



Administering iSupport

Use the following tools in the Options and Tools | Administer section to track and monitor iSupport:

- Agents perform tasks in the background that are an integral part of iSupport functionality. See [“Enabling and Scheduling Agents” on page 2](#) for more information.
- See [“Archiving and Database Maintenance” on page 14](#) for information on scheduling agents that maintain iSupport databases and move closed work items to archive databases.
- See [“Viewing the Event Log” on page 16](#) for information on displaying entries that reflect application errors and messages and the date and time that iSupport agents run.
- See [“Configuration Audit Tracking” on page 23](#) for information on displaying audit history entries for configuration updates in most modules.
- See [“Enabling iSupport Updates” on page 24](#) for information on enabling an automatic search for iSupport hotfix updates and automatic installation of available updates.
- See [“Chart/View Audit Tracking” on page 25](#) for information on displaying audit history entries for chart and view updates.
- See [“Generating iSupport Environment Reports” on page 26](#) for information on compiling a printable summary of configuration settings and information on the server on which the diagnosis is run.
- See [“Discussion Post Management” on page 27](#) for information on viewing, removing, or deleting discussion post entries.
- See [“Managing Access to Images” on page 28](#) for information on deleting and restricting access to folders and images uploaded via the Image Manager.
- See [“Viewing Rep Chat History” on page 29](#) for information on displaying chats between support representatives.
- See [“Managing Your iSupport License” on page 30](#) for information on administering the license for your iSupport application.
- See [“Configuring Password Complexity, Expiration, and Login Locks” on page 32](#) for configuring security options for support representatives.
- See [“Configuring Password Complexity, Expiration, and Login Locks for Customers” on page 40](#) for information on configuring security options for customers.
- See [“Using the Data Override Feature for Incidents, Problems, and Changes” on page 46](#) for information on overwriting fields on any saved incident, problem, or change.

This document also contains information on administering iSupport databases:

- [“Backing Up and Restoring iSupport Databases” on page 47.](#)
- See [“Changing iSupport’s Access to SQL Databases” on page 54](#) for using the iSupport Access Utility to modify the SQL database, database server, and SQL login to the iSupport databases.

Enabling and Scheduling Agents

Agents perform tasks that are an integral part of iSupport functionality such as sending notifications. Agents run in the background; to verify that an agent has run, go to Options and Tools | Administer | Event Log. Agent intervals start at the time the iSupport Agent Manager service last ran; therefore, if you wish for an interval-based agent to run at a certain time, stop and start the iSupport Agent Manager service at that time. For example, if you set an interval for an agent to 24 hours and wish to have the agent run at 2 a.m., stop and start the iSupport Agent Manager service at 2 a.m.

The iSupport Agent Manager Status icons in the upper right corner of the screen indicate the status of the iSupport Agent Manager service, which performs scheduled execution of iSupport agents. This service is required for the normal operation of iSupport. If the indicator is red, go to Administration Tools | Services on the server that is hosting iSupport and start the service.

Scheduling and Running Global Agents

Use the Global tab to disable or specify the interval for agents that affect the entire application. You can click the Run Now button to execute an agent immediately.

The screenshot displays the iSupport Agent Manager configuration page. At the top right, the status is shown as "iSupport Agent Manager Status: ● ○". On the left, a navigation menu includes "Global" (selected), "Incident/Change/Purchase", "Asset", and "Configuration Management". The main content area is divided into sections for different agents:

- Notification Agent:** Description: "This agent searches all configuration items and service contracts and sends configured event-related notifications." Interval: 2 minutes. Run Now button.
- Alert Agent:** Description: "This agent evaluates alerts and activates them as necessary." Interval: 5 minutes. Run Now button.
- Survey Agent:** Description: "For each active survey, this agent will first check the closed incident interval specified in the Survey Interval field. If the count has been reached, the agent will check the day interval and the date and recipient of the last survey sent. If the number of days that has passed is greater than or equal to the day interval, the survey will be sent to the customer associated with the closed incident." Interval: Daily, 5:00 PM. Run Now button.
- Time-Based Rules Agent:** Description: "This agent searches all configured time-based rules, monitors time frames, and performs configured actions if conditions in the rules are met." Enable: Yes (selected), No, Run Now button.
- Knowledge Entry Review Agent:** Description: "The Knowledge Entry Review agent sends notifications to reviewers of knowledge entries." Enable: Yes (selected), No, Run Now button. Time Agent Should Run Each Day: 11:00 PM.
- Discussion Digest Agent:** Description: "The Discussion Digest agent sends daily and weekly updates of discussion activity." Enable: Yes (selected), No, Run Now button. Time Agent Should Run Each Day: 11:00 PM.
- View Subscription Agent:** Description: "This agent sends scheduled exports of view data to recipients." Enable: Yes (selected), No, Run Now button.

Notification Agent Interval - Select the number of minutes in the interval for the Notification agent to search records and send event notifications configured via the Notifications tab in the Service Contract Basics and CMDB Types screens. Select Disabled if you do not wish to send these event notifications.

Alert Agent Interval - Alerts are configured to send an email or page, and/or appear at the top of the Desktop tabs, when a view field reaches a certain threshold. For example, you could configure an alert to trigger when a certain number of Emergency priority incidents is reached. Select the number of minutes or hours in the interval for the Alert agent to run and evaluate configured alerts, or select Daily to run the agent every day at a specified start time.

Survey Agent Interval - For each active survey, the Survey agent will first check the closed incident interval specified in the Survey Interval field. If the count has been reached, the agent will check the day interval and the date and recipient of the last survey sent. If the number of days that has passed is greater than or equal to the day interval, the survey will be sent to the customer associated with the closed incident. Select the number of minutes in the interval for the survey agent to check survey definitions, or select Daily to run the agent every day at a specified start time.

Time-Based Rules Agent - Time-Based rules incorporate time frames with conditions; when conditions are true upon save of an associated incident, problem, or change, the date and time that the interval time frame would be reached is recorded and monitored by this agent. This agent runs every minute. If the conditions required to meet the rule do not change before the interval time frame is reached, the agent performs the actions specified.

Knowledge Entry Review Agent - Select Yes to enable the Knowledge Entry Review agent to search for entries that match the date review date specified in a knowledge entry and send a notification to the reviewer. If the iSupport Default notification is used, a newsletter-style email will be sent; if a custom notification is used, a notification will be sent for each knowledge entry.

Discussion Digest Agent - Discussion-only feeds on both the Desktop and the mySupport portal include an icon the header for users to enable a digest email of discussion activity that can be sent daily or weekly; select Yes to enable the Discussion Digest agent that sends this email. After selecting Yes, select the number of minutes in the interval for agent to run or select Daily to run the agent every day at a specified start time. The email will list all new posts for the day or week, including the person submitting the post, the content of the post, and the date and time of the post.

View Subscription Agent - Select Yes to enable the View Subscription agent, which sends scheduled view exports via email to recipients designated via the View component. This agent runs on a five minute interval.

Scheduling and Running Incident, Change, and Purchase Agents

Use the Incident/Change/Purchase tab to schedule the Ticket Scheduling, Change Scheduling, Email Processing, Followup, Approval Reminder, and Service Contract agents. You can click the Run Now button to execute an agent immediately.

iSupport Agent Manager Status: ● ○

Ticket Scheduling Agent

This agent searches all scheduled tickets and changes the status from scheduled to an open status.

Interval

Change Scheduling Agent

This agent searches all scheduled changes and changes the status from scheduled to an open status.

Interval

Email Processing Agent

This agent searches a configured email mailbox for new messages. For each message, an incident is created and fields are populated as configured. A customer profile is also created for each new customer.

Interval

Followup Agent

The Followup agent sends notifications to assignees of incidents with a status other than Closed and an expired followup date.

Enable Yes No

Time Agent Should Run Each Day

Approval Reminder Agent

The Approval Reminder agent sends notifications to the approvers specified in the Approval Cycle screen, based on specified number of hours after approval request sent.

Interval

Service Contract Agent

This agent evaluates service contracts and sets them to expired if necessary.

Interval

Ticket Scheduling Agent Interval - Select the number of minutes in the interval for the Ticket Scheduling agent to check all scheduled tickets for start dates/times and, if the specified date/time is reached, changes the status from Scheduled to an open status. Ticket generation times are also checked and tickets are created if the specified time is reached.

Change Scheduling Agent Interval - Select the number of minutes in the interval for the Change Scheduling agent to check all scheduled changes for start dates/times and, if the specified date/time is reached, changes the status from Scheduled to an open status. Change generation times are also checked and change requests are created if the specified time is reached.

Email Processing Agent Interval - The Email Processing agent creates an incident or updates an existing incident, problem, purchase, or change for each message, processes defined rules, and creates a customer profile for each new customer. Select the number of minutes in the interval for the Email Processing agent to search the email mailbox for new messages, or select Disabled if you do not wish to use the email-submitted incident feature.

Followup Agent/Time the Followup Agent Should Run Each Day - Select Yes to enable the Followup agent that checks all incident followup dates. The agent sends email reminders to the incident assignees for each incident with an expired followup date and a status other than a Closed status. After selecting Yes, use the Time Agent Should Run Each Day field to select the time the agent should run.

Approval Reminder Agent Interval - Select Yes to enable the Approval Reminder agent that sends notifications to the approvers specified in the Approval Cycle screen, based on a specified number of hours after the approval request is sent. After selecting Yes, select the number of minutes in the interval for agent to run or select Daily to run the agent every day at a specified start time.

Service Contract Agent Interval - Select the number of minutes in the interval for the Service Contract agent to check all service contracts for counts and/or end dates/times; if the specified total count and/or end date/time is reached, the status changes to an Expired status. You can select Daily to run the agent every day at a specified start time.

Scheduling and Running Asset Agents

Use the following screen to enable or disable agents, or specify the interval for Asset Reminder, Unit Count Tracking, Scheduled Scan, Auto Asset Create, Asset Import, and License Management agents. You can click the Run Now button to execute an agent immediately.

Asset Reminder Agent

This agent sends notifications to the individuals specified in the Asset Configuration screen, based on the specified number of days prior to the warranty or maintenance expiration date.

Enable Yes No

Time Agent Should Run Each Day

Asset Unit Count Tracking Agent

This agent sends notifications to the individuals specified in the Asset Type Configuration screen based on the specified minimum threshold of remaining units.

Enable Yes No

Time Agent Should Run Each Day

Asset Scheduled Scan and Monitoring Agent

This agent checks scheduled scan definitions, initiates scans as scheduled, and enables monitoring if configured in an scheduled scan definition.

Enable Yes No

Monitoring includes device state change entries in the database; days to retain these entries

Auto Asset Create from Scheduled Scan Agent

This agent creates an Asset record for each asset scan that is not associated with an asset.

Enable Yes No

Populate Asset Serial Number Field using

Default Asset Record Template for Automatic Asset Creation [Laptop 1](#)

License Management Agent

This agent scans all inventory scans and searches for the software titles specified in Software License Profile records. It compares the actual quantities found against the condition specified in the profiles, flags the profiles that meet the condition, and updates the profiles with the actual counts.

Enable Yes No

Time Agent Should Run Each Day

Asset Reminder Agent/Time the Asset Reminder Agent Should Run Each Day - The Asset Reminder agent searches for warranty and maintenance expiration dates. If it is the specified number of days before the warranty or maintenance expiration date, it will send an email reminder to the individuals specified in the Asset record. Select Yes

to enable the Asset Reminder agent. After selecting Yes, use the Time Agent Should Run Each Day field to select the time the agent should run.

Asset Unit Count Tracking Agent - If count tracking is enabled for an asset type and the type is selected in the Asset screen, a count and low item threshold can be entered for an asset. The count can be decremented via entries in the Incident, Problem, and Change screens and notifications can be sent to the individuals specified in the Asset Type Configuration screen when the count reached the specified minimum number of remaining units. Select Yes to enable the agent to check unit counts and send notifications when the minimum is reached. After selecting Yes, use the Time Agent Should Run Each Day field to select the time the agent should run.

Asset Scheduled Scan and Monitoring Agent/Monitoring...days to retain these entries - Select Yes to enable the Asset Scheduled Scan and Monitoring agent that checks scheduled scan definitions, initiates scans according to schedule, and enables monitoring if configured in a scheduled scan definition. This agent runs every minute. Network monitoring processing adds device state change entries in the database. Use the Monitoring ...Days to Retain These Entries field to control database growth by entering the number of days in which these entries should stay in the database.

Auto Asset Create from Scheduled Scan Agent - Select Yes to enable the Auto Asset Create from Scheduled Scan agent that creates asset records for each machine involved in a scheduled scan that does not have an association with an asset record. The agent will run every hour based on the time at which the iSupport Agent Manager service is started. Asset records will be created using the asset selected in the Auto Asset Create Asset Record Template field as a template.

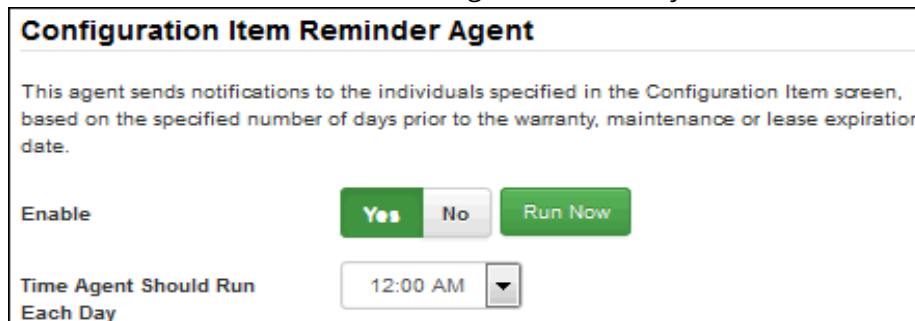
Populate Asset Serial Number Field With - Select Yes to populate the Asset Serial Number field with the operating system serial number when Asset records are created automatically for machines that are involved in scheduled scans but not associated with an existing record.

Asset Record Template for Automatic Asset Creation - Click this link to select the name of an existing Asset record to use as a template when the Auto Asset Create from Scheduled Scan agent is run. The record's asset type will determine the fields that will appear on the automatically-created record.

License Management Agent/Time the License Management Agent Should Run Each Day - Select Yes to enable the License Management agent that scans all existing scheduled scans and searches for the software titles specified in Software License Profile records. It compares the actual quantities found against the condition specified in the profiles, flags the profiles that meet the condition, and updates the profiles with the actual counts. Notifications are sent if configured. After selecting Yes, use the Time Agent Should Run Each Day field to select the time the agent should run.

Scheduling and Running Configuration Management Agents

Use the Configuration Management tab to schedule agents for CMDB notifications and for automatically creating and synchronizing configuration items based on existing asset, customer, company, and/or support representative records. You can click the Run Now button to execute an agent immediately.



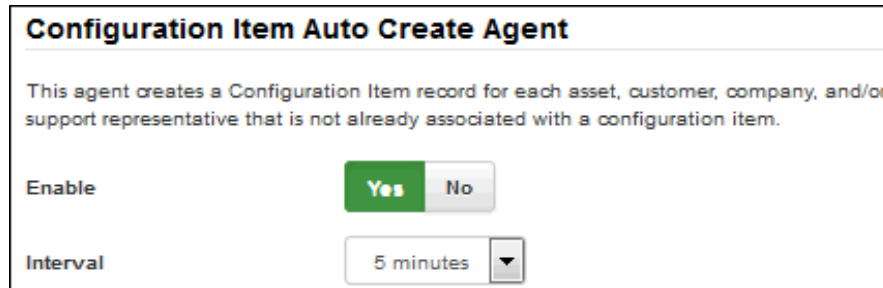
The screenshot shows a configuration window for the "Configuration Item Reminder Agent". At the top, there is a title bar with the agent name. Below the title bar, a descriptive text states: "This agent sends notifications to the individuals specified in the Configuration Item screen, based on the specified number of days prior to the warranty, maintenance or lease expiration date." Below this text, there are three buttons: "Yes", "No", and "Run Now". The "Yes" button is highlighted in green. Below the buttons, there is a label "Time Agent Should Run Each Day" followed by a dropdown menu showing "12:00 AM" and a downward arrow.

Configuration Item Reminder Agent - The Configuration Item Reminder agent searches for warranty, maintenance, and lease expiration dates. If it is the specified number of days before the warranty, maintenance, or lease expiration date, it will send an email reminder to the individuals specified in the Configuration Item record. To run the agent on an interval basis, select Yes in the Enabled field and then select the time at which the agent should run each day in the Time Agent Should Run Each Day field.

Agents for Creating CIs Automatically

Configuration Item Auto Create Agent - The Configuration Item Auto Create agent creates CI records for assets, customers, customer groups, companies, support representatives, and/or support representative groups that do not have an association with a CI record. In each applicable section you'll need to select an existing CI record to use as a template for populating the fields on the newly-created CI.

If you wish to create configuration items automatically on a one-time basis, you can select an existing CI record to use as a template and click the Run Now button to run the agent immediately. If you wish to create configuration items automatically on an interval basis, click the Yes button to enable and schedule the agent by selecting the number of minutes in the interval for the agent to run. You can select Daily to run the agent every day at a specified start time.



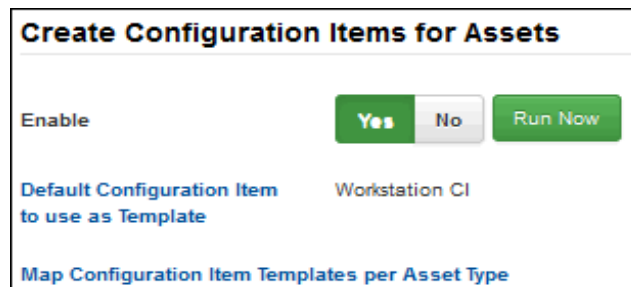
Configuration Item Auto Create Agent

This agent creates a Configuration Item record for each asset, customer, company, and/or support representative that is not already associated with a configuration item.

Enable Yes No

Interval ▾

Create Configuration Items for Assets/Configuration Item to Use as Template/Map Configuration Item Templates per Asset Type - This option enables you to create CI records for each asset that does not have an association with a CI record. Click the Configuration Item to Use as Template link to select the name of an existing CI record to use as a template for populating fields on newly-created CIs. Note that the CMDB type for the selected CI must have Assets enabled in the Associated Items section. The CMDB type, description, and custom and optional fields on the selected CI will be included on the CI records created. The source listed on the CI will be "Auto Create". The asset name will be used for the CI name.



Create Configuration Items for Assets

Enable Yes No

[Default Configuration Item to use as Template](#) Workstation CI

[Map Configuration Item Templates per Asset Type](#)

If creating configuration items for multiple asset types, you can click the Map Configuration Item Templates per Asset Type link to select a configuration item to use as a template for populating fields on records of each asset type.

Use the Run Now button to run the agent immediately on a one-time basis. To create configuration items automatically for assets on an interval basis, enable the Configuration Item Auto Create Agent and select Yes in the Enable field in this section.

Create Configuration Items for Customers/Configuration Item to Use as Template - This option enables you to create CI records for each customer that does not have an association with a CI record. Click the Configuration Item to Use as Template link to select the name of an existing CI record to use as a template for populating fields on newly-created CIs. Note that the CMDB type for the selected CI must have Customers enabled in the Associated

Items section. The CMDB type, description, and custom and optional fields on the selected CI will be included on the CI records created. The source listed on the CI will be "Auto Create". The customer name will be used for the CI name.

The screenshot shows two sections of a software interface. The top section is titled "Create Configuration Items for Customers" and contains an "Enable" field with "Yes" and "No" radio buttons, and a "Run Now" button. Below this is a link "Configuration Item to use as a Template" followed by the text "Customer CI". The bottom section is titled "Create Configuration Items for Customer Groups" and contains an "Enable" field with "Yes" and "No" radio buttons, and a "Run Now" button. Below this is a link "Configuration Item to use as a Template" followed by the text "Customer Group CI". At the bottom of this section is a dropdown menu labeled "Relationship of the Group to the Members" with the selected option "Includes - Member Of".

Use the Run Now button to run the agent immediately on a one-time basis. To create configuration items automatically for customers on an interval basis, enable the Configuration Item Auto Create Agent and select Yes in the Enable field in this section.

Create Configuration Items for Customer Groups/Configuration Item to Use as Template/Relationship of the Group to the Members - This option enables you to create CI records for each customer group and group member that does not have an associated CI. You'll need to select configuration items to be used as templates for populating fields in the newly-created customer CIs and customer group CIs; the CMDB type for the selected CIs must have Customer and Customer Group enabled in the Associated Items section. You'll also need to select the relationship of the group to the group members; this relationship must exist on the Relationships tab in the CMDB type of the selected CIs. You'll be able to use the relationships in both the Name and Corresponding Name columns on that tab.

Click the Configuration Item to Use as Template link in the Create Configuration Items for Customers section to select the name of an existing CI record to use as a template for populating fields on newly-created customer CIs, and then click the Configuration Item to Use as Template link in this section to select the name of an existing CI record to use as a template for populating fields on newly-created customer group CIs. The CMDB type, description, and custom and optional fields on the selected CIs will be included on the CI records created. The source listed on the CI will be "Auto Create". The customer name will be used for the CI name on customer CIs, and the customer group name will be used for the CI name on customer group CIs.

Use the Run Now button to run the agent immediately on a one-time basis. To create configuration items automatically for customer groups on an interval basis, enable the Configuration Item Auto Create Agent, select Yes in the Enable field in the Create Configuration Items for Customers section, and select Yes in the Enable field in this section.

Create Configuration Items for Companies/Configuration Item to Use as Template - This option enables you to create CI records for each company that does not have an association with a CI record. Click the Configuration Item to Use as Template link to select the name of an existing CI record to use as a template for populating fields on newly-created CIs. Note that the CMDB type for the selected CI must have Company enabled in the Associated Items section. The CMDB type, description, and custom and optional fields on the selected CI will be included on the CI records created. The source listed on the CI will be "Auto Create". The company name will be used for the CI name.

The screenshot shows a section titled "Create Configuration Items for Companies". It contains an "Enable" field with "Yes" and "No" radio buttons, and a "Run Now" button. Below this is a link "Configuration Item to use as a Template" followed by the text "Company CI".

Use the Run Now button to run the agent immediately on a one-time basis. To create configuration items automatically for companies on an interval basis, enable the Configuration Item Auto Create Agent and select Yes in the Enable field in this section.

Create Configuration Items for Support Reps/Configuration Item to Use as Template - This option enables you to create CI records for each support representative that does not have an association with a CI record. Click the Configuration Item to Use as Template link to select the name of an existing CI record to use as a template for populating fields on newly-created CIs. Note that the CMDB type for the selected CI must have Support Representative enabled in the Associated Items section. The CMDB type, description, and custom and optional fields on the selected CI will be included on the CI records created. The source listed on the CI will be "Auto Create". The support representative name will be used for the CI name.

Use the Run Now button to run the agent immediately on a one-time basis. To create configuration items automatically for support representatives on an interval basis, enable the Configuration Item Auto Create Agent and select Yes in the Enable field in this section.

Create Configuration Items for Support Rep Groups/Configuration Item to Use as Template/Relationship of the Group to the Members - This option enables you to create CI records for each support representative group and group member that does not have an associated CI. You'll need to select configuration items to be used as templates for populating fields in the newly-created support representative CIs and support representative group CIs; the CMDB type for the selected CIs must have Support Representative and Support Representative Group enabled in the Associated Items section. You'll also need to select the relationship of the group to the group members; this relationship must exist on the Relationships tab in the CMDB type of the selected CIs. You'll be able to use the relationships in both the Name and Corresponding Name columns on that tab.

The screenshot shows two sections of a configuration interface. The top section is titled "Create Configuration Items for Support Reps" and contains an "Enable" field with "Yes" and "No" radio buttons, a "Run Now" button, and a "Configuration Item to use as a Template" dropdown menu set to "Support Rep CI". The bottom section is titled "Create Configuration Items for Support Rep Groups" and contains an "Enable" field with "Yes" and "No" radio buttons, a "Run Now" button, a "Configuration Item to use as a Template" dropdown menu set to "Support Rep Group CI", and a "Relationship of the Group to the Members" dropdown menu set to "Includes - Member Of".

Click the Configuration Item to Use as Template link in the Create Configuration Items for Support Representatives section to select the name of an existing CI record to use as a template for populating fields on newly-created support representative CIs, and then click the Configuration Item to Use as Template link in this section to select the name of an existing CI record to use as a template for populating fields on newly-created support representative group CIs. The CMDB type, description, and custom and optional fields on the selected CIs will be included on the CI records created. The source listed on the CI will be "Auto Create". The support representative name will be used for the CI name on support representative CIs, and the support representative group name will be used for the CI name on support representative group CIs.

Use the Run Now button to run the agent immediately on a one-time basis. To create configuration items automatically for support representative groups on an interval basis, enable the Configuration Item Auto Create Agent, select Yes in the Enable field in the Create Configuration Items for Support Representatives section, and select Yes in the Enable field in this section.

Agents for Synchronizing Relationships for CIs with Customer or Support Representative Groups

Customer Support Rep Group Relationship Synchronization Agent/Sync Relationships for Customer Groups/Configuration Item to Use as Template for Group Members/Relationship of the Group to the Members - Use

this option to monitor existing customer group CIs and update any changes in the associated customer groups. For example, if a customer is added to a customer group, it creates a CI record for that customer and adds a relationship to the customer group CI.

Group Relationship Synchronization Agent

This agent synchronizes relationships for Configuration Item records that are associated with a customer group or support representative group.

Enable Yes No

Interval ▼

Sync Relationships for Customer Groups

Enable Yes No

Configuration Item to use as a Template

Relationship of the Group to the Members ▼

[i](#)

Sync Relationships for Support Rep Groups

Enable Yes No

Configuration Item to use as a Template

Relationship of the Group to the Members ▼

[i](#)

You'll need to specify a CI to use as a template and a relationship for the newly-created customer CIs; however, note that:

- The CMDB type for the configuration item must have customer groups enabled for associated items.
- **The relationship selected for synchronization will not be available for assignment to any other CI or group.** You may wish to add a relationship to the type of the CI used as a template for this purpose.

To run the agent immediately on a one-time basis, click the Run Now button in the Create Configuration Items for Customer Groups section. To run the agent on an interval basis, select Yes in the Enabled field in the Sync Relationships for Customer Groups section **and** at the top of the Customer Support Rep Group Relationship Synchronization Agent section. Then set the agent interval and save. You can select Daily to run the agent every day at a specified start time.

Sync Relationships for Support Rep Groups/Configuration Item to Use as Template for Group Members/ Relationship of the Group to the Members - Use this option to monitor existing support representative group CIs and update any changes in the associated support representative groups. For example, if a support representative is added to a support representative group, it creates a CI record for that support representative and adds a relationship to the support representative group CI. You'll need to specify a CI to use as a template and a relationship for the newly-created support representative CIs; however, note that:

The CMDB type for the configuration item must have support representative groups enabled for associated items.

The relationship selected for synchronization will not be available for assignment to any other CI or group. You may wish to add a relationship to the type of the CI used as a template for this purpose.

To run the agent immediately on a one-time basis, click the Run Now button in the Create Configuration Items for Support Representative Groups section. To run the agent on an interval basis, select Yes in the Enabled field in the Sync Relationships for Support Representative Groups section **and** at the top of the Customer Support Rep Group Relationship Synchronization Agent section. Then set the agent interval and save.

Archiving and Database Maintenance

Use the Options and Tools | Administer | Archiving and Database Maintenance screen to schedule agents that maintain iSupport databases and move closed work items to archive databases.

Database Maintenance Agent

This agent maintains data resulting from incomplete saves, deleted records, etc.

Time Agent Should Run Each Day: 11:30 PM

Archive Agent

This agent moves closed work items and sent correspondence documents that meet archive criteria to an archive database.

Time Agent Should Run Each Day: 12:00 AM

Max Duration: 4 Hour(s)

Chat Log Purge: 90 days

Scheduling the Database Maintenance Agent

Schedule the Database Maintenance agent to maintain data resulting from incomplete saves, deleted records, etc. Select the time at which the Database Maintenance agent should run each day.

Archiving

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.

- Eligible incidents and sent correspondence not associated with an open work item will be moved to the cSupport_Archive database. If an incident or change is part of a hierarchy template, the topmost parent in the hierarchy must meet the archive criteria before any closed work items are archived.
- Eligible changes will be moved to the cSupport_Archive_Change database
- Eligible problems will be moved to the cSupport_Archive_Problem database
- Eligible purchase orders will be moved to the cSupport_Archive_Purchase database

You can also configure purging, which permanently deletes items from the applicable archive database after the specified number of days/years past the archive date.

For each work item type, use the following fields to specify the items eligible for archiving. When finished, use the **Time Agent Should Run Each Day** field to select the time the Archive Agent should run. You can click Run Now to

run the agent immediately. In the Max Duration field, enter the amount of time (in hours) at which to terminate the archive agent if it is still running.

The screenshot shows the 'Incident' configuration page. On the left is a sidebar with menu items: Basics, Change, Correspondence, Incident (highlighted with a right arrow), Problem, and Purchase. The main area is titled 'Incident' and contains the following settings:

- Archive Enabled:** A toggle switch with 'Yes' selected (green) and 'No' (grey).
- Elapsed amount of time before a closed incident is moved from the production database to the cSupport_Archive database:** A numeric input field containing '1' and a dropdown menu set to 'Years'.
- Statuses to Archive:** A list box containing the status 'Closed'.
- Purge Enabled:** A toggle switch with 'Yes' selected (green) and 'No' (grey).
- Elapsed amount of time before archived incidents are purged from the cSupport_Archive database:** A numeric input field containing '1' and a dropdown menu set to 'Years'.

Archive Enabled - Select Yes to enable the Archive Agent to move eligible items from the production database to the applicable archive database. Items with one of the specified Closed statuses and a closed date that is past the specified number of days/years will be selected.

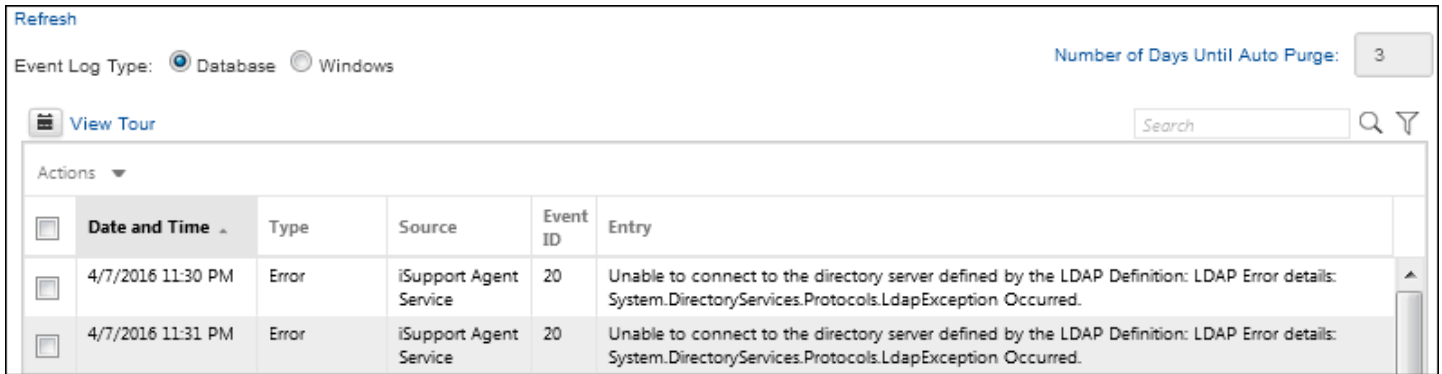
Elapsed amount of time before a closed <work item type> or sent correspondence (not associated with an open incident) is moved from the production database to the cSupport_<work item type>_Archive database - Enter the number of days to pass after the close date until an item with one of the specified Closed statuses is selected to be moved.

Statuses to Archive - Select one or more of the defined Closed statuses that will determine the items eligible for archiving.

Purge Enabled/Elapsed amount of time before archived <work item type> are purged from the <applicable archive database> - Select Yes to permanently delete items from the applicable archive database after the specified number of days/years past the archive date. In the **Elapsed amount of time before archived <work item type> are purged from the <applicable archive database>** field, enter the number of days/years past the archive date in which to remove items from the applicable archive database.

Viewing the Event Log

Use the Event Log screen to view Event Log entries that reflect application errors and messages and the date and time that iSupport agents run. You can also use the Event Log Desktop view or build a custom view using the Config - Event Log data source in the View Designer.



Informational messages and warnings from iSupport services, the Desktop, and mySupport portal are logged by default to a database table. You can specify logging to occur in the Windows Event Log instead by changing variables in the LoggingManagement section in the web.config file; see ["Specifying Logging Locations" on page 20](#) for more information.


Use the **Event Log Type** field to display entries in the database table or entries in the Windows Event Log. You can use the **Number of Days Until Auto Purge** field to specify a number of days after which entries will be deleted automatically by the Database Maintenance agent.

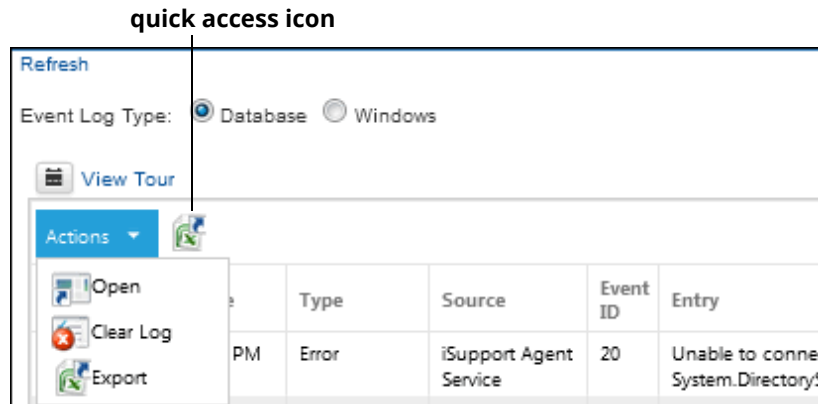
In the event the database logging provider fails to write an event to the database, the event and an additional event for the failure will be written to the iSupport Windows Event Log. If that fails, it will write to the Windows Application Log.

Database Logging Options


The Database option enables you to perform a search; use the **Search** field to perform a literal (but not case-sensitive) search for a character string within all data displayed in the current view. To perform a simple search, place the cursor in the Search field, enter the character string, and click the Quick Search icon. You can search for an incident number in an incident view, even if it doesn't exist in a displayed column.

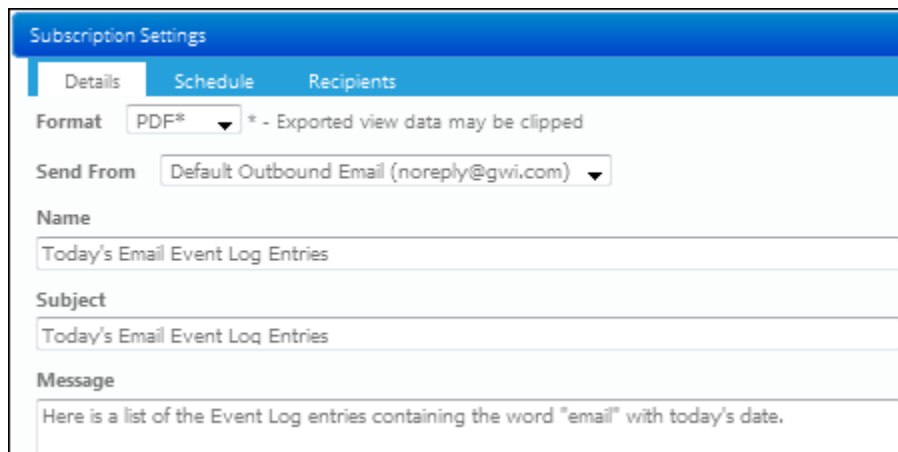
Click the **Advanced Search** icon to set criteria for filtering data in a chart. Use the Match *<All/Any>* field to specify whether you want **every** *<field> <comparison method> <value>* search condition to be met, or **any** configured condition to be met. Use the Add Condition and Remove Condition icons to display and remove a *<field> <comparison method> <value>* search condition. Click the Add Condition icon if you wish to include another condition. You can use the Add Condition Group icon to put a set of search conditions to be evaluated together in a group. Click the Save button to enter a name for the search and save it. The Saved Searches icon will display; hover over it to display saved searches.

Use the **Action dropdown menu** to open and export records and clear the event log. Use the Add to Quick Access Toolbar  icon to add icons to the top of a view. You can drag icons to change the order. The view action will remain on the Actions menu with a pin icon for removal from the quick access toolbar.



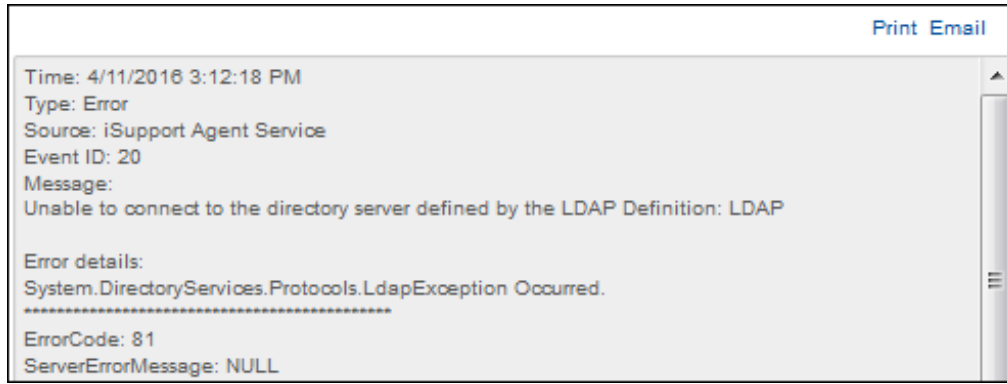
You can **export view data** in Microsoft® Excel (*.xls) format, Microsoft® Word (*.doc) format, Portable Document Format (*.pdf), or Comma Separated Value Format (*.csv). Comma Separated Value Format is usable with Microsoft Excel and other third party tools. Use the Export option on the Actions menu to export the data represented in the right frame; you'll be able to export all records at once, the current page, or a range of pages, all based on your current view, search, and sorting criteria.

Use the **Subscription**  icon 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, which runs on a five minute interval. You can utilize a saved search filter of the view.



On the Details tab in the Subscription Settings dialog, specify the name and format of the exported data, as well as the subject and body of the email to be sent. To apply a filter to the view before the export, select a saved search in the Applied Search field. On the Schedule tab, specify the days and times at which the export email should be sent. Use the Recipients tab to specify support representative(s) and others to receive the email. All of your configured view subscriptions are listed on the View Subscriptions tab in the Preferences screen, along with links for sending and deleting.

If you click on the date/time link of an entry, the entry will appear in a window for viewing, printing, or sending in an email.



Click the Email link to send the entry in an email. Change the To address, From address, or subject line in the Email Information dialog if applicable. Once you click OK, the email is sent.

The **Source** in the Event Log screen indicates the module in which the entry originated; entries include End User, Survey, Desktop, or iSupport Agent Service (which handles all of the iSupport agents).

The **Event ID** indicates the agent causing the error or informational message. Event IDs and corresponding agents are listed below:

Event ID	Agent	Agent Description
0	Configuration Agent	Updates Mobile Desktop and configuration settings from the iSupport database.
1	AD Synchronization Agent	Updates the records in iSupport Customer Profiles with the information in Active Directory®.
2	Archive Agent	Moves closed incidents and sent correspondence documents that meet archive criteria to an archive data set.
3	Auto Asset Create from Inventory Scan Agent	Creates asset records for each machine involved in an inventory scan that does not have an association with an asset record.
4	Asset Reminder Agent	Searches for warranty and maintenance expiration dates; if it is the specified number of days before the warranty or maintenance expiration date, sends an email reminder to the individuals specified in the Asset Configuration screen.
5	Asset Inventory Scan Agent	Checks inventory scan definitions and initiates scans according to schedule.
6	Domino Synchronization Agent	Performs a scheduled one-way synchronization between a specified IBM Lotus®/Domino™ Directory (previously termed "NAB") and the iSupport customer table.
7	Email Processing Agent	<ul style="list-style-type: none"> • Creates or updates an incident for each message. • Processes defined rules. • Creates a customer profile for each new customer.

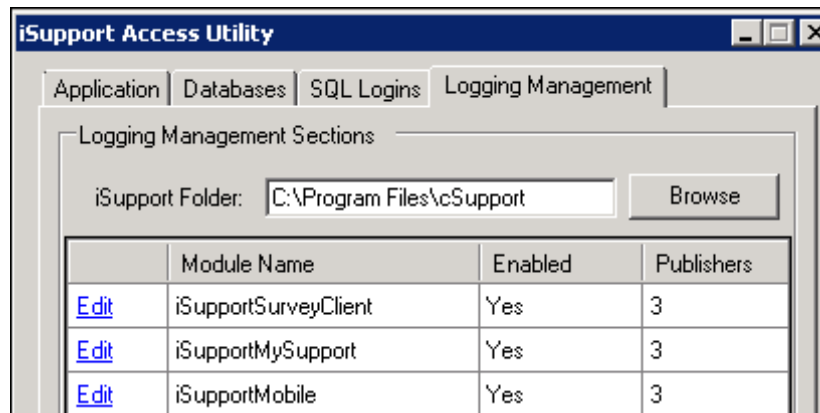
Event ID	Agent	Agent Description
8	Followup Reminder Agent	Checks all incident followup dates; sends email reminders to the incident assignees for all incidents with an expired followup date and a status other than Closed.
9	Database Maintenance Agent	Maintains data resulting from incomplete saves, deleted records, etc.
10	Memory Management Agent	Runs once every 24 hours; cleans up unused memory that is allocated but not properly reclaimed by the OS. This is/was due to a memory leak in the early 1.1x framework for service based applications.
11	Microsoft® CRM Synchronization Agent	Updates the records in iSupport Customer Profiles with the information in Microsoft® CRM.
12	Notification Agent	Sends problem and purchasing notifications.
13	Remote Database Synchronization Agent	Performs a scheduled one-way synchronization between a specified Microsoft SQL Server database and the iSupport Customers table.
14	SLA Agent	Searches open incidents, escalates those that have passed escalation time limits, and sends SLA-related notifications.
15	Statistics Agent	Runs every 5 minutes; updates open incident statistics.
16	Ticket Scheduling Agent	Checks all scheduled tickets for start dates/times and, if the specified date/time is reached, changes the status from Scheduled to an open status. Ticket generation times are also checked and tickets are created if the specified time is reached.
17	Approval Workflow Agent	Hosts the Approval Workflow Engine for incident and change approval functionality.
18	Asset Import Agent	Performs a scheduled one-way synchronization between a specified Microsoft SQL Server database and the iSupport Assets table.
19	License Management Agent	Checks all existing inventory scans and searches for the software titles specified in Software License Profile records. It compares the actual quantities found against the condition specified in the profiles, flags the profiles that do not meet the condition, and updates the profiles with the actual counts. Notifications are sent if configured.
20	LdapSyncAgent	Updates the records in iSupport Customer Profiles with the information in an LDAP source.
21	Alert Agent	Evaluates alerts and activates them as necessary. Alerts are configured to send an email or page, and/or appear at the top of the Desktop tabs, when a view field reaches a certain threshold.
22	Service Contract Agent	Evaluates service contracts and sets them to expired if necessary.
23	Configuration Item Reminder Agent	Sends notifications to specified individuals, based on the specified number of days prior to the warranty or maintenance expiration date.
24	Configuration Item Auto Create Agent	Creates a Configuration Item record for each asset, customer, company, and/or support representative that is not already associated with a configuration item.
25	Configuration Item Import Agent	Performs a scheduled one-way synchronization between a specified Microsoft SQL Server database and the iSupport CMDB table.
26	Change Scheduling Agent	Searches all scheduled changes and changes the status from scheduled to an open status.
27	Configuration Item Group Sync Agent	This agent synchronizes relationships for Configuration Item records that are associated with a customer group or support representative group.

Event ID	Agent	Agent Description
100	Service Events	Occurs when the agent manager service starts.

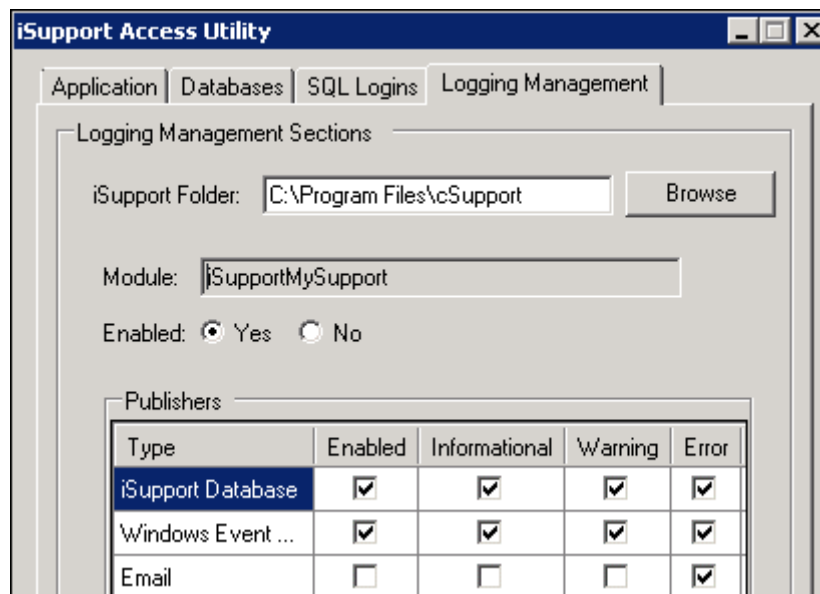
Specifying Logging Locations

Informational messages, errors, and warnings from iSupport services and the Desktop and mySupport databases are logged by default to a database table instead of the Windows Event Log. The LoggingManagement section in the web.config file contains logging settings for the iSupportDesktop module statement, which logs messages for functionality such as sending correspondence, and for the iSupportService module statement, which logs messages for agent-controlled functionality such as notifications, asset inventory scans, archiving, and data source integration.

You can use the Access Utility to change variables to enable or disable logging to the SQL database on which iSupport is installed and the Windows Event Viewer, and specify the types of messages that are logged. The iSupport Access Utility is located in the <directory in which iSupport is installed>\Utilities folder; on the Logging Management tab, click the Edit link next to the module in which you would like to configure logging.



In the Publishers section, use the checkboxes to enable or disable the type of logging. Click Save and OK when finished.



See the next section for information on configuring an email to be sent when informational messages, errors, and/or warnings from the iSupport services and Desktop and mySupport portal are logged (a new entry has been generated). If you wish to send view contents in an email on a scheduled basis regardless of any entries in the view, configure a view subscription for an Event Log view in the Desktop View component.

Note: In the event the database logging provider fails to write an event to the database, an entry for the event and an additional entry for the failure event will be written to the iSupport Windows Event Log. If that fails, it will write to the Windows Application Log.

It's important to check the size of the Microsoft Windows Event Viewer and increase it if necessary. If an error appears on the server indicating that the event log is full, go to the Microsoft Windows Event Viewer, right-click on cSupport, and select Properties. In the cSupport Properties dialog, make adjustments in the fields in the Log Size section and specify the action to take when the maximum log size is reached.

Setting Up Log Entry Notifications

You can configure an email to be sent when informational messages, errors, and/or warnings from the iSupport services, Desktop, and mySupport portal are logged. (For example, you could enable an email to be sent whenever an error occurs during an asset inventory scan.) The message will be included in the body of the email.

To configure the email to be sent, you'll need to enable the event via the Access Utility and change variables in the LoggingManagement section in the web.config file in the directories in which the Desktop and mySupport functionality are installed (Rep and User by default).

Replace the variables in bold below:

```
emailToAddress="example@example.com"
```

```
emailSubject="Desktop/iSupport Service" (Note that a different variable may be included depending on the web.config you are editing.)
```

```
emailPriority="High" />
```

- The emailSubject, includeServerNameInSubject, and includeFirstLineInSubject variables affect the subject line of the email. By default all are enabled, separated by colons - the server is listed first, then the emailSubject variable, and then the first line of the log entry. An example is shown below:
LBL-00: Desktop: System.Web.UI.ViewStateException Occurred
 - Change the **emailSubject="Desktop/iSupport Service"** variable if you wish to enter custom text for the subject line.
 - Change the **includeServerNameInSubject="true"** variable to "false" if you wish to omit the server name from the subject line of the email.
 - Change the **includeFirstLineInSubject="true"** variable to "false" if you wish to omit the first line of the log entry from the subject line of the email.
- Enter applicable email addresses for the **emailToAddress** variable. You can include multiple email addresses; separate each with a comma.
- Change **emailPriority="High"** to reflect the priority at which the email should be sent.
- If you wish to send the email through a different email provider than what is specified in your default outbound mail settings, add a publisher element to the logging management section of the web.config file in the Desktop or mySupport directory (Rep by default):
<module name="iSupportDesktop" mode="on">

For rep desktop logging, add the following and replace the variables in bold:

```
<publisher mode="on" assembly="GWCommon" type="Gwi.LoggingManagement.SmtpEmailPublisher"
smtpServer="mailserver" emailFromAddress="fromAddress" emailToAddress="toAddress"
emailSubject="iSupport Desktop" includeServerNameInSubject="true" includeFirstLineInSubject="true"
supportedLogLevels="*" emailPriority="high" />
</module>
<module name="iSupportService" mode="on">
```

For iSupport Agent logging, add the following and replace the variables in bold:

```
<publisher mode="on" assembly="GWCommon" type="Gwi.LoggingManagement.SmtpEmailPublisher"
smtpServer="mailserver" emailFromAddress="fromAddress" emailToAddress="toAddress"
emailSubject="iSupport Desktop" includeServerNameInSubject="true" includeFirstLineInSubject="true"
supportedLogLevels="*" emailPriority="high" />
</module>
```

</loggingManagement>

Troubleshooting

If entries are not included in the log or email is not sent, exception messages (including the original message) are written to the Application log in the Microsoft® Windows Event Viewer. On the server, check the Microsoft Windows Event Viewer by selecting Start | Programs | Administrative Tools | Event Viewer | Application.

Configuration Audit Tracking

Use the Options and Tools | Administer | Configuration Audit Tracking screen to display audit history entries for configuration updates. Entries will appear as shown in the example below. You can use the Number of Days Until Auto Purge field to specify a number of days after which messages will be deleted automatically by the Database Maintenance agent.

Created Date ▼	Modified By	Module	Named Item	Message
4/11/2016 1:55:09 PM	Barry White	Rules	Emergency Priority	- Added to Rule Groups: Printer Maintenance.
4/11/2016 1:55:09 PM	Barry White	Rule Groups	Printer Maintenance	- Added to Time-Based Rules: Emergency Priority.
4/11/2016 1:24:09 PM	Barry White	Rule Groups	Printer Maintenance	- Added to Time-Based Rules: Suspended Change Notification.
4/11/2016 1:24:09 PM	Barry White	Rules	Suspended Change Notification	- Added to Rule Groups: Printer Maintenance.

Use the Filter by Modules dropdown to select the modules and features for which entries should appear.

Refresh

Filter by Modules ▼

Number of Days Until Auto Purge: 90

- Select All
 - Administration Tools
 - Agents
 - Configuration Audit History Purge Settings
 - Event Log Purge Settings
 - Authentication Applications
 - Asset Management

Enabling iSupport Updates

Use the iSupport Update screen to enable an automatic search for iSupport hotfix updates and automatic installation of available updates.

iSupport Update Agent

This agent performs a scheduled check for iSupport updates. When Automatic Update Installation is not enabled and an update is available, maintenance administrators will be notified via email and a Desktop dialog. An internet connection is required for this agent; use the Check Now button to test your connection. When updates are installed, iSupport will be unavailable for several minutes. Any active iSupport sessions will be dropped when the update begins.

Enabled Yes No

Time Agent Should Run Each Day

Automatic Update Installation Enabled Yes No

New iSupport Update Available

Current Version: xxxxx

New Version: xxxxx

Install Scheduled For:

Update in Progress Page

Page Title:

Page Content

abc [Rich Text Editor Icons] Segoe UI 2 Heading 3 A

The iSupport website is undergoing routine maintenance. We apologize for any inconvenience.

The iSupport Update Agent performs a daily check for iSupport hotfix updates; select Yes in the **Enabled** field and then select the time at which the agent should run each day to perform the check. You can click the **Check Now** button to perform the check immediately.

In the **Automatic Update Installation Enabled** field, select Yes to automatically install any update as soon as it becomes available. If you select No in this field, the **Schedule Install For** field will appear for you to specify the date and time at which installation should occur. Note that if automatic update installation is not enabled, a dialog will appear on the Desktop to those designated as maintenance administrators in their support representative profile.

Use the **Page Title** and **Page Content** fields to configure the page that will appear when someone tries to access iSupport while the update is occurring.

Chart/View Audit Tracking

Use the Options and Tools | Administer | Chart/View Audit Tracking screen to display audit history entries for chart and view updates. Entries will appear as shown in the example below. You can use the Number of Days Until Auto Purge field to specify a number of days after which entries will be deleted automatically by the Database Maintenance agent.

Desktop / Configuration / Options and Tools / Administer / Chart/View Audit Tracking		
Refresh		Number of Days Until Auto Purge: 30
Created Date ▾	Modified By	Entry
4/20/2016 4:31:39 PM	Barry White	Action: view modified Name: This Week's Priority Open Incidents Shared: True
4/20/2016 4:28:16 PM	Barry White	Action: view modified Name: This Week's Priority Open Incidents Shared: True

Generating iSupport Environment Reports

Use the Options and Tools | Administer | iSupport Environment feature to compile a printable summary of configuration settings and information on the server on which the report is run. Click the Create link and complete the following fields and then click the Create button.

Report Title	April Configuration Report
Report Comments	This report documents current configuration settings.

Report Title - Enter a title to be included in the Report Title field in the Report Information section at the top of the report.

Report Comments - Enter text to be included in the Comments field in the Report Information section at the top of the report.

You'll be able to print or email the report after it is generated.

Discussion Post Management

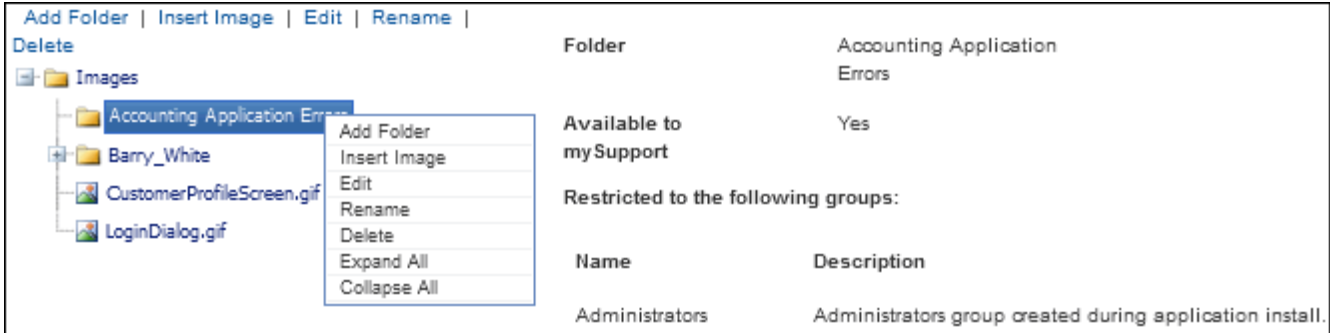
Use the Options and Tools | Administer | Discussion Post Management screen to view, remove, or delete discussion post entries that have been posted via a dashboard news feed, mySupport news feed, or knowledge entry on the mySupport portal. When an entry is removed, the text "This post has been removed due to content that violates our user guidelines" (text configured via Resource Editor). Deletion will permanently remove the entry from all feeds and the Discussion Post Management screen.

<input type="checkbox"/> Created ▲	Removed	Customer	Rep	Location	Likes	Dislikes	Following	Message
<input type="checkbox"/> 1/5/2014 10:16:44 PM	No		Barry White	Hardware Support	0	0	0	Hey everyone, the printer in Accounting is down - use the Sales printer instead.
<input type="checkbox"/> 1/5/2014 10:21:36 PM	No	Steve Johnson		Hardware Support	0	0	0	I can't print using the Sales printer either.

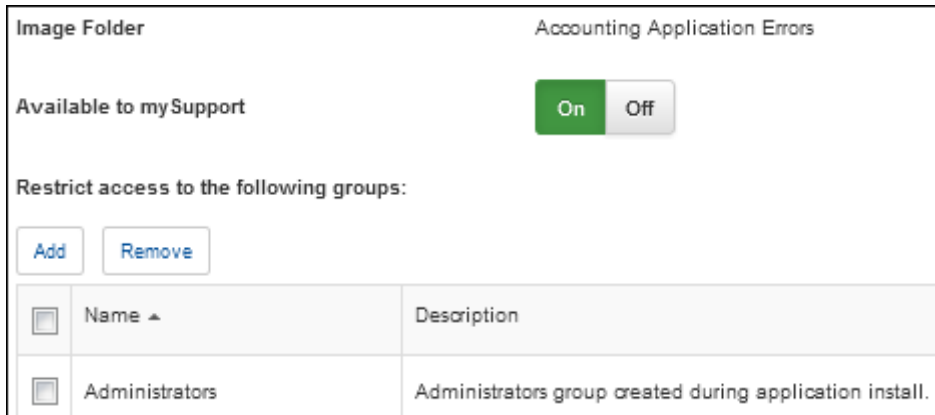
Managing Access to Images

In iSupport entry fields with a toolbar, you can use the Image Upload  icon to upload saved screenshots and other images. Images are saved in the cSupport_Image_Store database and associated with folders on which group access restrictions can be enabled.

Go to Options and Tools | Administer | Image Management to delete and restrict access to folders and images uploaded via the Image Manager.



To only enable certain support representative groups to access the Images folder and/or one or more folders below it, select the folder and click the Edit link. The following appears; click the Add link to select the group(s) that can upload to or access the files in the selected folder. Use the Available to mySupport checkbox to enable customers to view the images in that folder that are included in iSupport records such as incidents, problems, changes, knowledge entries, etc.



Viewing Rep Chat History

Go to Options and Tools | Administer | Rep Chat History to view chats between support representatives. You can use the Number of Days Until Auto Purge field to specify a number of days after which chats will be deleted automatically by the Database Maintenance agent.

Refresh		Number of Days Until Auto Purge: 90	
Created Date ▾	Initiator	Recipient	Conversation
04/11/2016 4:46:25 AM	Barry White	Jorge Quentin	Hide Conversation <ul style="list-style-type: none">• Barry White 04/11/2016 8:45:06 PM Hello Jorge, can you cover for me at lunch today?• Jorge Quentin 04/11/2016 8:45:19 PM Sure!• Barry White 04/11/2016 8:45:40 PM Thanks!
04/11/2016 4:45:18 AM	Barry White	Jorge Quentin	Show Conversation

Your iSupport license is associated with the server that runs the iSupport application, so it is very important to deactivate the license **before** making changes to server. If you do not deactivate, your license will become invalid.

After clicking this button, it will change to Activate License; after making the server changes, you can click the Activate License button to use your production license.

- Use the **Show Offline Actions** button if the server not connected to the Internet. It will enable you to enter a serial number for using a new license by or enter codes for activating or updating your license.

License Actions

To update your license, enter the update code and click the Update License button.

Update Code:

Click the Deactivate License button to deactivate your iSupport license on the server on which iSupport is installed.

Configuring Password Complexity, Expiration, and Login Locks

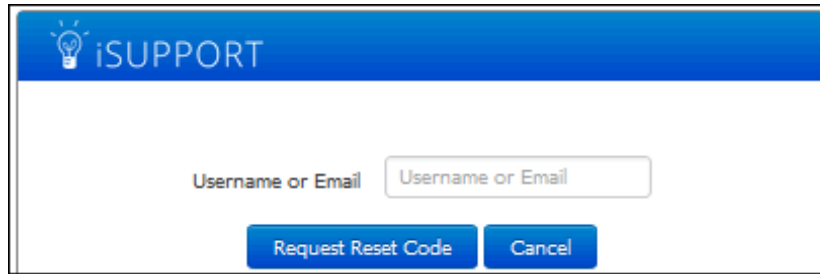
If you are not using Microsoft® Windows-based authentication with iSupport, you can use the Rep Security screen to enable password security options, enter text for the login screen, and configure locks to prevent a support representative who has exceeded a specified number of failed login attempts from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

Configuring Password Complexity and Expiration

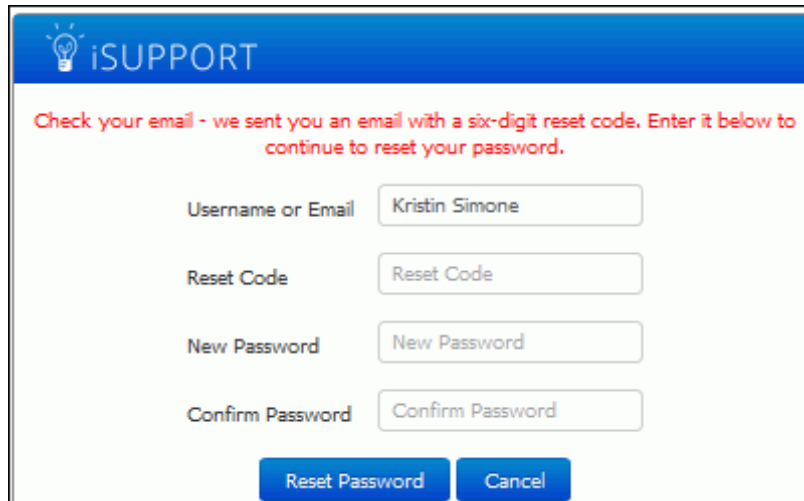
Use the Password section to enable a Forgot Password link, password expiration after a specified number of days, a previous password check with a specified number of previous passwords, and minimum password requirements. You can also force a password reset for all support representatives.

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

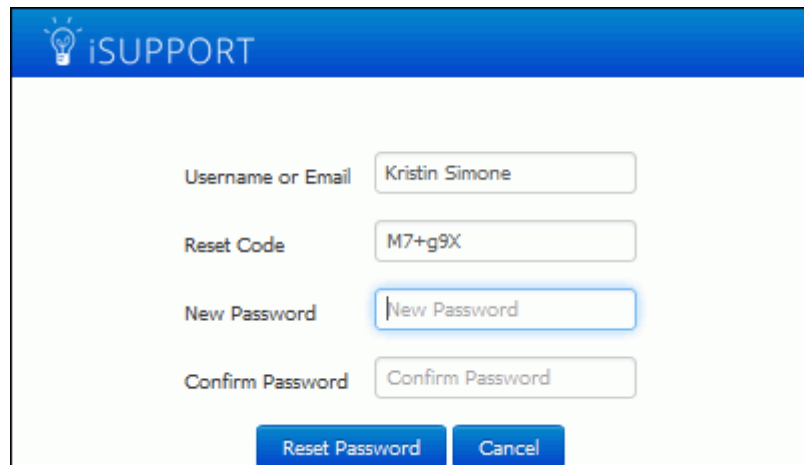
After the support representative clicks the Forgot Password link, a prompt for a username or email address will appear if the support representative hasn't entered one in the login dialog.



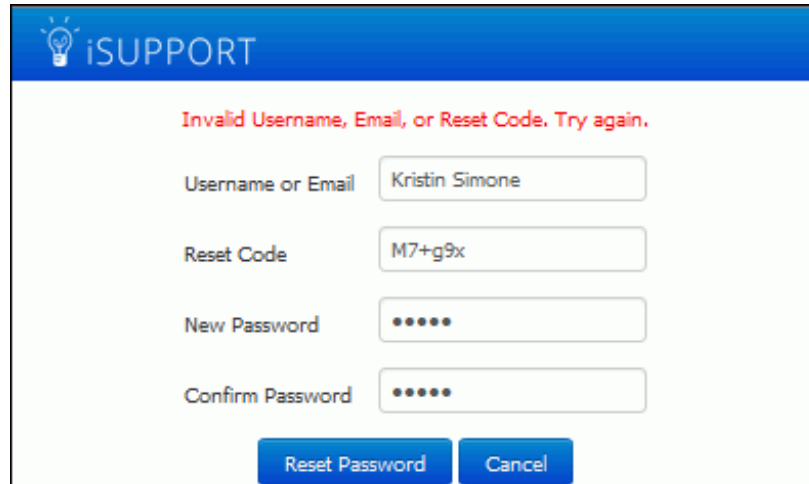
After an existing username or email address has been entered, the following dialog will appear:



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 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.

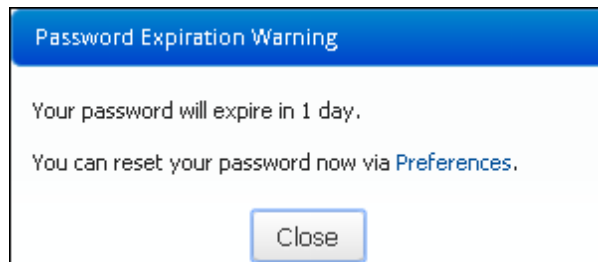
Username or Email

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

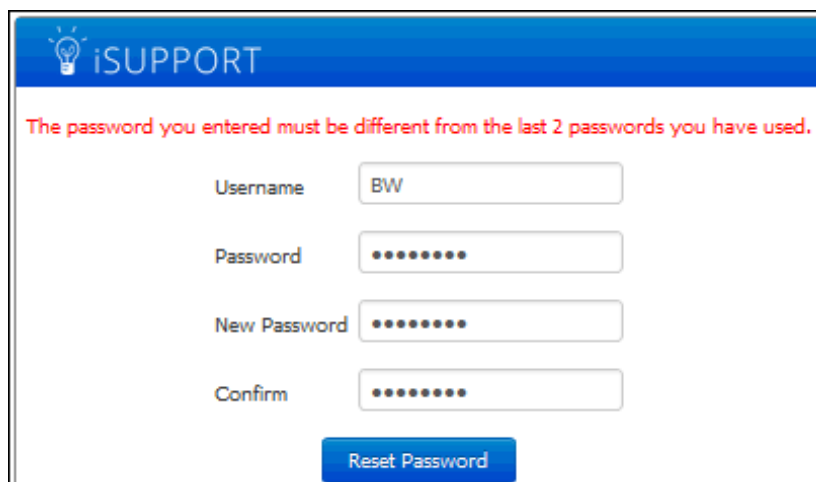
Your password will expire in 1 day.

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

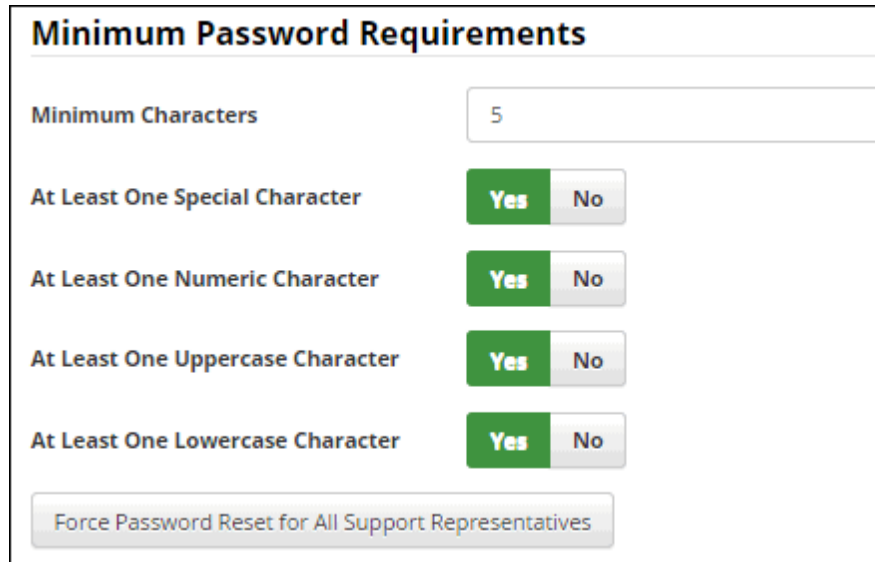
New Password

Confirm

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

Minimum Password Requirements

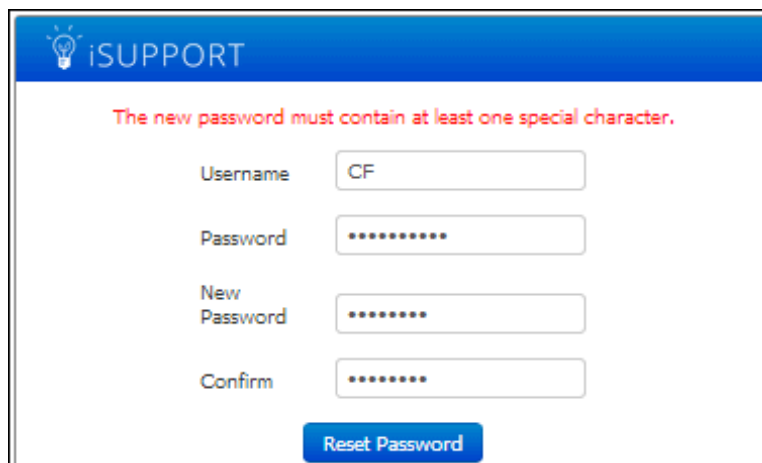
Use the fields in this section to require new passwords to contain at least one special character, numeric character, uppercase character, and lowercase character, as well as a minimum number of characters.



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 a password reset dialog box with the "iSUPPORT" logo at the top. A red error message reads: "The new password must contain at least one special character." Below the message are four input fields: "Username" (containing "CF"), "Password", "New Password", and "Confirm". A blue "Reset Password" button is located at the bottom.

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

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

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

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

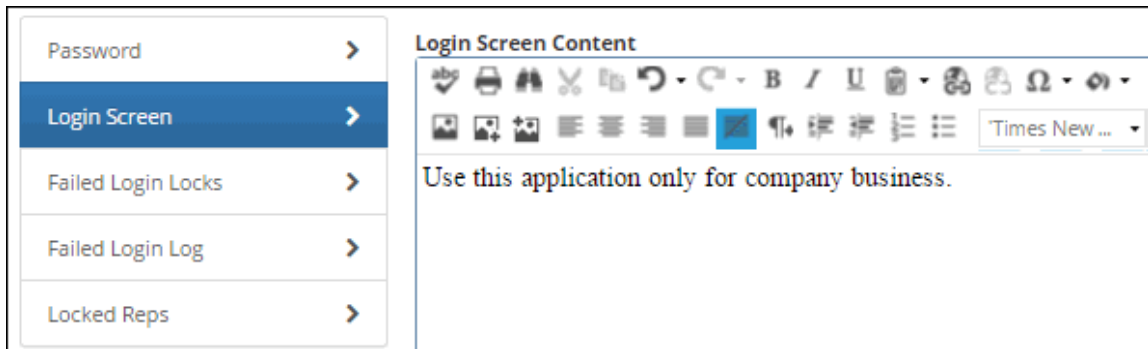
At Least One Uppercase Character - Select Yes to require a support representative's newly entered password to contain at least one capital letter.

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

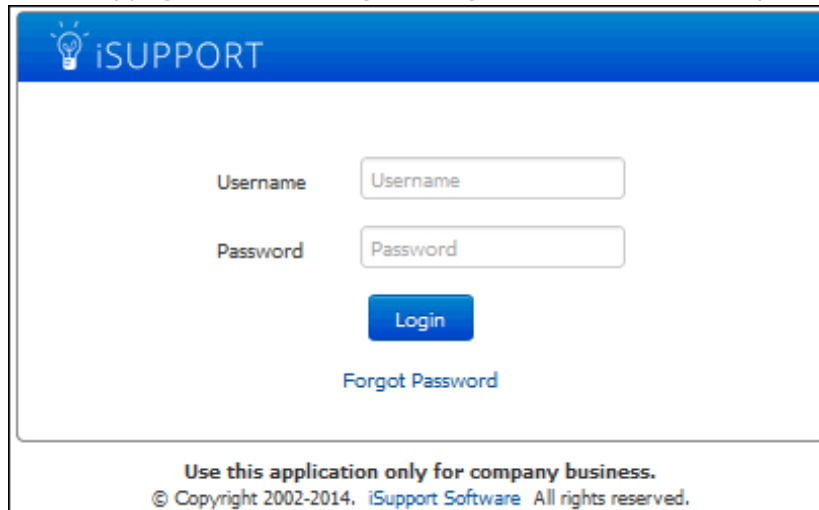
Force Password Reset for All Support Representatives - Select this button to, for each support representative, display the password reset dialog the next time the support representative logs in and require a new password to be entered.

Configuring Login Screen Text

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



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



Configuring Failed Login Locks

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

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

Failed Login Locks

The locks below enable you to prevent a support representative who has exceeded a specified number of failed login attempts from attempting another login until the conditions required to remove the active lock are met.

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

Timed Lock Enabled **Yes** No

After failed login attempts, prevent login for minute(s).

Notifications

Admins + ✎

Locked Rep + ✎

Admins to Notify

Add Admin

Connor Flynn ✕

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.

Email Lock Enabled **Yes** No

After failed login attempts, prevent login and email the support rep an unlock link.

Notifications

Admins + ✎

Locked Rep + ✎

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

Admin Lock Enabled Yes No

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

▼ Notifications

Admins + ✎

Locked Rep + ✎

Admin Lockout Content Enabled Yes No

Admin Lockout Content

Rich text editor toolbar with icons for undo, redo, bold, italic, link, unlink, list, indent, outdent, font color, background color, font size, font name, and paragraph style.

Font Name: Size: Paragraph St...: A:

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

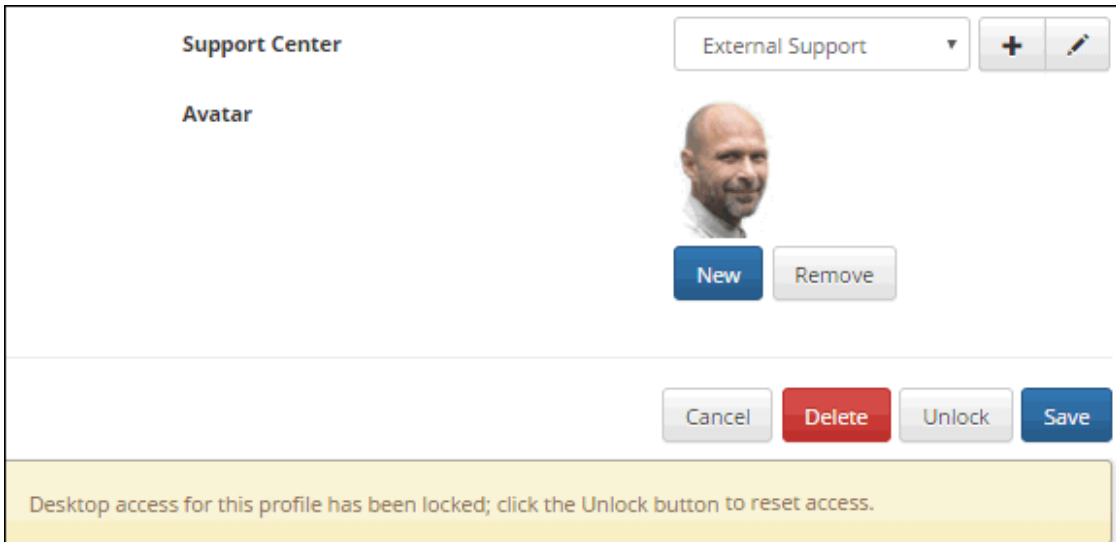
View

Locked Support Representatives ▼

Actions ▼

	Failed Login Count	Name	Login
<div style="display: flex; align-items: center;"> UNLOCK ACCESS </div>			
<div style="display: flex; align-items: center;"> EXPORT </div>			
<div style="display: flex; align-items: center;"> Timed </div>	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.



Configuring Password Complexity, Expiration, and Login Locks for Customers

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

Configuring Password Complexity and Expiration

Use the Password tab 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 customers.

The screenshot shows the 'Password' configuration screen. On the left is a navigation menu with 'Password' selected, and other options: 'Failed Login Locks', 'Failed Login Log', and 'Locked Customers'. The main area contains several settings:

- Enable Password Expiration:** A toggle switch set to 'Yes'.
- Expire Password After:** A text input field containing '60' and a 'days' label.
- Warn Customer:** A text input field containing '1' and a 'days before expiration' label.
- Enable Previous Password Check:** A toggle switch set to 'Yes'.
- Number of Previous Passwords:** A text input field containing '2'.

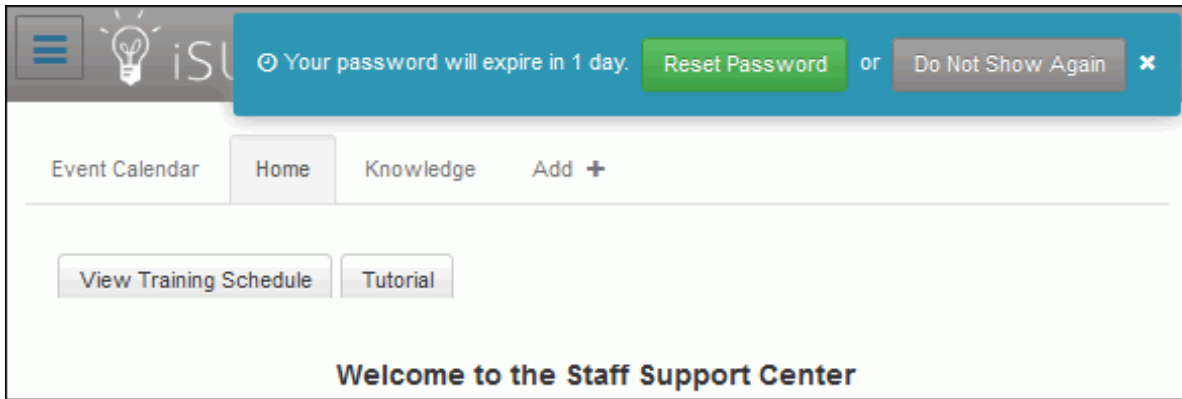
Below these settings is a section titled **Minimum Password Requirements** with the following options:

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

At the bottom of the screen is a button labeled 'Force Password Reset for All Customers'.

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 customer after every login via the mySupport portal until the configured time frame has been reached. The expiration timeframe will be based on the last time a

customer reset their password or the date and time at which the Password Expiration feature was last configured. Note that expiration warnings will not appear on the mobile client.



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 customer reset their password or the date and time at which the Password Expiration feature was last configured.

Warn Customer 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 customer's new password with a configured number of the customer's previous passwords and prevent use of a matching password.

A screenshot of a password reset form. At the top, a grey error message box states: "The password you entered must be different from the last 2 passwords you have used." Below this are four input fields: "Username" containing "Steve Johnson", "Current Password" with masked characters, "New Password", and "Re-enter Password". Each field has a small exclamation mark icon on the right side.

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

Minimum Password Requirements

Use the fields in this section to require new passwords to contain at least one special character (not a number or a letter), numeric character (0-9), uppercase character, and lowercase character, as well as a minimum number of

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

You must reset your password.

Username

Current Password

New Password The new password must contain at least one special character.

Re-enter Password

Login

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

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

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

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

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

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

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

Configuring Failed Login Locks

Use the Failed Login Locks tab to configure locks to prevent a customer 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 a support rep lock which requires an administrator to reset the login lock.

The screenshot shows the configuration interface for Failed Login Locks. On the left is a navigation menu with 'Failed Login Locks' selected. The main area contains a header explaining the purpose of the locks and a note about their order. Below this are two lock configurations:

- Timed Lock Enabled:** A toggle set to 'Yes'. The configuration is 'After 1 failed login attempts, prevent login for 2 minute(s)'. Below this is a 'Notifications' section with dropdowns for 'Support Reps' and 'Locked Customer', both set to 'iSupport Default', and '+' and edit icons.
- Email Lock Enabled:** A toggle set to 'Yes'. The configuration is 'After 4 failed login attempts, prevent login and email the customer an unlock link.' Below this is a 'Notifications' section with a right-pointing arrow.

On the right side, there is a 'Reps to Notify' section with an 'Add Rep' button and a list containing 'Stuart Copeland' with a close icon.

You can use the Failed Login Log tab to display information on customers who have unsuccessfully attempted a login, and the Locked Customers tab to display those who are locked out due to exceeding the configured number of failed login attempts.

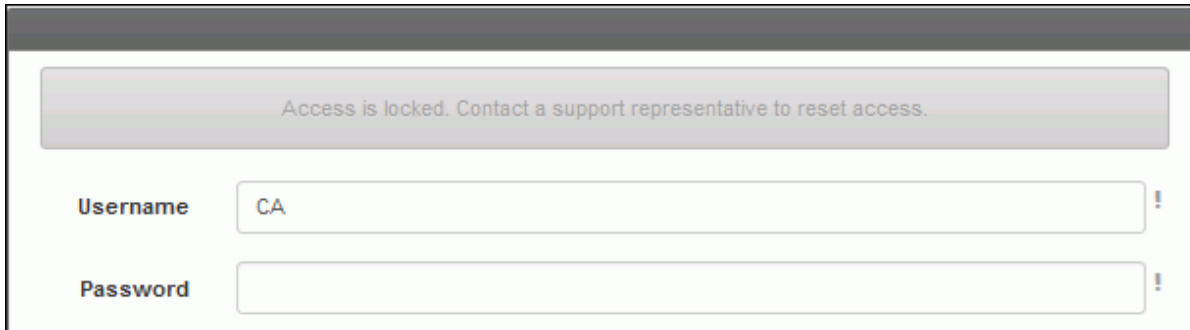
You can send notifications for each type of lock; support representatives selected in the Reps to Notify field will be notified for each notification selected for a lock. These notifications can be customized via the Custom Notifications screen. The three types of locks are ordered when used in combination; if you enable more than one, the number of login attempts must be progressively larger starting with the timed lock.

Email and Timed Locks

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

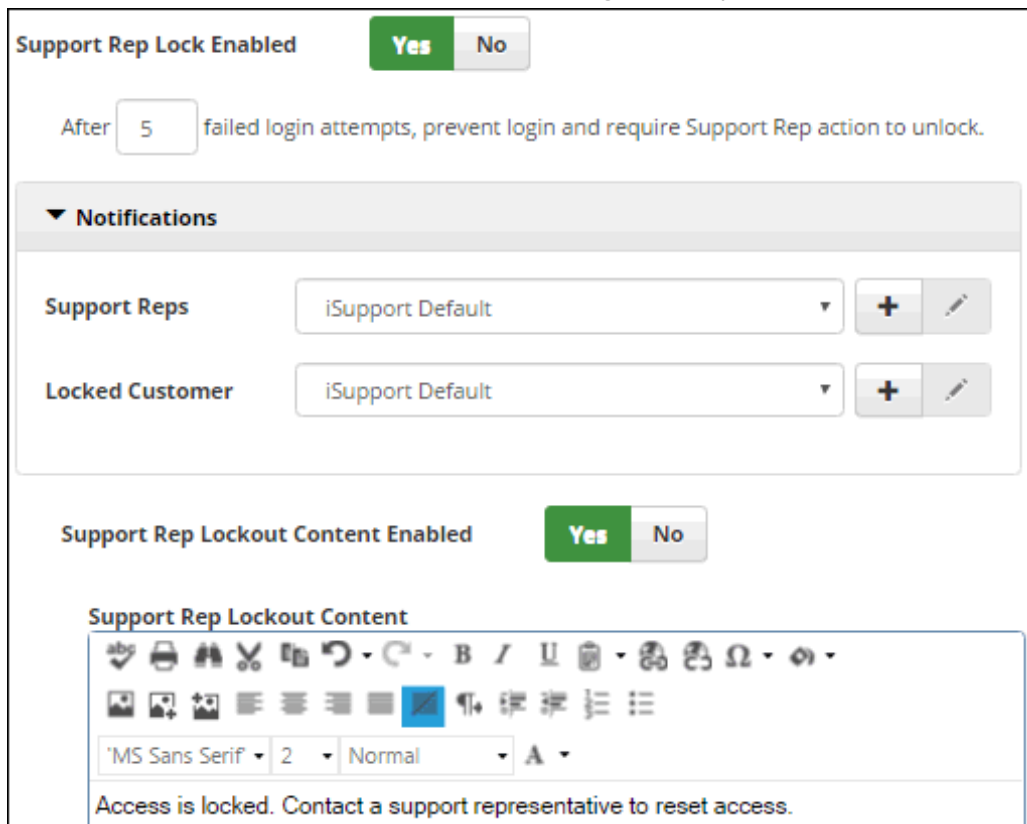
Support Rep Locks

An even more restrictive **support rep lock** prevents the customer from logging in until a support representative unlocks his/her customer profile. A configurable message will appear to the customer if the configured number of failed login attempts has been exceeded.



A screenshot of a login form. At the top, a grey banner displays the message: "Access is locked. Contact a support representative to reset access." Below the banner are two input fields: "Username" containing the text "CA" and "Password" which is empty. Both fields have a small exclamation mark icon to their right.

To configure a support rep lock, select Yes in the Support Rep Lock Enabled field, enter the number of failed login attempts, and select notifications to be sent to the support representative and customer if applicable. You can use the Support Rep Lockout Content Enabled and Support Rep Lockout Content fields to configure the content of the message to appear to the customer after the number of failed login attempts has been exceeded.

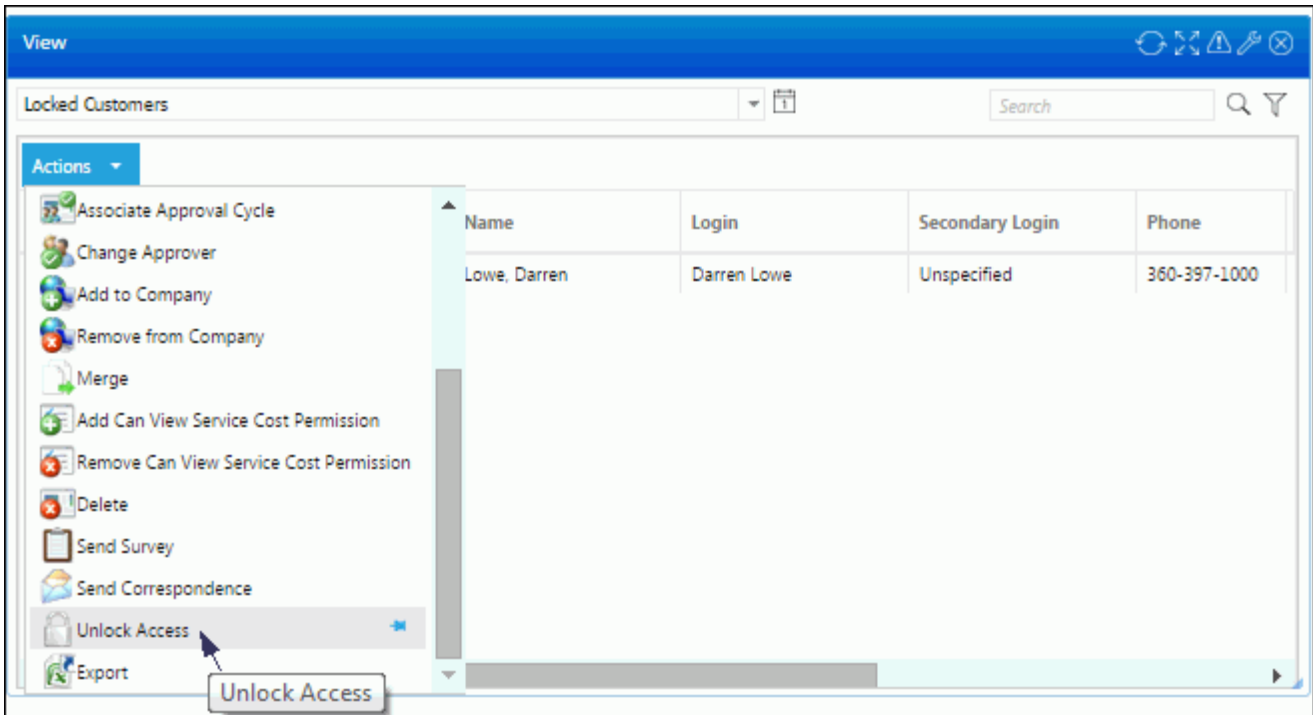


A screenshot of the configuration interface for Support Rep Locks. It features several sections:

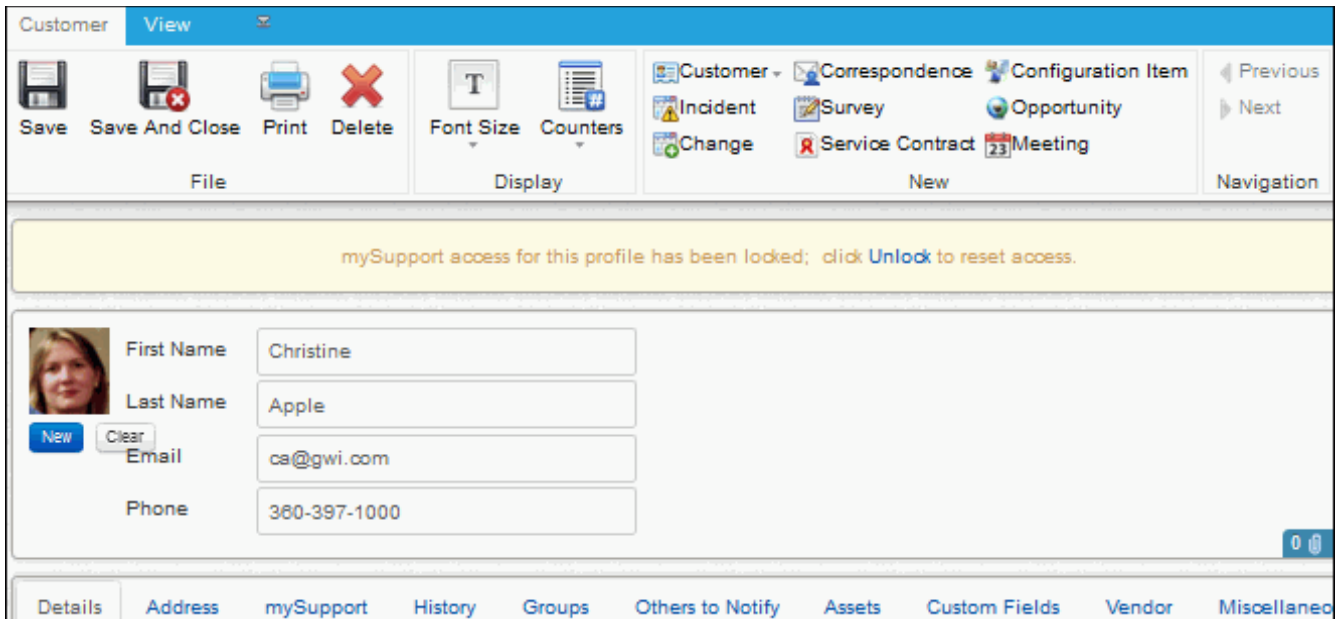
- Support Rep Lock Enabled:** A toggle switch set to "Yes".
- After:** A text input field containing the number "5", followed by the text "failed login attempts, prevent login and require Support Rep action to unlock."
- Notifications:** A section with two dropdown menus: "Support Reps" and "Locked Customer", both currently set to "iSupport Default". Each dropdown has a "+" icon and an edit icon.
- Support Rep Lockout Content Enabled:** A toggle switch set to "Yes".
- Support Rep Lockout Content:** A rich text editor with a toolbar containing icons for undo, redo, bold, italic, underline, link, unlink, list, and other text formatting options. Below the toolbar, the font is set to "MS Sans Serif", size "2", and style "Normal". The text area contains the message: "Access is locked. Contact a support representative to reset access."

Support representatives with Customers | Unlock mySupport Access permission can unlock a Customer Profile in the following ways; both will set the failed login attempt count to zero.

- Select the Unlock Access option on the Actions menu on the Locked Customers tab or Locked Customers view on the Desktop.



- Click the Unlock link that displays in the banner in the Customer Profile screen when a profile is locked.



Using the Data Override Feature for Incidents, Problems, and Changes

Use the Options and Tools | Administer | Data Override feature to overwrite fields on any saved incident, problem, or change. 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.

To access this feature, use the Override Data option on the applicable menu. It is available if the Allow Data Override field is enabled in your Rep Profile record.

The screenshot displays the 'Incident Data Override' interface. It is divided into two main sections: 'Details' and 'Assets'. The 'Details' section contains a list of customer information fields: Name (Steve Johnson), Customer ID (8675309), Location (Headquarters), Department (Administration), Company (LBLSoft, Inc.), Phone (360-397-1004), and Email (sj@example.com). To the right, there are fields for Number (D67F4A65A6), Status (Closed), and Priority (Medium), each with a dropdown arrow. Below these is a 'Categorization' section with a tree view showing 'Hardware' > 'Network' > 'Connection'. The 'Assets' tab is currently inactive. Below the details is the 'Issue' section, which has two tabs: 'Issue' (active) and 'History'. It contains three text areas: 'Short Description' (Chat Request Question : My laptop just crashed and I need to take it out), 'Description' (Customer cannot connect to the network; permissions changed due to department transfer.), and 'Resolution' (Upgraded permissions and Steve can now connect to the network.). At the bottom, there are three buttons: 'Save', 'Save and Close', and 'Go To Incident'.

Backing Up and Restoring iSupport Databases

Backing Up iSupport Databases

In order for you to update iSupport or recover data in case of loss, you'll need to back up:

- The cAsset, cSupport, cSupport_Archive, cSupport_Archive_Change, cSupport_Archive_Problem, cSupport_Archive_Purchase, cSupport_Bomgar, cSupport_Image_Store, cSupport_Workflow, and cSupportReporting databases and transaction logs in the SQL data directory for SQL Server 2008, (\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data) or the same named databases using an equivalent database backup utility.
- The Web.config file in the directories in which the Rep Desktop, mySupport portal, Mobile Desktop, and survey functionality are installed (RepClient, UserClient, MobileClient, and SurveyClient by default).
- File of words to be ignored during spell-check in <Desktop install directory>\Configuration\data\en-US-CustomDictionary.txt.
- If using RightAnswers, the <Desktop install directory>\Rightanswers\declarations.inc file.

These steps cover the cSupport database backup in SQL Server 2008; to back up the other databases, select the other database in turn.

To perform the backup operation:

- If you are using the SIMPLE Recovery Model, refer to Method A below.
- If you using the FULL Recovery Model, refer to Method B below.

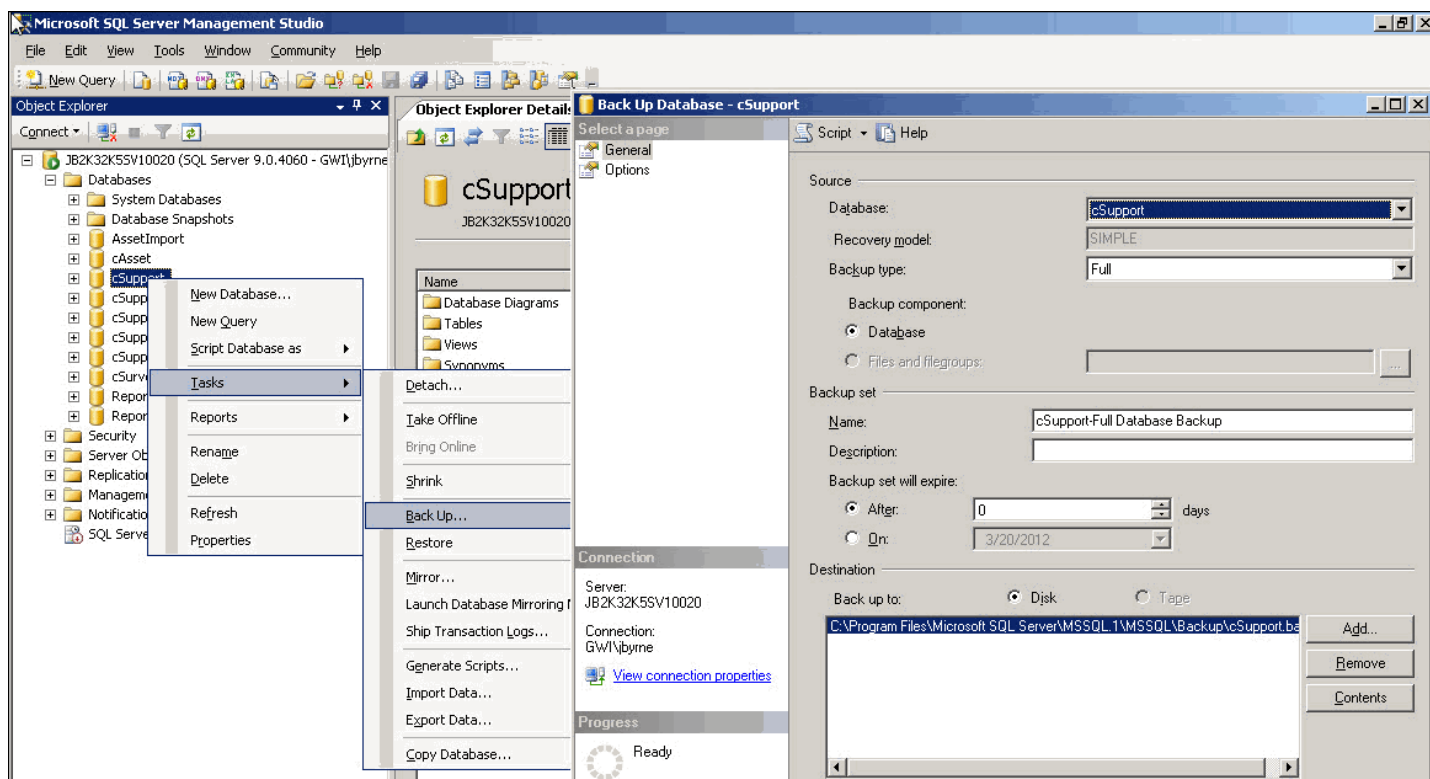
There are other methods for backing up the cSupport database which are not discussed here.

Note: For additional parameters and more information on backing up and restoring SQL Server databases, go to www.microsoft.com.

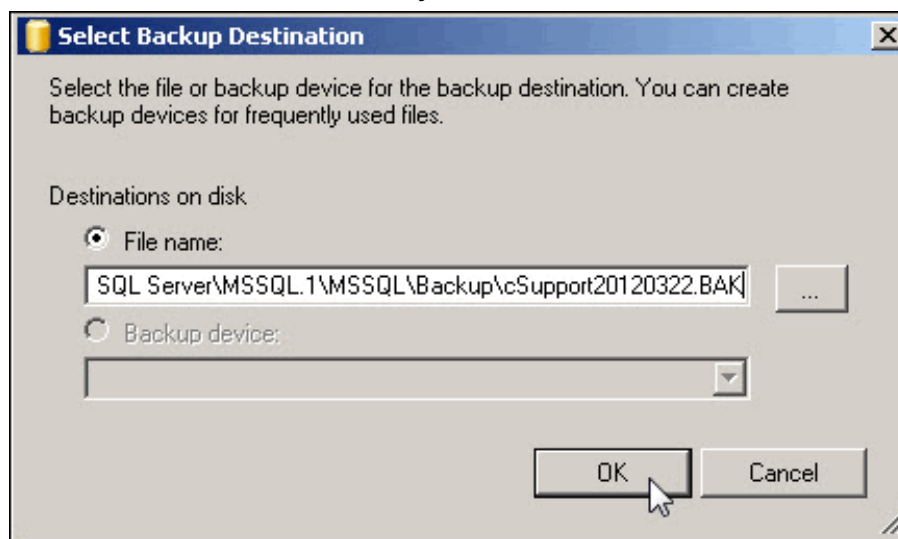
Method A - Backing Up SQL Server Databases using the SIMPLE Recovery Model

- 1** Create a folder for the backup file; for example, C:\Program Files\Microsoft SQL Server\MSSQL\Backup\cSupportBackup. Note: By default backups will be stored in the Backup folder.
- 2** Open SQL Management Studio. Expand Databases in the Object Explorer pane. Right-click on the cSupport database and select Tasks | Back Up from the shortcut menu. This will open the Back Up Database dialog box, with the cSupport database selected as the backup source.
 - Set the Backup Type to FULL.
 - Provide a name for this backup set and a description if applicable.
 - The Backup Set Will Expire option gives you the choice to set the backup to expire in a specified number of days, or on a specified date. Setting this to zero (0) days is equivalent to never expires.
 - Choose where the backup will be placed. In most cases, this type of backup will be stored on disk. If a file and location have already been set in this text area and you do not want to either append to the existing backup

set or to overwrite it, use the Remove button to eliminate this backup from this backup set. Removing the file from this list does not delete the actual backup file. Click the Add button to create a new backup file or set.



- 3 Use the Select Backup Destination dialog to specify the location for the backup and the name of the backup file. Be sure to give the file name the BAK extension. Without this extension, you will not see this file in the set of available backups to restore from later, if necessary. Click OK to save this as the new file and location.



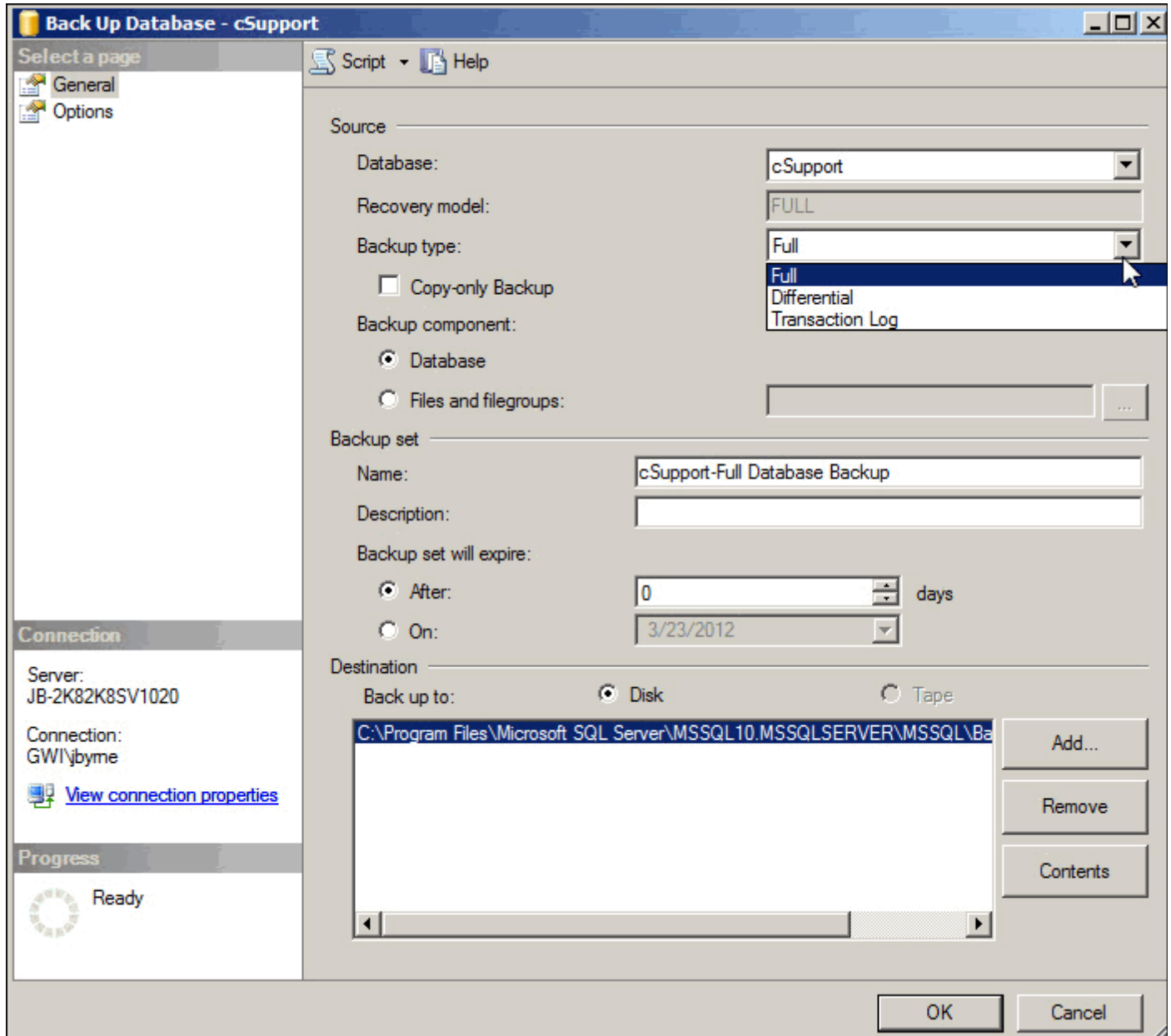
- 4 Click on Options to open this page. If you are creating a new backup set, the only additional options that you may want to select would be to Verify Backup When Finished, and Perform Checksum Before Writing to Media.
- 5 Click the OK button to start the backup. Once completed, follow these same steps for the remaining six cSupport databases.

Method B - Backing Up SQL Server Databases using the FULL Recovery Model

This method will require that you do two backups. The first will be a full backup of the cSupport database. The second will be a Transaction Log backup.

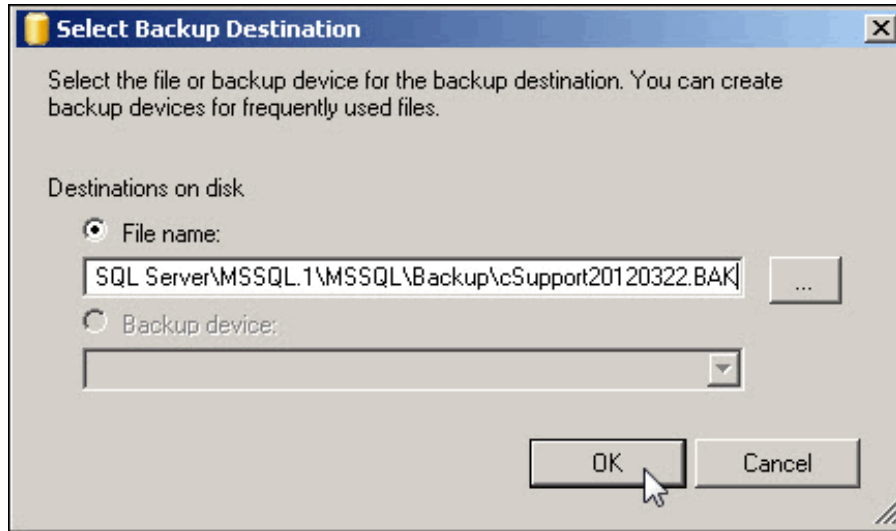
Completing a Full Database Backup

- 1 Create a folder for the backup file; for example: C:\Program Files\Microsoft SQL Server\MSSQL\Backup\cSupportBackup.
- 2 Open SQL Management Studio. Expand Databases in the Object Explorer pane. Right-click on the cSupport database, and select Tasks | Back Up from the shortcut menu. This will open the Back Up Database dialog box, with the cSupport database selected as the backup source.
 - Set the Backup Type to FULL. This drop-down list will have two additional options: Differential (not discussed here) and Transaction Log. You will do a Transaction Log backup after the FULL backup.
 - Provide a name for this backup set and description if applicable.



- The Backup Set Will Expire option gives you the choice to set the backup to expire in a specified number of days, or on a specified date. Setting this to zero (0) days is equivalent to never expires.
- Now choose where the backup will be placed. In most cases, this type of backup will be stored on disk. If a file and location have already been set in this text area and you do not want to either append to the existing backup set or to overwrite it, use the Remove button to eliminate this backup from this backup set. Removing the file from this list does not delete the actual backup file. Click the Add button to create a new backup file or set.

- 3 Use the Select Backup Destination dialog to specify the location for the backup and the name of the backup file. Be sure to give the file name the BAK extension. Without this extension, you will not see this file in the set of available backups to restore from later, if necessary. Click OK to save this as the new file and location.

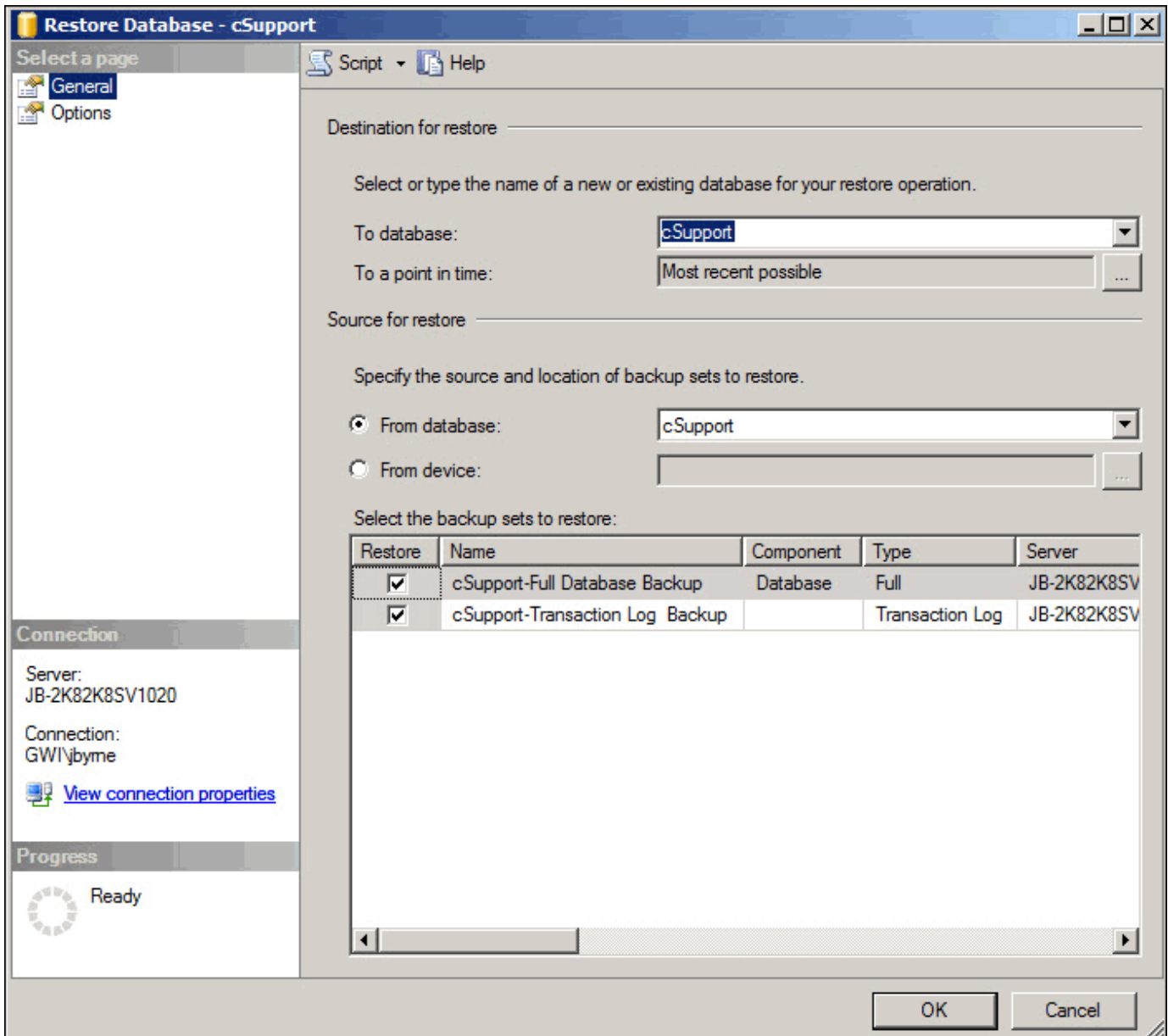


- 4 Click on Options to open this page. If you are creating a new backup set, the only additional options that you may want to select would be to Verify Backup When Finished, and Perform Checksum Before Writing to Media.
- 5 Click the OK button to start the backup. Once completed, follow these same steps for the remaining six cSupport databases.

Note: The database backup file size may be smaller than the current database file because the backup contains only the actual data in the database and not empty space.

Completing a Transaction Log Backup

Once the Full backup of the database has been completed a transaction log backup is done to force any transaction that has not been written to the database to be committed or saved. Any data contained in the transaction log can be lost if it has not been committed.



- 1 Follow steps 1 and 2 above, but select the Backup Type of Transaction Log.
- 2 As in step 3 above, you will specify the location for the new transaction log backup to be stored. When entering the necessary data in the Select Backup Destination dialog, give the filename the extension of TRN. This extension tells SQL that this is a transaction log backup.
- 3 Follow steps 4 and 5 above to finish.

Restoring cSupport Databases

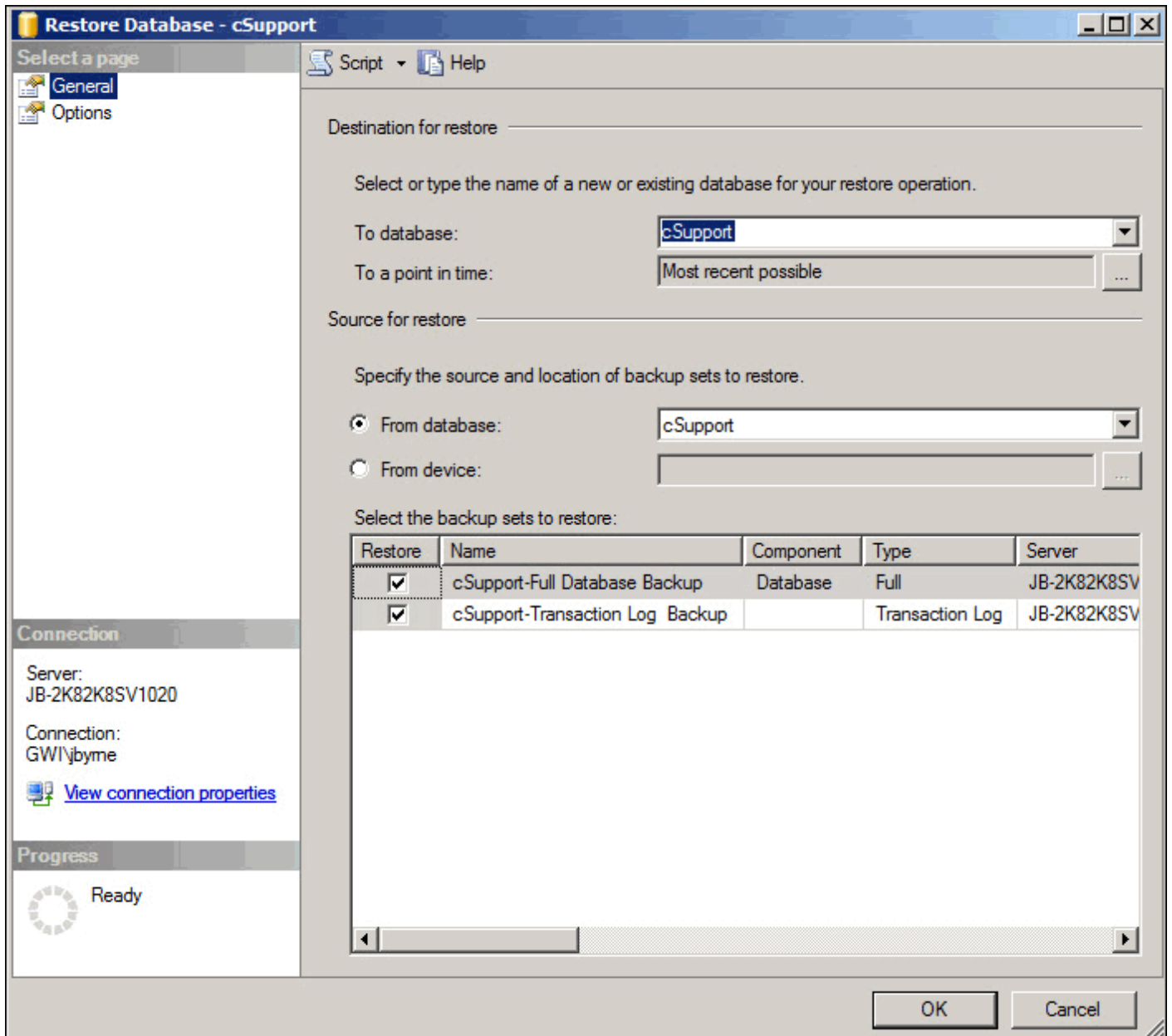
Restoring a database enables you to utilize a full backup file to recreate the cSupport database. The restored database will be a copy as it existed when the backup operation completed.

The only difference between restoring a database set with the SIMPLE Recovery model and one that is set to use the FULL Recovery model is that the FULL Recovery model requires that you restore the database backup first and then the transaction log backup. You cannot restore a FULL Recovery model database without the transaction log.

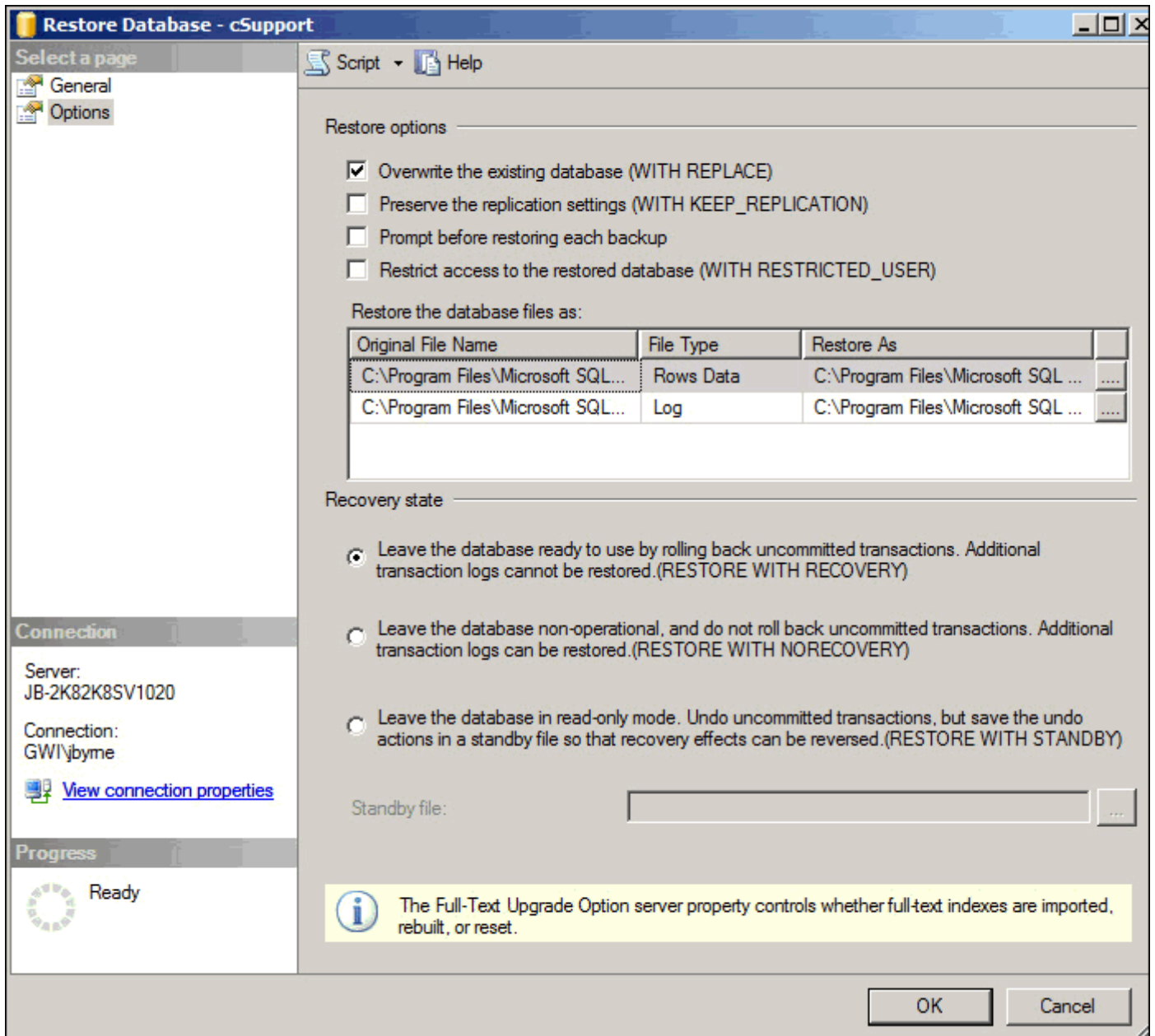
Note: All databases must be online and must have the same iSupport version number.

These steps cover the cSupport database restore; to restore the other databases, substitute the other database names in the commands. Start by opening the SQL Management Studio application.

- 1 Right-click on the database that you want to restore, and select Task | Restore | Database. This will open the Restore Database dialog.
- 2 The To Database option will show the name of the database you selected.
- 3 If you just recently performed the database backup, it should now be listed in the Select the Backup Sets to Restore list. If you do not see the backup files you need, click the From Device radio button and you will be able to browse to and select the backup file you need.



- 4 Click Options to go to the Options page.



- 5 Check the first check box labeled Overwrite the Existing Database (WITH REPLACE).
- 6 In the Restore the Database Files as option is only needed if you are also moving the database files to a new location, or if you are restoring backups from a different SQL Server.
- 7 Be sure to select the first radio button labeled Leave the Database Ready to Use by Rolling Back Uncommitted Transactions. The only reason that you would choose the second option is if you are using a different backup mode.
- 8 Click the OK button to start the restore operation. A dialog will appear if the dialog was or was not successful.

Changing iSupport's Access to SQL Databases

The iSupport Access Utility in the <directory in which iSupport is installed>\Utilities folder enables you to modify the SQL database, database server, and SQL login to the iSupport databases. The installation process initially populates these fields on the Databases tab. Use the Advanced button to specify advanced properties.

The screenshot shows the 'iSupport Access Utility' dialog box with the 'Databases' tab selected. The dialog has three tabs: 'Application', 'Databases', and 'SQL Logins'. A message at the top states: 'iSupport requires Windows Authentication for SQL server access.' Below this, there are two sections: 'iSupport Database' and 'Asset Database'. Each section contains fields for 'Database Server', 'Database', 'Authentication' (with radio buttons for 'Windows Authentication' and 'SQL Server Authentication (Versions prior to 6.0)'), 'User Name', and 'Password'. There are 'Test Connection' and 'Advanced' buttons for each section. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

iSupport Access Utility

Application Databases SQL Logins

iSupport requires Windows Authentication for SQL server access.

iSupport Database

Database Server: LBLSOFT

Database: cSupport

Authentication:

Windows Authentication SQL Server Authentication (Versions prior to 6.0)

User Name: []

Password: []

Test Connection Advanced

Asset Database

Database Server: LBLSOFT

Database: cAsset

Authentication:

Windows Authentication SQL Server Authentication (Versions prior to 6.0)

User Name: []

Password: []

Test Connection Advanced

OK Cancel Apply