



Configuring iSupport[®] Support Representative Functionality

Support Representative functionality controls the features available to support representatives throughout the iSupport application. Contact information, access to features, and more are set in Support Representative Profile records.

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.
- If you already have support representative information in an LDAP-enabled directory server such as Microsoft Active Directory, you'll be able to later use the **Data Source Integration** feature to automatically create support representative profile records in iSupport and synchronize with your source. See ["Using the Data Source Integration Feature" on page 61](#). However, you'll first need to ensure that iSupport is set up to receive all of the information you want from your current data sources.
- If applicable, use the Core Settings | Support Representatives | Roles screen to 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. Access the Roles screen via the Support Representatives option in configuration; see ["Configuring Roles and Permissions" on page 24](#).
- Use the Core Settings | Groups screen to create **support representative groups**; support representatives must be assigned to a primary group. The Administrators group and the Support group are included by default in iSupport. Support representative groups are an important feature in iSupport; in addition to setting roles/permissions for controlling access to iSupport functionality, you can enable Desktop components, the work items/features involved in global search, work item UI settings, and mySupport chat settings for group members. Groups are also used in routing and reporting. See ["Configuring Support Representative Groups" on page 3](#) for more information.
- If applicable, use the Core Settings | Support Representatives | Locations screen to create **locations** for reporting, location-based routing, and setting the display time zone for multiple support representatives. See ["Configuring Locations" on page 49](#) for more information.
- If applicable, use the Core Settings | Support Representatives | Support Centers screen to create **support centers** to assign 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. If a support representative is assigned to a support center, the time-zone for that support center will be used in hours of operation calculations for rule-based actions; if no support center is assigned, the server's time zone will be used. See ["Setting Up Support Centers" on page 50](#) for more information.
- Use the Support Representative Profile screen to create and update individual Support Representative Profile records. There are many options in that screen for controlling access to features, including:
 - Setting routing availability and Outlook/Google Calendar work day hours
 - Enabling access to knowledge approval, approval override, and data override functionality

- Enabling access to the Configuration module/iSupport update notifications, mobile device use, and advanced discussion feed options
- Designating a support representative as a vendor for purchase requests

See [“Configuring Support Representative Profiles” on page 11](#) for more information.

Optional Customization

- Configured roles and permissions will determine whether a support representative can create, edit, and delete a personal or shared dashboard; in the **Alerts and Dashboards Manager** (accessed via the  Desktop Content menu on the Desktop) to optionally add, delete, and rename dashboards and control dashboard access, and automatically push dashboards to the Desktops of all support representatives. Support representatives can customize their Desktop interface by adding personal (private) dashboards with components and a Quick Access icon toolbar. See [“Managing Dashboards for Support Representatives” on page 58](#).
- 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 59](#).

Authentication and Security

- 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 71](#) for more information.
- Enable a third party application (such as Shibboleth and Otko) to pass user credentials so that a user can sign in to mySupport or the iSupport Desktop with the same credentials that they use to log into another application. See [“Setting Up Single Sign On Authentication for the Desktop” on page 1](#).
- If you are not using Microsoft® Windows-based authentication with iSupport, use the Options and Tools | Administer | **Security** screen to enable CAPTCHA, multi-factor authentication, password security options, enter text for the login screen, and configure locks. See [“Configuring Password Complexity, Login Security, Expiration, and Login Locks” on page 8](#) 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. 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. See [“Monitoring Active and Exceeded Sessions” on page 51](#).

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.

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.

Associated Roles	
Name	Description
<input type="checkbox"/> Hardware Repair Role	Permissions for the Hardware Repair group of support representatives

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 8](#).

Limit Route to Primary Members - Select Yes to filter the listed support representatives in the group to only the members of the group who are available and who have the group set as their primary group.

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 24](#) for information on configuring roles.

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

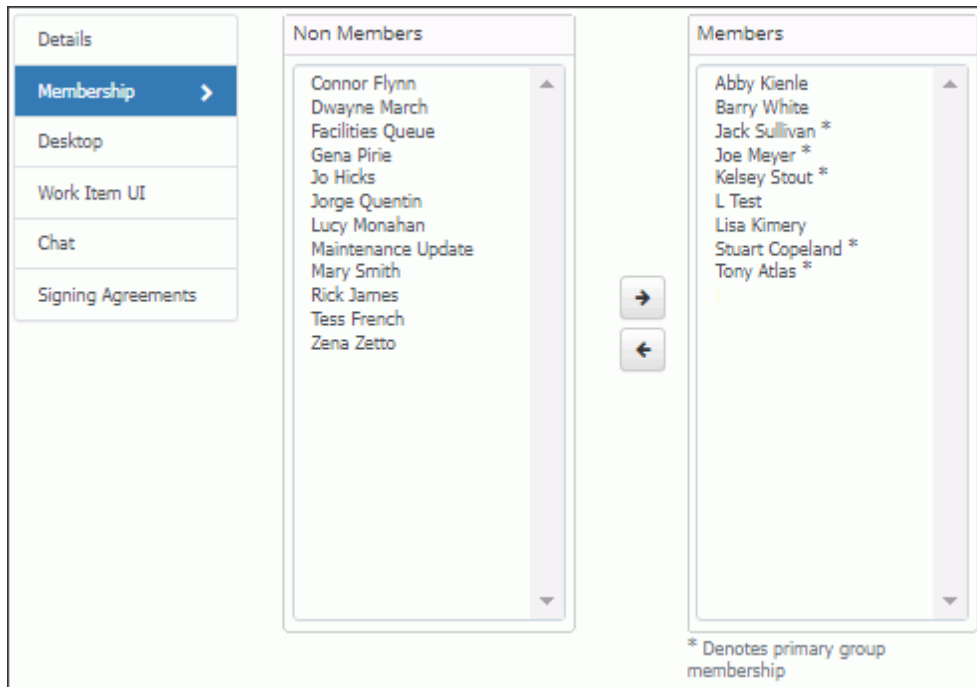
The screenshot shows a user interface with two tabs: "Associated Roles" and "Effective Permissions". The "Effective Permissions" tab is active. On the left, there is a vertical menu with the following items: "Assets", "Changes", "Configuration Items", "Customers", "Desktop Content", "FAQs", "Headlines", "Incidents" (highlighted in blue), "License Management", "Opportunity", and "Personal Correspondence". Each item has a right-pointing arrow. Below the menu is a "Show All" link. The main area displays three roles, each with a checked checkbox and a list of permissions in a scrollable box:

- Reader
 - View My Assigned
 - View My Authored
 - View My Groups
 - View My Location
 - View All
- Author
 - Create New
 - Use Hierarchy Templates
 - Add Work History to All
- Editor
 - 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
 - Route
 - Route By Group Only
 - Route to Unavailable Reps
 - Schedule Recurring
 - Change Approvers
 - Update Via News Feed
 - Delete

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 and  left arrow options. You can also add support representatives to a group via the Rep Profile

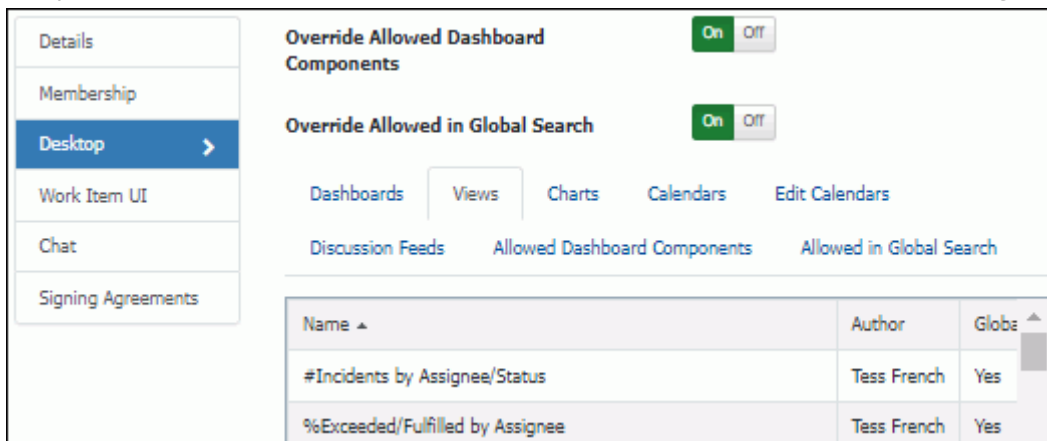
screen; an asterisk indicates that the group has been designated as the support representative's primary group in that screen.



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

Use the Desktop section to:

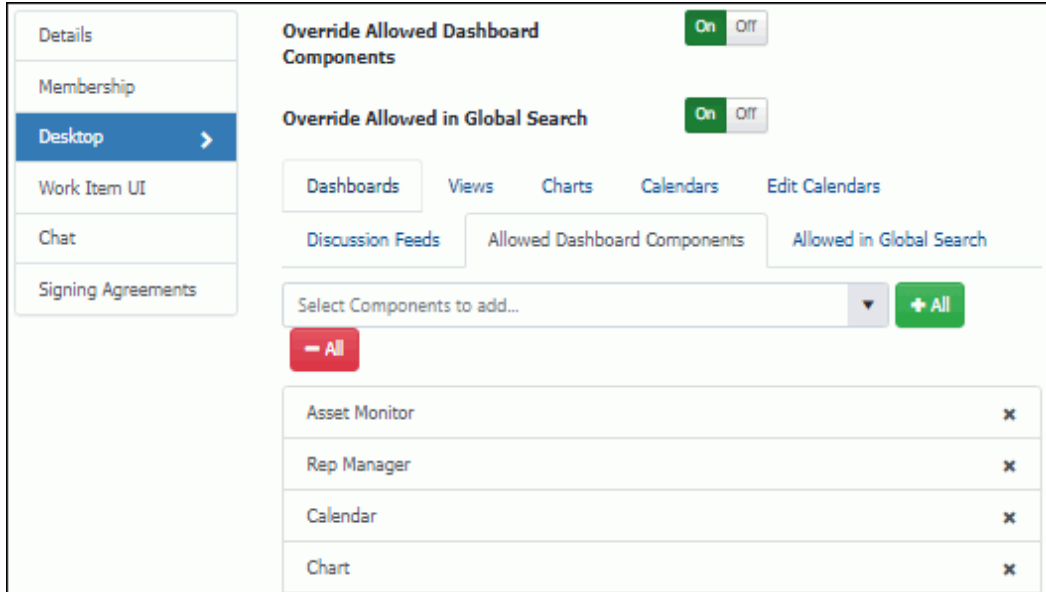
- View the Desktop items (dashboards, views, charts, calendars, and discussion feeds) that the group has access to.



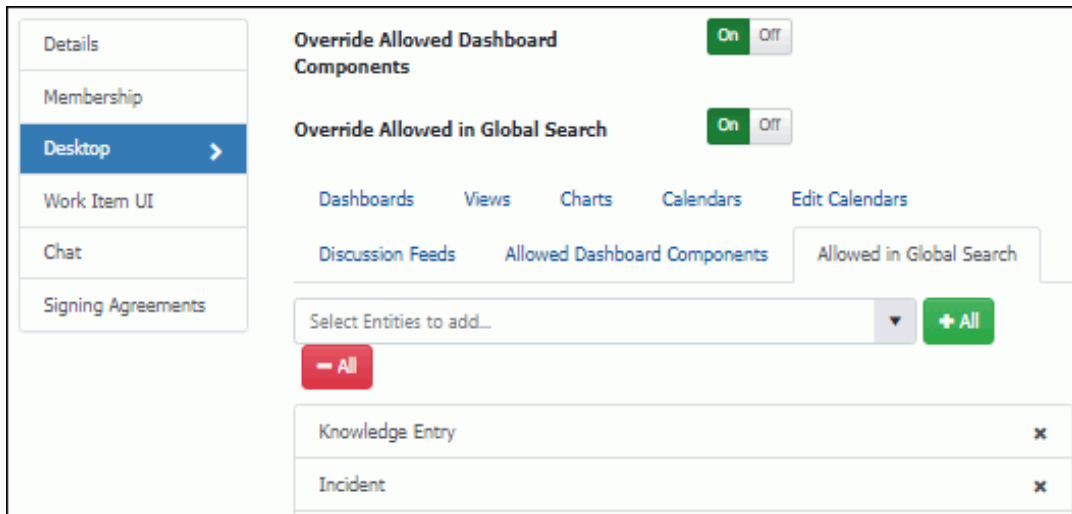
A Yes in the Globally Shared column indicates that there are no group access restrictions for an item; a No in that column indicates that the item has been restricted via one of the following methods:

- 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.





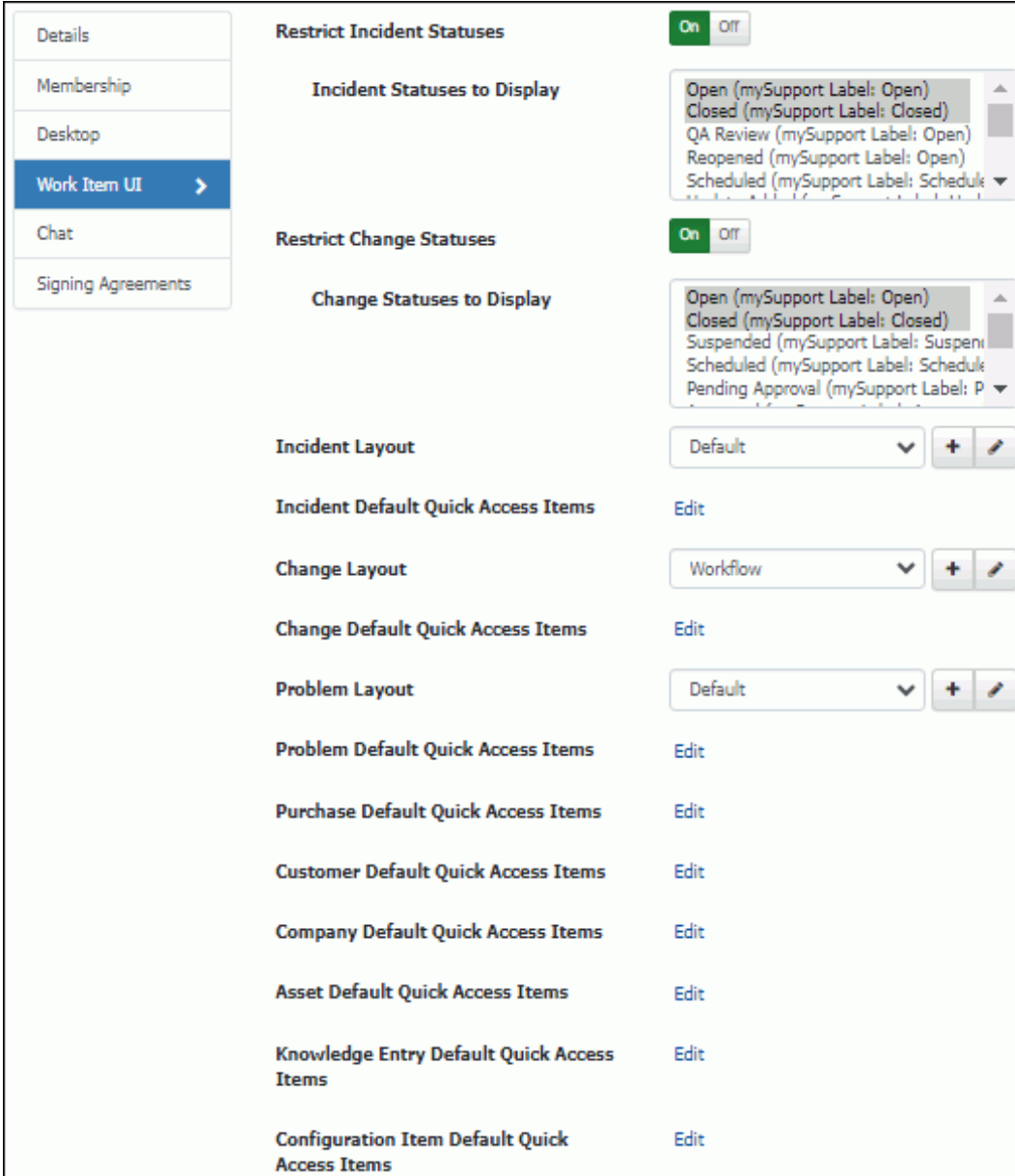
Override Allowed in Global Search - A Global search can be performed via the Global Search component on the Desktop as well as the View | Search feature in the Incident screen. The types of records and features that are involved in a global search are specified in the Dashboard Settings screen; select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



Restricting Statuses, Associating Layouts, and Adding Quick Access Icons

Use the Work Item UI tab to restrict status labels to appear in entry screens and select layouts and quick



access icons to appear to support representatives in the group. You can use the Create New  and View/Edit  icons to access the Layouts configuration screen.



Restrict Incident Statuses/Incident Statuses to Display - To designate the status labels that will be available for selection in incidents created by the template, select On and then select the labels. Note that this applies only to each support representative's primary group.

Restrict Change Statuses/Change Statuses to Display - To designate the status labels that will be available for selection in incidents created by the template, select On and then select the labels. Note that this applies only to each support representative's primary group.

Note: Use the **Order of Precedence** link in the Custom Status Labels screen to set which will prevail if both a template and a support representative group have a restricted status.

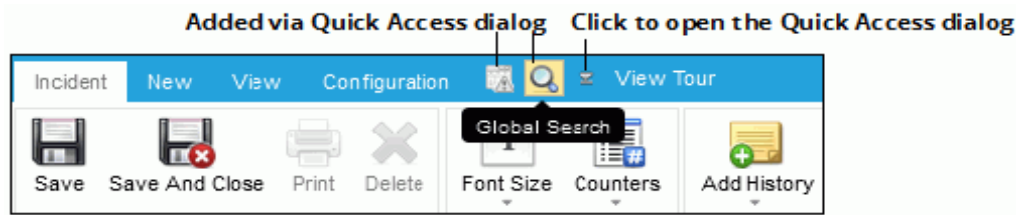
Incident Layout - Select the layout containing the fields and tabs that will display when support representatives in the group access the Incident screen. You can use the  New and  View/Edit options to access the Layouts configuration screen.

Change Layout - This field appears if you have the Service Desk Edition. Select the layout containing the fields and tabs that will display when support representatives in the group access the Change screen. You can use the  New and  View/Edit options to access the Layouts configuration screen.

Problem Layout - This field appears if you have the Service Desk Edition. Select the layout containing the fields and tabs that will display when support representatives in the group access the Problem screen. You can use the New and View/Edit options to access the Layouts configuration screen.

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).

Quick Access Items - 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 option as shown in the example below.



Setting Customer Chat Options

Use the Chat section to set options for support representatives in the group who chat with customers using mySupport. Note that these options do not apply to support representatives chatting with each other.

- Details
- Membership
- Desktop
- Work Item UI
- Chat >
- Signing Agreements

Auto Create Incident for Accepted Chats On Off

Incident Template for Chats Incident Created Via Ch: ▼ + ✎

Max Number of Chats Per Rep

Chat Accepted Response Here to Help ▼ + ✎

Chat Ended by Rep Message

Request Incident Feedback at End of Chat On Off

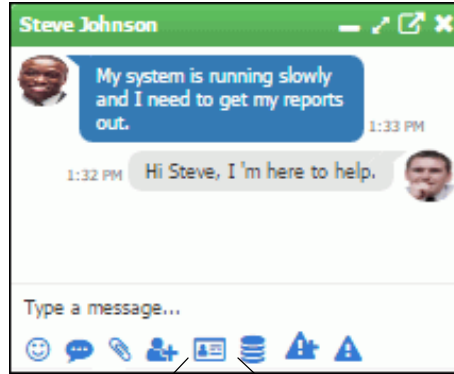
Incident Feedback Satisfied With Our Servix ▼ + ✎

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

	today	6/9/2024	6/10/2024	6/11/2024	6/12/2024	6/13/2024	6/14/2024	6/15/2024
all day	Jack	Jack	Jack	Jack	Jack	Jack	Jack	Jack
8:00 AM								

iSupport Software
Page 8

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, icons will be added for adding the chat transcript to an incident.



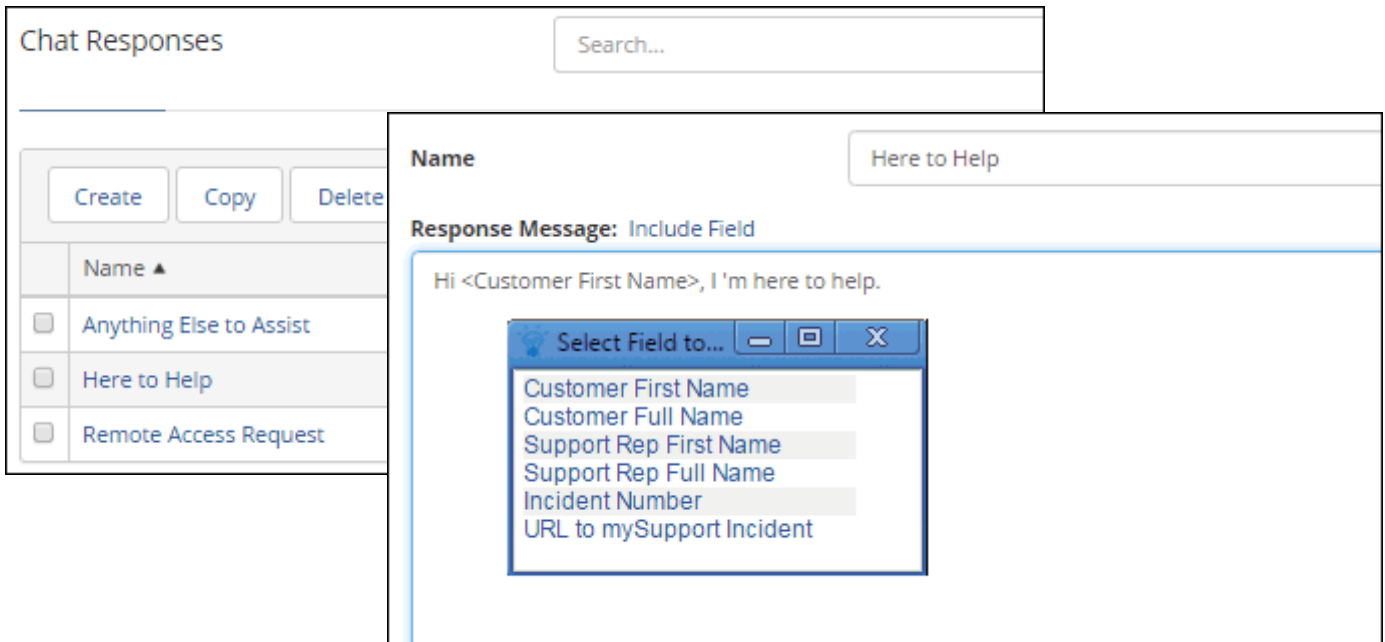
Add chat transcript to history of a new incident

Add chat transcript to history of an existing incident

Incident Template for Chats - Select or create (via the + Create New option) 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).

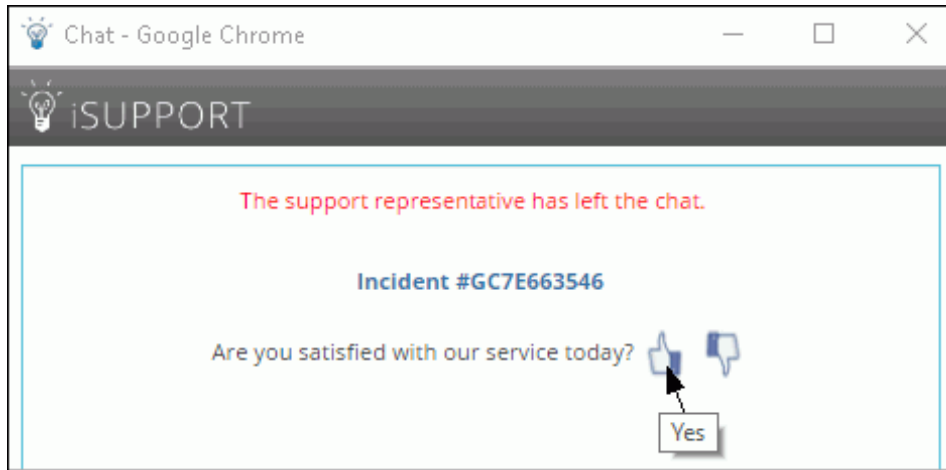
Max Number of Chats Per Rep - Enter the maximum number of accepted chat dialogs that can be open at one time for a support representative.

Chat Accepted Response - Select or create (via the + Create New option) 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.

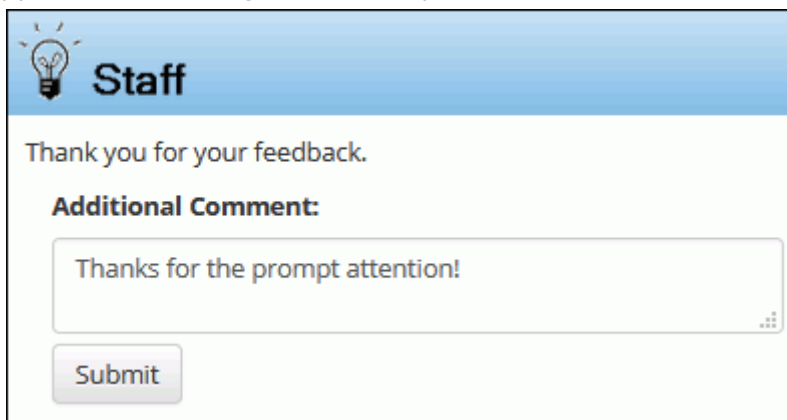


Chat Ended by Rep Message - Enter the message to appear to the customer when the support representative ends the chat.

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.



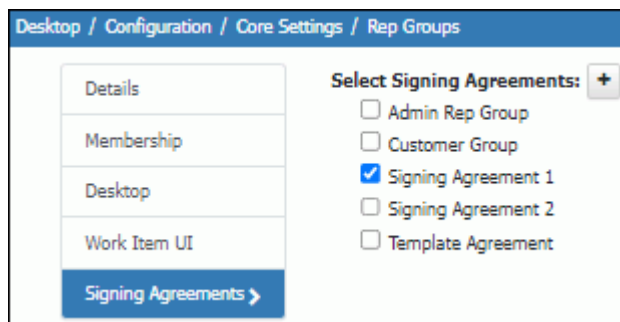
The Comments field will appear after selecting a feedback option.



Associating Signing Agreements

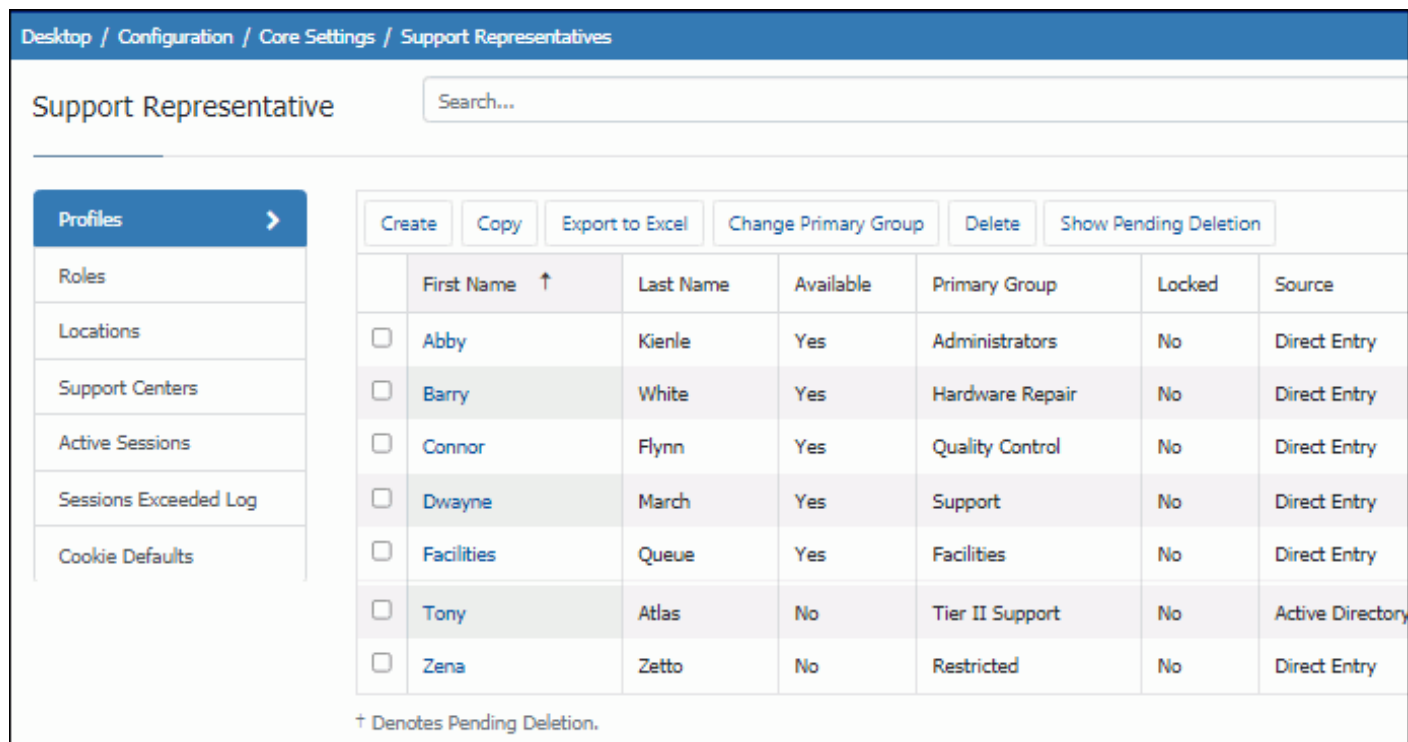
Use a signing agreement to display details in the Sign dialog in the Incident and Change work item screens. Signing agreements can be associated with customer and support representative groups, categories, and incident and change templates. If an incident or change involves more than one associated signing agreement (group, category, or template), all will be included in the Sign dialog in a dropdown for selection. (Note that "Blank" is also included for displaying no text above the signing line.)

On the Signing Agreements tab, select the agreements to appear for selection in the dropdown when the incident or change involves the associated support representative group. Use the plus sign icon to create an agreement via the Signing Agreements configuration screen.



Configuring Support Representative Profiles

Contact information, access to features, and more are set in Support Representative Profile records; use the Support Representative Profile screen to create and update individual Support Representative Profile records.



Desktop / Configuration / Core Settings / Support Representatives

Support Representative

Search...

Profiles >

Roles

Locations

Support Centers

Active Sessions

Sessions Exceeded Log

Cookie Defaults

Create Copy Export to Excel Change Primary Group Delete Show Pending Deletion


	First Name ↑	Last Name	Available	Primary Group	Locked	Source
<input type="checkbox"/>	Abby	Kienle	Yes	Administrators	No	Direct Entry
<input type="checkbox"/>	Barry	White	Yes	Hardware Repair	No	Direct Entry
<input type="checkbox"/>	Connor	Flynn	Yes	Quality Control	No	Direct Entry
<input type="checkbox"/>	Dwayne	March	Yes	Support	No	Direct Entry
<input type="checkbox"/>	Facilities	Queue	Yes	Facilities	No	Direct Entry
<input type="checkbox"/>	Tony	Atlas	No	Tier II Support	No	Active Directory
<input type="checkbox"/>	Zena	Zetto	No	Restricted	No	Direct Entry

† Denotes Pending Deletion.

You can use the Show Pending Deletion link to display records that have been deleted by an iSupport user but are retained in the system because of references to other records (incidents, correspondence, etc.) The Database Maintenance agent ultimately removes these records. When the Show Pending Deletion link is selected, records that are pending deletion will display with a cross symbol.

Completing Rep Details

Desktop / Configuration / Core Settings / Support Representatives

Details >	First Name	Barry
Advanced	Last Name	White
Groups	Email Address	BW@lblsoft.com
Roles	Alt Email Address	BW@example.com
Skills	Phone	360-397-1000
Calendar	Fax	360-397-1007
Dashboards	Mobile	360-397-1008
Rep Manager Groups	SMS Carrier	Verizon Wireless <input type="button" value="+"/> <input type="button" value="✎"/>
Routing Availability	Login	BW
Routing Availability Log	Password	Reset
	First Rep to Notify	Abby Kienle <input type="button" value="v"/>
	Second Rep to Notify	Connor Flynn <input type="button" value="v"/>
	Location	Headquarters <input type="button" value="+"/> <input type="button" value="✎"/>
	Support Center	West Coast <input type="button" value="+"/> <input type="button" value="✎"/>
	Avatar	 <input type="button" value="New"/> <input type="button" value="Remove"/>

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 for iSupport email notifications (and SMS notifications if Twilio integration is not configured and no value exists in the Alt Email Address field).

Alt Email Address - Enter an alternate email address for the support representative. In addition to informational purposes, this number will be used for SMS notifications and authentication codes sent by iSupport if Twilio integration is not configured. (If a value in this field is unavailable, the address in the Email field will be used.)

Phone - Enter the phone number for the support representative.

Fax - Enter the fax number for the support representative.

Mobile - Enter the support representative's mobile phone number. In addition to informational purposes, this number will be used for SMS notifications and authentication codes sent by iSupport if Twilio integration is configured. (If Twilio is not configured, the address in the Alt Email field will be used; if that is unavailable, to the address in the Email field will be used.)

SMS Carrier - Select the carrier that will be added to the mobile number to form the address that will be used for SMS notifications and multi-factor authentication. Available carriers are set up in the Options and Tools | Integrate | SMS Carriers screen.

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 71 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 their 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, Login Security, Expiration, and Login Locks"](#) on page 8 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.

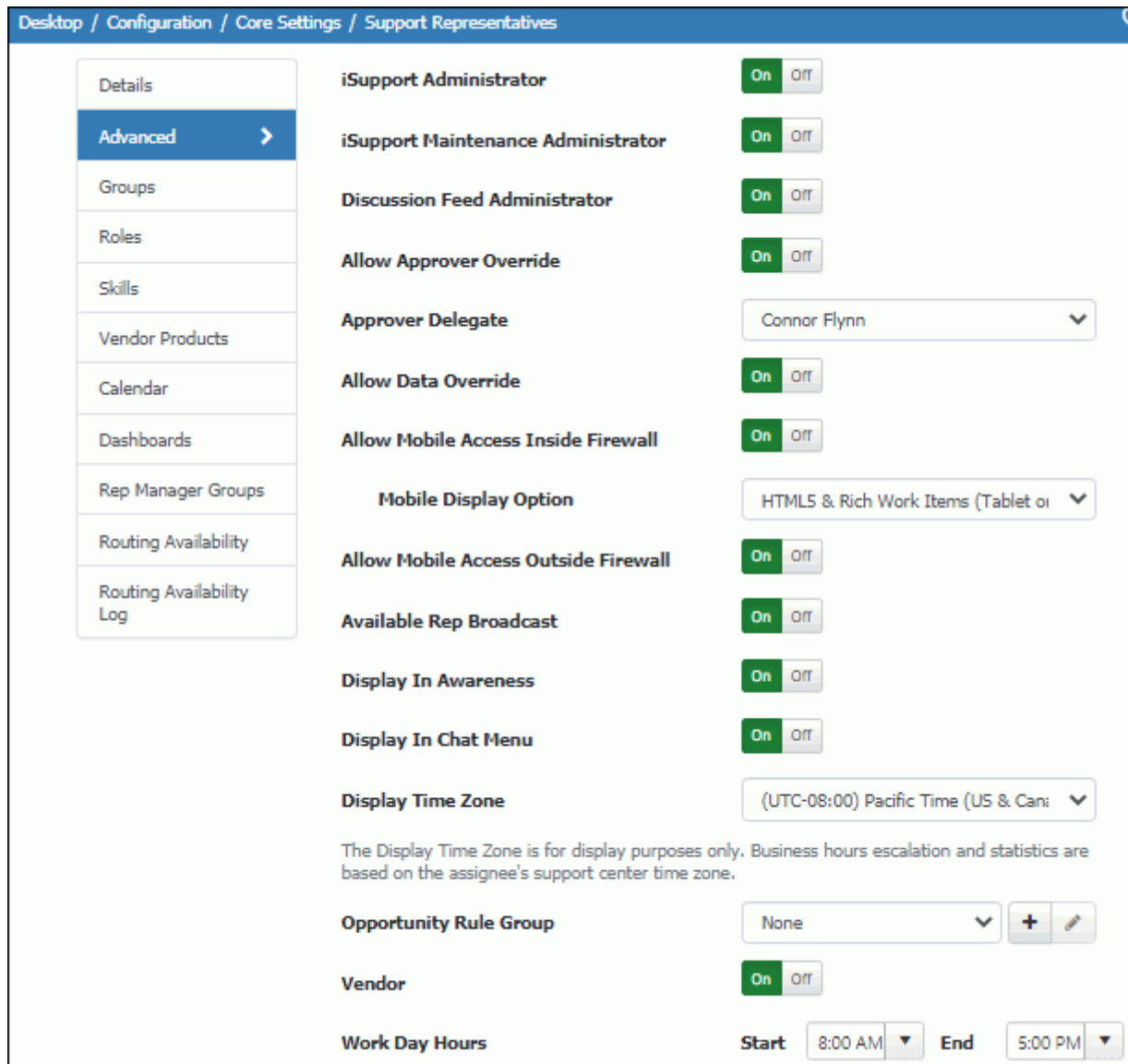
Location - Enter locations via the Location tab in the list view that appears. Select the location for the support representative. Locations are used for location-based routing and setting the display time zone for multiple support representatives.

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

Use the Advanced tab to set miscellaneous options for controlling the support representative's access to iSupport functions.



Desktop / Configuration / Core Settings / Support Representatives

Details

Advanced

Groups

Roles

Skills

Vendor Products

Calendar

Dashboards

Rep Manager Groups

Routing Availability

Routing Availability Log

iSupport Administrator On Off

iSupport Maintenance Administrator On Off

Discussion Feed Administrator On Off

Allow Approver Override On Off

Approver Delegate Connor Flynn

Allow Data Override On Off

Allow Mobile Access Inside Firewall On Off

Mobile Display Option HTML5 & Rich Work Items (Tablet or

Allow Mobile Access Outside Firewall On Off

Available Rep Broadcast On Off

Display In Awareness On Off

Display In Chat Menu On Off


Display Time Zone (UTC-08:00) Pacific Time (US & Can:)

The Display Time Zone is for display purposes only. Business hours escalation and statistics are based on the assignee's support center time zone.

Opportunity Rule Group None


Vendor On Off

Work Day Hours Start 8:00 AM End 5:00 PM

iSupport Administrator - Select On to enable the  Configuration option to appear on the Desktop for access to the Configuration module for configuring all iSupport functionality. 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 following for the support representative:

- When configuring a news feed, the Access tab will display with options for setting a feed to shared (allowing others to view it) and restricting a feed to specified groups or support representatives
- The ability to edit configuration options on a shared feed (via the  Edit option next to the name of a shared feed in the News Feed component or the Edit button in the Content Manager)
- The Delete, Remove, Move, Merge, Disallow Replies, and Pin options for discussion feed entries (posts and replies) in the News Feed component on the Desktop.

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

Approver Delegate - Select a support representative who can specify a verdict on work items pending approval for the support representative. In effect, this substitutes the delegate for the support representative in any approval cycles that activate while this field is populated. Note that a support representative can change their approver delegate via the Desktop Preferences screen.

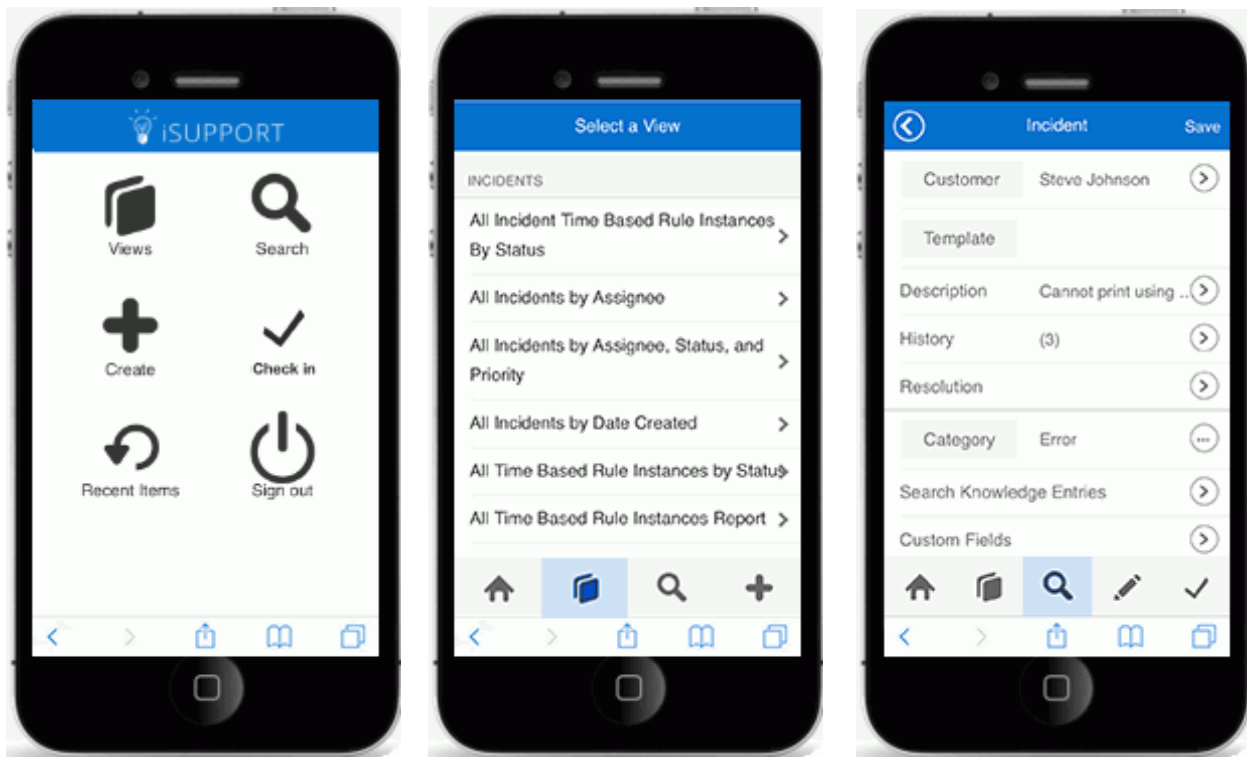
Allow Data Override - Select On to enable the support representative to overwrite fields on any saved or closed incident, problem, change, or service contract. When a change is made using this feature, it will be logged in the Audit History field and notifications will be suppressed. If an approval cycle 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.

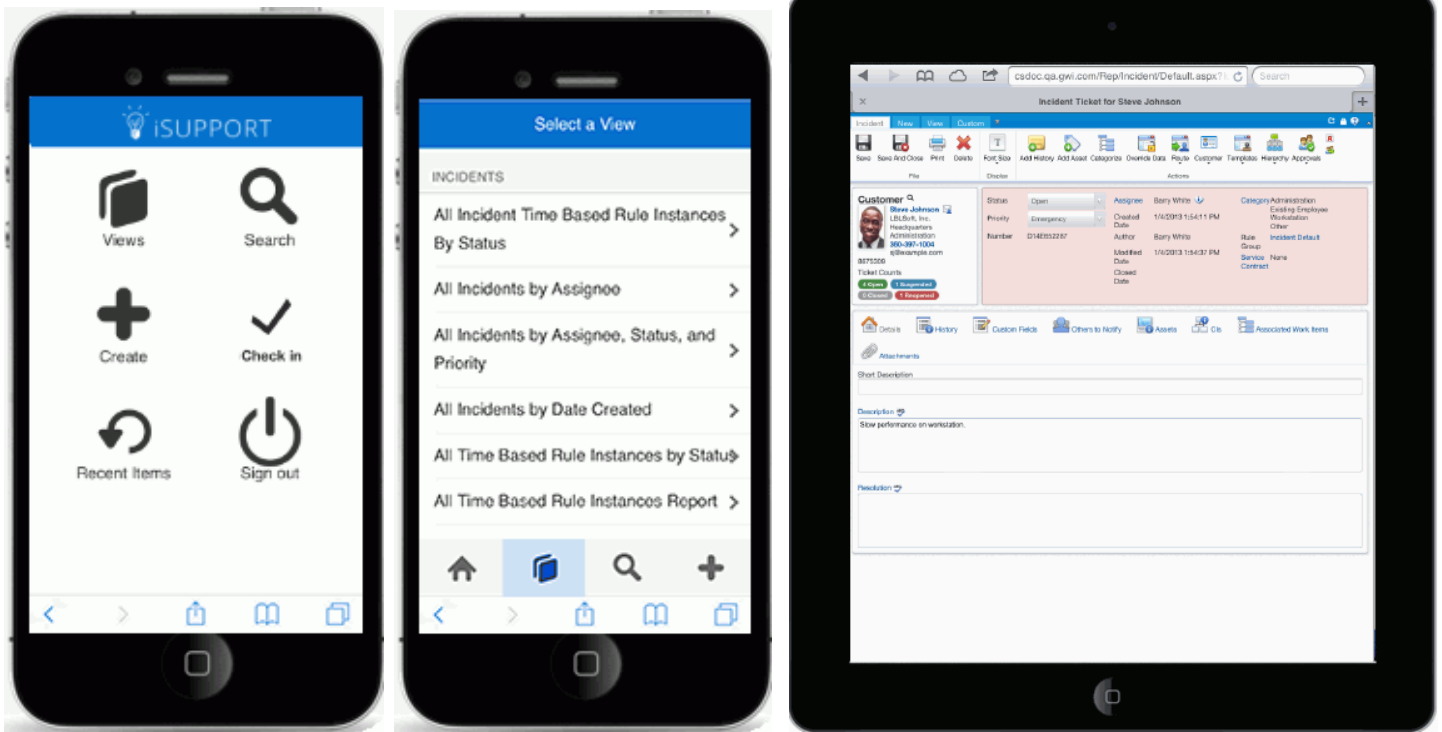
Mobile Display Option - If accessing iSupport inside the firewall via a smart phone or tablet, select HTML5 to display the HTML5 interface via a phone or tablet. Select HTML5 & Rich Work Items (Tablet Only) to enable work items to appear in an interface when accessed via a tablet.

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  alert 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 in Chat Menu - Select Off to prevent a support representative from being included in the list of support representatives available for chat.


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 their display time zone in the Preferences screen, it will be updated in their Support Representative record.

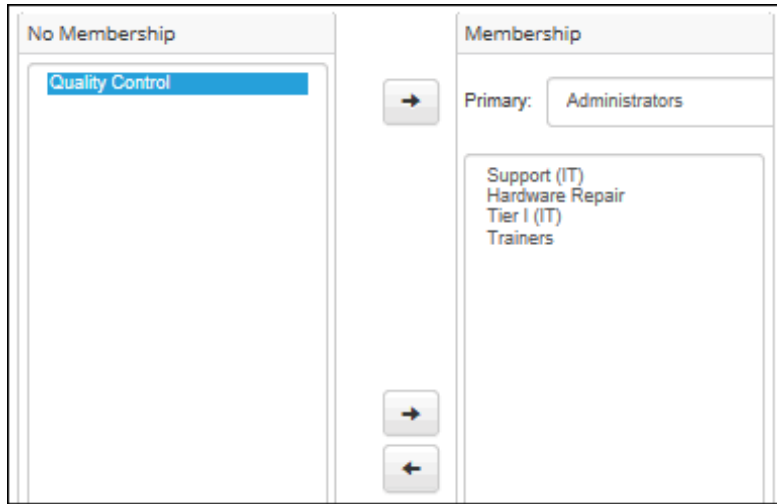
Opportunity Rule Group - If you have the Service Edition and Opportunity Management functionality is enabled, select the opportunity rule group to be applied when the support representative is assigned to an opportunity.

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

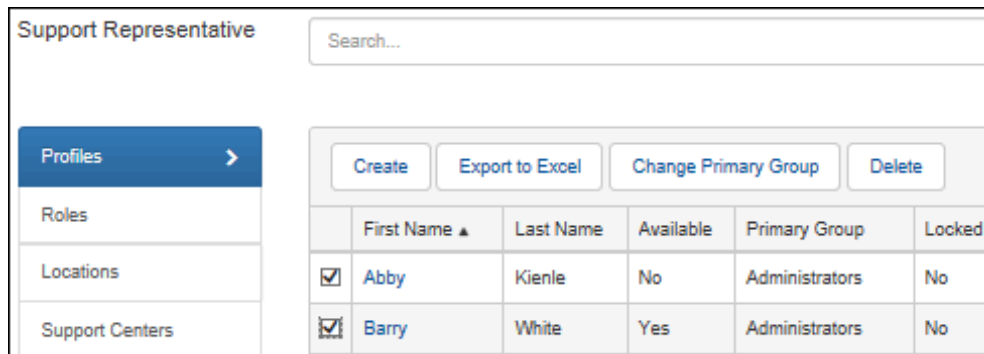
Use the Groups section to designate the support representative as a member of groups for reporting, group-based routing, and permissions. Support representatives must be assigned to a primary group. To designate the support representative's primary group, select the group in the No Membership field and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



When the primary group of a support representative is initially set or edited, an option appears for pushing all of the shared dashboards that it has specific permissions to access.

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.



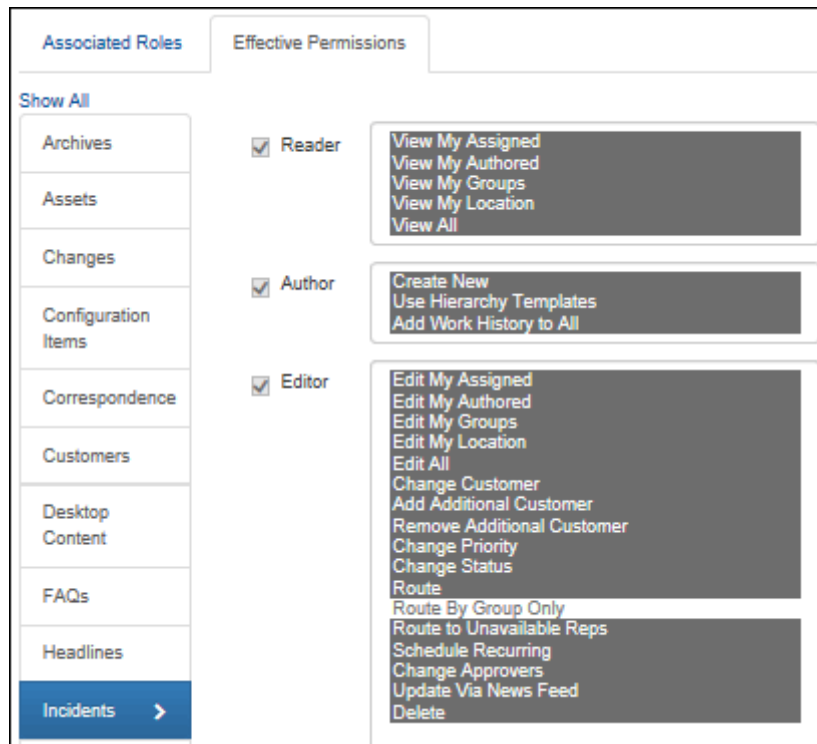
Associating Roles

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 24](#) 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.

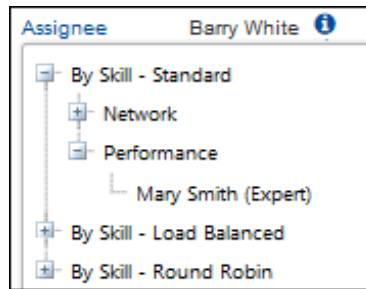


Designating Skills

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

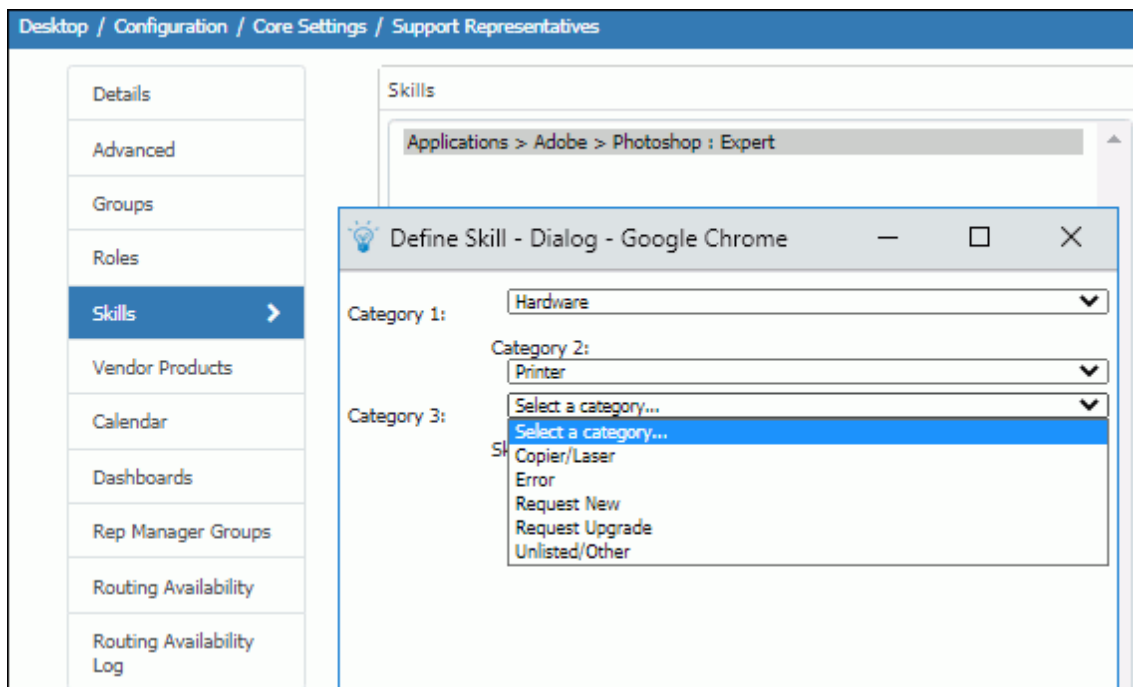
After a support representative classifies the incident, problem, or change (if enabled) and selects skill-based routing, the selected category levels will appear along with the support representative(s) that have those skills configured in their profile.



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.

	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.

Calendar to add new appointments to:
 Google Calendar™ Microsoft® Outlook® Both

5/29/2019 - DAY WEEK MONTH TIMELINE

Sun, 29 Mon, 30 Tue, 31 Wed, 1 Thu, 2 Fri, 3 Sat, 4

all day

8 am

9 am

10 am

11 am

12 pm

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>

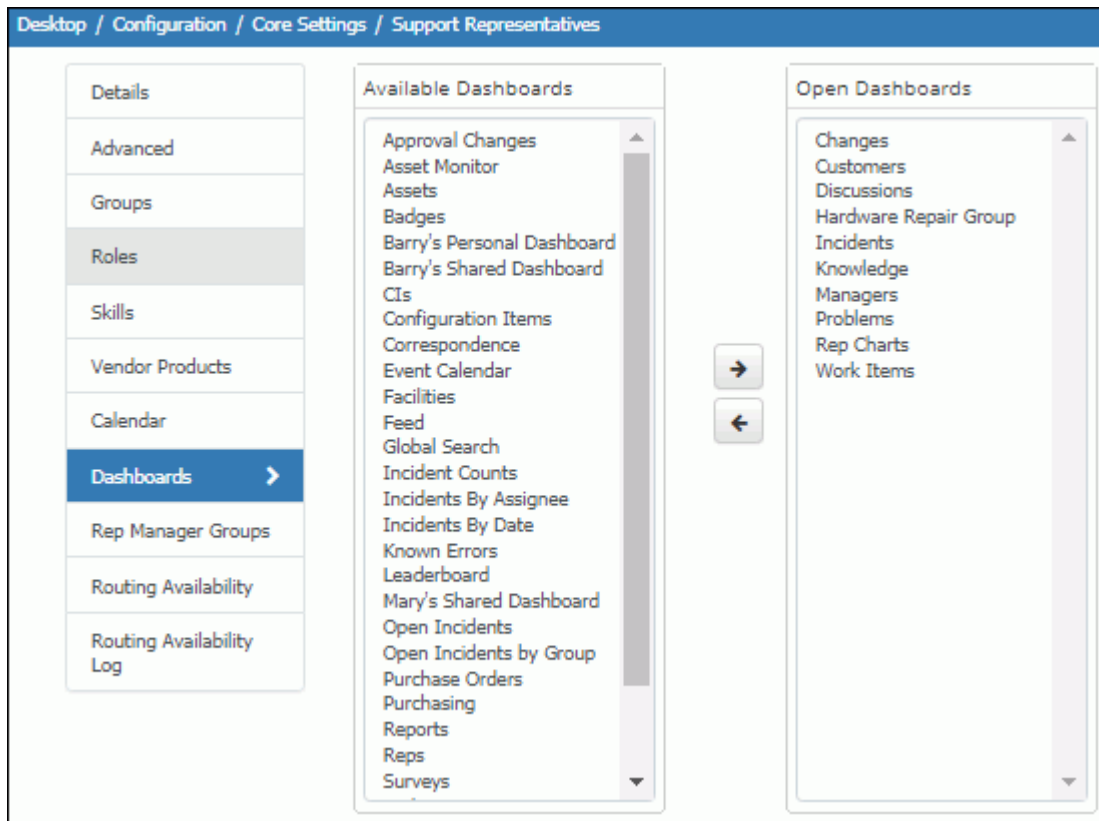
Working on Incident E8SD686A77

Managing Dashboards

The Dashboards tab displays the dashboards available to the support representative and the dashboards currently open on their Desktop. You can:

- Select dashboards in the Available Dashboards section and click the right arrow to push the dashboards to the support representative's Desktop, and

- Select dashboards in the Open Dashboards section and click the left arrow icon to close dashboards on the support representative's Desktop.

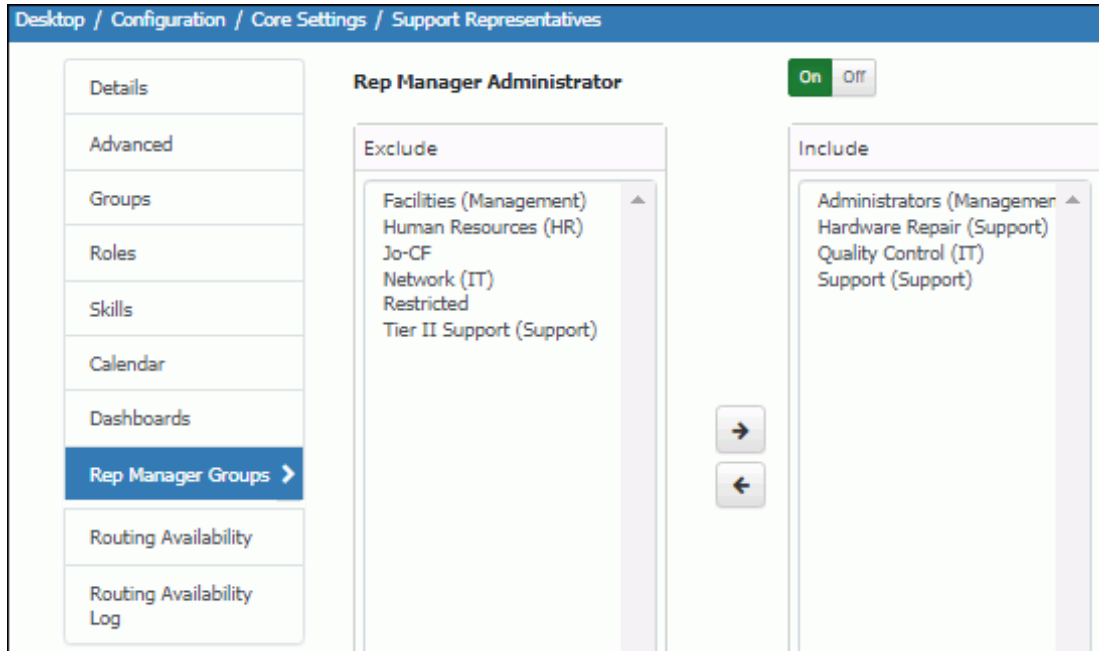


When the primary group of a support representative is initially set or edited, an option appears for pushing all the shared dashboards the new primary group has explicit permissions to access. If the administrator selects OK to push the group's dashboards, the Groups tab will be updated automatically to reflect any new dashboards that will open for the support representative when the profile is saved. Further changes can be manually applied after the group's dashboards are pushed into the Open Dashboards section.

Designating Rep Manager Groups

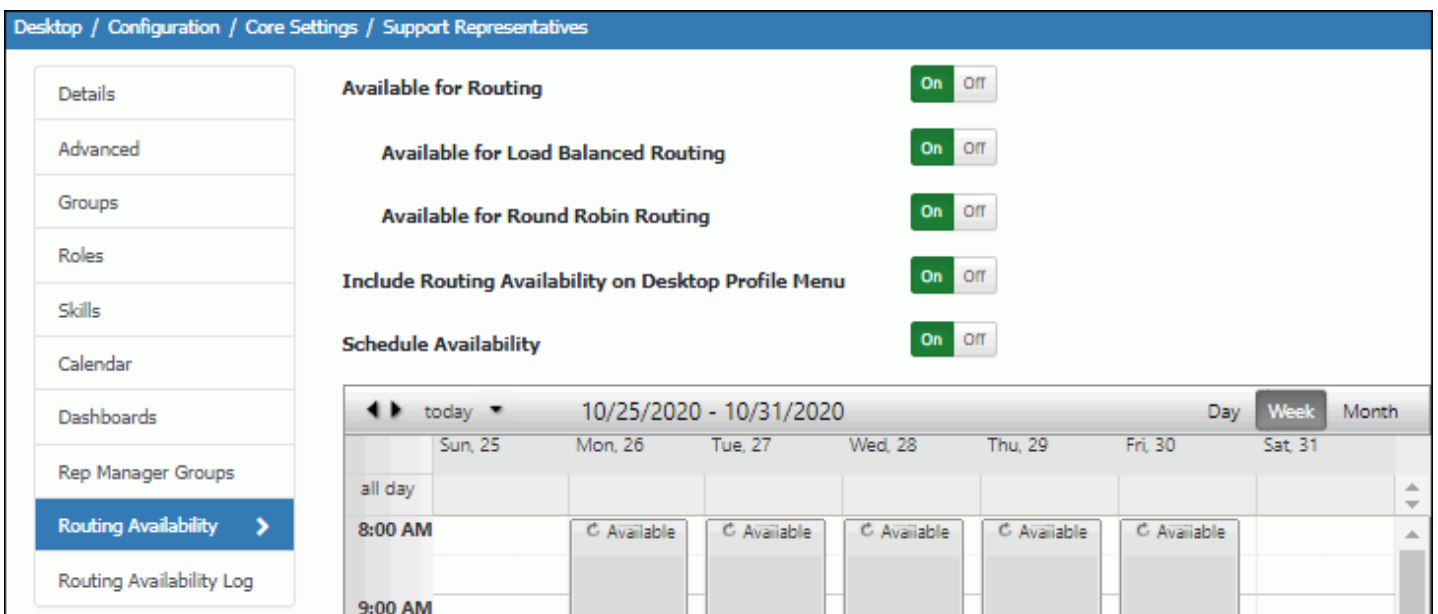
Use the Rep Manager Groups tab to designate the support representative groups that will appear to the support representative in the Desktop Rep Manager component which enables a support representative or administrator to control routing availability. Enable component availability via the Desktop Settings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



Setting Routing Availability Options

Use the Routing Availability tab to set individual routing options for the support representative.

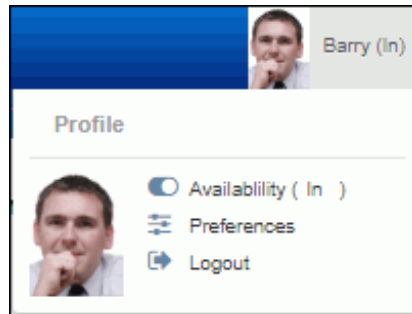


Available For Routing - Select:

- On to designate the support representative as available for assignment of incidents (and problems and changes 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 assignee of incidents and changes submitted via a mySupport portal, an incident or change template, and email-submitted incidents and changes.

- **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.

Include Routing Availability on Desktop Profile Menu - Select On to display the Availability (In/Out) option on the Profile menu that appears after clicking a support representative's avatar/name on the Desktop.

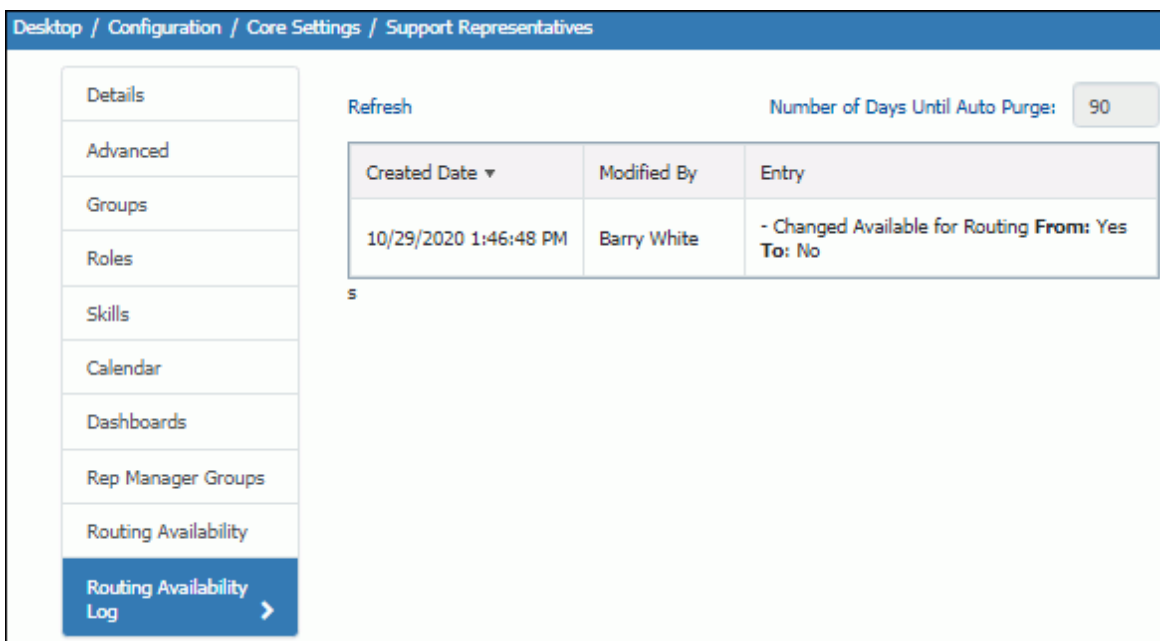


Schedule Availability - Select On to display a calendar and set the times that the support representative can be assigned incidents (and problems and changes if enabled). Note that this will not prevent assignment if the support representative is the default assignee of incidents/problems/changes submitted via the mySupport portal, an incident or change template, and email-submitted incidents and changes. Note that routing availability can also be manually controlled via the following:

- If enabled, the Availability (In/Out) option on the Profile menu that appears after clicking a support representative's avatar/name on the Desktop.
- The Rep Manager Desktop component.

Viewing the Routing Availability Log

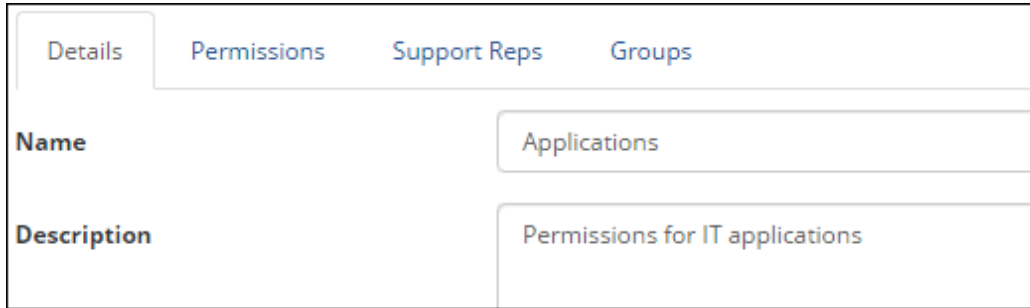
Use the Routing Availability Log tab to view the date and time of routing availability changes along with the name of the support representative who made the change and specifics about which of the three routing availability-related settings changed.



Configuring Roles and Permissions

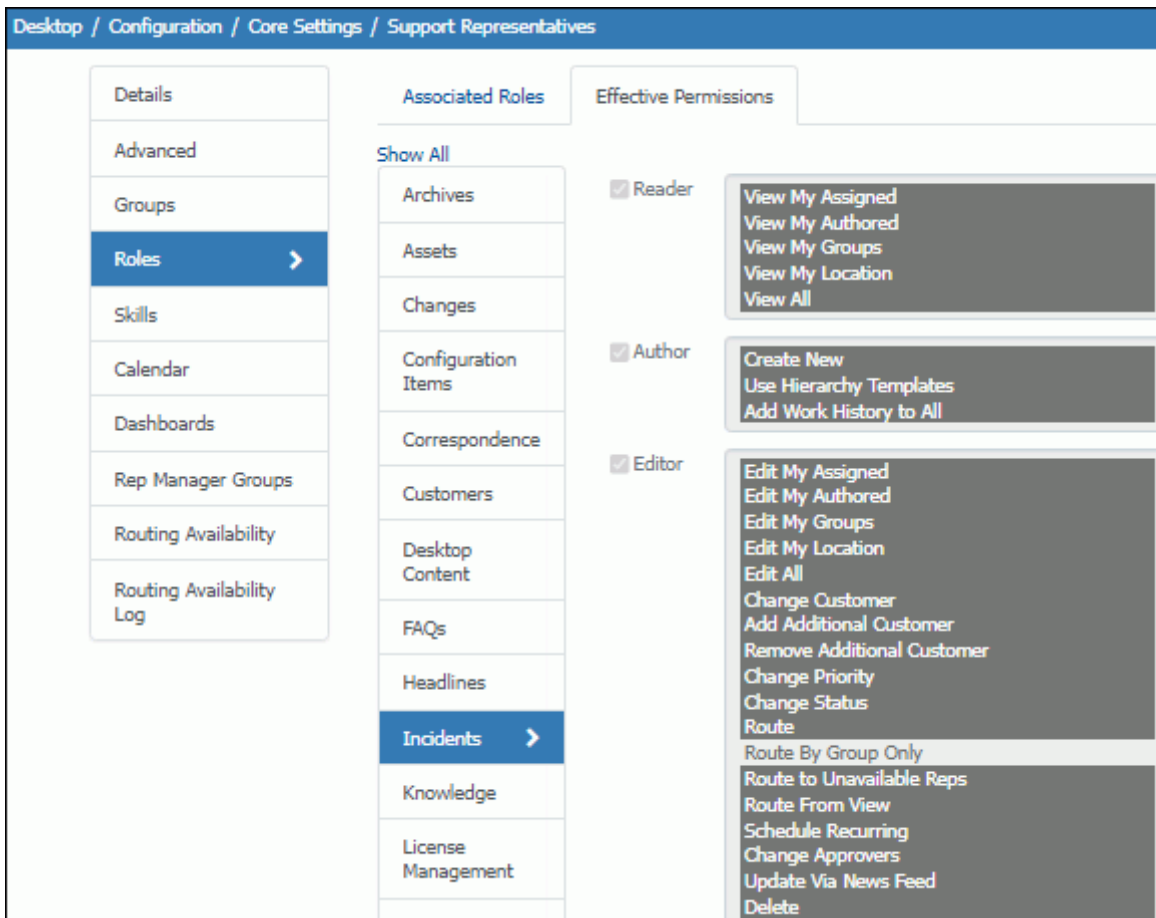
iSupport's permissions allow or disallow certain types of access to functionality; enable roles to select and assign a set of permissions to individual support representatives or groups of support representatives. This functionality is completely configurable; for example, you could create department-based roles or roles with more restrictive permissions for beginners and less restrictive permissions for managers.

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.



The screenshot shows a form with four tabs: Details, Permissions, Support Reps, and Groups. The 'Details' tab is active. It contains two input fields: 'Name' with the value 'Applications' and 'Description' with the value 'Permissions for IT applications'.

If multiple roles are associated with a support representative or group, **all** permissions associated with those roles will be in effect. You can view all of the permissions in effect for a support representative via the Effective Permissions subtab in the Roles screen.



The screenshot shows the 'Effective Permissions' subtab in the Roles screen. The breadcrumb trail is 'Desktop / Configuration / Core Settings / Support Representatives'. The left sidebar has 'Roles' selected. The main content area is divided into 'Associated Roles' and 'Effective Permissions'. Under 'Associated Roles', 'Incidents' is selected. Under 'Effective Permissions', three roles are listed: 'Reader', 'Author', and 'Editor', each with a checked checkbox. The 'Reader' role has permissions: View My Assigned, View My Authored, View My Groups, View My Location, and View All. The 'Author' role has permissions: Create New, Use Hierarchy Templates, and Add Work History to All. The 'Editor' role has permissions: 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, Route, Route By Group Only, Route to Unavailable Reps, Route From View, Schedule Recurring, Change Approvers, Update Via News Feed, and Delete.

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.

The screenshot shows the 'Permissions' tab for the 'Incidents' section. On the left, a list of categories is shown, with 'Incidents' selected and highlighted in blue. The main area is divided into three sections based on roles: Reader, Author, and Editor. Each role has a list of permissions that can be selected or deselected. On the right side, there are links for 'Select All Incident Permissions' and 'Clear All Incident Permissions'.

Role	Permissions
<input checked="" type="checkbox"/> Reader	View My Assigned View My Authored View My Groups View My Location View All
<input checked="" type="checkbox"/> Author	Create New Use Hierarchy Templates Add Work History to All
<input checked="" type="checkbox"/> Editor	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

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. Use the Archives tab in the Support Representative Management | Roles | Permissions screen to allow or disallow access to archived work items and sent correspondence.

The screenshot shows the 'Permissions' tab for the 'Archives' section. The 'Archives' tab is selected and highlighted in blue. A note is displayed: 'Note: The Archive Viewer allows display of archived work items and sent correspondence (not associated with an open work item). All archived work item information will appear even if permissions have been restricted for viewing the information.' Below the note, there are two sections for roles: Reader and Editor. The Reader role has a 'View' permission, and the Editor role has a 'Delete' permission. On the right side, there are links for 'Select All Archive Permissions' and 'Clear All Archive Permissions'.

Role	Permissions
<input checked="" type="checkbox"/> Reader	View
<input checked="" type="checkbox"/> Editor	Delete

Reader - Click the Reader checkbox or select **View** to allow the support representative 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 on archived work items, even if incident permissions have been restricted. This includes archived incidents (with a Closed status that have been moved to an archive database), archived correspondence (displays archived sent correspondence that was not associated with open incidents), etc.

Editor - Click the Editor checkbox or select **Delete** to allow the support representative to delete archived work items.

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.

Role	Permissions
<input checked="" type="checkbox"/> Reader	View Asset View Scan/Comparison
<input checked="" type="checkbox"/> Author	Create New Asset Use Multiple Asset Wizard Create Scan/Comparison
<input checked="" type="checkbox"/> Editor	Edit Asset Edit Count Used Delete Scan/Comparison Delete Asset

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 Asset option will not be included on the Desktop Create menu, 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 you have the Service Desk Edition and Change functionality is enabled; select Changes to allow or disallow access to Change functions such as creating, viewing, updating fields, and routing.

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 Change option will not be included on the Desktop Create 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 option 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.

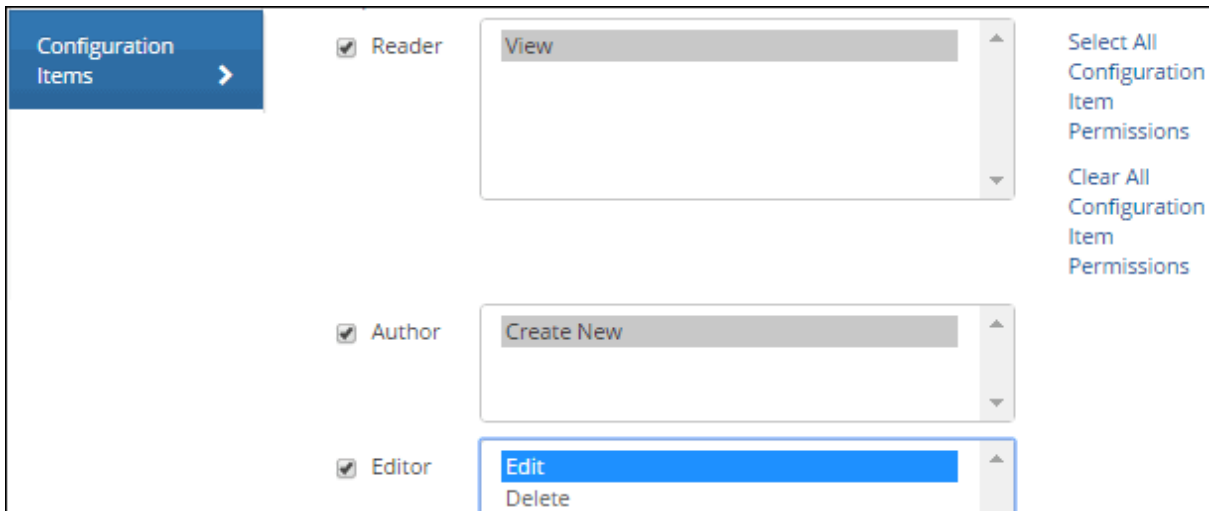
- **Edit My Assigned:** Select to allow the support representative to update any Change record to which they are assigned. If this option is not selected, the support representative will not be able to update their assigned Change records. Note: the View My Assigned permission is required for this permission.
- **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.
- **Publish:** Select to allow the support representative to select the Publish to mySupport field for a saved Change record. Note: 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 option 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 you have the Service Desk Edition and 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.



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.

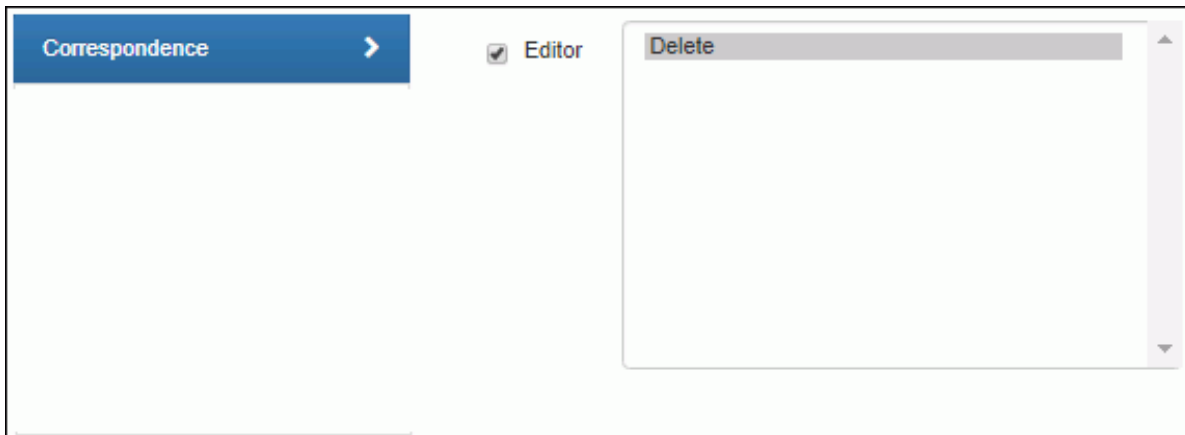
Author - Click the Author checkbox or select **Create New** to allow the support representative to create new Configuration Item records. If this option is *not* selected, the Configuration Item option will not be available to the support representative on the Desktop Create menu and in the Configuration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

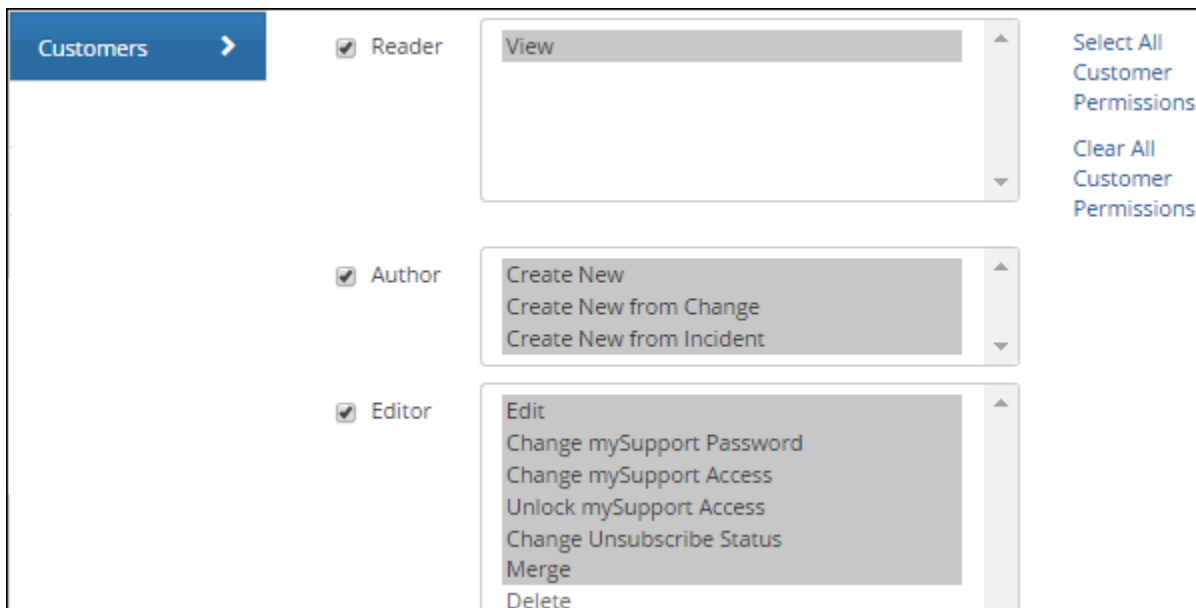
Select Correspondence in the Support Representative Roles screen to allow or disallow a support representative to delete a correspondence document.



Editor - Click the Editor checkbox or select **Delete** to allow the support representative to delete a correspondence document. When a correspondence that is related to a work item or customer is deleted, the correspondence and the related correspondence history will both be removed. The audit history related to the original correspondence will remain and a new audit history entry detailing the delete action will be added. There will also be a deletion shadow; if the link in the original audit history is clicked, details regarding the deletion will appear in a dialog.

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.




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 Customer and Company options will not be included on the Desktop Create menu and 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.

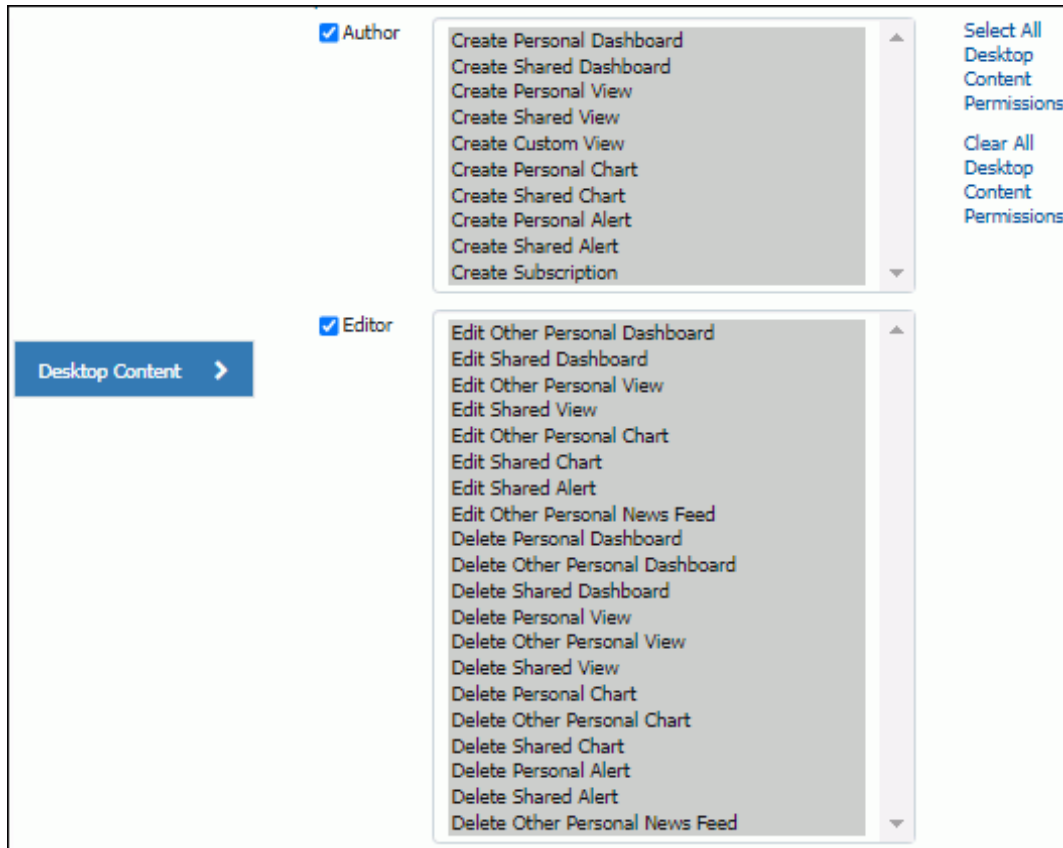
- Select **Create New from Change** to allow the support representative to create Customer Profile and Company records only from the Change screen.
- Select **Create New from Incident** to allow the support representative to create Customer Profile and Company records only from the Incident screen.

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 73 for more information.
- **Merge:** Select to display the  Merge option 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 in the Permissions screen to allow or disallow a support representative to create, edit, or delete a personal or shared dashboard, view, chart, and alert on the Desktop.



Author -

- **Create Personal Dashboard:** Select to include the Personal Dashboard option on the  Add Dashboard Desktop menu for the support representative, enabling creation of a dashboard for their Desktop. A personal dashboard will not appear under Add Existing on that menu for other support representatives to add to their Desktops.
- **Create Shared Dashboard:** Select to include the Shared Dashboard option on the  Add Dashboard Desktop menu for the support representative, enabling creation of a dashboard that can be added by another support representative via the Add Existing option on that menu. This permission will also enable the This permission requires the Create Personal Dashboard permission to also be enabled.
- **Create Personal View:** Select to include the Standard View Designer and Report View Designer options on the  Desktop Content menu for the support representative, enabling creation of a view that can be added to their Desktop.
- **Create Shared View:** Select to include the Access field in the Standard and Report View Designers for the support representative. This permission requires the Create Personal View permission to also be enabled, so the support representative will be able to create both personal and shared views.
- **Create Custom View:** Select this option to include the Design Custom View link in the Standard and Report View Designers for the support representative. The Design Custom View link enables users to access existing custom SQL queries within an iSupport SQL table. This permission requires the Create Personal View permission to also be enabled.
- **Create Personal Chart:** Select to include the Chart Designer option on the  Desktop Content menu for the support representative, enabling creation of a chart that can be added to their Desktop.
- **Create Shared Chart:** Select this option to include the Access field in the Chart Designer for the support representative; it enables a chart to be designated as Shared. This permission requires the Create Personal Chart

permission to also be enabled, so the support representative will be able to create both personal and shared charts.

- **Create Personal Alert:** Select to include the Alert Designer option to appear on the  Desktop Content menu, the  Alert to appear in the View and Chart components, and the Alert button to appear in the View and Chart Designers for the support representative. This will enable creation of an alert that will appear to only the support representative.
- **Create Shared Alert:** Select to include the Send To field in the Alert Designer screen for the support representative; this enables selection of the support representatives and/or support representative groups that should receive the alert when the criterion is met. This permission requires the Create Personal Alert permission to also be enabled.
- **Create Subscription:** Select to include the  Subscription option in the View component to send an email with an attached file of exported view data to configured recipients on a schedule. The email will be sent via the View Subscription agent.

Editor -

- **Edit Other Personal Dashboard:** Select to allow the support representative to display, change the content, and change the access of another support representative's personal dashboard. Dashboard access can be set via the Access option on the dashboard's right-click menu or the Alerts and Dashboards Manager.
- **Edit Shared Dashboard:** Select to allow the support representative to change the content and access of a shared dashboard. Other support representatives can add dashboards designated as Shared to their own Desktops.
- **Edit Other Personal View:** Select to allow the support representative to display and change the content and access of another support representative's personal view. Use the Other Personal option under Availability in the Content Manager to access these views. Views are designated as Personal or Shared via the Access field in the Standard and Report View Designers.
- **Edit Shared View:** Select to allow the support representative to change the content of a view that is designated as Shared access via the Standard and Report View Designers. Note that iSupport includes several shared views by default; these views cannot be changed but you can make a copy that can be changed.
- **Edit Other Personal Chart:** Select to enable the support representative to display another support representative's personal chart (personal charts will appear Shared charts in the component configuration dialog), and change the content of another support representative's personal chart. Use the Other Personal option under Availability in the Content Manager to access these charts. Charts are designated as Personal or Shared via the Access field in the Chart Designer.
- **Edit Shared Chart:** Select to allow the support representative to change the content of a chart that is designated as Shared access. Charts are designated as Personal or Shared via the Access field in the Chart Designer. Note that iSupport includes several shared charts by default; these charts cannot be changed but you can make a copy that can be changed.
- **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 their own personal dashboard via the right-click dashboard menu or Content Manager.
- **Delete Other Personal Dashboard:** Select to allow the support representative to delete another support representative's personal dashboard via the Alerts and Dashboards Manager.
- **Delete Shared Dashboard:** Select to allow the support representative to delete a dashboard that is designated as Shared.
- **Delete Personal View:** Select to enable the support representative to delete their own personal view.
- **Delete Other Personal View:** Select to enable the support representative to delete another support representative's personal view via the Other Personal Availability option in the Content Manager.
- **Delete Shared View:** Select to allow the support representative to delete a shared view via the Content Manager. Views are designated as Personal or Shared via the Access field in the Standard and Report View Designers. Note that iSupport includes several shared views by default; these views cannot be deleted.

- **Delete Personal Chart:** Select to allow the support representative to delete their own personal chart via the Content Manager. Charts are designated as Personal or Shared via the Access field in the Chart Designer.
- **Delete Other Personal Chart:** Select to allow the support representative to delete another support representative's personal chart. Use the Other Personal option under Availability in the Content Manager to access these charts. Charts are designated as Personal or Shared via the Access field in the Chart Designer.
- **Delete Shared Chart:** Select to allow the support representative to delete a chart that is designated as Shared. Charts are designated as Personal or Shared via the Access field in the Chart Designer. Note that iSupport includes several shared charts by default; these charts cannot be deleted.
- **Delete Personal 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.

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:

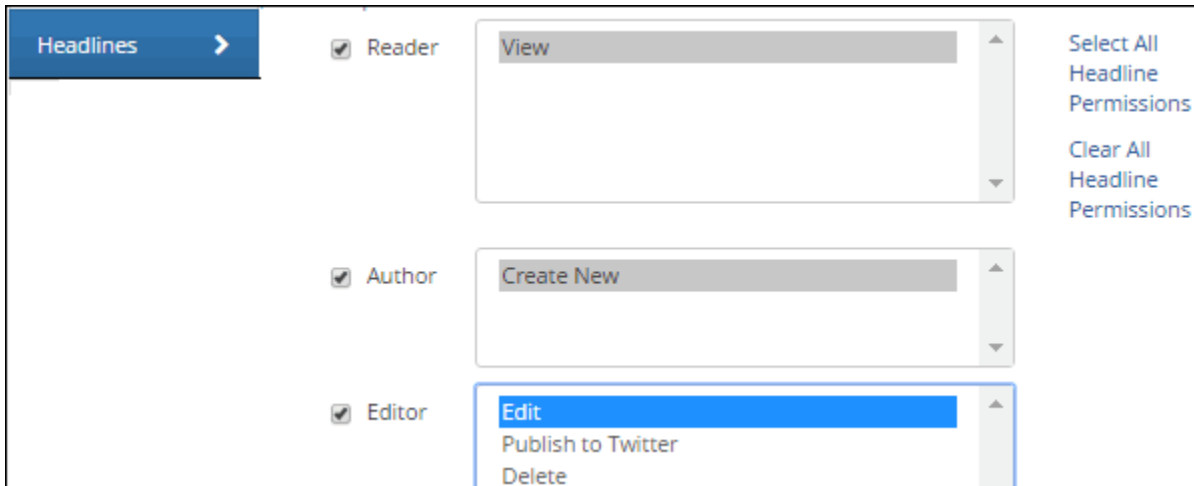
- **Create New Topic** to allow the support representative to create topics for sorting frequently asked questions on the Desktop and mySupport portal. If this option is *not* selected, the Topic field label will not be a link in the FAQ entry screen.
- **Create New FAQ** to allow the support representative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



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 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' configuration page. On the left, there is a blue button labeled 'Incidents' with a right-pointing arrow. The main area is divided into three sections, each with a role name and a checked checkbox:

- Reader** (checked): A list of permissions including 'View My Assigned', 'View My Authored', 'View My Groups', 'View My Location', and 'View All'.
- Author** (checked): A list of permissions including 'Create New', 'Use Hierarchy Templates', and 'Add Work History to All'.
- Editor** (checked): A list of permissions including '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', 'Route', 'Route By Group Only', 'Route to Unavailable Reps', 'Route From View', 'Schedule Recurring', 'Change Approvers', 'Update Via News Feed', and 'Delete'.

On the right side of the interface, there are two blue links: '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 Incident option will not be included in the Desktop Create 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 option 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.

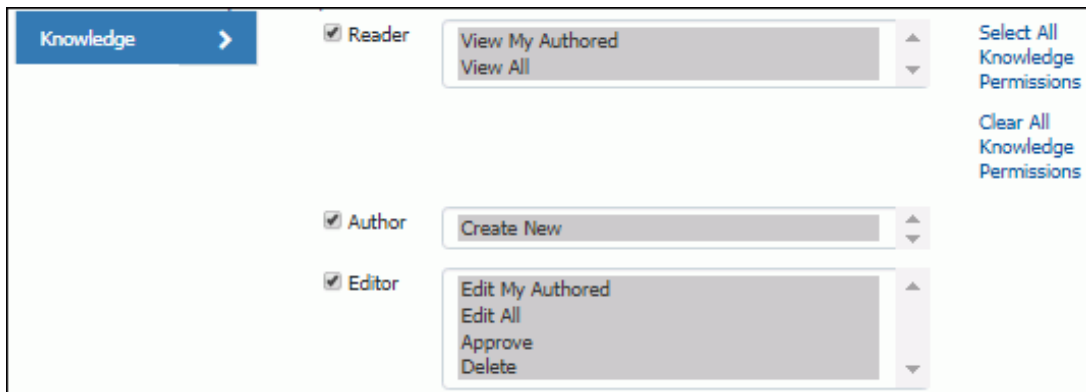
Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note that selecting an Edit permission will restrict the support representative's access to only that permission. If a support representative has the Author | Create New permission but no Editor | 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 option 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 Knowledge Permissions

Select Knowledge to allow or disallow access to knowledge functions such as modifying and viewing knowledge entries.



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

- **View My Authored** to allow the support representative to view only the knowledge entries that they created.
- **View All** to allow the support representative to view all knowledge entries.

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

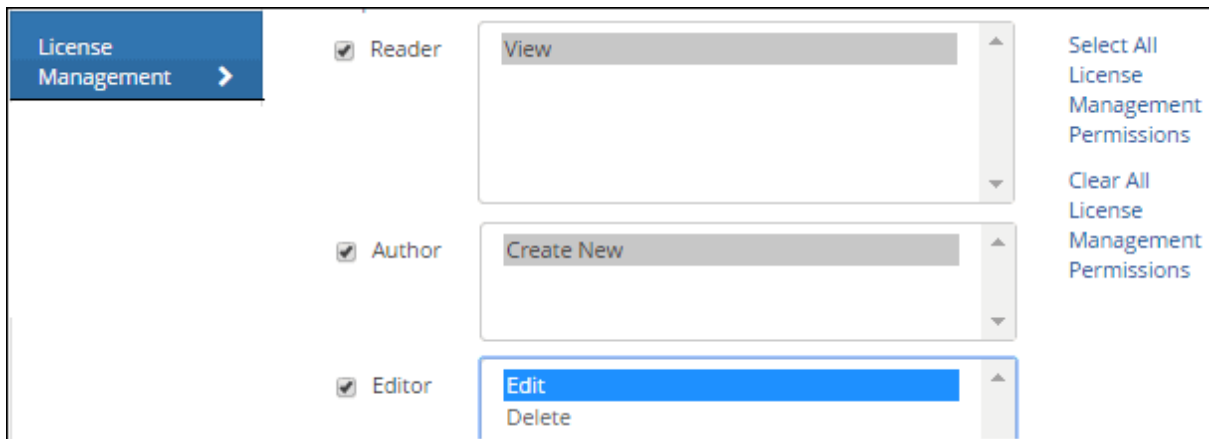
Editor - Click the Editor checkbox to select both Editor permissions, or select one or all of the following. Note: the View permission is required in order to select any of these permissions.

- **Edit My Authored:** Select to allow the support representative to update only the knowledge entry records that they authored.
- **Approve:** This option appears if Knowledge Approval functionality is enabled on the Knowledge Management tab in Feature Basics. Select to enable the support representative to approve or decline knowledge entries.
- **Edit My All:** Select to allow the support representative to update all knowledge entry records.
- **Delete:** Select to allow the support representative to delete any knowledge entry record.

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.

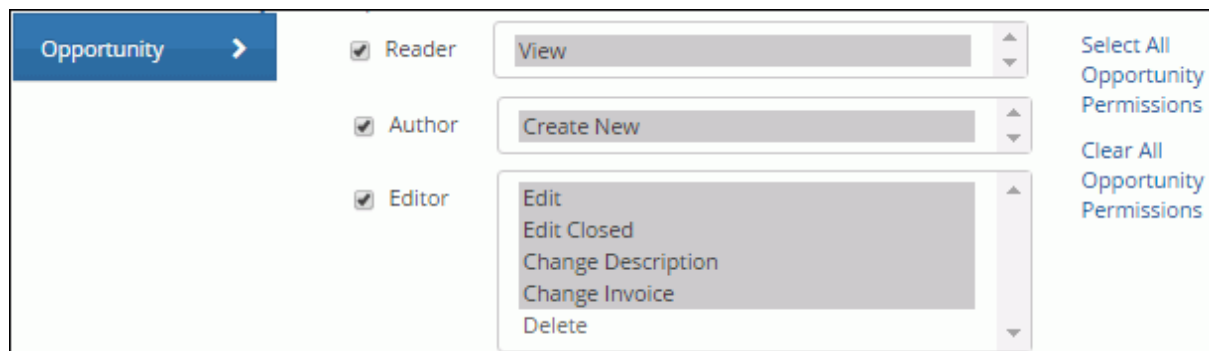
Author - Click the Author checkbox or select **Create New** to allow the support representative to create new Software License Profile records. If this option is *not* selected, the License Profile option will not be available to the support representative on the Desktop Create menu and in the Software 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 you have the Service Desk Edition and Opportunity functionality is enabled; select Opportunity to allow or disallow access to iSupport's Opportunity functionality.



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 Create 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

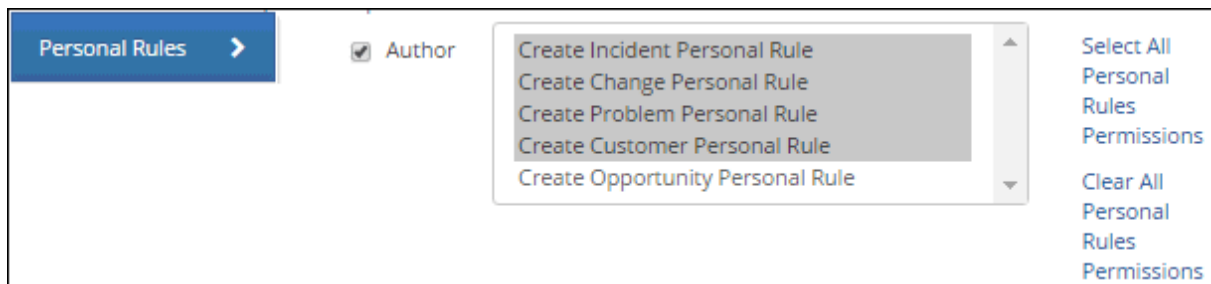
A personal correspondence template appears only to the support representative who created it in the list of correspondence templates available in iSupport. Select Personal Correspondence to allow or disallow creation of personal correspondence templates.



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 you have the Service Desk Edition and 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 'Problems' header with a right-pointing arrow. Below the header are three sections, each with a checked checkbox and a list of permissions:

- Reader** (checked):
 - View My Assigned
 - View My Authored
 - View My Groups
 - View My Location
 - View All
- Author** (checked):
 - Create New
 - Add Work History to All
- Editor** (checked):
 - 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
 - Route From View
 - Update Via News Feed
 - Delete

On the right side of the interface, there are two buttons: '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:

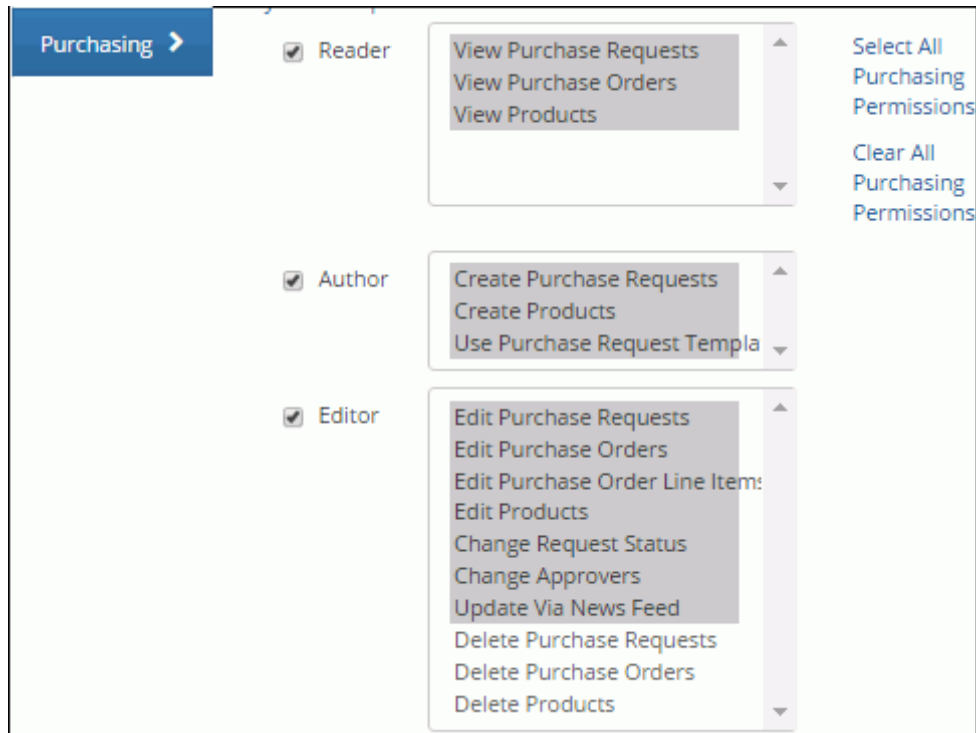
- **Create New:** Select to allow the support representative to create new Problem records. If this option is *not* selected, the Problem option will not be included on the Desktop Create menu and the New menu in the Problem screen.
- **Add Work History to All:** Select to allow the support representative 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 option 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 you have the Service Desk Edition and 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 Purchase Request option will not be included on the Desktop Create menu 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.

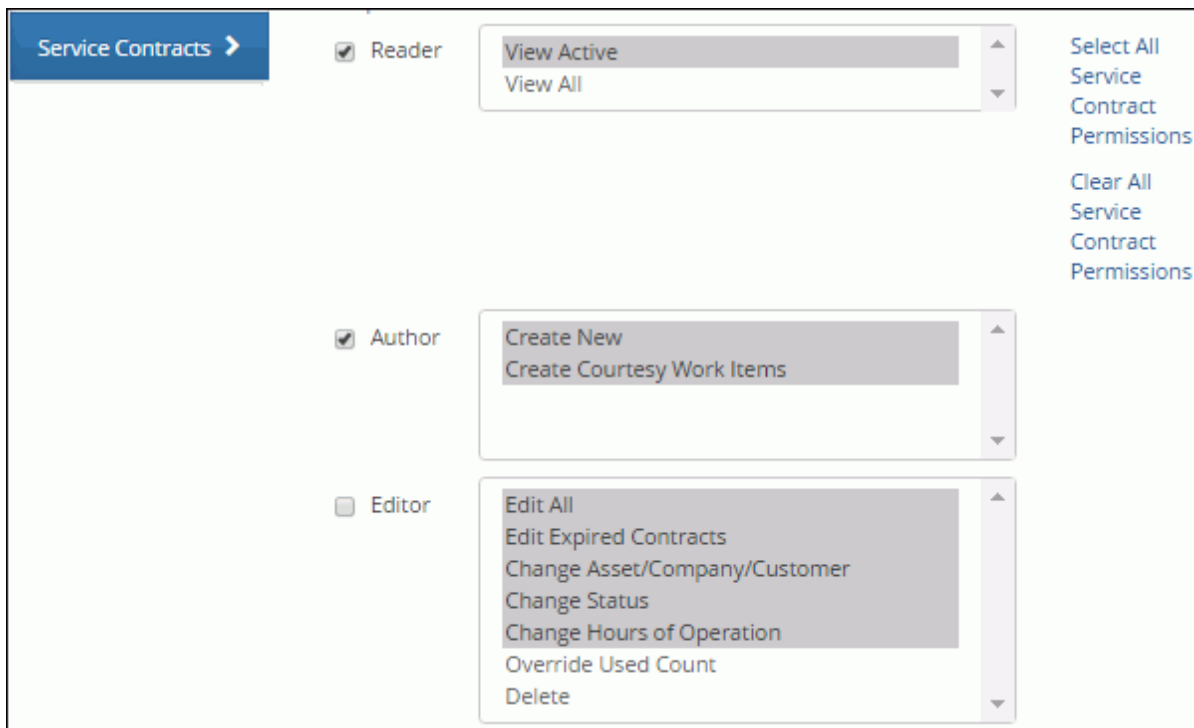
Editor - Click the Editor checkbox to select all Editor permissions, or select one or more of the following. Note: the View permission is required for these permissions. If a support representative has the Author | Create New permission but no Editor | Edit permission, the Save and Close Window menu 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 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.



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:

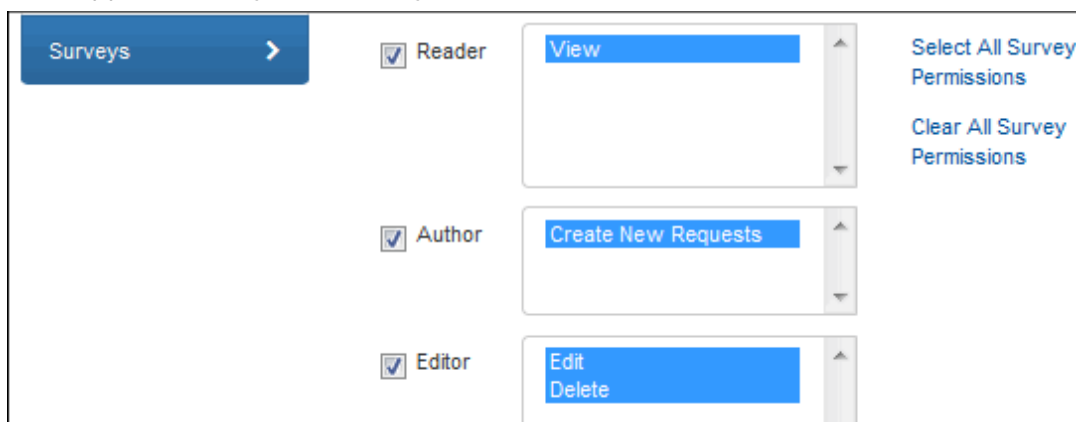
- **Create New:** Select to allow the support representative to create new service contracts. If this option is *not* selected, the Service Contract option will not be included on the Desktop Create menu and the New menu in the Service Contract screen for the support representative.
- **Create Courtesy 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.



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 Create 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
<input type="button" value="Add"/>		<input type="button" value="Remove"/>		
<input type="checkbox"/>	Name ▲	Description		
<input type="checkbox"/>	Tier I (IT)	Reps with first customer contact		

Configuring Locations

Locations are used for location-based routing and reporting. You can also use this screen to assign a display time zone for multiple support representatives at one time. Location functionality is an optional feature. If you choose not to use the Location feature, the time zone settings of the server hosting iSupport will be used for time/date display. To access the Location entry screen, use the Locations tab in the Core Settings | Support Representatives screen..

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. This is for display purposes only on the Desktop client.

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.
- To remove a support representative from the location, select the support representative in the Members field and click the ← left arrow.

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. If a support representative is assigned to a support center, the time-zone for that support center will be used in hours of operation calculations for rule-based actions; if no support center is assigned, the server's time zone will be used.

A support representative can be assigned to only one support center. To access the Support Center entry screen, select the Support Centers tab in the Core Settings | Support Representatives screen. Then click Create.

The screenshot shows a web form for creating a support center. It includes the following fields and controls:

- Support Center Name:** A text input field containing "West Coast".
- This is the Default Support Center:** A toggle control with "Yes" (highlighted in green) and "No" buttons.
- Time Zone:** A dropdown menu showing "(UTC-08:00) Pacific Time (US & Canada)".
- Non Members:** A list box containing the names: Barry White, Dwayne March, Gena Pirie, Jack Sullivan, Jorge Quentin, Kelsey Stout, Mary Smith, Stuart Copeland, and Tess French.
- Members:** A list box containing the names: Abby Kienle and Connor Flynn.
- Navigation:** Two arrow buttons (right and left) are positioned between the Non Members and Members list boxes.

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 in hours of operation calculations for rule-based actions.

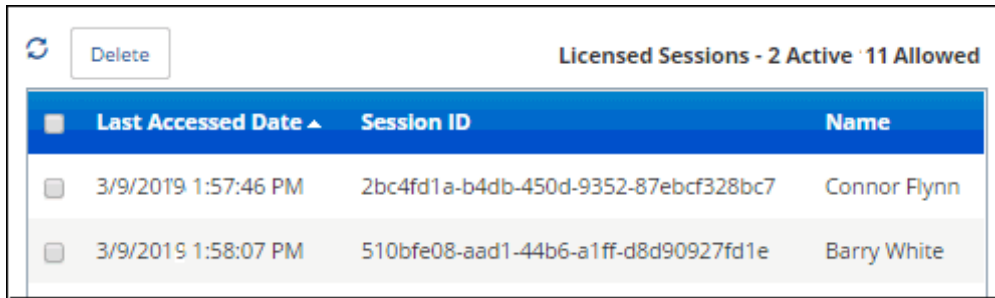
Nonmembers/Members - Use these fields to assign support representatives to a support center. A support representative can be assigned to only one support center.

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.
- To remove a support representative from the support center, select the support representative in the Members field and click the ← left arrow.

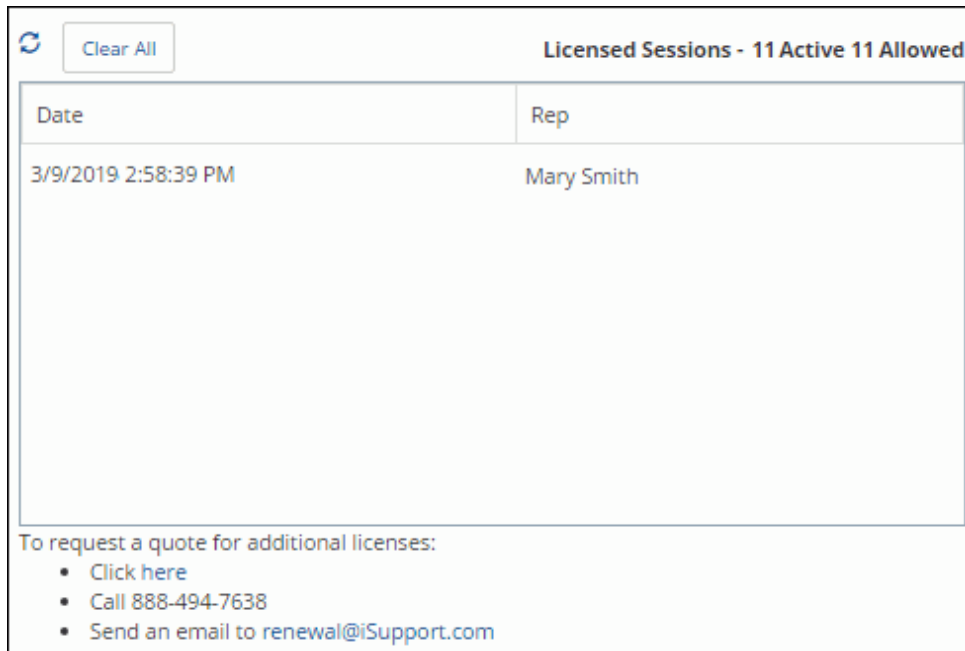
Monitoring Active and Exceeded Sessions

Use the Active Sessions tab in the Core Settings | Support Representatives 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.



Licensed Sessions - 2 Active · 11 Allowed			
<input type="checkbox"/>	Last Accessed Date ▲	Session ID	Name
<input type="checkbox"/>	3/9/2019 1:57:46 PM	2bc4fd1a-b4db-450d-9352-87ebcf328bc7	Connor Flynn
<input type="checkbox"/>	3/9/2019 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.) This screen will include information regarding how to request additional licenses.




Licensed Sessions - 11 Active 11 Allowed	
Date	Rep
3/9/2019 2:58:39 PM	Mary Smith

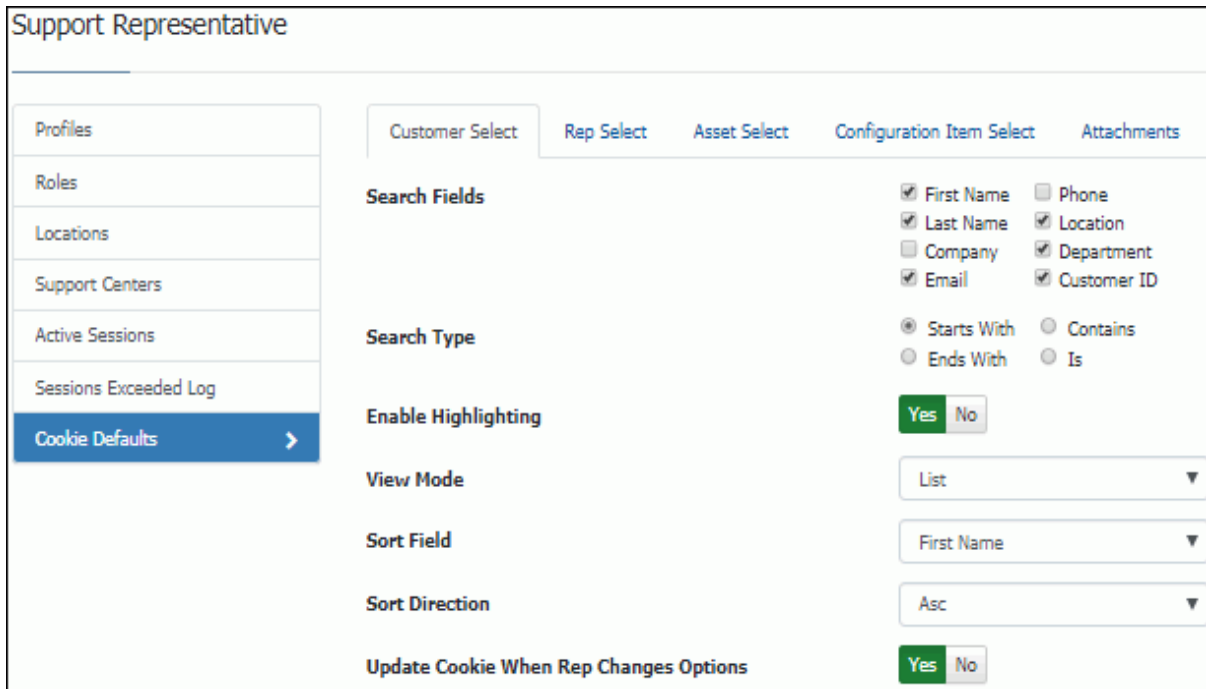
To request a quote for additional licenses:

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

Configuring Cookie Defaults

Use the Cookie Defaults settings in the Support Representative list screen to set defaults for the options used when support representatives search for customers, other support representatives, assets, and configuration items. These settings are set by support representatives via the  Search Options option and stored in a cookie.

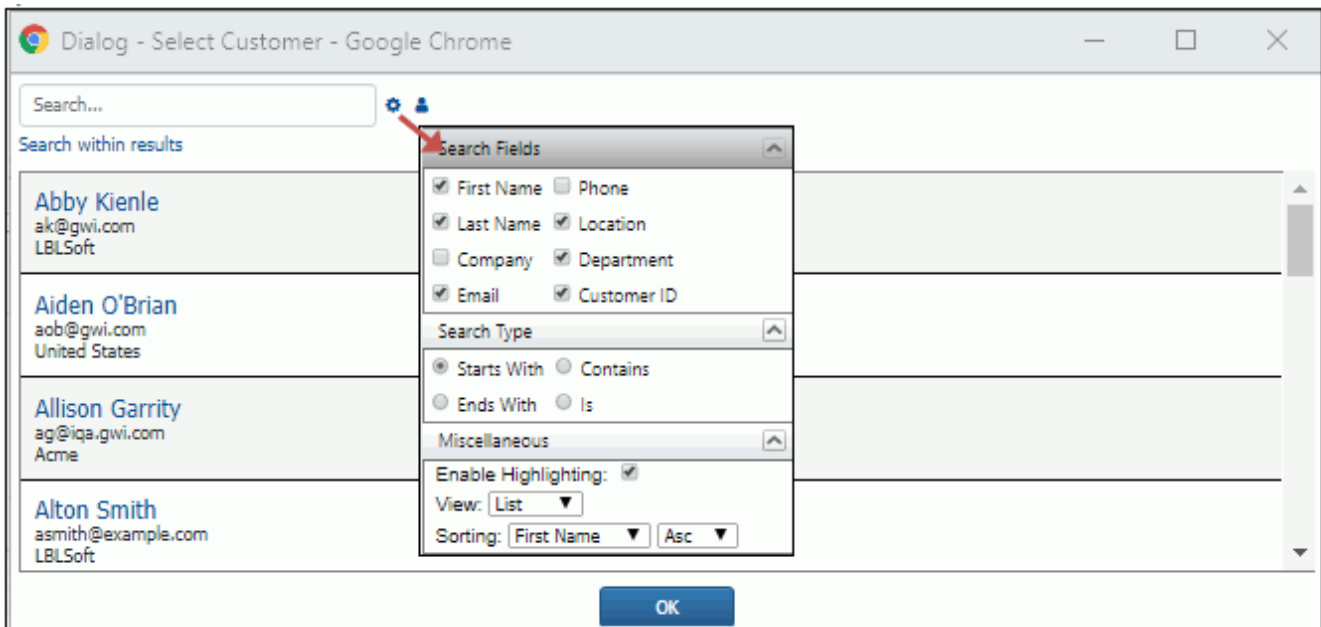
Use the Customer Select tab to set the defaults for search options when customer searches are performed by support representatives in work item screens.



The screenshot shows the 'Support Representative' configuration page with the 'Cookie Defaults' tab selected. The page includes a left sidebar with navigation options: Profiles, Roles, Locations, Support Centers, Active Sessions, Sessions Exceeded Log, and Cookie Defaults (highlighted). The main content area has tabs for 'Customer Select', 'Rep Select', 'Asset Select', 'Configuration Item Select', and 'Attachments'. The 'Customer Select' tab is active, showing search configuration options:

- Search Fields:** First Name (checked), Last Name (checked), Company (unchecked), Email (checked), Phone (unchecked), Location (checked), Department (checked), Customer ID (checked).
- Search Type:** Starts With (selected), Ends With (radio), Contains (radio), Is (radio).
- Enable Highlighting:** Yes (selected), No (radio).
- View Mode:** List (dropdown).
- Sort Field:** First Name (dropdown).
- Sort Direction:** Asc (dropdown).
- Update Cookie When Rep Changes Options:** Yes (selected), No (radio).

Example:



The screenshot shows a 'Dialog - Select Customer - Google Chrome' window. A search bar at the top left contains 'Search...'. Below it, a list of search results is visible, including Abby Kienle, Aiden O'Brian, Allison Garrity, and Alton Smith. A search options dialog box is overlaid on the results, showing the same configuration options as the 'Cookie Defaults' page. A red arrow points to the gear icon in the search bar. An 'OK' button is at the bottom of the dialog.

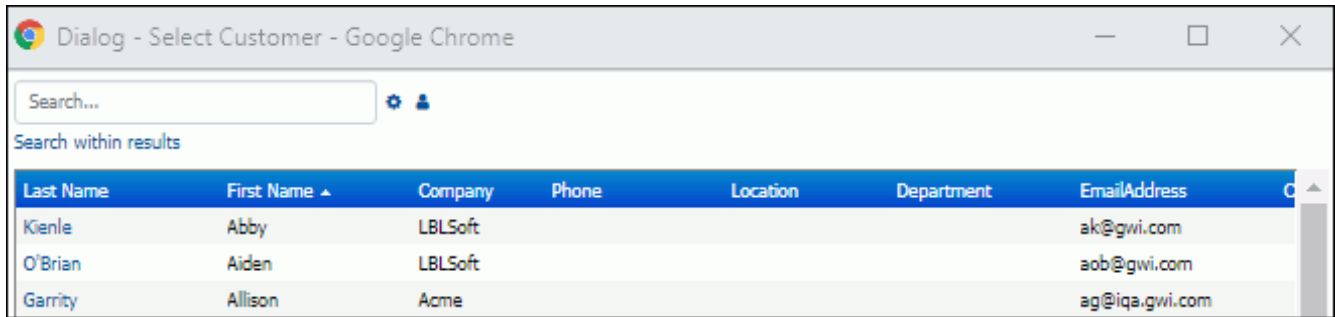
Search Fields - Select the customer field to be searched by default.

Search Type - Select the methods by which the search should be executed by default: Starts With, Contains, Ends With, and/or Is.

Enable Highlighting - Select Yes to shade the background of search terms in search results.

View Mode - Select the type of view in which search results display by default: classic or list.

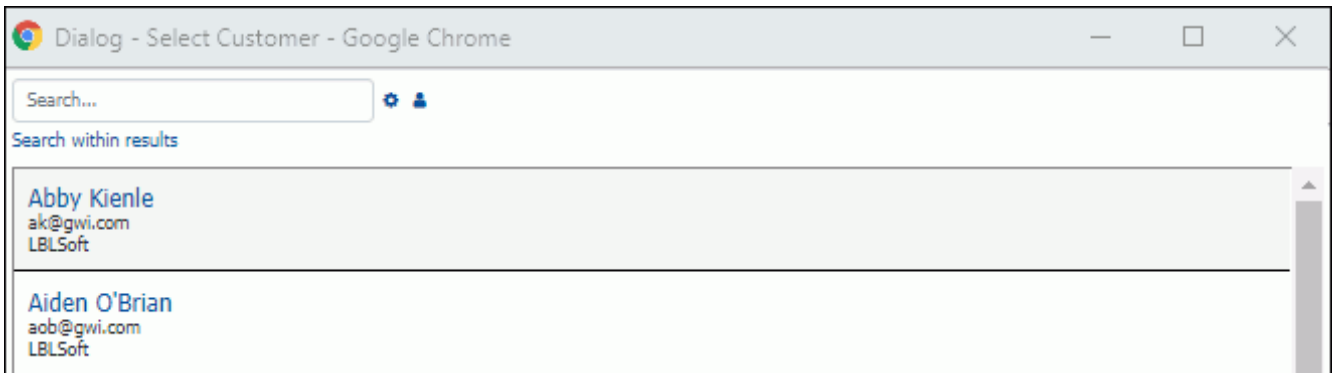
Classic View Mode



A screenshot of a web browser window titled "Dialog - Select Customer - Google Chrome". It shows a search interface with a search bar and a table of results. The table has columns for Last Name, First Name, Company, Phone, Location, Department, and EmailAddress. The results are sorted by Last Name.

Last Name	First Name	Company	Phone	Location	Department	EmailAddress
Kienle	Abby	LBLSoft				ak@gwi.com
O'Brian	Aiden	LBLSoft				aob@gwi.com
Garrity	Allison	Acme				ag@iqa.gwi.com

List View Mode



A screenshot of a web browser window titled "Dialog - Select Customer - Google Chrome". It shows a search interface with a search bar and a list of results. Each result is a card containing the name, email address, and company name.

Abby Kienle ak@gwi.com LBLSoft
Aiden O'Brian aob@gwi.com LBLSoft

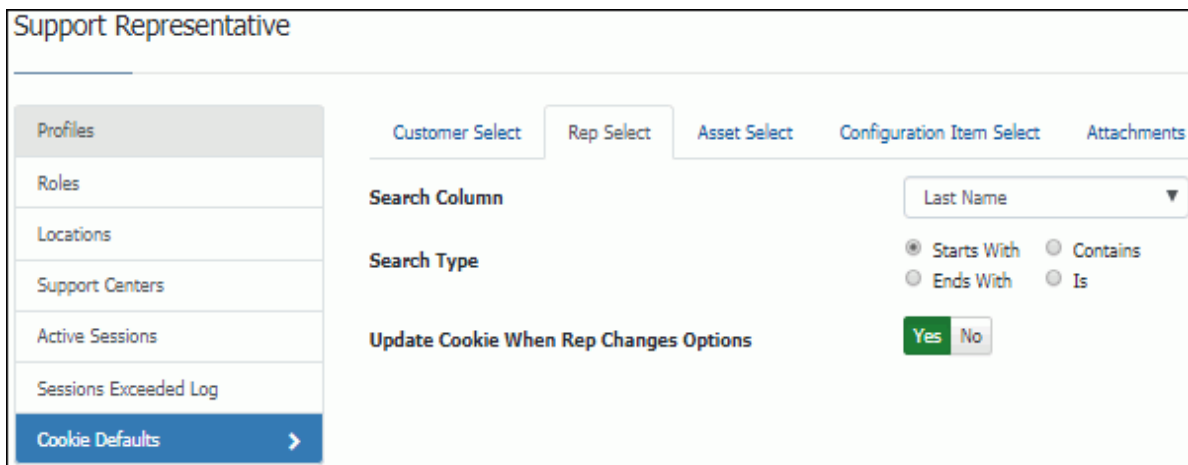
Sort Field - Select the field by which the search results are sorted by default.

Sort Direction - Select the direction by which search results are sorted by default.

Update Cookie When Rep Changes Options - Select Yes to update the cookie with the search selections made when a support representative conducts a search. If No is selected in this field, the cookie will not be updated with the search selections and the default settings configured in this screen will apply the next time the search is conducted.

Setting Rep Select Options

Use the Rep Select tab to set the defaults for search options when support representative searches are performed via the Others to Notify field in work item screens and the Recipient, Requested By, and Bill To fields in the Purchase Request screen.



A screenshot of the "Support Representative" settings page. The "Rep Select" tab is active. The "Search Column" is set to "Last Name". The "Search Type" is set to "Starts With". The "Update Cookie When Rep Changes Options" is set to "Yes".

Support Representative

Profiles
Roles
Locations
Support Centers
Active Sessions
Sessions Exceeded Log
Cookie Defaults

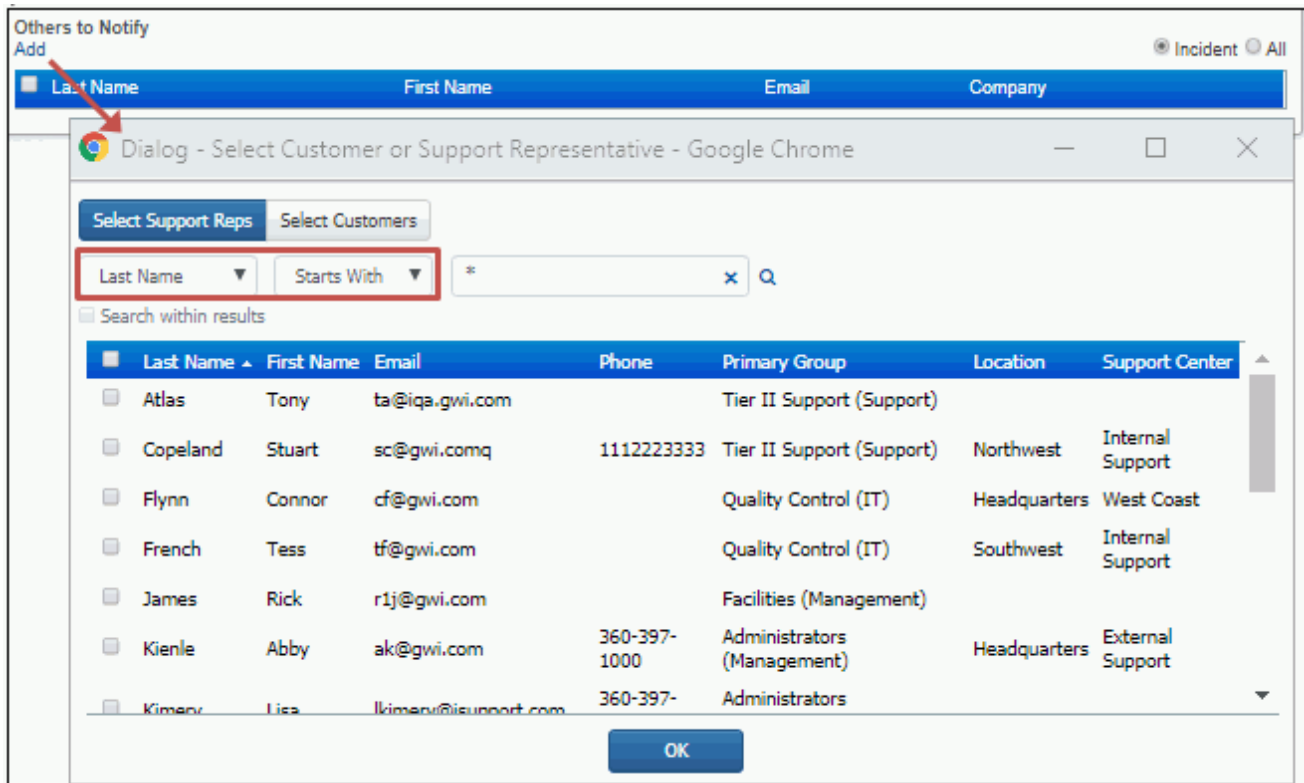
Customer Select | **Rep Select** | Asset Select | Configuration Item Select | Attachments

Search Column: Last Name

Search Type: Starts With Contains Ends With Is

Update Cookie When Rep Changes Options: Yes No

Example:



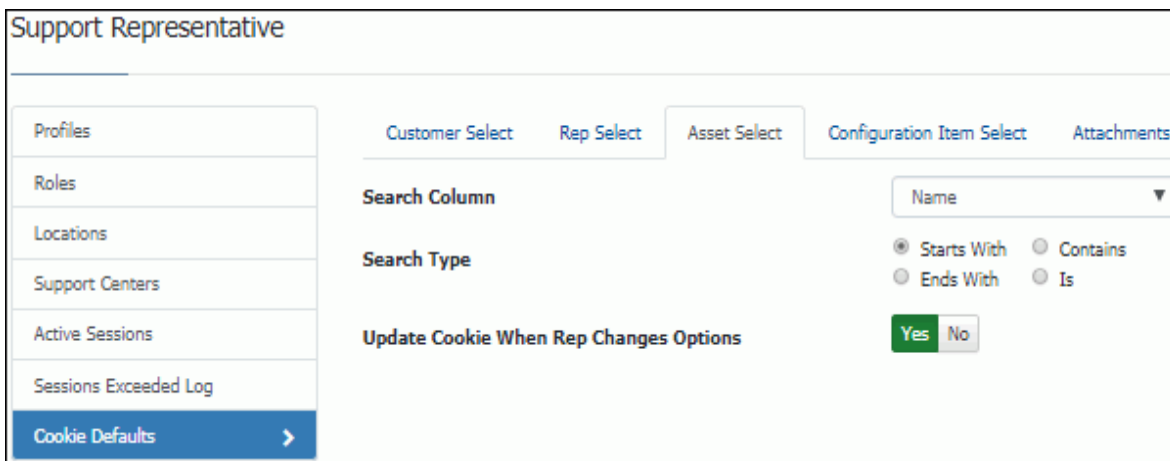
Search Column - Select the support representative field to be searched by default.

Search Type - Select the methods by which the search should be executed by default: Starts With, Contains, Ends With, and/or Is.

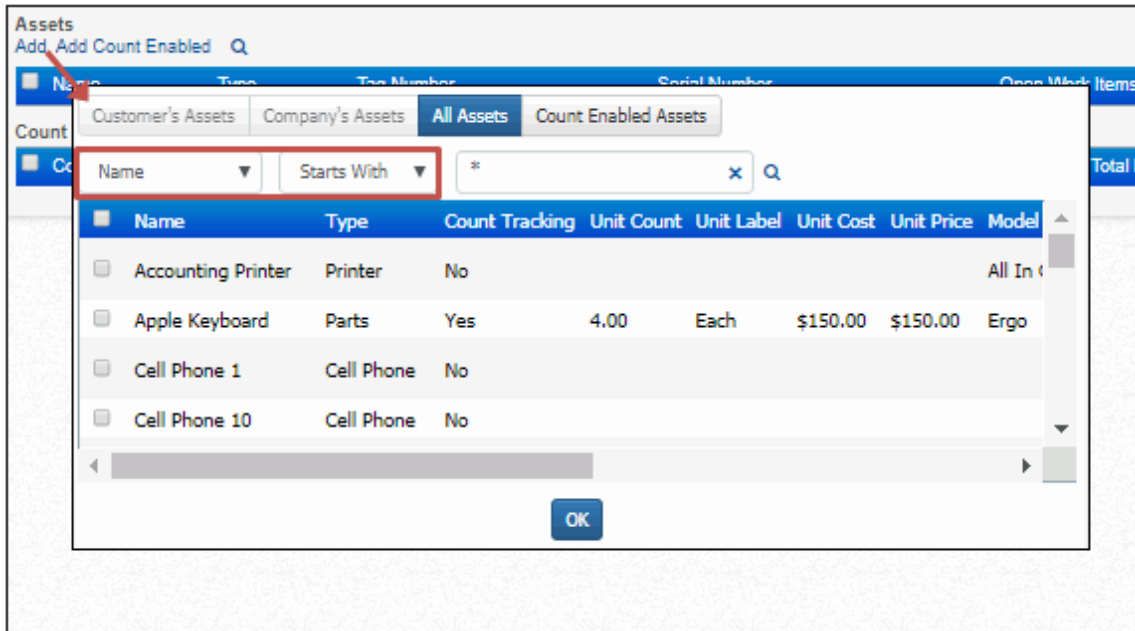
Update Cookie When Rep Changes Options - Select Yes to update the cookie with the search selections made when a support representative conducts a search. If No is selected in this field, the cookie will not be updated with the search selections and the default settings configured in this screen will apply the next time the search is conducted.

Setting Asset Select Options

Use the Asset Select tab to set the search option defaults for asset searches performed by support representatives via the Add Existing link on the Asset field in work item screens.



Example:



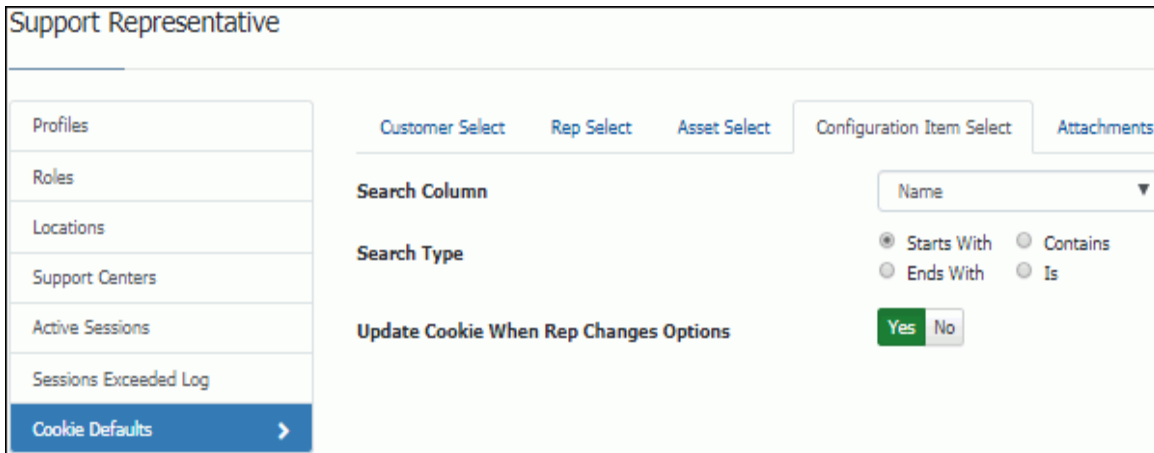
Search Column - Select the asset field to be searched by default.

Search Type - Select the methods by which the search should be executed by default: Starts With, Contains, Ends With, and/or Is.

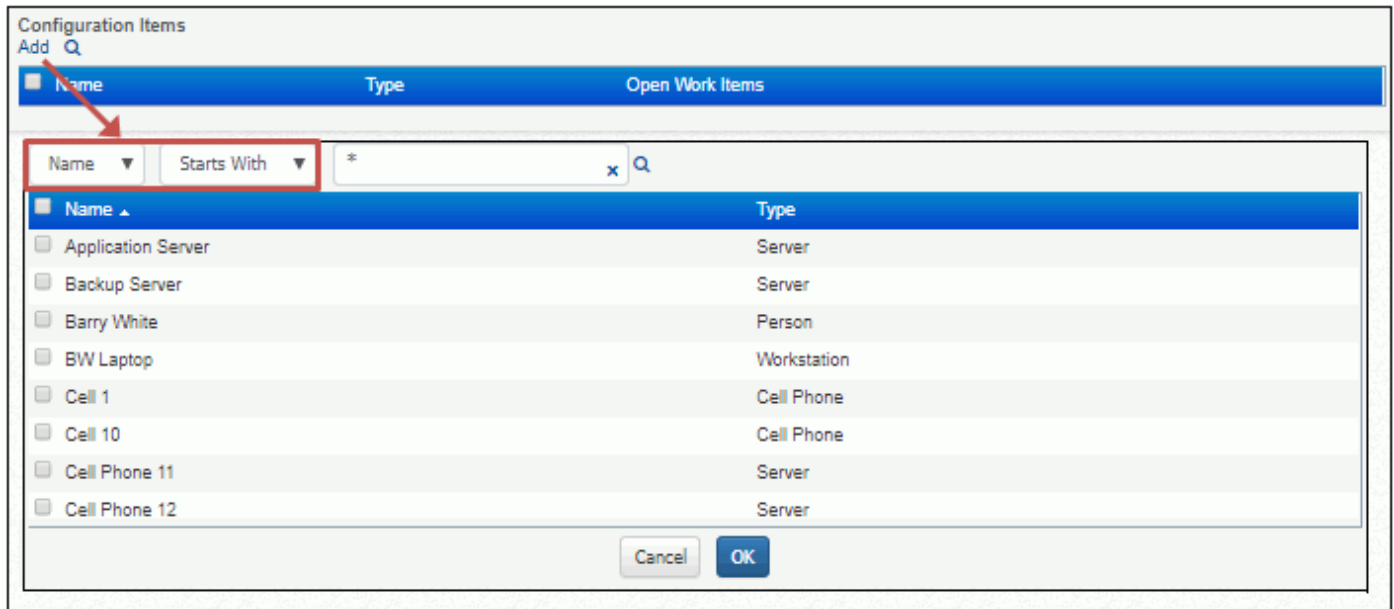
Update Cookie When Rep Changes Options - Select Yes to update the cookie with the search selections made when a support representative conducts a search. If No is selected in this field, the cookie will not be updated with the search selections and the default settings configured in this screen will apply the next time the search is conducted.

Setting Configuration Item Select Options

Use the Configuration Item Select tab to control the parameters for configuration item searches performed by support representatives.



Example:



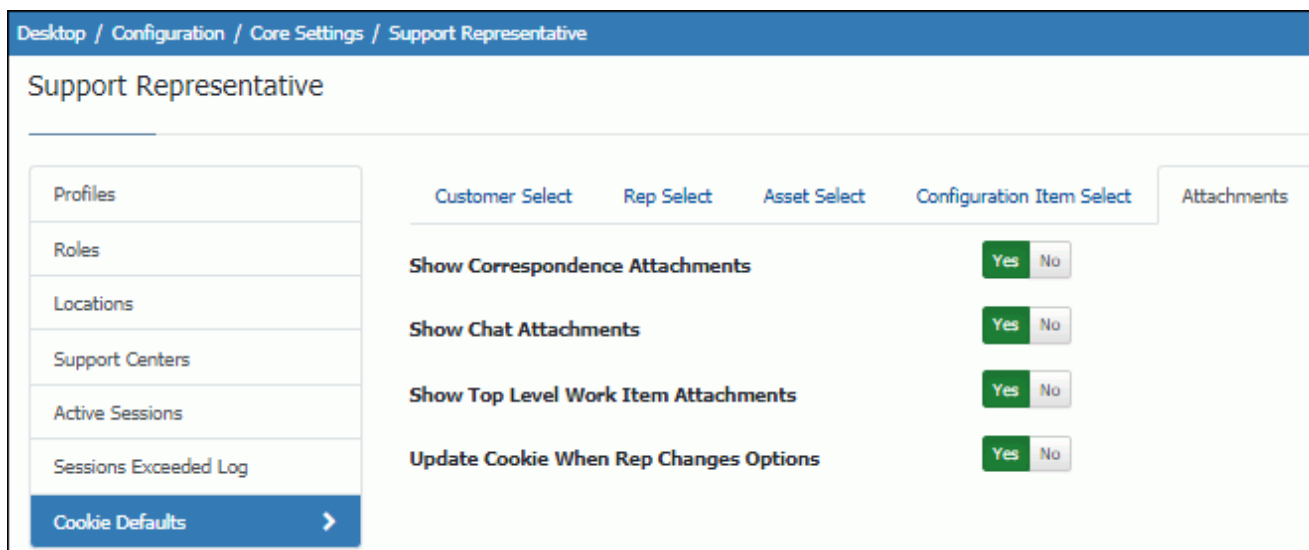
Search Column - Select the configuration item field to be searched by default.

Search Type - Select the methods by which the search should be executed by default: Starts With, Contains, Ends With, and/or Is.

Update Cookie When Rep Changes Options - Select Yes to update the cookie with the search selections made when a support representative conducts a search. If No is selected in this field, the cookie will not be updated with the search selections and the default settings configured in this screen will apply the next time the search is conducted.

Setting Attachment Options

Use the Attachments tab to set the defaults for Show Correspondence Attachments and Show Chat Attachments checkboxes in the Attachments field in work item screens.



Example:

Attachments				
File Name	Size	Type	Date File Attached	Source
TroubleshootingTips.docx	12.219K	application/vnd.openxmlformats-officedocument.wordprocessingml.document	11/17/2020 2:50:05 PM	Correspondence - (Subject: Troubleshooting Tips) <input type="button" value="Copy"/>
venprod2.xls	17.408K	application/vnd.ms-excel	11/17/2020 2:45:41 PM	Incident <input type="button" value="Delete"/>
venprod2.xls	17.408K	application/vnd.ms-excel	11/17/2020 2:45:41 PM	Incident KBHF493A4A <input type="button" value="Copy"/>
PrinterDrivers.pdf	49.541K	application/pdf	11/17/2020 2:37:52 PM	Customer Chat <input type="button" value="Copy"/>

Show Correspondence Attachments - Select Yes to enable the Show Correspondence Attachments checkbox by default in the Attachments field in work item screens.

Show Chat Attachments - Select Yes to enable the Show Chat Attachments checkbox by default in the Attachments field in work item screens.

Show Top Level Work Item Attachments - Select Yes to enable the Show To Level Work Item Attachments checkbox by default in the Attachments field in Incident and Change screens; it will display files attached directly to the top level parent incident or change in a hierarchy.


Update Cookie When Rep Changes Options - Select Yes to update the cookie with the search selections made when a support representative selects the Show Correspondence Attachments checkbox and/or Show Chat Attachments checkbox in the Attachments field. If No is selected in this field, the cookie will not be updated with the selections and the default settings configured in this screen will apply the next time the Attachments field is displayed.

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 Alerts and Dashboards Manager (accessed via the Desktop Content menu) 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.

You can use the Dashboards tab in the Support Representative Profile screen to display the dashboards available to a support representative and the dashboards currently open on their Desktop. You can push dashboards to the support representative's Desktop, and close any open dashboards.

The Dashboards tab in the Alerts and Dashboards screen lists all dashboards created and designated as Shared, as well as all personal dashboards that a support representative has created. Click the Add link to add a dashboard and specify its access.



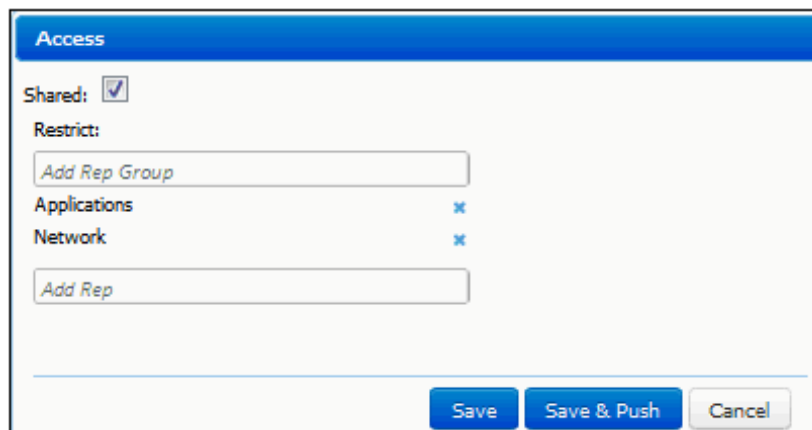
The screenshot shows the 'Alerts and Dashboards Manager' interface. On the left, there are tabs for 'Alerts' and 'Dashboards'. The 'Dashboards' tab is selected. Above the table are 'Add' and 'Delete' buttons. The table has the following columns: Name, Author, Access, Usage, and Components. There are also checkboxes and edit/delete icons for each row.

		Name ▲	Author	Access	Usage	Components
<input type="checkbox"/>	<input type="checkbox"/>	Approval Changes	Jack Sullivan	Shared	1	1
<input type="checkbox"/>	<input type="checkbox"/>	Asset Monitor	Barry White	Personal	0	1
<input type="checkbox"/>	<input type="checkbox"/>	Assets	Abby Kienle	Shared	6	1
<input type="checkbox"/>	<input type="checkbox"/>	Badges	Connor Flynn	Personal	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.



The screenshot shows the 'Access' dialog box. It has a 'Shared' checkbox which is checked. Below it is a 'Restrict' section with two input fields: 'Add Rep Group' and 'Add Rep'. There are also 'Applications' and 'Network' sections, each with a small 'x' icon. At the bottom, there are three buttons: 'Save', 'Save & Push', and '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.

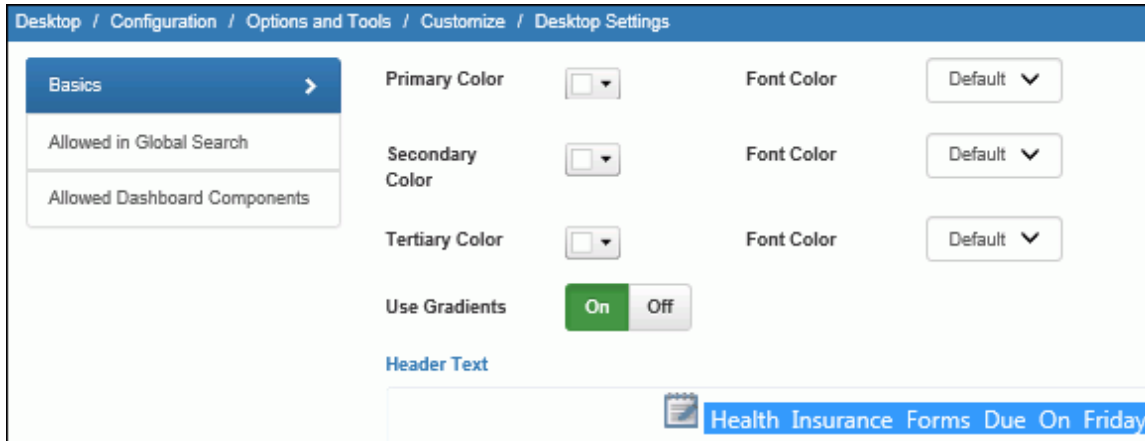
Components - The number of content frames on the dashboard.

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. Select  No Color 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 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.



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.



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.

<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.x.xx:xxx	Customers
<input type="checkbox"/>	Main AD Sync	Active Directory	No	LDAP://xx.xx.x.xx:xxx	Customers
<input type="checkbox"/>	Microsoft CRM	Microsoft CRM	Yes		Customers

Select the data source type.

<input type="checkbox"/>	Type	Active	Source
Shared			
<input type="checkbox"/>	Active Directory		
<input type="checkbox"/>	LDAP		
Customer			
<input type="checkbox"/>	Domino Directory		
<input type="checkbox"/>	Microsoft CRM		
<input type="checkbox"/>	Customer RDB		
Asset			
<input type="checkbox"/>	Asset RDB		
CMDB			
<input type="checkbox"/>	CMDB RDB		

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.

- Desktop dashboards that have been granted access will be assigned to a new support representative's primary group.
- 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 >	AD Source Name	Main AD Sync
Sync Definitions	Search Root	LDAP://xx.xx.x.xxx
Field Mappings	Connect As	Anonymous Specified User
Exclusions	Username	xxAdmin
	Password
		Test Connection
	Active	On Off
	Synchronization Interval	15 minutes ▾

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 page. On the left is a navigation menu with 'Sync Definitions' selected. The main area contains the following fields:

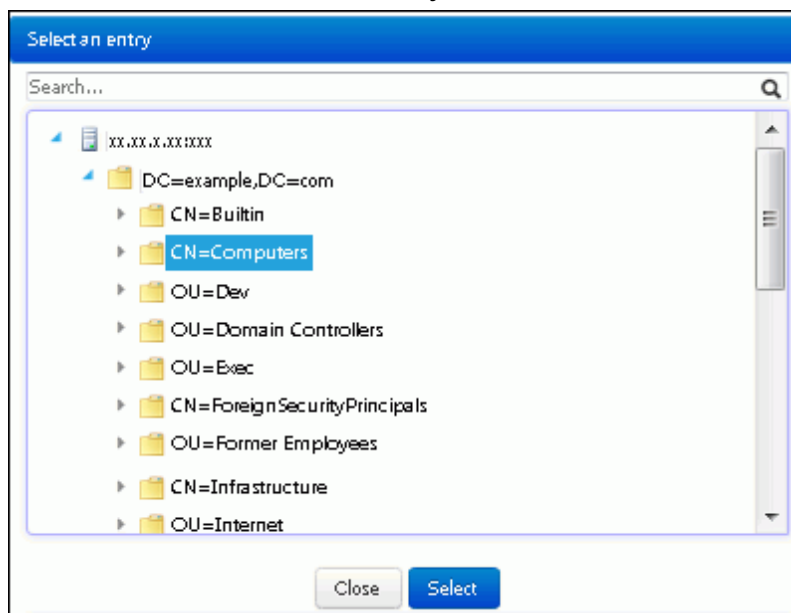
- Active:** A toggle switch set to 'Yes'.
- Sync Entries As:** A dropdown menu set to 'Support Representatives'.
- Default Primary Group:** A dropdown menu set to 'Support' with '+' and edit icons.
- Base DN:** A text box containing 'ou=Production,DC=example,DC=com'.
- Search Filter:** A text box containing 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=*)
)
```

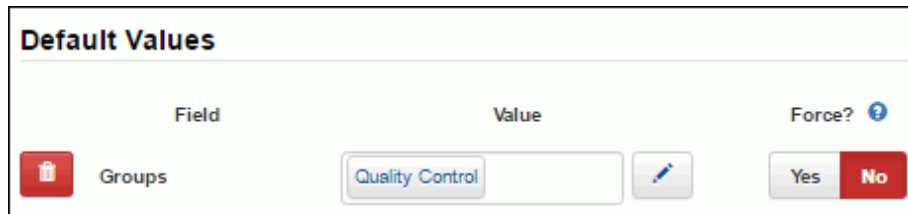


```
(userPrincipalName=*@*)
(samAccountName=*)
)
```

Setting Default Values

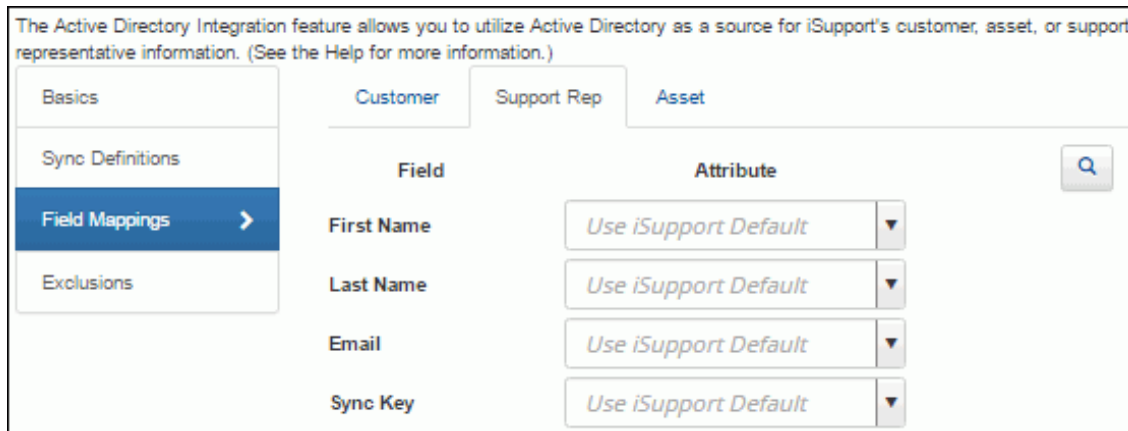
Use the Default Values section to set Support Representative field values based upon the AD sync setting entry from which a record was created. For example, if AD users are organized into a specific OU or group that indicates other user properties (such as location) and if the AD user profiles don't 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.



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.

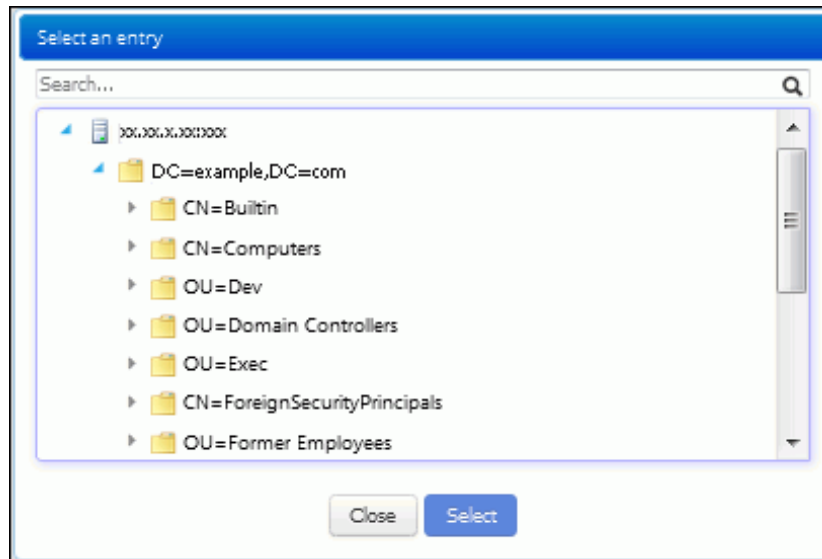


Mapping options include:

- 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.

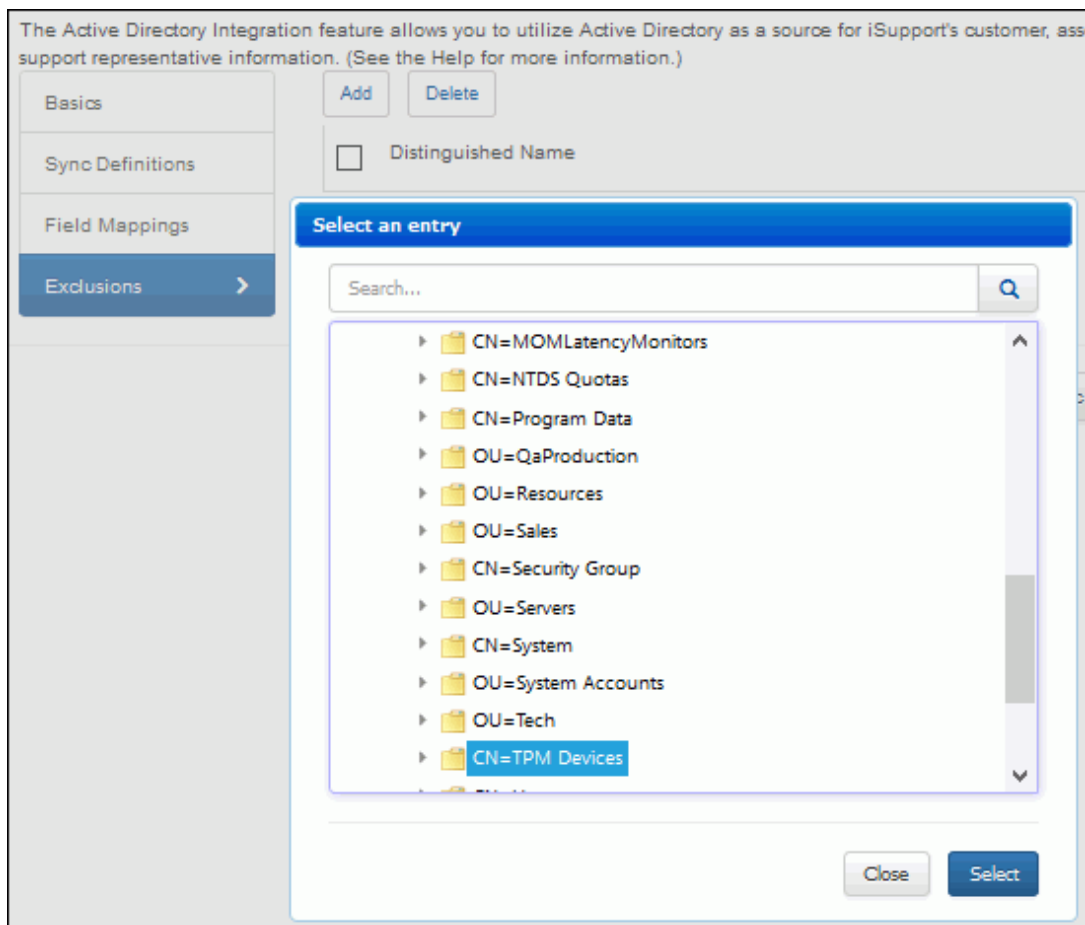
Use the Sync Key field to map to a value that is an unchanging unique identifier field in the source database.

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.
- Desktop dashboards that have been granted access will be assigned to a new support representative's primary group.
- 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

Server

Use SSL On Off

Connect As Anonymous Specified User

Username

Password

Active On Off

Synchronization Interval ▼

Sync Definitions

<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

Sync Definitions

Field Mappings

Exclusions

Active: Yes No

Sync Entries As: Support Representatives

Default Primary Group: Support

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

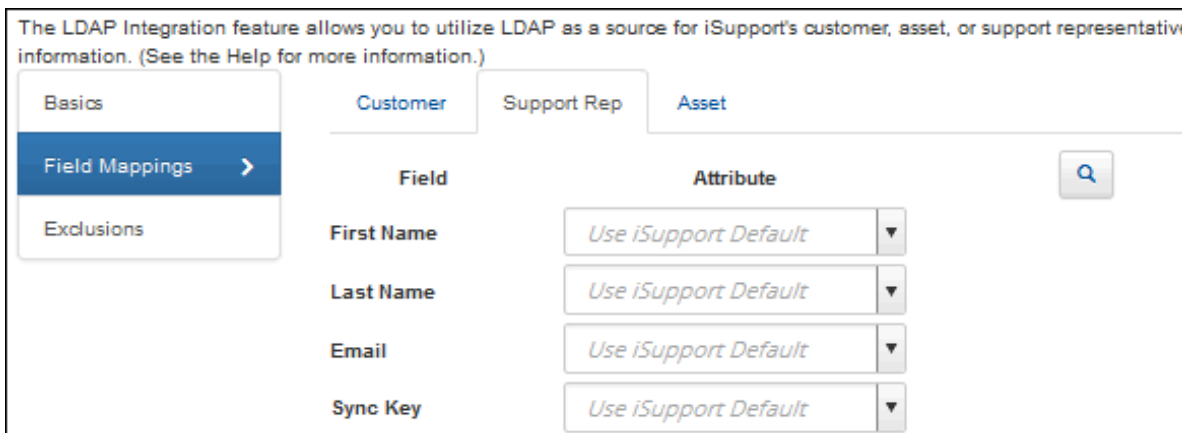
Use the Default Values section to set Support Representative field values based upon the LDAP sync setting entry from which a record was created. For example, if LDAP users are organized into a specific OU or group that indicates other user properties (such as location) and if the LDAP user profiles 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.

Field	Value	Force?
Groups	Quality Control	Yes 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

Search

Mapping options include:

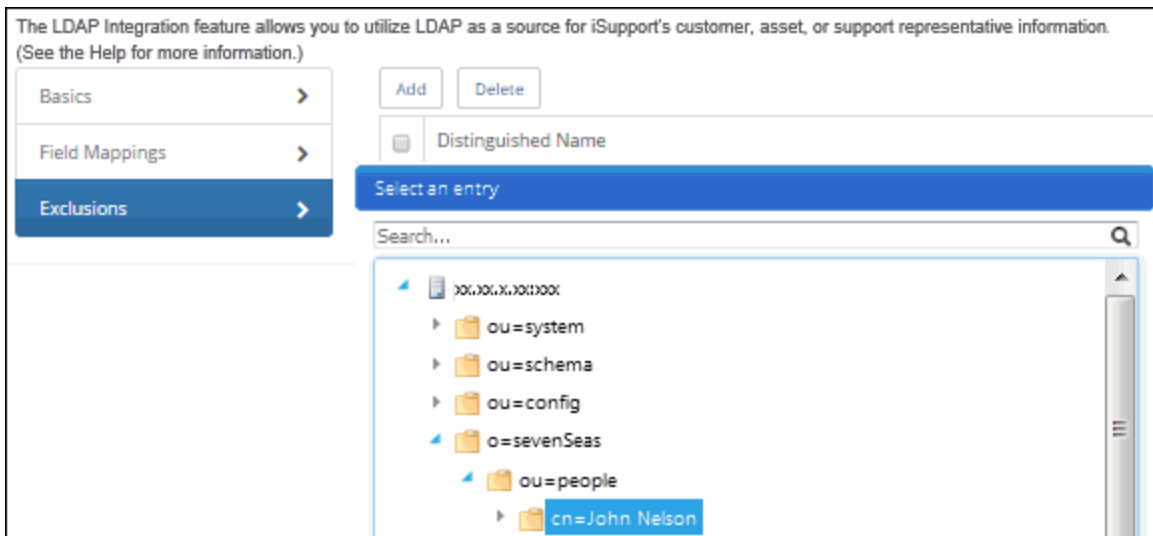
- Use iSupport Default which populates the default mapping. Note that we recommend that you use iSupport's default for the Sync Key and Avatar fields because the applicable schema property may vary depending on your version of LDAP.
- An applicable schema property (selected via the dropdown)
- [Unmapped] 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...

- o=sevenSeas
 - ou=system
 - ou=schema
 - ou=config
 - 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.

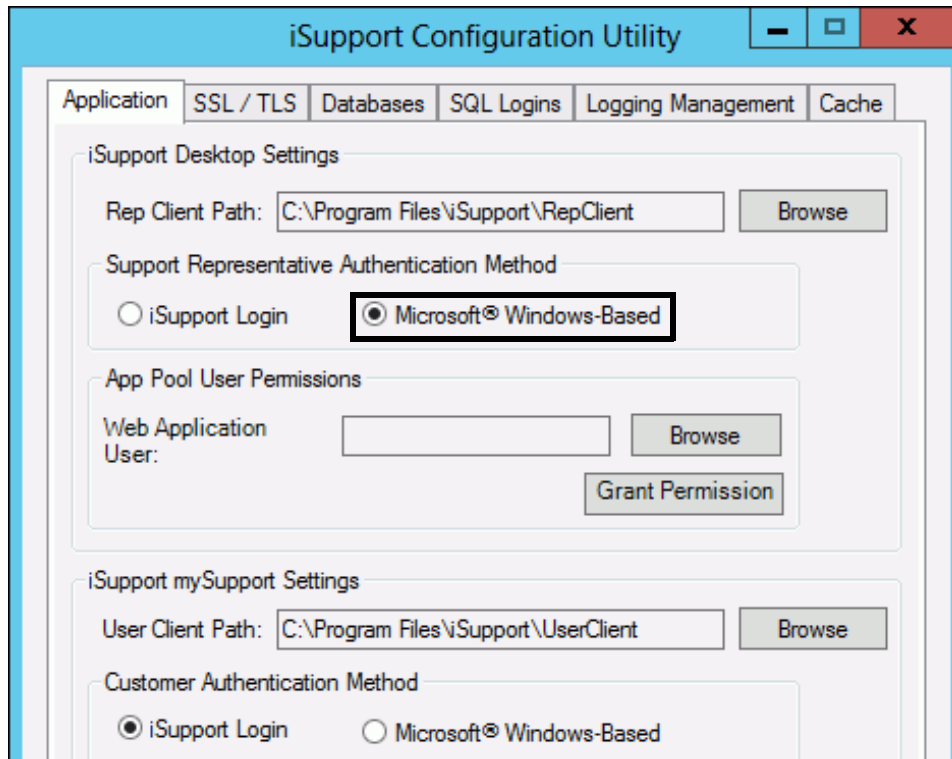
Use the following steps to enable Microsoft® Windows-based authentication for the Desktop. Because this procedure affects support representative logins, it's a good idea to do it after work hours.

- 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 input fields. The first field is labeled 'Login' and contains the text 'ExampleCo\BW'. The second field is labeled 'Password' and is currently empty. To the right of the Password field is a blue button labeled 'Reset'.

- 2 Open the iSupport Configuration Utility in the *<directory in which iSupport is installed>\Utilities* folder. 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 Configuration Utility' window. The 'Application' tab is selected. The 'iSupport Desktop Settings' section is expanded. The 'Rep Client Path' field contains 'C:\Program Files\iSupport\RepClient' and has a 'Browse' button. The 'Support Representative Authentication Method' section has two radio buttons: 'iSupport Login' (unselected) and 'Microsoft® Windows-Based' (selected and highlighted with a black box). The 'App Pool User Permissions' section has a 'Web Application User' field with a 'Browse' button and a 'Grant Permission' button. The 'iSupport mySupport Settings' section is expanded. The 'User Client Path' field contains 'C:\Program Files\iSupport\UserClient' and has a 'Browse' button. The 'Customer Authentication Method' section has two radio buttons: 'iSupport Login' (selected) and 'Microsoft® Windows-Based' (unselected).

Setting Up Single Sign On Authentication for the Desktop

Use the Options and Tools | Integrate | Single Sign On Integrations screen to enable a third party application (such as Shibboleth and Otka) to pass user credentials so that a user can sign in to mySupport, the iSupport Desktop, or the Mobile interface with the same credentials that they use to log into another application. Note that iSupport's login method (forms-based) must be enabled for the applicable mySupport, Mobile, or Desktop interface (not Microsoft Windows-based authentication).

In order to use a third party integrity provider (IP) for this SAML-based SSO Integration feature, you will need to do some setup in the administration screens of your IP and the URLs below may be needed. If you need to register iSupport with an identity provider that will be used for authentication, it must be done prior to creating/obtaining the metadata file from the identity provider. Then use the metadata file in the Load Settings From Metadata File field; when loaded, it will populate the Issuer, Single Sign On URL, and X509 Certificate fields. The following provider and consumer URLs for all four iSupport sites might be needed to register iSupport with an identity provider that will be used for authentication:

Rep Portal

Issuer: *rep_url*

Consumer: *rep_url*/SingleSignOn.aspx

User Portal (mySupport)

Issuer: *user_portal_url*

Consumer: *user_portal_url*/Account/SSO

Mobile (external)

Issuer: *mobile_url*

Consumer: *mobile_url*/SingleSignOn.aspx

Mobile(internal)

Issuer: *rep_url*/Mobile

Consumer: *rep_url*/Mobile/SingleSignOn.aspx

If using Shibboleth, you'll need to change the URL in the Issuer field to the URL for the applicable iSupport interface (Rep or User) and change **POST** to **Redirect** in the URL in the Single Sign On URL field. The iSupport login dialog will include a button labeled with the contents of the Login Button Text field in the Single Sign On Integrations screen; further dialogs will appear as required by the identity provider.

Desktop / Configuration / Options and Tools / Integrate / Single Sign On Integrations

Name	Shibboleth Rep
Active	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Target	Rep Desktop
Login Button Text	Log In via Shibboleth
Load settings from metadata file	<input type="button" value="Add"/>
Issuer	<input type="text" value="http://<servername>/rep"/>
Single Sign On URL	<input type="text" value="https://<servername>/adp/profile/SAML2/Redirect/SSO"/>
X509 Certificate	MIIDMzCCAhugAwIBAgIUbe25AxTHb+FSaA9I3ZwlQh6KXaYwDQYJKoZIhvcNAQELBQAwHTEBMBkGA1UEAwwvSapNol_XYidM50dSSpd2kuY29uMB4YDTE4MDMwMTkw...

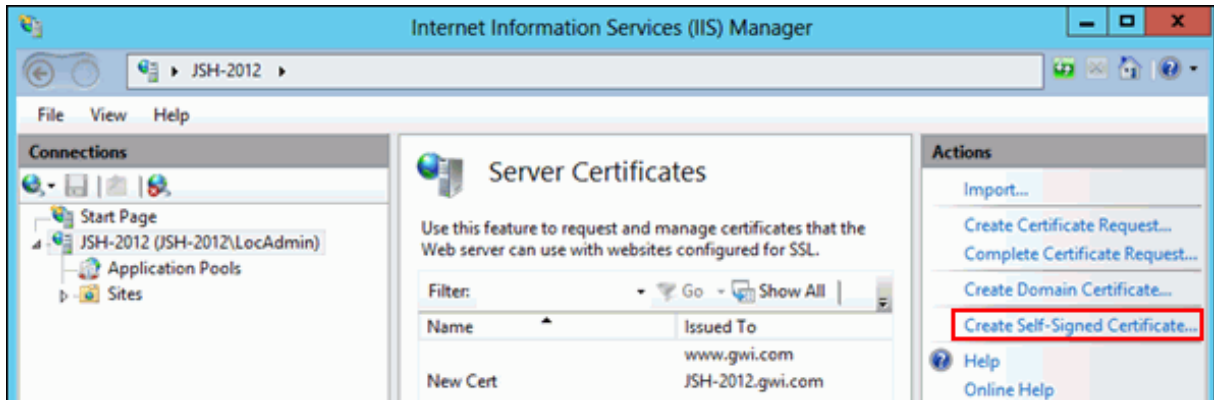
Change to the URL for the iSupport Desktop

Change "POST" to "redirect"

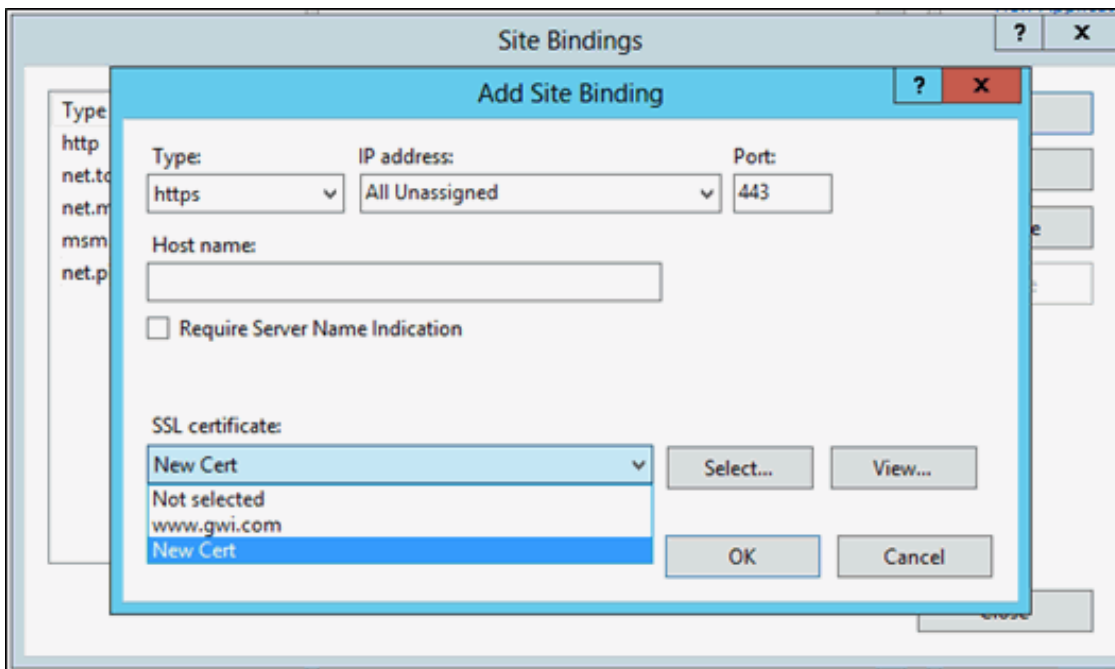
Setting Up SAML With Microsoft Azure Active Directory

Prerequisites

- 1 The iSupport webserver must be configured to use SSL. This includes creating/buying a valid certificate, applying it to the webserver, and creating the binding in IIS. (Consult your webserver administrator to perform this process.) This document covers the most basic of the certs, creating a self-signed cert, and using it.
 - a Open IIS and go to Server Certificates.
 - b On the menu on the right, select Create Self-Signed Certificate (the cert will use as authority and validity the FQDN of your machine; if you do not wish to use that as your URL, you must select a different method).



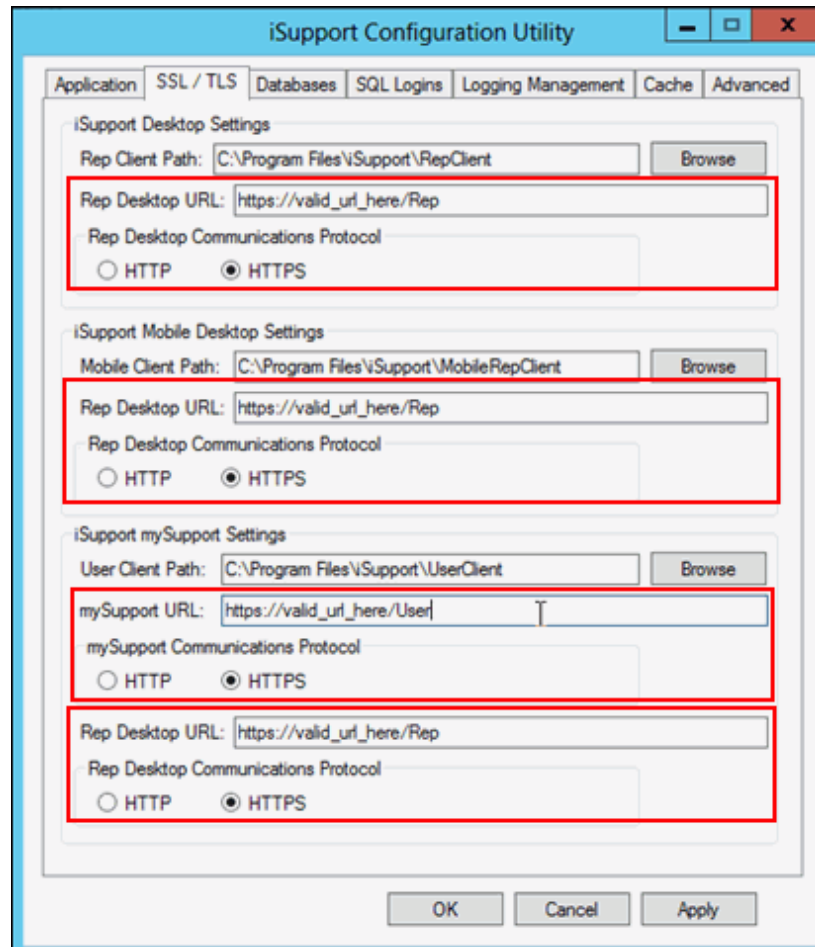
- c Expand the sites folder in IIS and select the website in which you installed iSupport. Note that it will use Default Website unless otherwise specified. On the menu on the right, select Bindings. For Type, select HTTPS. For Port, leave it at industry standard 443. For SSL Certificate, select the cert you generated on the previous step.



- d Your website is now enabled and configured to use SSL. As an example, for any of the next steps where you see `https://valid_url_here`, you would use `https://jsh-2012.gwi.com` which is the URL our provided certificate can validate.

Note: self-signed certs are only trusted by the machine that generated it; your users will get cert warnings when they hit the page. You can distribute your cert to them, ask your administrator to push the cert via a GPO, or simply use one of the other cert methods (purchase, in-house cert authority).

- 2 TLS 1.2 must be enabled in the registry, and the .NET Framework must be forced to use TLS 1.2. For more information, see <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-client>.
- 3 Update your iSupport web.config to use SSL via the iSupport Configuration Utility.exe; the utility can be found on the path you installed iSupport under (default is C:\Program Files\iSupport\Utilities). Then go to the SSL/TLS tab and update your URL and radio buttons accordingly. Note that the URL you enter must resolve to the webserver and must be valid for the SSL cert configured in step 1.



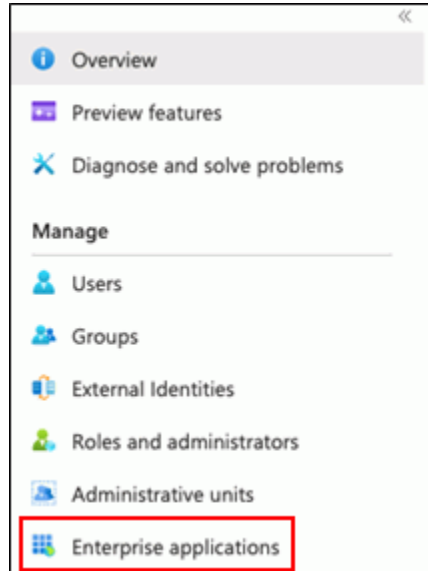
- 4 In order to use Single Sign-on (SAML), the Rep or mySupport interface must be configured to use Forms Authentication; it does not work with Windows Authentication. Verify that the Rep or mySupport interface is configured to use Forms Authentication via the Application tab on the iSupport Configuration Utility.
- 5 Update the Rep URL in the iSupport Application URL field in the Configuration | Core Settings | Global Settings screen. If using the mobile interface, update the Mobile Desktop URL field. Note that you must use the URL that was used in the web.config file.
- 6 Update the mySupport URL in the Configuration | Core Settings | mySupport | Portals screen. For each portal you wish to update, select the name in the list screen to open its configuration settings. Select the cog icon to the right of the Name field and then update the URL field on the Basics tab. Select Finish in the bottom right corner of the screen, and then select the Save disk icon in the upper right corner.

Setting Up an Application On Microsoft Azure

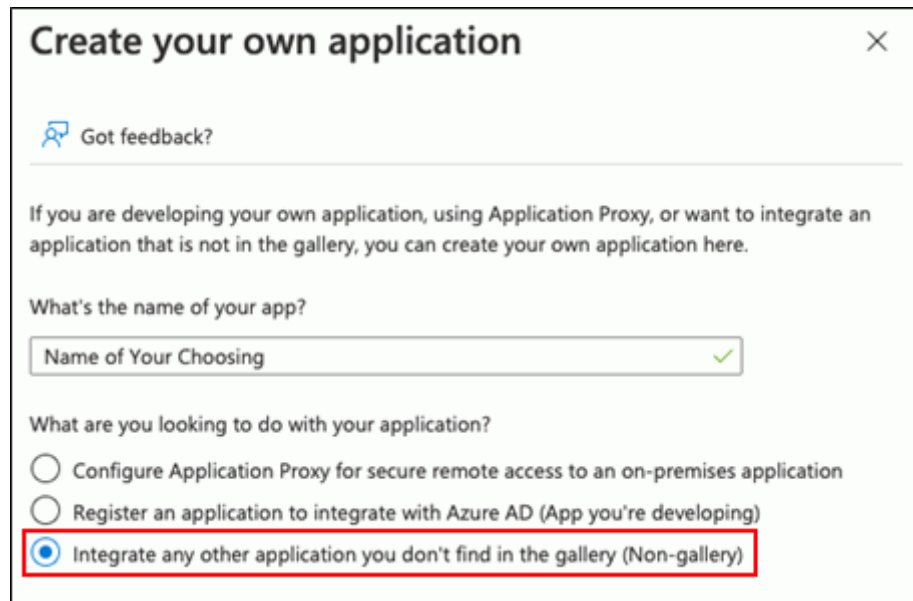
Note that paths are subject to change at Microsoft's prerogative. To configure the Microsoft side you must log in to Azure with a company administrator account.

- 1 Log in to Microsoft at <https://portal.azure.com/>
- 2 From Services, select Azure Active Directory.

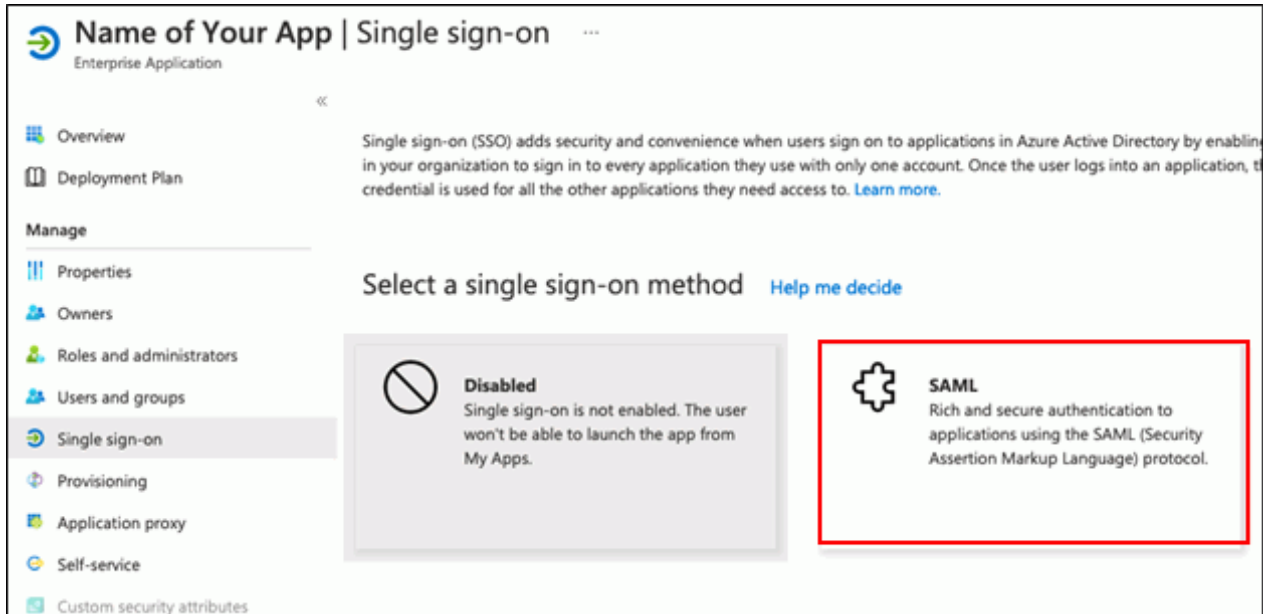
- 3 From the Manage menu, select Enterprise Applications.



- 4 Select New Application and then select Create Your Own Application. In the Create Your Own Application screen, enter an app name and select the Integrate Any Other Application You Don't Find In The Gallery (Non-Gallery) option.

A screenshot of the 'Create your own application' screen in the Azure AD portal. The screen has a title bar with a close button (X). Below the title is a 'Got feedback?' link. The main text reads: 'If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.' Below this is a text input field for the app name, containing 'Name of Your Choosing' with a green checkmark. Underneath is a section titled 'What are you looking to do with your application?' with three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Azure AD (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected and highlighted with a red rectangular box.

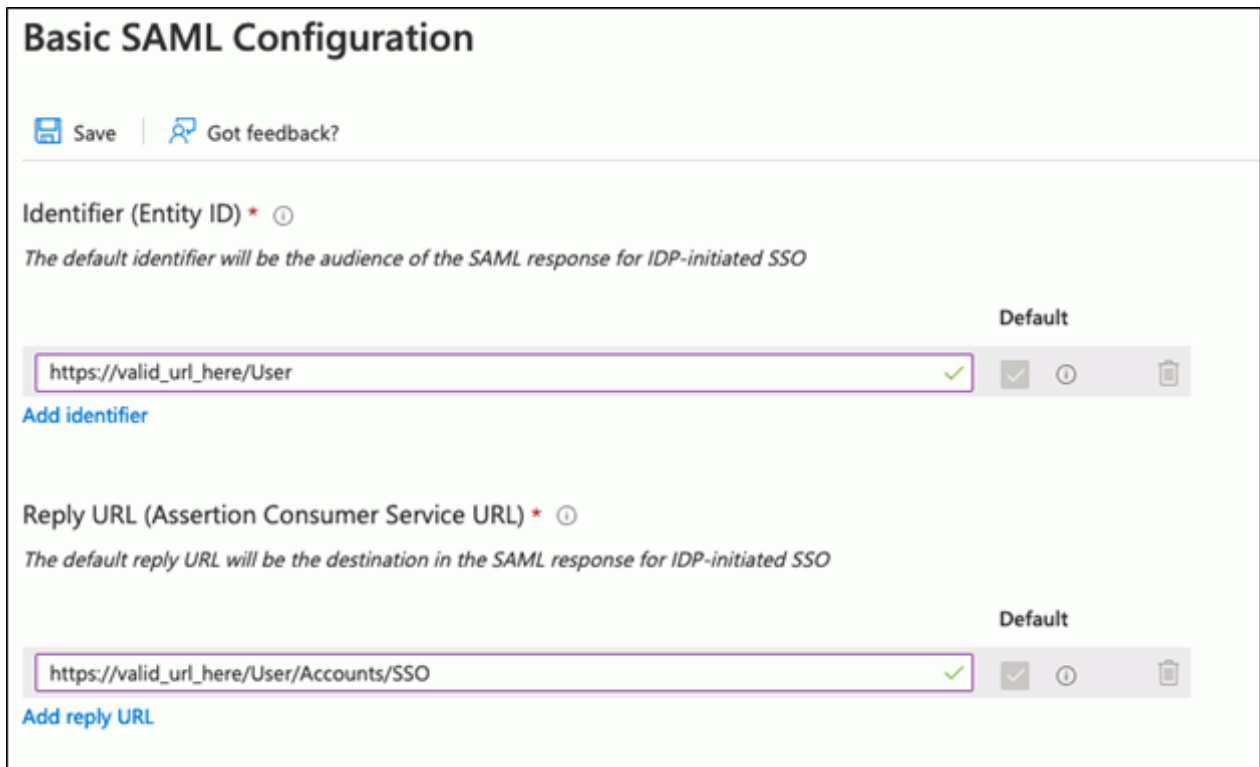
- 5 Once the app is created, select the Set Up Single Sign On (either from Manage or the Getting Started menu). When prompted to select a single sign-on method, select SAML.



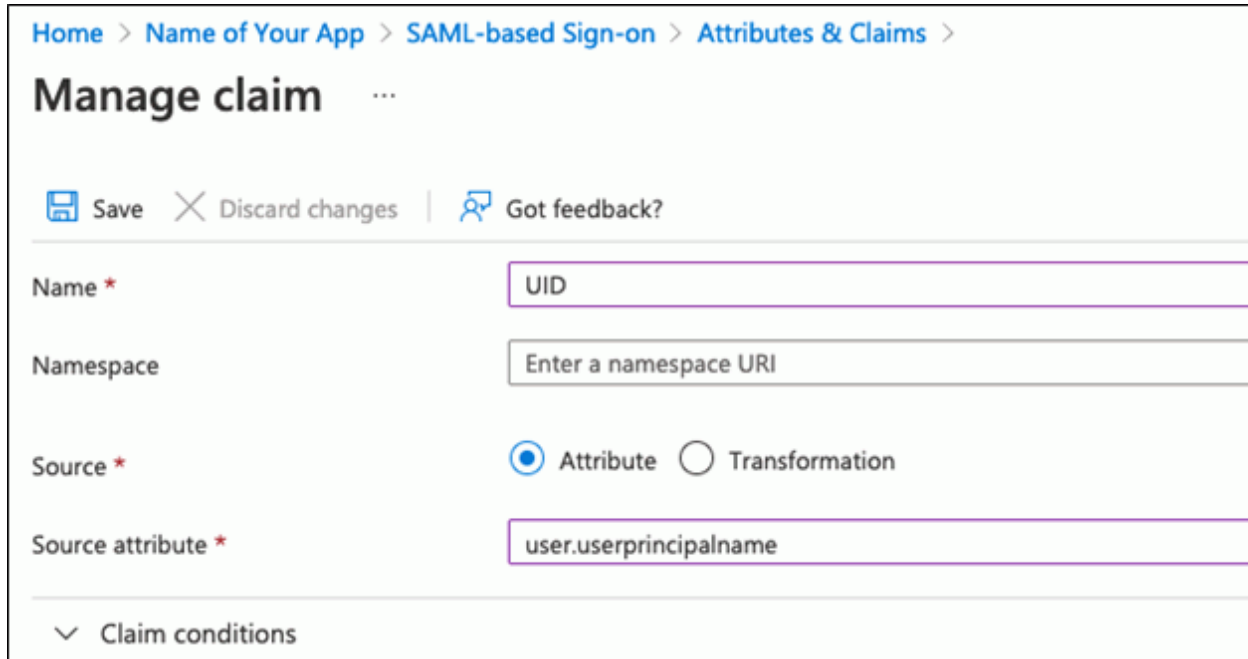
- 6 For Step 1: Basic SAML Configuration, select Edit and provide the following required information. Note that iSupport's online help has a Configuring Single Sign On Integrations topic that covers URLs.

- Identifier (Entity ID) - this is the issuer URL
- Reply URL (Assertion Consumer Service URL) - this is the consumer URL

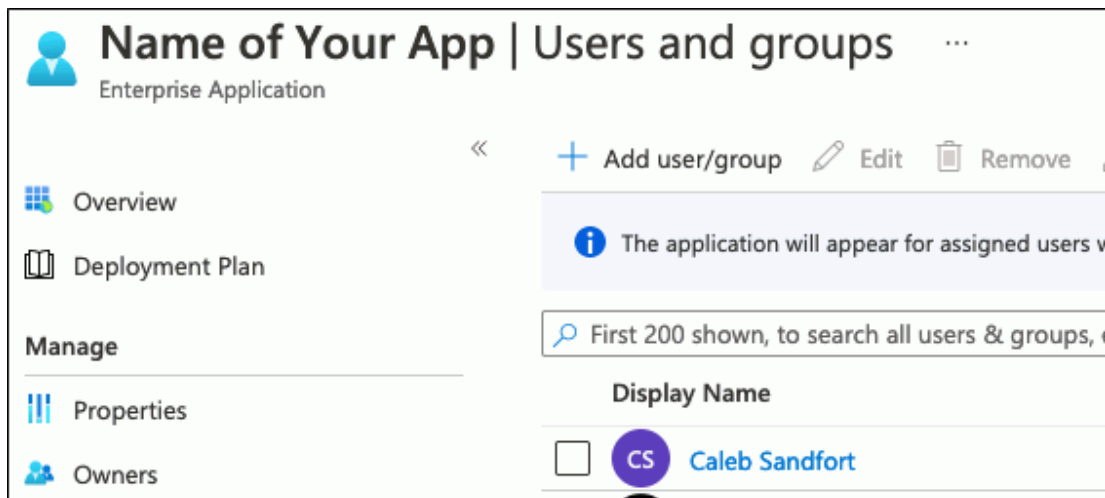
In our example, with mySupport, the Identifier would be `https://valid_url_here/User` and the Reply URL would be `https://valid_url_here/User/Account/SSO`.



- 7 For Step 2: Attributes and Claims, iSupport needs one attribute UID. You can map this to whatever you want but that value must match a login or secondary login of a Customer record or login of a Rep record. In this example, a claim named UID will be added and mapped to the UserPrincipalName.



- 8 For Step 3: SAML Signing Certificate, simply click and download from Federation Metadata XML (you will use this in iSupport).
- 9 Go back to the App properties, select Users and Groups, and add the users and/or groups that will be allowed to access the application in order to log in. Only those listed here will be able to access iSupport.



This concludes configuration of the Microsoft side, but you can come back if you wish to perform a test after you have set up single sign on in iSupport.

- 10 In iSupport, go to Configuration | Options and Tools | Integrate | Single Sign On Integrations and select Create.
- Enter a name and select On in the Active field.
 - Select your target; note that this must match what you configured in Microsoft. For example, if you used Rep Provider and Rep Consumer, your target is Rep. In our example, we have been using mySupport so mySupport will be selected here. If On is selected in the Hide Login Content on mySupport, the default mySupport forms login button will be hidden and only the Azure SAML login button will be shown.
 - In the Login Button Text field, enter the text to appear on the login button.

- d In the Load Settings From Metadata File field, select the Add button and use the file downloaded in step 8. This will populate the Issuer, Single Sign On URL, and X509 Certificate fields.
- e Important: update the Issuer field to include your Issuer URL. (The value that Microsoft XML file loads is incorrect.)
- f Select the Save button.

Desktop / Configuration / Options and Tools / Integrate / Single Sign On Integrations

Name

Active On Off

Target

Hide Login Content on mySupport On Off

Login Button Text

Load settings from metadata file

Issuer

Single Sign On URL

X509 Certificate

Testing

Log in to Microsoft and click the Test button or access your user portal and try logging in. Note that:

- The user must have been assigned when configuring the app in Microsoft.
- The mapped UID attribute in Microsoft must match the login or secondary login of the record in iSupport.
- In the case of mySupport, the customer record must have access to use mySupport. If any group restriction has been applied to the portal, they must be part of the group.

Configuring Password Complexity, Login Security, Expiration, and Login Locks

If you are not using Microsoft® Windows-based authentication with iSupport, you can use the Options and Tools | Administer | Rep Security screen to enable password security options, CAPTCHA, and multi-factor authentication; 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

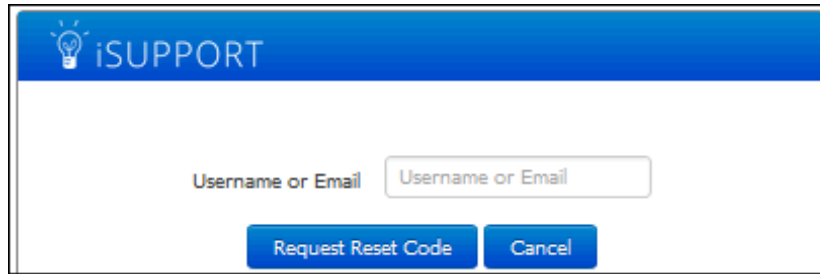
Use the Password section to enable a Forgot Password link, password expiration after a specified number of days, a previous password check with a specified number of previous passwords, and minimum password requirements. You can also force a password reset for all support representatives.

The screenshot shows the configuration interface for Password settings. The breadcrumb trail is Desktop / Configuration / Options and Tools / Administer / Security / Rep Security. A left-hand menu contains: Password (selected), Login Security, Login Screen Content, Failed Login Locks, Failed Login Log, and Locked Reps. The main configuration area includes: 'Enable Forgotten Password' with a 'Yes' button selected; a 'Forgotten Password Notification' section with a dropdown menu set to 'iSupport Default' and '+' and edit icons; 'Enable Password Expiration' with a 'Yes' button selected; 'Expire Password After' set to '60 days'; 'Warn Support Representative' set to '2 days before expiration'; 'Enable Previous Password Check' with a 'Yes' button selected; and 'Number of Previous Passwords' set to '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 options to access the Custom Notifications screen.

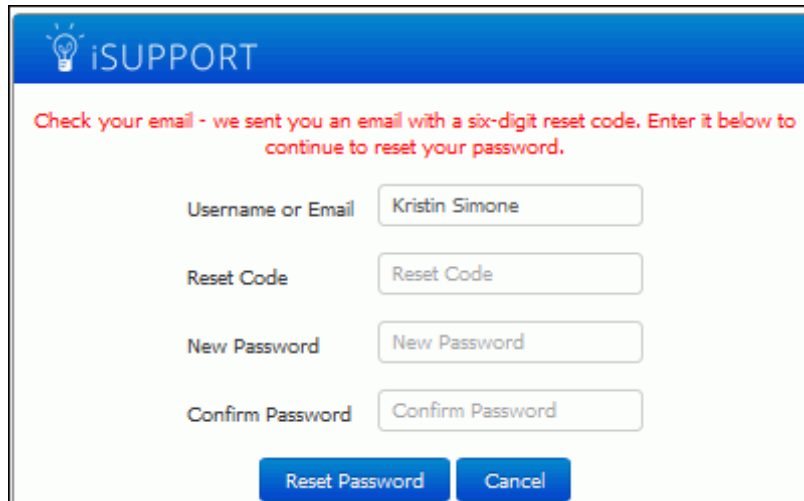
The screenshot shows the iSupport login interface. At the top is the iSUPPORT logo. Below it are two input fields: 'Username' and 'Password'. A blue 'Login' button is positioned below the password field. At the bottom of the form is a blue link labeled 'Forgot Password'.

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.



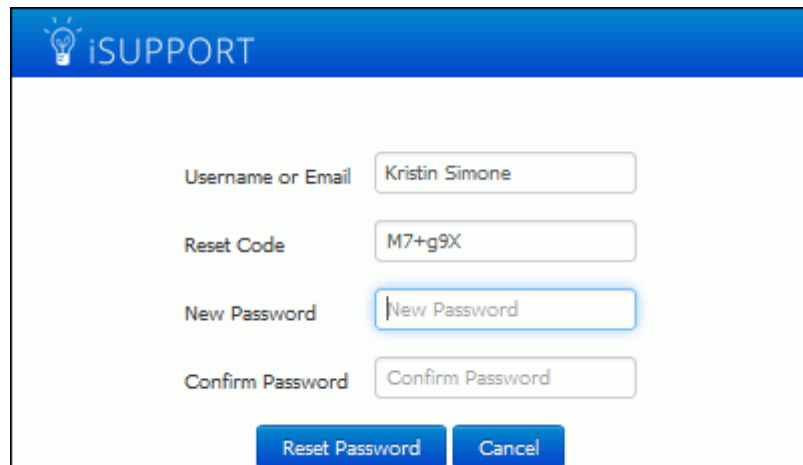
The screenshot shows the iSUPPORT interface with a blue header containing a lightbulb icon and the text 'iSUPPORT'. Below the header, there is a form with a label 'Username or Email' and a text input field containing the placeholder text 'Username or Email'. At the bottom of the form, there are two buttons: 'Request Reset Code' and 'Cancel'.

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



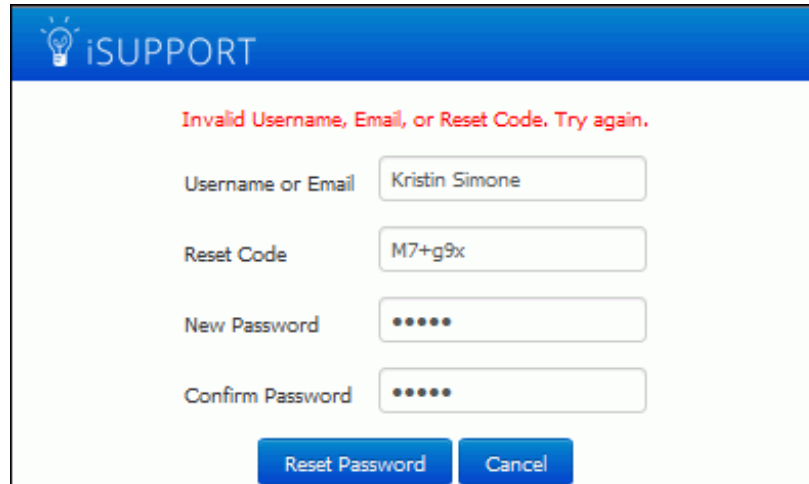
The screenshot shows the iSUPPORT interface with a blue header containing a lightbulb icon and the text 'iSUPPORT'. Below the header, there is a red instruction: 'Check your email - we sent you an email with a six-digit reset code. Enter it below to continue to reset your password.' Below this instruction, there are four form fields: 'Username or Email' with the value 'Kristin Simone', 'Reset Code' with the placeholder 'Reset Code', 'New Password' with the placeholder 'New Password', and 'Confirm Password' with the placeholder 'Confirm Password'. At the bottom, there are two 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.



The screenshot shows the iSUPPORT interface with a blue header containing a lightbulb icon and the text 'iSUPPORT'. Below the header, there are four form fields: 'Username or Email' with the value 'Kristin Simone', 'Reset Code' with the value 'M7+g9X', 'New Password' with the placeholder 'New Password', and 'Confirm Password' with the placeholder 'Confirm Password'. At the bottom, there are two buttons: 'Reset Password' and 'Cancel'.

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.



iSUPPORT

Invalid Username, Email, or Reset Code. Try again.

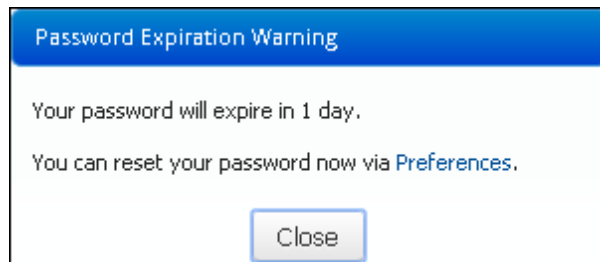
Username or Email

Reset Code

New Password

Confirm Password

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.



Password Expiration Warning

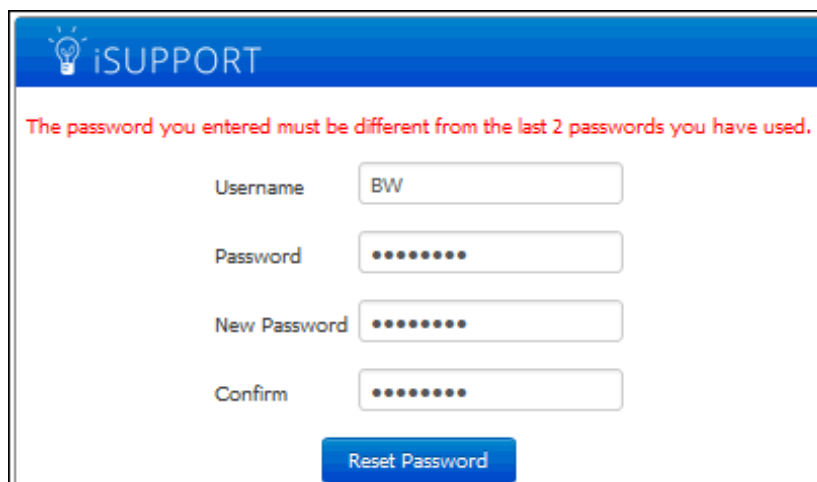
Your password will expire in 1 day.

You can reset your password now via [Preferences](#).

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.



iSUPPORT

The password you entered must be different from the last 2 passwords you have used.

Username

Password

New Password

Confirm

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 the following fields and options:

- Minimum Characters:** A text input field containing the number "5".
- At Least One Special Character:** Two radio buttons, "Yes" (selected) and "No".
- At Least One Numeric Character:** Two radio buttons, "Yes" (selected) and "No".
- At Least One Uppercase Character:** Two radio buttons, "Yes" (selected) and "No".
- At Least One Lowercase Character:** Two radio buttons, "Yes" (selected) and "No".
- Force Password Reset for All Support Representatives:** A button at the bottom of the window.

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 dialog. At the top, there is a blue header with the iSUPPORT logo. Below the header, a red error message reads: "The new password must contain at least one special character." The dialog contains the following fields:

- Username:** A text input field containing "CF".
- Password:** A password input field with masked characters (dots).
- New Password:** A password input field with masked characters (dots).
- Confirm:** A password input field with masked characters (dots).
- Reset Password:** A blue button 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 Security

Use the Login Security tab to set options for support representatives authenticating to iSupport.

The screenshot shows the 'Rep Security' configuration page in iSupport. The breadcrumb trail is 'Desktop / Configuration / Options and Tools / Administer / Security / Rep Security'. On the left is a navigation menu with 'Login Security' selected. The main area contains several toggle switches: 'Enable Captcha' (Yes), 'Enable Multi-factor Authentication' (Yes), and 'Enable SMS' (Yes). A yellow warning box states: 'Multi-factor authentication login codes will be sent via email to support representatives without a Mobile specified on their profile.' Below this, there is a 'Twilio Integration' dropdown menu set to 'Twilio1' and a 'Show Send Code Via Email Link' toggle switch set to 'Yes'.

Enable CAPTCHA - Select Yes to display a CAPTCHA image with a code (example below) in the Login dialog and require the user to enter the code in order to access the Desktop. Note that this feature is not available for the Mobile client.

The screenshot shows the iSupport login dialog. At the top, it says 'iSUPPORT'. Below that, a red message reads 'You have been logged out due to inactivity.' There are input fields for 'Username' and 'Password'. Below these is a CAPTCHA image showing the code 'BL126' with a mouse cursor pointing to it. To the right of the CAPTCHA are icons for a speaker and a refresh button. Below the CAPTCHA is a text input field with the placeholder 'Enter the code from the captcha image above'. At the bottom, there is a blue 'Login' button and a link for 'Forgot Password'.

Enable Multi-factor Authentication - Select Yes to enable an authentication code to be sent to a support representative after login in order to access iSupport.

Enable SMS - Select Yes to send a multi-factor authentication code via Short Message Service (commonly known as text messaging) to the support representative. SMS carriers are defined in the Options and Tools | Integrate | SMS Carriers screen in configuration.

- If SMS is enabled:
 - If a Twilio account is specified and the rep has a Mobile specified in their Profile record, the code will be sent to that number via SMS.
 - If the code has not been sent and the rep has a Mobile and SMS Carrier specified in their Profile record, the code will be sent to the <mobile number>@<SMS carrier email> via SMS.
 - If the code has not been sent and the rep has a specified Alt Email Address that ends with the email from any of the defined SMS carriers, the code will be sent to that address via SMS.

- If SMS is **not** enabled, the code is sent to the email address in the rep's Profile record.

Twilio Integration - Select or create the Twilio integration to be used for sending authentication codes to support representatives via SMS.

Show Send Code Via Email Link - Select Yes to include a Send Code Via Email link on the Validate Authentication Code dialog when the code is sent via SMS. This allows the code to be sent to an email address if the support representative doesn't have access to the phone that the code was sent to.

Configuring Login Screen Content

Login Screen Content - Enter the content to appear at the bottom of the login dialog; you can include formatted text and images.

Desktop / Configuration / Options and Tools / Administer / Security / Rep Security

Password

Login Security

Login Screen Content

Failed Login Locks

Failed Login Log

Locked Reps


Login Screen Content

abc 123 456 789 0 - B / U - Ω -

MS Sans Ser... 2 Normal A

Use this application only for company business.

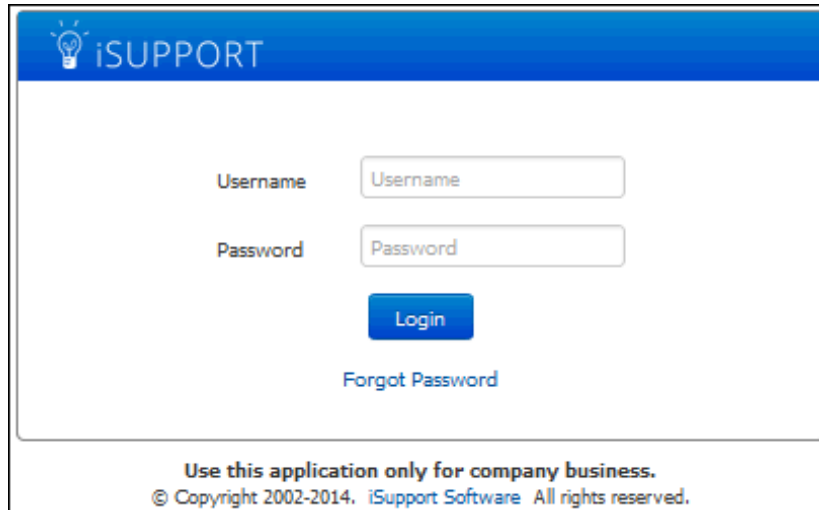
Background Image (Max File Size 2MB)



Add Remove

Background Image Fit Stretch Tile

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

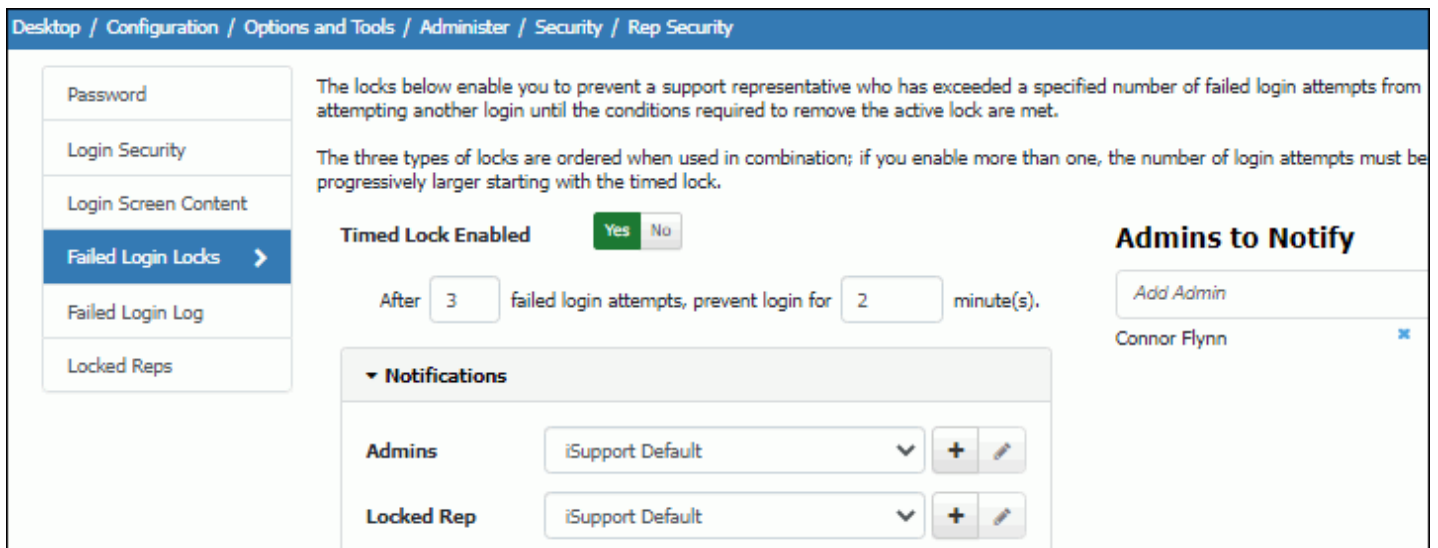


Background Image - Select the image to fill the screen around the login dialog.

Background Image Fit - Select Stretch to stretch the image and fit it in the window. (Note that this may cause some distortion.) Select Tile to display the image's fixed size in multiple tiles in the window. (Note that this option is best suited to small images.)

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.



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).

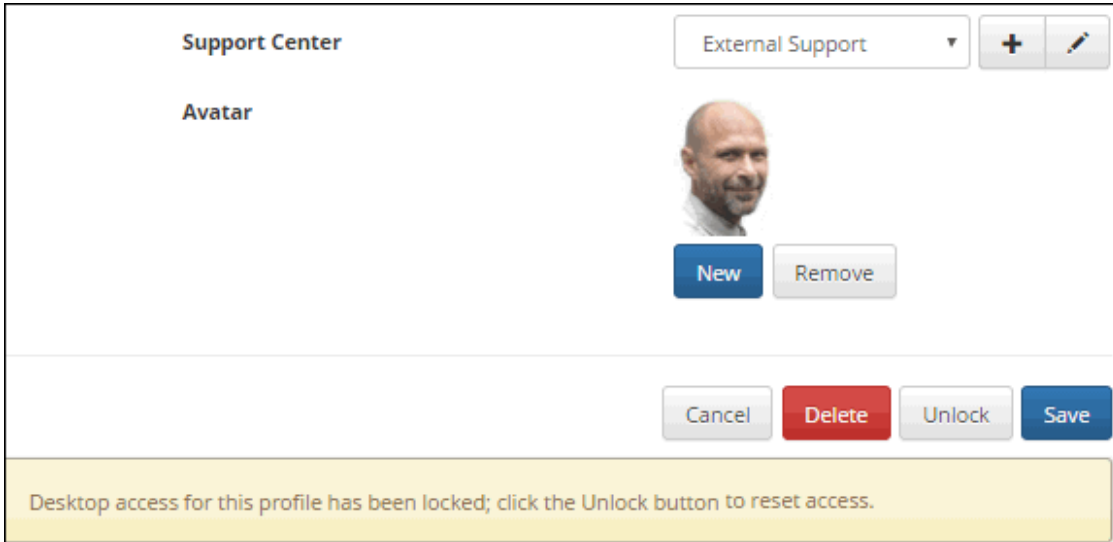
- A more restrictive **email lock** which displays a message regarding the lock and sends an email to the support representative, who must use the link in the email to reconnect to the login page in order to continue. If the support representative doesn't use the link and logs in directly, the lock would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

- 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.

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

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.



Viewing the Failed Login Log

Use the Failed Rep Login Log to display information on support representatives who have unsuccessfully attempted a login. Note that you can use the Locked Support Representatives view to display those who are locked out due to exceeding the configured number of failed login attempts.

