support representatives in their location. Note: the View My Assigned permission is required for this permission.
- **View All:** Select to allow the support representative to view any Problem record in the iSupport application. Note: All View permissions are required for this permission.

Author - Click the Author checkbox to select all Author permissions, or select one or more of the following:

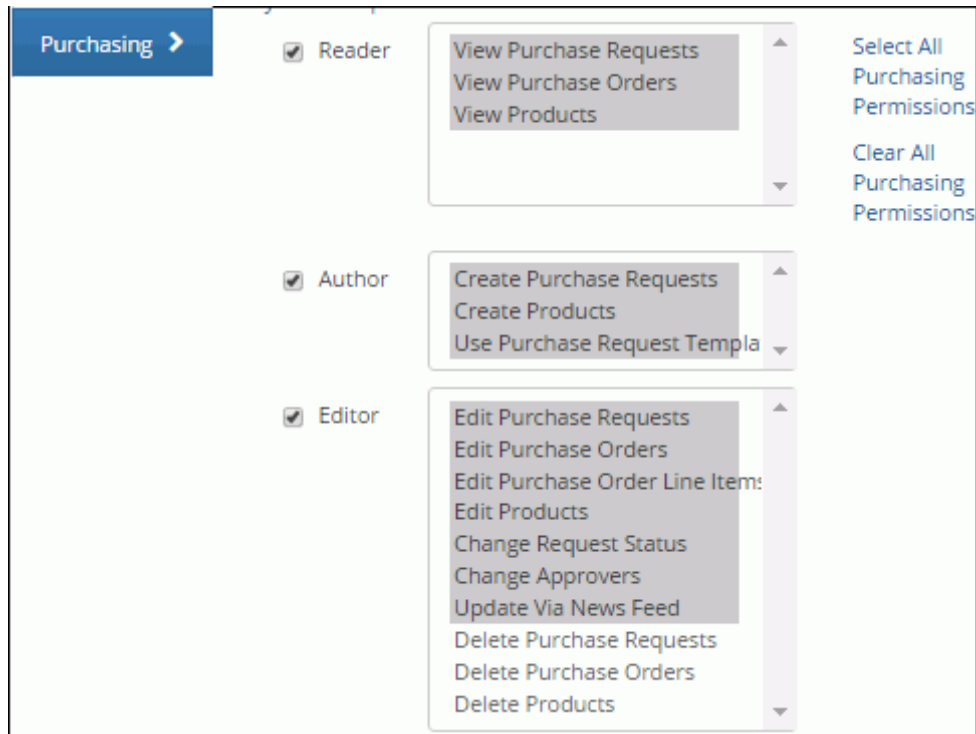
- **Create New:** Select to allow the support representative to create new Problem records. If this option is *not* selected, the Create Problem option will not be included on the Desktop menu and the New menu in the Problem screen.
- **Add Work History to All:** Select to allow the support representative to update the Work History field on any Problem record that the support representative can view in the iSupport application. This option is not affected by the Editor options; its purpose is to allow you to restrict updates to only the Work History field if needed.

Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note: if a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after the problem is initially saved.

- **Edit My Assigned:** Select to allow the support representative to update any Problem record to which they are assigned. If this option is *not* selected, the support representative will not be able to update the Problem records to which they are assigned. Note: the View My Assigned permission is required for this permission.
- **Edit My Authored:** Select to allow the support representative to update any Problem record they create. If this option is *not* selected, the support representative will not be able to update the Problem records they create. Note: the View My Authored permission is required for this permission.
- **Edit My Groups:** Select to allow the support representative to update Problem records assigned to any member of any group to which the support representative is assigned. Note: the Edit My Assigned, View My Groups, and View My Assigned permissions are required for this permission.
- **Edit My Location:** Select to allow the support representative to update Problem records assigned to any support representative in their location. Note: the Edit My Assigned, View My Location, and View My Assigned permissions are required for this permission.
- **Edit All:** Select to allow the support representative to update any Problem record in the iSupport application. Note: The View All permission is required for this permission.
- **Change Priority:** Select to allow the support representative to select a priority for a saved Problem record. If this option is *not* selected, the Priority field will display in the Problem screen but the drop-down list will be disabled. Note: one of the View permissions is required for this permission.
- **Change Status:** Select to allow the support representative to select a status for a saved problem. If this option is *not* selected, the Status field will display in the Problem screen but the drop-down list will be disabled. Note: one of the View permissions is required for this permission.
- **Change Impact:** Select to allow the support representative to make a selection in the Impact field for a saved Problem record. If this option is *not* selected, the Impact field will display in the Problem screen but the drop-down list will be disabled. Note: the Impact and Urgency fields cannot be enabled or disabled individually; you either enable both or disable both. One of the View permissions is required for this permission.
- **Change Urgency:** Select to allow the support representative to make a selection in the Urgency field for a saved Problem record. If this option is *not* selected the Urgency field will display in the Problem screen but the drop-down list will be disabled. Note: the Impact and Urgency fields cannot be enabled or disabled individually; you either enable both or disable both. One of the View permissions is required for this permission.
- **Publish:** Select to allow the support representative to select the Publish to mySupport field for a saved Problem record. Note: one of the View permissions is required for this permission.
- **Publish to Twitter:** Select to allow the support representatives to publish headlines to Twitter (if configured via the Social Media Integration screen).
- **Route:** Select to allow the support representative to assign a Problem record to another support representative. If this option is *not* selected, for all members of the group, the Route icon and menu option will not be included in the Problem screen and the Assignee link will be disabled. Note: one of the View permissions is required for this permission.
- **Route by Group Only:** Select to restrict support representative to routing only to other support representatives in his/her assigned group(s). Note: one of the View permissions is required for this permission.
- **Route to Unavailable Reps:** Select to enable the support representative to route to support representatives who are unavailable for routing. Support representatives who are unavailable for routing will be designated as "Out". This only affects manual routing functionality; automated routing initiated from an email or by rule using load balancing or round robin methods still includes available reps.
- **Update Via News Feed:** Select to include the Update link next to problems in the News Feed dashboard component for the support representative.
- **Delete:** Select to allow the support representative to delete Problem records. If this option is *not* selected, the Delete option will not be included in the Problem screen. Note: one of the View permissions is required for this permission.

Assigning Purchasing Permissions

This option will appear if Purchasing functionality is enabled in the Feature Basics screen. Select Purchasing to allow or disallow access to purchasing functions such as creating and viewing purchasing requests. (Note that if no approval cycle applies to a purchase request, the purchase request will become a purchase order upon saving.)



Reader - Click the Reader checkbox to select all Reader permissions, or select one or more of the following:

- **View Purchase Requests:** Select to allow the support representative to view any purchase request. If this option is *not* selected, all views of purchase requests will not be included on the Desktop, and the View Purchase Request option will not be included in the Incident screen for the support representative.
- **View Purchase Orders:** Select to allow the support representative to view purchase orders via the Desktop.
- **View Products:** Select to allow the support representative to view Product records via the Desktop.

Author - Click the Author checkbox to select all Author permissions, or select one or more of the following:

- **Create Purchase Requests:** Select to allow the support representative to create purchase requests. If this option is *not* selected, the Create Purchase Request option will not be included on the Desktop and the New Purchase Request option will not be included in the Incident, Problem, and Change screens for the support representative.
- **Create Products:** Select to include the Create Product option on the Desktop for the support representative.
- **Use Purchase Request Templates:** Select to allow the support representative to use purchase request templates in the Purchase Request screen.

Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note: the View permission is required for these permissions. If a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after a purchase request is initially saved.

- **Edit Purchase Requests:** Select to allow the support representative to update Purchase Request records. If this option is *not* selected, the support representative can view purchase requests but the fields will be disabled.
- **Edit Purchase Orders:** Select to allow the support representative to update Purchase Order records. If this option is *not* selected, the support representative can view purchase orders but the fields will be disabled.
- **Edit Purchase Order Line Items:** Select to allow the support representative to add or modify line items on an open purchase order. All line item additions/modifications will be tracked in the Audit History field. This

permission is independent of the other purchasing edit permissions, so a support representative could edit line items but not change the other fields on the purchase order.

- **Edit Products:** Select to allow the support representative to update Product records. If this option is *not* selected, the support representative can view Product records but the fields will be disabled.
- **Change Request Status:** Select to allow the support representative to update the Status field in the Purchase Request screen.
- **Change Approvers:** Select to allow the support representative to change approvers when an ad hoc approval cycle is initiated.
- **Update Via News Feed:** Select to include the Update link next to purchase requests in the News Feed dashboard component for the support representative.
- **Delete Purchase Requests:** Select to allow the support representative to delete purchase requests. If this option is *not* selected, the Delete option will not be included in the Purchase Request screen and on the Desktop when purchase request views appear for the support representative.
- **Delete Purchase Orders:** Select to allow the support representative to delete Purchase Order records. If this option is *not* selected, the Delete option will not be included in the Purchase Order screen and on the Desktop when purchase order views appear.
- **Delete Products:** Select to allow the support representative to delete Product records. If this option is *not* selected, the Delete option will not be included in the Product screen and on the Desktop when product views appear.

Assigning Permissions for SSRS Reporting Functionality

This option will appear if iSupport's SQL Reporting functionality is installed via the iSupport SQL Reporting Setup Wizard. Select Reports to allow or disallow access to the SSRS Report Viewer component, Ad Hoc Reports dashboard, and Group Access functionality for SQL reports.

SSRS Reports >	View SSRS Reports	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	?
	Create SSRS Reports	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off	?
	Manage Group Access for SSRS Reports	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off	?

View SSRS Reports - Select Yes to enable display of the SSRS Report Viewer component and Ad Hoc Reports dashboard (accessed via the SSRS Reports option on the Desktop menu) for viewing SQL reports. Report data will not be filtered by other iSupport permissions in effect for the support representative.

Create SSRS Reports - Select Yes to, if you have a version of Microsoft SQL Server 2008 R2 other than Express Edition, enable the support representative to create an SSRS report via the New Report option on the Ad Hoc Reports dashboard right-click menu.

Manage Group Access for SSRS Reports - Select Yes to enable display of the Manage Group Access icon next to the SSRS reports. The Group Access feature enables support representatives to set group access permissions on SQL reports.

Assigning Service Contract Permissions

This option will appear if Service Contract functionality is enabled in the Enable Features screen. Select Service Contracts to allow or disallow access to service contract functions such as creating, viewing, and updating service contract fields.

The screenshot shows a web interface for assigning permissions to 'Service Contracts'. On the left, there is a blue header with the text 'Service Contracts' and a right-pointing arrow. To the right of this header are three permission categories, each with a checkbox and a list of specific permissions in a dropdown menu:

- Reader** (checkbox checked):
 - View Active
 - View All
- Author** (checkbox checked):
 - Create New
 - Create Courtesy Work Items
- Editor** (checkbox unchecked):
 - Edit All
 - Edit Expired Contracts
 - Change Asset/Company/Customer
 - Change Status
 - Change Hours of Operation
 - Override Used Count
 - Delete

On the far right, there are two links: 'Select All Service Contract Permissions' and 'Clear All Service Contract Permissions'.

Reader - Click the Reader checkbox to select all Reader permissions, or select one or more of the following:

- **View Active:** Select to allow the support representative to view the service contracts with a status of Active (current duration time frame and/or the count of incidents and/or changes is greater than zero).
- **View All:** Select to allow the support representative to view all service contracts, regardless of status level.

Author - Click the Author checkbox to select all Author permissions, or select one or more of the following:

- **Create New:** Select to allow the support representative to create new service contracts. If this option is *not* selected, the Service Contract option will not be included on the Desktop menu and the New menu in the Service Contract screen for the support representative.
- **Create Courtesy Work Items:** A courtesy work item is an incident or change that does not count against the service contract in effect for a customer, company, or asset; it is created for an incident or change if the Mark This a Courtesy Work Item checkbox is enabled in the Select Service Contract dialog that appears after a customer is selected. Select this permission to allow the support representative to select the Mark This a Courtesy Work Item checkbox in the Select Service Contract dialog.

Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note: if a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu option and icon will not be available after a service contract is initially saved.

- **Edit All:** Select to allow the support representative to update any service contract record in the iSupport application. Note: The View All permission is required for this permission.
- **Edit Expired Contracts:** Select to allow the support representative to update service contracts with a status of Expired.
- **Change Asset/Company/Customer:** Select to allow the support representative to add or remove an asset, customer, or company for a service contract. If this option is *not* selected, for all members of the group, assets, customers, or companies that have been selected for a saved contract will appear but the Add and Delete links will be disabled. Note: one of the View permissions is required for this permission.

- **Change Status:** Select to allow the support representative to change the Status field for a saved service contract. If this option is *not* selected, the Status field will display in the Service Contract screen but the drop-down list will be disabled. Note: one of the View permissions is required for this permission.
- **Change Hours of Operation:** Select to allow the support representative to change the Hours of Operation for a saved service contract. If this option is *not* selected, the Hours of Operation field will display in the Service Contract screen but the selection dropdown will be disabled. One of the View permissions is required for this permission.
- **Override Used Count:** Select to allow the support representative to make a change in the Used field for a saved service contract. If this option is *not* selected, the Used field will display in the Service Contract screen but the entry field will be disabled. Note: one of the View permissions is required for this permission.
- **Delete:** Select to allow the support representative to delete service contracts. If this option is *not* selected, the Delete option will not be included in the Service Contract screen. Note: one of the View permissions is required for this permission.

Assigning Permissions for Survey Functionality

This option will appear if Survey functionality is enabled in the Enable Features screen. Select Surveys to allow or disallow access to iSupport's Survey functionality.

The screenshot shows the 'Permissions' tab for 'Surveys'. The 'Reader' checkbox is checked, and the 'View' permission is selected. The 'Author' checkbox is checked, and the 'Create New Requests' permission is selected. The 'Editor' checkbox is checked, and the 'Edit' and 'Delete' permissions are selected. On the right, there are links for 'Select All Survey Permissions' and 'Clear All Survey Permissions'.

Reader - Click the Reader checkbox or select **View** to allow the support representative to view a survey. If this option is *not* selected, views of surveys will not be included on the Desktop for the support representative.

Author - Click the Author checkbox or select **Create New Requests** to enable the support representative to send a survey. If this option is *not* selected, the Survey option will not be included on the Desktop menu and the New menu in the Incident and Customer screens for the support representative.

Editor - Click the Editor checkbox to select both Editor permissions, or select one or more of the following. Note: the View permission is required for these permissions.

- **Edit:** Select to enable the support representative to change the survey status and make an entry in followup fields. Note that if the survey status is Sent or Closed, it will be inactive so it cannot be edited. A rep can save a survey with a status of Submitted if the survey had a Submitted status prior to editing.
- **Delete:** Select to enable the support representative to delete a survey.

Using Permissions Views

Use the following options in the Administer | Permissions section to view permissions and roles for support representatives.

- **Flat by Support Representative** - a list of each permission for each support representative, with one per row. You can use the Export All to Microsoft Excel link to export the data in this view to a Microsoft[®] Excel spreadsheet.

Export All to Microsoft Excel				
First Name ▲	Last Name	Primary Group	Module	Permission
Abby	Kienle	Administrators	Configuration	Administrator
Abby	Kienle	Administrators	Knowledge	Approver
Abby	Kienle	Administrators	Incident Data Override	Allowed

- **Summarized by Support Representative** - a list of all of the permissions for each support representative/group.

Name	Group
Abby Kienle	Administrators
Alerts Author:	Create Personal Create Shared
Alerts Editor:	Edit Shared Delete Personal Delete Shared

- **Flat by Role** - a list of each permission for each support representative, with one per row. You can use the Export All to Microsoft Excel link to export the data in this view to a Microsoft[®] Excel spreadsheet.

Export All to Microsoft Excel		
Role Name ▲	Module	Permission
Applications	Changes	Reader: View My Groups
Applications	Configuration Items	Reader: View
Applications	Opportunity	Reader: View Opportunities
Applications	Opportunity	Author: Create New Opportunity
Applications	Configuration Items	Editor: Edit

- **Summarized by Role** - a list of all permissions for each role.

Print	
Name	
Applications - Group	
Alerts Author:	Create Personal
	Create Shared
Alerts Editor:	Edit Shared
	Delete Personal
	Delete Shared
Archive Viewer	
Assets Author:	Create New Asset
	Use Multiple Asset Wizard
	Create Scan / Comparison
Assets Editor:	Edit Asset
	Edit Count Used

Assigning Support Representatives to a Role

Assign the role to individual support representatives via the Support Reps tab.

Details Permissions Support Reps Groups					
Add Remove					
<input type="checkbox"/>	Last Name ▲	First Name	Email	Phone	Primary Group
<input type="checkbox"/>	Flynn	Connor	cf@example.com	360-397-1058	Support (IT)
<input type="checkbox"/>	Kienle	Abby	ak@example.com	360-397-1000	Administrators

Assigning Support Rep Groups to a Role

Assign the role to support representative groups via the Groups tab.

Details Permissions Support Reps Groups		
Add Remove		
<input type="checkbox"/>	Name ▲	Description
<input type="checkbox"/>	Tier I (IT)	Reps with first customer contact

Configuring Locations

Use the Locations screen to configure locations for location-based routing. You can also use this screen to assign a display time zone for multiple support representatives at one time.

Location Name

Headquarters

Display Time Zone

(UTC-08:00) Pacific Time (US & Canada)

Non Members

Gena Pirie
Jack Sullivan
Jorge Quentin
Kelsey Stout
Mary Smith
Stuart Copeland
Tess French

Members

Abby Kienle
Barry White
Connor Flynn
Dwayne March

→

←

☒ Apply the selected display time zone to members of this location upon save

*The Display Time Zone is for display purposes only. Incident business hour escalation and statistics are based on the assignee's support center time zone setting.

Location Name - Enter the name of the location. This name will appear for selection in the location-based routing dialogs.

Display Time Zone - Select the time zone to use for date/time stamps that will display for those in the Members field.

Nonmembers/Members - The Nonmembers field includes support representatives set up in the Support Representative screen.

- To assign a support representative to the location, select the support representative in the Nonmembers field and click the right arrow → icon.
- To remove a support representative from the location, select the support representative in the Members field and click the left arrow ← icon.

Apply the Selected Display Time Zone to Members of This Location Upon Save - Use this checkbox to assign the selected display time zone to those in Members field. This will update the display time zone in each member's Support Representative record.

Note: Only one location can be assigned to a support representative.

Setting Up Support Centers

You can use support centers for assigning support representatives to different areas within a single iSupport installation. For example, you could set up support centers for geographic areas such as West Coast and East Coast, or for functional areas such as external and internal support. The Time Zone field will be used for date/time display.

A support representative can be assigned to only one support center. If you choose not to use the Support Center feature, the time zone settings of the server hosting iSupport will be used. Click Create in the Support Center screen.

Support Center Name

This is the Default Support Center ☒ Yes ☐ No

Time Zone

Non Members

- Barry White
- Dwayne March
- Gena Pirie
- Jack Sullivan
- Jorge Quentin
- Kelsey Stout
- Mary Smith
- Stuart Copeland
- Tess French

Members

- Abby Kienle
- Connor Flynn

Support Center Name - Enter the name of the support center.

This is the Default Support Center - Select this checkbox to use the selected support center as default when you create Support Representative records.

Time Zone - Select the time zone for the support center. For all support representatives assigned to this support center, this time zone will be used for date/time display.


Nonmembers/Members - Use these fields to assign support representatives to a support center. A support representative can be assigned to only one support center.

The Nonmembers field includes support representatives set up in the Support Representative screen.


- To assign a support representative to the support center, select the support representative in the Nonmembers field and click the right arrow → icon.
- To remove a support representative from the support center, select the support representative in the Members field and click the left arrow ← icon.

Monitoring Active and Exceeded Sessions

Use the Options and Tools | Administer | Active Sessions screen to display the support representatives currently logged into iSupport. You can log off a support representative by selecting an entry and clicking the Delete link.

	Delete	Licensed Sessions - 2 Active 11 Allowed		
<input type="checkbox"/>	Last Accessed Date ▲	Session ID	Name	
<input type="checkbox"/>	3/9/2016 1:57:46 PM	2bc4fd1a-b4db-450d-9352-87ebcf328bc7	Connor Flynn	
<input type="checkbox"/>	3/9/2016 1:58:07 PM	510bfe08-aad1-44b6-a1ff-d8d90927fd1e	Barry White	

Use the Sessions Exceeded Log screen to display the occurrences when a support representative logs in after the maximum number of sessions for your license has been reached. (The support representative will be prevented from logging in and a warning dialog will appear.)



Clear All

Licensed Sessions - 11 Active 11 Allowed

Date	Rep
3/9/2016 2:58:39 PM	Mary Smith

To request a quote for additional licenses:

- [Click here](#)
- Call 888-494-7638
- Send an email to renewal@iSupport.com

Managing Dashboards for Support Representatives

Configured roles and permissions will determine whether a support representative can create, edit, and delete a personal or shared dashboard; use the Dashboards tab in the Content Manager (accessed via the Desktop Content icon) to add, delete, and rename dashboards and specify dashboard access. You can also use the Save and Push option to automatically add a dashboard to all support representative desktops.

This screen lists all dashboards created and designated as Shared, as well as all personal dashboards that you have created. Click the Add link to add a dashboard and specify its access.

Add Delete						
<input type="checkbox"/>		Name ▲	Author	Access	Usage	Components
<input type="checkbox"/>	 	<input type="text" value="Default"/>	Barry White	Shared	11	4
<input type="checkbox"/>		Discussions	Barry White	Personal	1	1
<input type="checkbox"/>		Incident Counts	Barry White	Shared	1	1

Name - Enter the dashboard name. If renaming a dashboard, you'll need to log off the Desktop and log back in to display the change.


Author - The support representative who created the dashboard.


Access - Click the Personal or Shared link to enable or disable shared access, and if shared, specify the individual support representative(s) or group(s) that can access the dashboard. Shared access will make the dashboard available to other support representatives. To make the dashboard available only to specified groups, place your cursor in the Add Rep Group field and select the group(s). To make the dashboard available only to selected support representatives, place your cursor in the Add Rep field and select the support representatives. If you select Save in this dialog, support representatives will be able to add the dashboard to add to their Desktops via the Add Existing dashboard menu option; if you select Save and Push, the dashboard will be automatically added to all support representative desktops.

Access

Shared: ☒

Restrict:

Applications 

Network 

Save

Save & Push

Cancel


Usage - The number of support representatives that have added the dashboard. This number will change if you add support representatives and members of support representative groups added via the Personal or Shared link in the Access column.

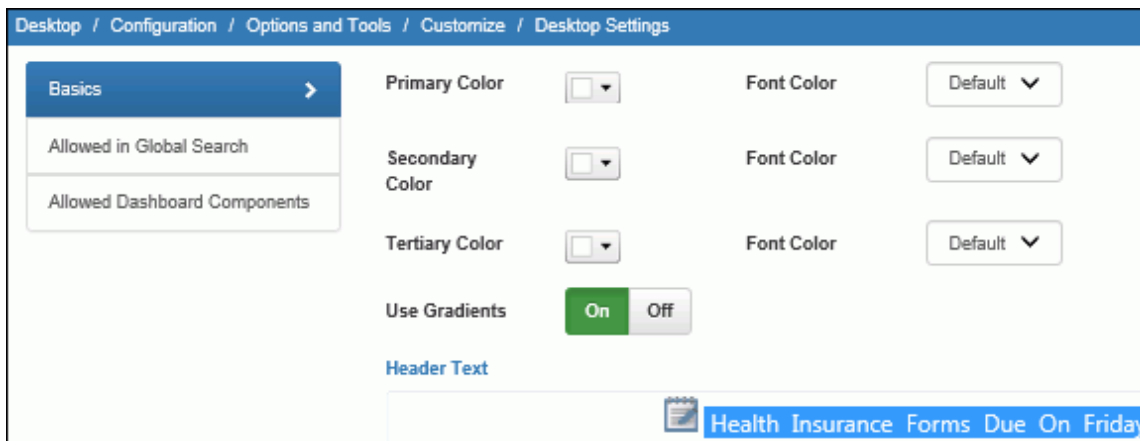
Components - The number of content frames on the dashboard.

Managing Components, Colors, Header Text, and Global Search

Use the Options and Tools | Customize | Desktop Settings screen to set the colors of dashboard elements and Desktop header text, the components that all support representatives can add to dashboards, and the records/features involved in global searches performed by all support representatives. Note that you can use the Support Representative Group screen to override these settings for members of a support representative group.

Configuring Colors and Header Text

Use the Colors section to configure the colors of Desktop elements; select colors via the color picker or enter an HTML color code. Use the No Color  icon to remove a selected color and reset back to default.




Primary - Set the color of the Desktop header, Chat tab, and component title bars.

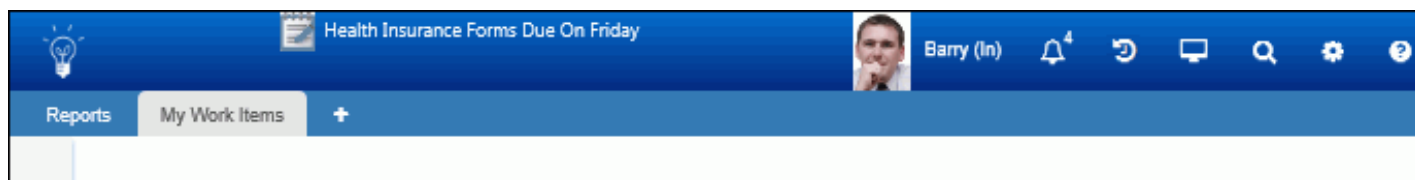
Secondary - Set the color of activated Desktop dashboard tabs and icon bar options.

Tertiary - Set the color of the Desktop dashboard tab bar.

Font Color - Set the font color to black or white, or you can select Default to enable the system to, based on the selected color, automatically assign black or white depending on which gives the better contrast. (For example, black will be assigned if yellow is the selected color.) This can be overridden by selecting White or Black.

Use Gradients - Select On to display color gradually from light-to-dark; select Off to display color in a flat, saturated manner.

Header Text - Enter text to appear at the top of the Desktop, between the Desktop Create  icon and Profile image. (Note that the text is white, centered, and selected in the Header Text field example above.)



Specifying Items for Global Search

A global search can be performed via the Global Search component on the Desktop as well as the View | Search feature in the Incident screen. To include a record type or feature in global searches performed by all support

representatives, drag it from the Don't Include column to the Include column on the Allowed in Global Search section.

Colors	Select Entities to add...	<input type="button" value="+ All"/>	<input type="button" value="- All"/>
Allowed in Global Search	Headline	✕	
Allowed Dashboard Components	Change	✕	
	Knowledge Entry	✕	
	Incident	✕	
	Customer	✕	

Specifying Allowed Dashboard Components

To make a component available for **all** support representatives to add to their Desktop dashboards, drag the component name from the Don't Include column to the Include column. Note that some components will not appear until functionality is configured as described below.

- The Calendar component will not appear in this list until Calendar Integration is enabled in the Calendar Integration configuration screen.
- The Mass Mailing Manager will not appear in this list until enabled in the Mass Mailings configuration screen.
- The Twitter Monitor component will not appear in this list until a Twitter application is configured and enabled for the Desktop in the Social Media Integration configuration screen.
- The Rep Manager component will not appear to a support representative that does not have Rep Manager access enabled in his/her profile.

Colors	Select Components to add...	<input type="button" value="+ All"/>	<input type="button" value="- All"/>
Allowed in Global Search	Asset Monitor	✕	
Allowed Dashboard Components	Rep Manager	✕	
	Calendar	✕	

Using the Data Source Integration Feature

Use the Data Source Integration feature to utilize Active Directory and LDAP as a source for iSupport's support representative information.

To get started, click the Create link in the Options and Tools | Integrate | Data Source Integration screen.

<div>Create ▼ Delete Order of Precedence</div>					
<input type="checkbox"/>	Name ▲	Type	Active	Source	Synced Record Types
<input type="checkbox"/>	Domino Directory	Domino Directory	Yes		Customers
<input type="checkbox"/>	LDAP Source	LDAP	No	xx.xx.xx.xx	Customers
<input type="checkbox"/>	Main AD Sync	Active Directory	No	LDAP://xx.xx.xx.xx	Customers
<input type="checkbox"/>	Microsoft CRM	Microsoft CRM	Yes		Customers

Select the data source type.

Create ▼ Delete Order of Precedence

Shared

Active Directory

LDAP

Customer

Domino Directory

Microsoft CRM

Customer RDB

Asset

Asset RDB

CMDB

CMDB RDB

Type

Active

Source

Integrating with Active Directory

The Active Directory Integration feature enables an agent that updates and synchronizes iSupport Customer Profile, Asset, and Support Representative Profile records with the information in one or more Active Directory sources.

You'll create a data source integration definition to specify the server and related settings, field mappings, and exclusions, and use sync definitions to specify the type of record you are synchronizing and the directory node and filters for the data to be synchronized. You can utilize both filtering and exclusions to specify the values that should not be synchronized; what you use will depend on how much you need to prevent from synchronizing for the level in the targeted source. You can also set default values based upon the AD sync setting entry from which a record was created. Exclusions target everything under a node in a directory and apply to all sync definitions of the same record type within a data source integration definition. Filters use syntax that can target multiple nodes in a tree, and apply to a specified base directory node in a sync definition.

The following occurs when the agent runs:

- If there is an entry in Active Directory that does not exist in iSupport, the entry is created in iSupport. In order for an entry to be added from Active Directory, it must contain a first name, last name, and email address.
- The first name, last name, and email address in Active Directory are compared with those values in iSupport. If all of those values in an Active Directory record match all of those values in a directly entered Support Representative Profile, the Support Representative Profile record is updated with the latest information from Active Directory; if one of those values does not match, a new record is created in Support Representative Profiles. Therefore, more than one Support Representative Profile record will result if both contain one of the same values (for example, email address) but one or both of the other fields differ. For example, if there is a

directly entered Support Representative Profile named Jon Smith with an email address jsmith@example.com and Active Directory has the rep listed with the name Jonathan Smith and the same email address of jsmith@example.com, the result will be two Support Representative Profile records with the same email address.

- If an entry is deleted in the Active Directory, the record will be flagged for deletion and:
 - If work items or assets are **not** associated with that name, the entry will be deleted from Support Representative Profiles when the Database Maintenance agent runs.
 - If work items or assets are associated with the name, the entry will remain flagged for deletion in Support Representative Profiles until those incident records no longer exist.

When the feature is enabled, the agent runs immediately and then as specified according to the configured interval. Note that the Active Directory Integration feature does not modify the contents in Active Directory in any way.

Basics

Use the Basics tab to specify the primary connection and authentication details for accessing the data source; these settings will apply to all of the sync definitions you create for that data source.

The Active Directory Integration feature allows you to utilize Active Directory as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics >

Field Mappings

Exclusions

AD Source Name

Main AD Sync

Search Root

LDAP://xx.xx.x.xx:xxx

Connect As

Anonymous Specified User

Username

xxAdmin

Password

Reset

Test Connection

Active

On Off

Synchronization Interval

3 hours

Sync Definitions

Create Delete

<input type="checkbox"/> Sync Root ▾	Record Type	Active	mySupport Access
<input type="checkbox"/> ou=Production,DC=example,DC=com	Support Reps	Yes	

AD Source Name - Enter a name for the AD source definition.

Search Root - Enter the directory server machine name or IP address for querying user information in the Active Directory source; precede your entry with the following: LDAP://

Connect As - Select Anonymous to connect to the data source as an anonymous user or Specified User to enter a login for connecting to the data source.

Username/Password - If anonymous Active Directory connections are not allowed in your environment, use these optional fields to enter a username and password for authentication when queries are performed. If anonymous connections are allowed, leave these fields blank.

Active - Select Yes to enable the Active Directory Integration agent that updates the records in iSupport with the information in Active Directory. The agent runs immediately and then continues to run as scheduled in the AD Synchronization Interval field.

AD Synchronization Interval - Select the amount of time in the interval for the synchronization to be performed.

Configuring a Sync Definition

Use the Sync Definition section to select the type of record that you are synchronizing, select the directory node that contains the data to be synchronized, and enter a search filter if applicable. Click the Create link to create a sync definition.

The screenshot shows the 'Sync Definitions' configuration window. On the left is a sidebar with tabs: 'Basics', 'Sync Definitions' (selected), 'Field Mappings', and 'Exclusions'. The main area has the following fields:

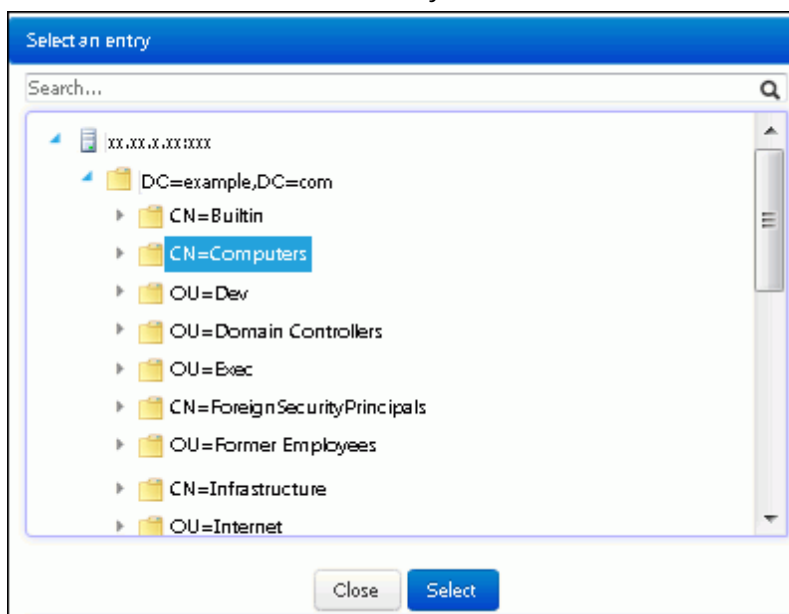
- Active:** A toggle switch set to 'Yes'.
- Sync Entries As:** A dropdown menu showing 'Support Representatives'.
- Default Primary Group:** A dropdown menu showing 'Support' with '+' and '-' icons.
- Base DN:** A text box containing 'ou=Production,DC=example,DC=com'.
- Search Filter:** A text box containing the LDAP filter: `(&(objectCategory=person)(objectClass=user)(givenName=*))`.

Active - Select Yes to enable the sync definition.

Sync Entries As - Select the type of record that you are synchronizing: Customer Profile. The **Enable mySupport Access** field will appear; select Yes to enable the Approved to Access mySupport field by default. If a login name and password exists in the Active Directory record, it will be included in the mySupport login fields for authentication to the mySupport portal. This is not a mapped or synchronized value; it can be edited in iSupport.

This feature utilizes LDAP (Light Weight Directory Access Protocol), which defines how information can be accessed in directories. Active Directory supports the LDAP search filter syntax as specified in RFC 1960. For information on LDAP and search filters, see <http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx#Examples>.

Base DN - Click this button to select the node in the directory server that contains the data to be synchronized.



Search Filter - Enter the conditions that must be met for returning a specific set of information to iSupport. Note that a filter is only needed if the selected Base DN contains unwanted lower level nodes or if the data source's exclusions do not already remove the unwanted nodes.

Examples

- All users that contain a first and last name:

```
(&
(objectCategory=Person)
(objectClass=user)
(givenName=*)
(sn=*)
)
```

- All users that contain a first and last name excluding Tom Jones and SQL Account:

```
(&
(objectCategory=Person)
(objectClass=user)
(givenName=*)
(sn=*)
(!name =Tom Jones)
(!name=SQL Account)
)
```

- All users and contacts that contain a first and last name:

```
(&
(objectCategory=Person)
(givenName=*)
(sn=*)
(|
(objectClass=user)
(objectClass=contact)
)
)
```

- All users and contacts that contain a first and last name, excluding Tom Jones, Barry White, and SQL Account:

```
(&
(objectCategory=Person)
(|
(objectClass=user)
(objectClass=contact)
)
(givenName=*)
(sn=*)
(!name =Tom Jones)
(!name=SQL Account)
(!name =Barry White)
)
```

- All users with a valid Microsoft Windows user name (*domainname\username*):

```
(&
(objectCategory=Person)
```

```
(objectClass=user)
(givenName=*)
(sn=*)
(userPrincipalName=*@*)
(samAccountName=*)
)
```

Setting Default Values

Use the Default Values section to set Support Representative field values based upon the AD sync setting entry from which a record was created. For example, if AD users are organized into a specific OU or group that indicates other user properties (such as location) and if the AD user profiles don't have the location attribute populated in the directory, you can simply add a default value for the location field to the sync setting entry that is linked to the OU or group.

In the Force column, select Yes if you wish to have the configured default value override the AD value in cases where the attribute was populated in the source user profile. If the Force field is set to No, the default value will only be applied if the AD attribute is either unmapped or has no value on the user profile.

Default Values

Field	Value	Force?
<div>Groups</div>	<div>Quality Control</div>	<div>Yes</div> <div>No</div>

Field Mappings

Use the Support Rep subtab to specify the attributes in your Active Directory source from which data will be pulled for corresponding iSupport fields.

The Active Directory Integration feature allows you to utilize Active Directory as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics

Syno Definitions

Field Mappings

Exclusions

Customer

Support Rep


Asset

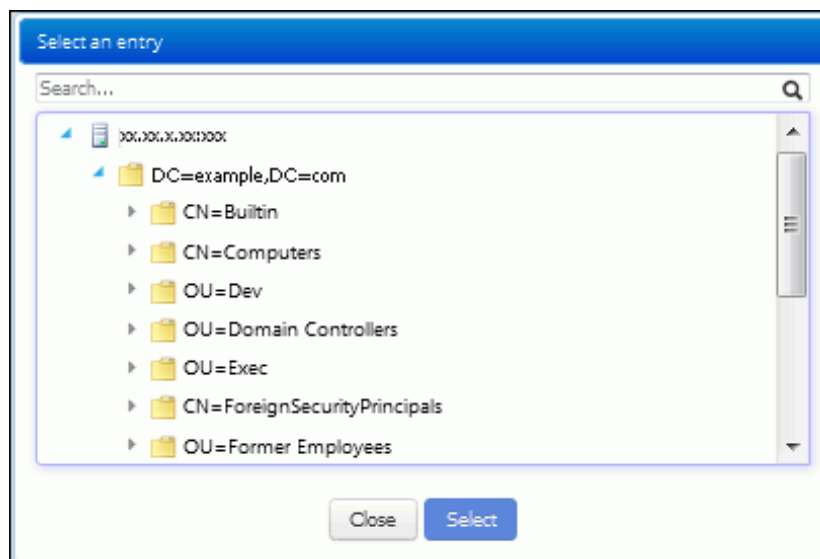
Field	Attribute
First Name	Use iSupport Default
Last Name	Use iSupport Default
Email	Use iSupport Default
Syno Key	Use iSupport Default

Mapping options include:

- Use iSupport Default which populates the default mapping. Note that we recommend that you use iSupport’s default for the Sync Key and Avatar field because the applicable schema property may vary depending on your version of Active Directory. If iSupport Default is selected for the Groups field, all groups associated with a support representative will be created via the MemberOf attribute.
- An applicable schema property. Defaults appear in the dropdown; to add an attribute, enter its exact name and it will be retained in the list.
- [Unmapped] which will enable entry in the field. Note that the First Name, Last Name, Email, Sync Key, and Login fields cannot be left unmapped for customers.

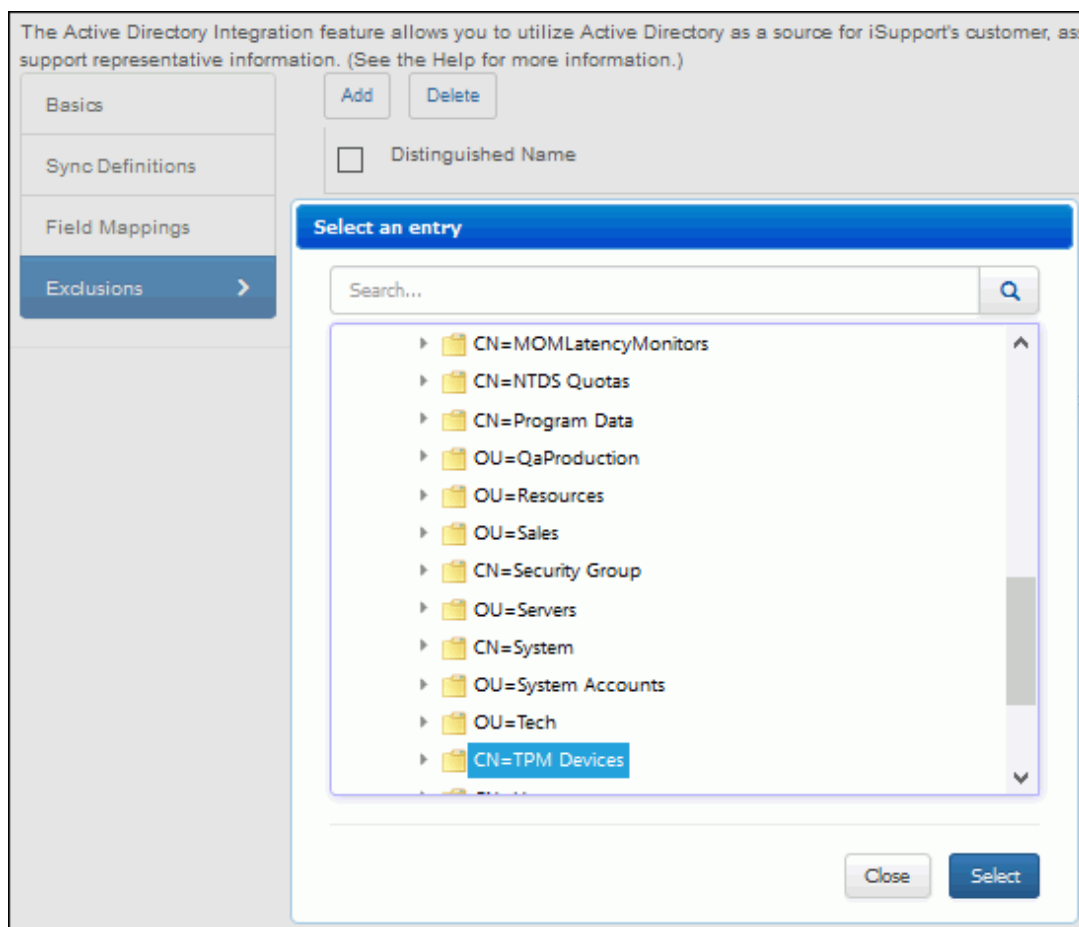
Use the Sync Key field to map to a value that is an unchanging unique identifier field in the source database.

Use the Preview  button to select a record to use for verifying your selections. Values from the record will appear next to the fields.



Configuring Exclusions

Use the Exclusions tab to specify the nodes or directory objects that should not be synchronized; click the Add link to select the directory nodes or objects that should be excluded. All lower level nodes will also be excluded. Note that exclusions apply to all sync definitions of the same record type within a data source integration definition.



Integrating with LDAP

The LDAP Integration feature enables an agent that updates and synchronizes iSupport Support Representative records with the information in one or more LDAP sources.

You'll create a data source integration definition to specify the server and related settings, field mappings, and exclusions, and use sync definitions to specify the type of record you are synchronizing and the directory node and filters for the data to be synchronized. You can utilize both filtering and exclusions to specify the values that should not be synchronized; what you use will depend on how much you need to prevent from synchronizing for the level in the targeted source. Exclusions target everything under a node in a directory and apply to all sync definitions of the same record type within a data source integration definition. Filters use syntax that can target multiple nodes in a tree, and apply to a specified base directory node in a sync definition.

The following occurs when the agent runs:

- If there is an entry in LDAP that does not exist in iSupport, the entry is created in iSupport. In order for an entry to be added from LDAP, it must contain a first name, last name, and email address.
- If an email address matches an email address in Support Representative Profiles and the record was directly entered via Support Representative Profiles, depending on the configured order of precedence, the Support Representative Profile record is updated with the latest information from LDAP.
- If an entry is deleted in the LDAP, the record will be flagged for deletion and:
 - If work items or assets are **not** associated with that name, the entry will be deleted from Support Representative Profiles when the Database Maintenance agent runs.
 - If work items or assets are associated with the name, the entry will remain flagged for deletion in Support Representative Profiles until those incident records no longer exist.

When the feature is enabled, the agent runs immediately and then as specified according to the selection in the LDAP Synchronization field. The LDAP Integration feature does not modify the contents in the LDAP source in any way.

Go to the following links for more information:

- <http://www.rfc-archive.org/getrfc.php?rfc=3377> - Top level LDAPv3 Technical specs
- <http://www.rfc-archive.org/getrfc.php?rfc=2254> - Search Filters (with examples)
- <http://www.rfc-archive.org/getrfc.php?rfc=2255> - URL formats (examples for Search Root field)
- <http://www.rfc-archive.org/getrfc.php?rfc=2256> - User Schema (standard available attributes, useful for mapping)

Configuring Basics

Use the Basics tab to specify the primary connection and authentication details for accessing the data source; these settings will apply to all of the sync definitions you create for that data source.

The LDAP Integration feature allows you to utilize LDAP as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics >

Field Mappings

Exclusions

LDAP Source Name

LDAP Data Source

Server

LDAP://xx.xx.x.xxx:xxx

Use SSL

On Off

Connect As

Anonymous Specified User

Username

uid=sampleuser,ou=people,dc=example,dc=edu

Password

.....

Test Connection

Active

On Off

Synchronization Interval

15 minutes ▼

Sync Definitions

Create Delete

<input type="checkbox"/> Sync Root ▲	Record Type	Active	mySupport Access
<input type="checkbox"/> ou=people,o=sevenSeas	Support Reps	Yes	

LDAP Source Name - Enter a name for the LDAP source definition.

Server - Enter the server on which the source entries are located.

Use SSL - SSL is an encryption method that overlays the connection between the cSupport server and the LDAP source server. Select Yes if SSL encryption is enabled on the LDAP source server. Use the Test Connection link to verify access.

Active - Select Yes to enable the agent that updates the applicable records in iSupport with the information in the LDAP source. The agent runs immediately and then continues to run as scheduled in the LDAP Synchronization Interval field.

LDAP Synchronization Interval - Select the amount of time in the interval for the synchronization to be performed.

Username/Password - If anonymous connections are not allowed in your environment, use these optional fields to enter a username and password for authentication when queries are performed. If anonymous connections are allowed, leave these fields blank.

Use the fully qualified Distinguished Name for best results. If accessing a server hosting an Active Directory installation, it will work with several formats. For example, if the user name is lbladmin and it is in the lbl domain, you could enter lbladmin, lbl\lbladmin, lbladmin@lbl.soft.com. All of these entries would work, but you could also enter the full Distinguished Name for the lbladmin user account (cn=lbladmin,cn=users,dc=lbl,dc=soft,dc=com). Note that

if you are connecting to a non-AD server like E-directory, the Username field must contain the fully qualified Distinguished Name.

Configuring a Sync Definition

Use the Sync Definition section to select the type of record that you are synchronizing, select the directory node that contains the data to be synchronized, and enter a search filter if applicable.

The LDAP Integration feature allows you to utilize LDAP as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics	Active	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Sync Definitions >	Sync Entries As	Support Representatives
Field Mappings	Default Primary Group	Support + ✎
Exclusions	Base DN	OU=people,o=sevenSeas
	Search Filter	(& objectClass=person) (objectClass=user) (memberof=CN=Example,DC=sevenSeas,DC=com))

Active - Select Yes to enable the sync definition.

Sync Entries As - Select the type of record that you are synchronizing: Support Representative Profile. When synchronization occurs, the record will be created if there is an entry in the LDAP source that does not exist in iSupport.

This feature utilizes LDAP (Light Weight Directory Access Protocol), which defines how information can be accessed in directories. Active Directory supports the LDAP search filter syntax as specified in RFC 1960. For information on LDAP and search filters, see <http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx#Examples>.

Base DN - Click this button to select the directory node that contains the data to be synchronized.

Search Filter - Enter the conditions that must be met for returning a specific set of information to iSupport. Note that a filter is only needed if the selected Base DN contains unwanted lower level nodes or if the data source's exclusions do not already remove the unwanted nodes.

Setting Default Values

Use the Default Values section to set Support Representative field values based upon the LDAP sync setting entry from which a record was created. For example, if LDAP users are organized into a specific OU or group that indicates other user properties (such as location) and if the LDAP user profiles don't have the location attribute populated in the directory, you can simply add a default value for the location field to the sync setting entry that is linked to the OU or group.

In the Force column, select Yes if you wish to have the configured default value override the LDAP value in cases where the attribute was populated in the source user profile. If the Force field is set to No, the default value will only be applied if the LDAP attribute is either unmapped or has no value on the user profile.

Default Values		
Field	Value	Force? ?
Groups	<input type="text" value="Quality Control"/> ✎	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Field Mappings

Use the Support Rep subtab under the Field Mappings tab to specify the attributes in your LDAP source from which data will be pulled for corresponding iSupport fields.

The LDAP Integration feature allows you to utilize LDAP as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics | Customer | Support Rep | Asset

Field Mappings >

Exclusions

Field	Attribute
First Name	Use iSupport Default
Last Name	Use iSupport Default
Email	Use iSupport Default
Sync Key	Use iSupport Default

Mapping options include:

- Use iSupport Default which populates the default mapping. Note that we recommend that you use iSupport's default for the Sync Key and Avatar fields because the applicable schema property may vary depending on your version of LDAP.
- An applicable schema property (selected via the dropdown)
- [Unmapped] which will enable entry in the field. Note that the First Name, Last Name, Email, Sync Key, and Login fields cannot be left unmapped.

Use the Sync Key field to map to a value that is an unchanging unique identifier field in the source database.

Use the Preview  button to select a record to use for verifying your selections. Values from the record will appear next to the fields.

Configuring Exclusions

Use the Exclusions tab to specify the values that should not be synchronized; click the Add link to select the directory nodes or objects that should be excluded. All lower level nodes will also be excluded. Note that exclusions apply to all sync definitions within a data source integration definition.

The LDAP Integration feature allows you to utilize LDAP as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics > | Field Mappings > | Exclusions >

Add Delete

Distinguished Name

Select an entry

Search...

- ou=system
- ou=schema
- ou=config
- o=sevenSeas
 - ou=people
 - cn=John Nelson

Setting Up Microsoft Windows-Based Authentication for the Desktop

You can set up Microsoft® Windows-based authentication with iSupport, enabling support representatives to bypass the Login prompt for accessing the Desktop. It will apply to all support representatives.

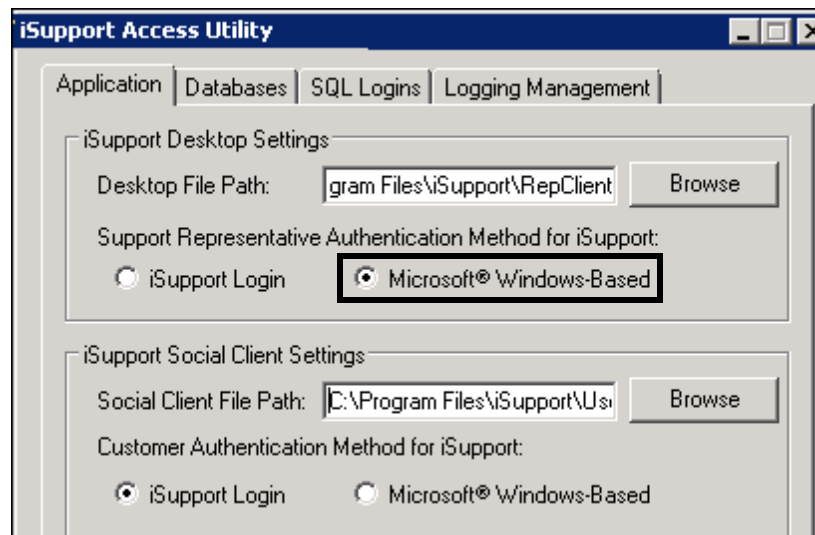
Use the following steps to enable Microsoft® Windows-based authentication for the Desktop. Because this procedure affects support representative logins, it's a good idea to do it after work hours.

- 1 For each support representative, enter the complete Microsoft Windows user name (*domainname\username*) in the Login field on the Details tab in the Support Representative Profile screen.



The screenshot shows a form with two main sections. The top section is labeled 'Login' and contains a text input field with the value 'ExampleCo\BW'. The bottom section is labeled 'Password' and contains a 'Reset' button.

- 2 Open the iSupport Access Utility in the *<directory in which iSupport is installed>\Utilities* folder. In the iSupport Access Utility screen, verify that the Desktop File Path field contains the correct path to the RepClient folder, or change it if necessary. (If the Desktop File Path field does not contain an entry, use the Browse button to select the location of the RepClient folder.) Select the Microsoft® Windows-based radio button in the Desktop Settings section. Then click OK.



The screenshot shows the 'iSupport Access Utility' window. It has a tabbed interface with 'Application', 'Databases', 'SQL Logins', and 'Logging Management'. The 'Application' tab is selected. Under 'iSupport Desktop Settings', the 'Desktop File Path' is 'gram Files\iSupport\RepClient' with a 'Browse' button. The 'Support Representative Authentication Method for iSupport' section has two radio buttons: 'iSupport Login' and 'Microsoft® Windows-Based', with the latter selected. Below this is the 'iSupport Social Client Settings' section, which has a 'Social Client File Path' of 'C:\Program Files\iSupport\Us...' with a 'Browse' button, and a 'Customer Authentication Method for iSupport' section with two radio buttons: 'iSupport Login' and 'Microsoft® Windows-Based', with the former selected.

Configuring Password Complexity, Expiration, and Login Locks

If you are not using Microsoft® Windows-based authentication with iSupport, you can use the Rep Security screen to enable password security options, enter text for the login screen, and configure locks to prevent a support representative who has exceeded a specified number of failed login attempts from logging in.

Configuring Password Complexity and Expiration

Use the Password section to enable a Forgot Password link, password expiration after a specified number of days, a previous password check with a specified number of previous passwords, and minimum password requirements. You can also force a password reset for all support representatives.

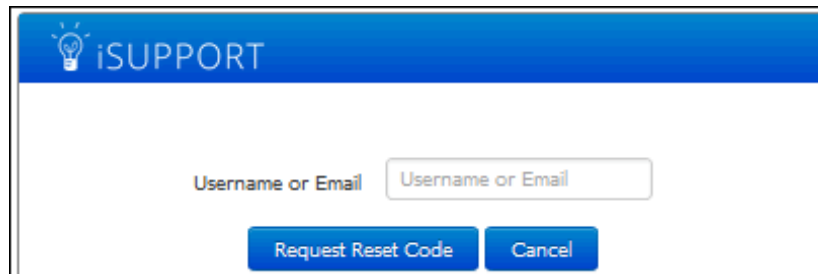
The screenshot shows the 'Password' configuration screen. On the left is a sidebar with navigation links: 'Password', 'Login Screen', 'Failed Login Locks', 'Failed Login Log', and 'Locked Reps'. The main content area has the following settings:

- Enable Forgotten Password:** A toggle switch set to 'Yes'.
- Forgotten Password Notification:** A section with a dropdown menu for 'Rep' set to 'iSupport Default', and '+' and edit icons.
- Enable Password Expiration:** A toggle switch set to 'Yes'.
- Expire Password After:** A text input field with '60' and a 'days' unit selector.
- Warn Support Representative:** A text input field with '2' and a 'days before expiration' unit selector.
- Enable Previous Password Check:** A toggle switch set to 'Yes'.
- Number of Previous Passwords:** A text input field with '3'.

Enable Forgotten Password - Select Yes to include a Forgot Password link in the login dialog and send an email to a support representative with a password reset code. In the Notification field, select iSupport Default to use iSupport's default Forgotten Password notification or use the Create New and View/Edit icons to access the Custom Notifications screen.

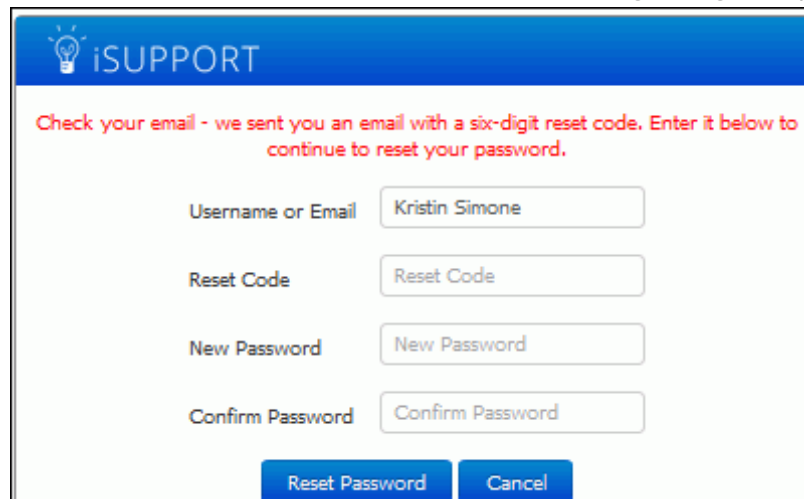
The screenshot shows the iSupport login screen. At the top is a blue header with the iSupport logo. Below the header are two text input fields labeled 'Username' and 'Password'. Below these fields is a blue 'Login' button. At the bottom of the screen is a link labeled 'Forgot Password'.

After the support representative clicks the Forgot Password link, a prompt for a username or email address will appear if the support representative hasn't entered one in the login dialog.



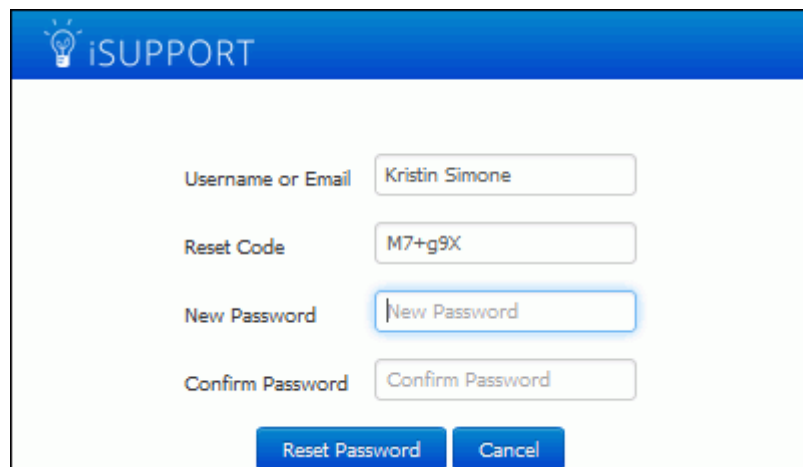
The dialog features a blue header with a lightbulb icon and the text 'iSUPPORT'. Below the header, there is a label 'Username or Email' followed by a text input field containing the same text. At the bottom, there are two blue buttons: 'Request Reset Code' and 'Cancel'.

After an existing username or email address has been entered, the following dialog will appear:



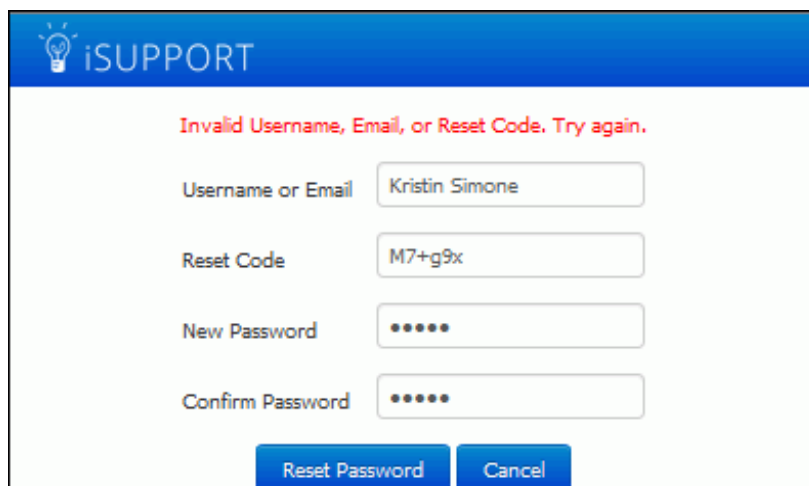
The dialog has a blue header with a lightbulb icon and 'iSUPPORT'. Below the header, a red message reads: 'Check your email - we sent you an email with a six-digit reset code. Enter it below to continue to reset your password.' There are four input fields: 'Username or Email' (containing 'Kristin Simone'), 'Reset Code' (containing 'Reset Code'), 'New Password' (containing 'New Password'), and 'Confirm Password' (containing 'Confirm Password'). At the bottom are two blue buttons: 'Reset Password' and 'Cancel'.

The selected notification will be sent to the support representative with a six-digit reset code and a link to the Desktop login screen. When the link is clicked, a dialog with a Reset Code field will appear.



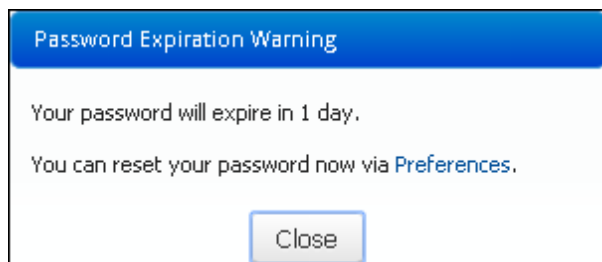
This dialog is identical to the previous one, but the 'Reset Code' field now contains the text 'M7+g9X'. The 'New Password' field is highlighted with a blue border, indicating it is the active field.

The reset code expires if more than 15 minutes has passed since the password request; the following dialog will appear. The support representative can click Cancel to click the Forgot Password link again, and a new reset code must be configured by the administrator.



The image shows a web-based password reset dialog for iSUPPORT. At the top is a blue header with a lightbulb icon and the text 'iSUPPORT'. Below the header, a red error message reads 'Invalid Username, Email, or Reset Code. Try again.' There are four input fields: 'Username or Email' containing 'Kristin Simone', 'Reset Code' containing 'M7+g9x', 'New Password' with masked characters, and 'Confirm Password' with masked characters. At the bottom are two buttons: 'Reset Password' and 'Cancel'.

Enable Password Expiration - Select Yes to specify a number of days after which a newly entered login password will expire. The Password Expiration Warning dialog will display to the support representative after every login via the iSupport Desktop until the configured time frame has been reached. Note that expiration warnings will not appear on the mobile client.

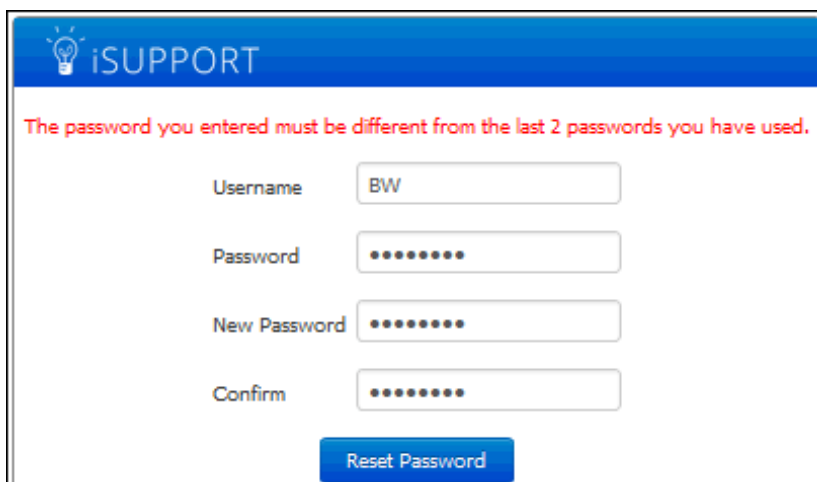


The image shows a 'Password Expiration Warning' dialog box. It has a blue header with the title 'Password Expiration Warning'. The main text says 'Your password will expire in 1 day.' followed by 'You can reset your password now via [Preferences](#).' At the bottom is a 'Close' button.

Expire Password After xx Days - Enter the number of days after which a newly entered login password will expire. The expiration time frame will be based on the last time a support representative reset their password or the date and time at which the Password Expiration feature was last configured.

Warn Support Representative xx Days Before Expiration - Enter the number of days before the expiration date in which to display the Password Expiration Warning dialog.

Enable Previous Password Check - Select Yes to compare a support representative's new password with a configured number of the support representative's previous passwords and prevent use of a matching password.

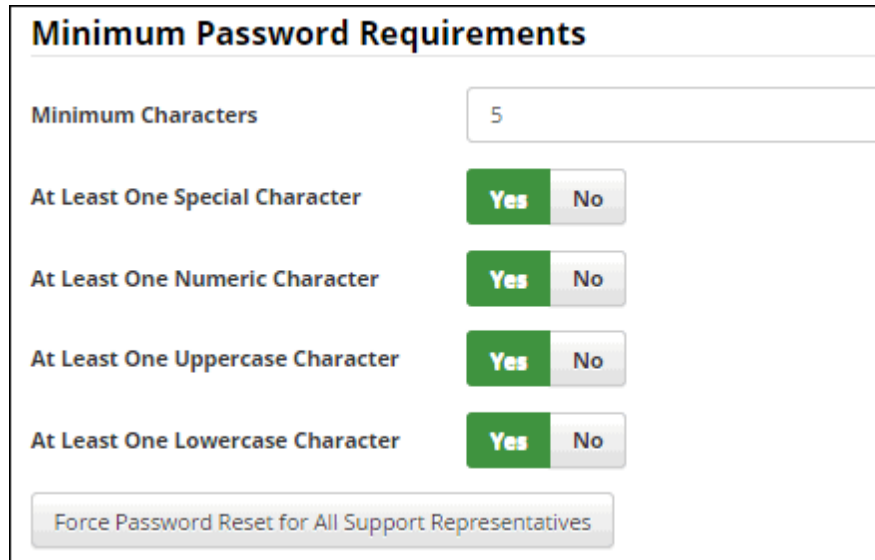


The image shows a web-based password reset dialog for iSUPPORT. At the top is a blue header with a lightbulb icon and the text 'iSUPPORT'. Below the header, a red error message reads 'The password you entered must be different from the last 2 passwords you have used.' There are four input fields: 'Username' containing 'BW', 'Password' with masked characters, 'New Password' with masked characters, and 'Confirm' with masked characters. At the bottom is a 'Reset Password' button.

Number of Previous Passwords - Enter the number of passwords to check against a support representative's new password.

Minimum Password Requirements

Use the fields in this section to require new passwords to contain at least one special character, numeric character, uppercase character, and lowercase character, as well as a minimum number of characters.

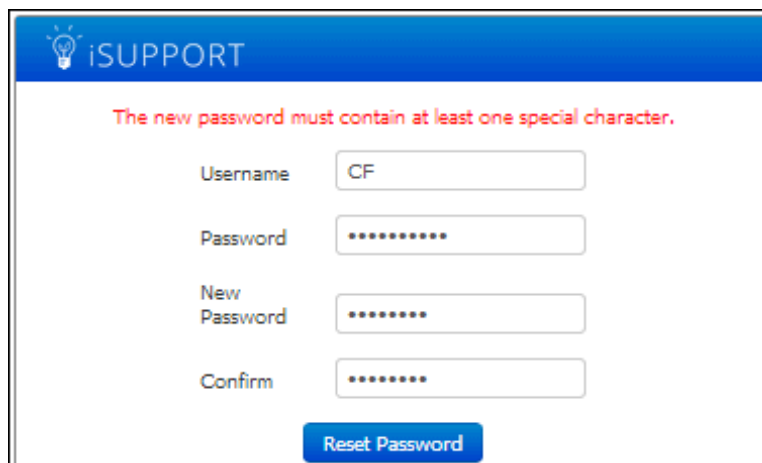


The screenshot shows a configuration window titled "Minimum Password Requirements". It contains five settings:

- Minimum Characters:** A text input field with the value "5".
- At Least One Special Character:** A toggle switch set to "Yes".
- At Least One Numeric Character:** A toggle switch set to "Yes".
- At Least One Uppercase Character:** A toggle switch set to "Yes".
- At Least One Lowercase Character:** A toggle switch set to "Yes".

At the bottom of the form is a button labeled "Force Password Reset for All Support Representatives".

If a support representative tries to enter a password without the minimum requirements, a message will appear with the missing requirement.



The screenshot shows the iSUPPORT password reset interface. At the top, a red error message states: "The new password must contain at least one special character." Below the message are four input fields: "Username" (containing "CF"), "Password", "New Password", and "Confirm", all masked with dots. A blue "Reset Password" button is at the bottom.

Note that configured password requirements will be enforced when you enter a password in the Rep Profile screen.

Minimum Characters - Enter the minimum number of characters that a support representative can use in a newly-entered password.

At Least One Special Character - Select Yes to require a support representative's newly entered password to contain at least one special character that is not a number or letter.

At Least One Numeric Character - Select Yes to require a support representative's newly entered password to contain at least one number.

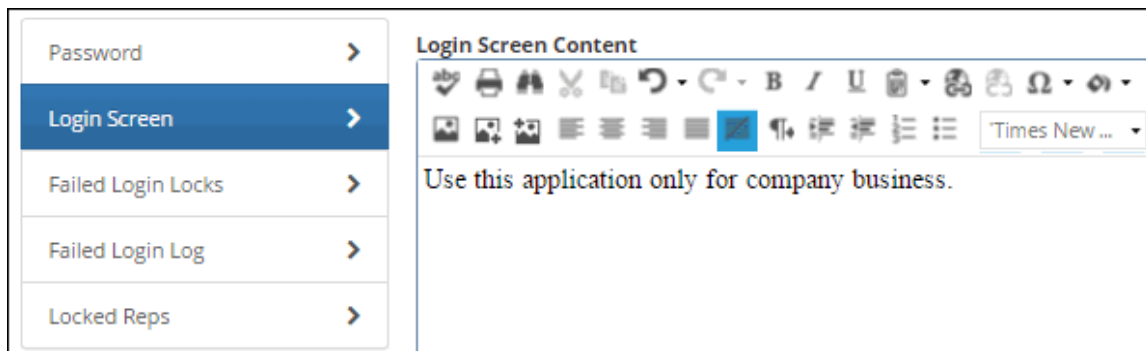
At Least One Uppercase Character - Select Yes to require a support representative's newly entered password to contain at least one capital letter.

At Least One Lowercase Character - Select Yes to require a support representative's newly entered password to contain at least one small letter.

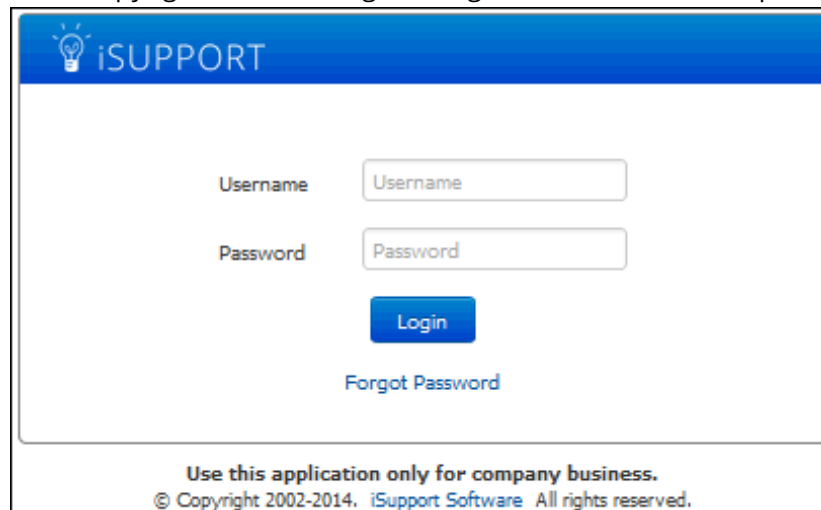
Force Password Reset for All Support Representatives - Select this button to, for each support representative, display the password reset dialog the next time the support representative logs in and require a new password to be entered.

Configuring Login Screen Text

On the Login Screen section, enter the content to appear at the bottom of the login dialog; you can include formatted text and images.



The text will appear above the copyright line in the login dialog as shown in the example below.



Configuring Failed Login Locks

Use the Failed Login Locks section to configure locks to prevent a support representative who has exceeded a specified number of failed login attempts from logging in. You can set a timed lock, an email lock requiring login via a link in an email, or an admin lock which requires an administrator to reset the login lock. You can use the Failed Login Log section to display information on support representatives who have unsuccessfully attempted a login, and the

Locked Reps section to display those who are locked out due to exceeding the configured number of failed login attempts.

The screenshot shows the 'Failed Login Locks' configuration page. On the left is a sidebar with navigation links: Password, Login Screen, Failed Login Locks (highlighted), Failed Login Log, and Locked Reps. The main content area has a header explaining that locks prevent support representatives from attempting another login until conditions are met. Below this, there's a section for 'Timed Lock Enabled' with 'Yes' and 'No' radio buttons, where 'Yes' is selected. A configuration line states: 'After 3 failed login attempts, prevent login for 2 minute(s)'. To the right, under 'Admins to Notify', there's an 'Add Admin' button and a list containing 'Connor Flynn' with a close icon. A 'Notifications' section is expanded, showing two rows: 'Admins' and 'Locked Rep', both with a dropdown menu set to 'iSupport Default' and buttons for adding (+) and editing (pencil) notifications.

You can send notifications for each type of lock; iSupport administrators selected in the Admins to Notify field will be notified for each Admin notification selected for a lock. These notifications can be customized via the Custom Notifications screen.

You can configure the following locks; the three types of locks are ordered when used in combination, and if you enable more than one, the number of login attempts must be progressively larger starting with the timed lock.

- A **timed lock** which prevents login for a specified period of time (the lock would prevail during that time even if the correct login were entered).
- A more restrictive **email lock** which displays a message regarding the lock and sends an email to the support representative, who must use the link in the email to reconnect to the login page in order to continue. If the support representative doesn't use the link and logs in directly, the lock would prevail even if the correct login were entered.

The screenshot shows the 'Email Lock' configuration page. It features a section for 'Email Lock Enabled' with 'Yes' and 'No' radio buttons, where 'Yes' is selected. The configuration line states: 'After 4 failed login attempts, prevent login and email the support rep an unlock link.' Below this, a 'Notifications' section is expanded, showing two rows: 'Admins' and 'Locked Rep', both with a dropdown menu set to 'iSupport Default' and buttons for adding (+) and editing (pencil) notifications.

- An even more restrictive **admin lock** which prevents the support representative from logging in until an iSupport Administrator unlocks his/her profile in the following ways; both will set the failed login attempt count to zero.

Admin Lock Enabled Yes No

After failed login attempts, prevent login and require administrator action to unlock.

▼ Notifications

Admins + ✎

Locked Rep + ✎

Admin Lockout Content Enabled Yes No

Admin Lockout Content

Font Name Size Paragraph St... ⌵

- Use the Unlock Access option on the Actions menu on the Locked Support Representatives section or Desktop view.

View			
Locked Support Representatives			
<div> <div>Actions</div> <div> <div>UNLOCK ACCESS</div> <div>EXPORT</div> <div>Timed</div> </div> </div>			
Failed Login Count	Name	Login	
6	Copeland, Stuart	sc	


- Use the Unlock button in the Rep Profile screen. A Lock button will appear in this screen for support representatives without a lock; you can use it to manually lock out a support representative.

Support Center

External Support

+

Avatar



New

Remove

Cancel

Delete

Unlock

Save

Desktop access for this profile has been locked; click the Unlock button to reset access.

Copyright

©Copyright 1995-2016 Groupware Incorporated. Under the copyright laws, neither the documentation nor the software may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form in whole or in part, without the prior written consent of Groupware Incorporated, except in the manner described in the documentation.

All Rights Reserved.

Groupware Incorporated d.b.a. iSupport Software
110 E 17th Street
Vancouver, Washington 98663
Phone: 360-397-1000
Fax: 360-397-1007

iSupport and mySupport are registered trademarks of Groupware Incorporated. Microsoft, Microsoft Windows, Microsoft SQL Server, Microsoft Active Directory, Microsoft Lync, and Microsoft Windows NT are either registered trademarks or trademarks of the Microsoft Corporation in the United States and/or other countries. Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Apple, iPad, and Safari are trademarks of Apple, Inc., registered in the U.S. and other countries. GoToAssist is a registered trademark of Citrix Systems, Inc. ITIL is a registered trademark of AXELOS Limited. All other product or service names mentioned herein are trademarks of their respective owners. Groupware Inc. makes no warranties, expressed or implied, including without limitation the implied warranties of merchantability and fitness for a particular purpose regarding the software. Groupware Inc. does not warrant, guarantee, or make any representations regarding the use or the results of the use of the software in terms of its correctness, accuracy, reliability, currentness or otherwise. The entire risk as to the results and performance of the software is assumed by you as the customer. The exclusion of implied warranties is not permitted by some jurisdictions. The above exclusion may not apply to you as the customer. Officers, employees, or may not be held liable to you as the customer for any consequential, incidental or indirect damages (including damages for loss of business profits, business interruption, loss of business information and the like) arising out of the use of or inability to use the software even if Groupware Inc. has been advised of such damages, because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitations may not apply to you as the customer.

Portions of iSupport are derived from works created by the following companies; all rights reserved.

- Licensing software developed by XHEO INC (<http://www.xheo.com>)
- Some icons provided by VistalCO.com
- HTML parsing functionality from HTML Agility Pack by Simon Mourier (simonm@microsoft.com)
- Text Editor toolbar functionality from Telerik (www.telerik.com)
- Charting functionality from Visifire (www.visifire.com)
- Twitterizer functionality copyright (c) 2010, Patrick "Ricky" Smith (www.twitterizer.net)
- json.NET functionality copyright (c) 2007 James Newton-King (www.james.newtonking.com)
- <http://www.fatcow.com/free-icons>
- Bootstrap functionality copyright (c) 2014 Twitter, Inc (www.getbootstrap.com)
- Timeline functionality from Vis.js copyright (C) 2010-2015 Almende B.V.
- SQL Server Maintenance Solution, copyright (c) 2013 Ola Hallengren. The software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use or other dealings in the software.

iSupport utilizes or integrates with several third party applications and resources such as Twitter®, Facebook®, Microsoft® Internet Explorer®, Mozilla® FireFox®, Google Chrome™, Apple® Safari®, and jQuery. Changes in these external applications and resources may have a negative impact on functionality in iSupport. Depending on the nature and degree of the change, iSupport will, at its discretion, revise the current version of iSupport or make a corrective change in a future release of iSupport.