Administering iSupport®

Tracking and Monitoring iSupport Usage

- See “Configuration Audit Tracking” on page 3 for information on displaying audit history entries for configuration updates in most modules.
- See “Chart/View Audit Tracking” on page 4 for information on displaying audit history entries for chart and view updates.
- See “Discussion Post Management” on page 5 for information on viewing, removing, or deleting discussion post entries.
- See “Viewing Rep Chat History” on page 6 for information on displaying chats between support representatives.

Security and Access

- See “Configuring Password Complexity, Login Security, Expiration, and Login Locks” on page 7 for configuring security options for support representatives.
- See “Configuring Password Complexity, Expiration, and Login Locks for Customers” on page 16 for information on configuring security options for customers.
- See “Managing Access to Images” on page 22 for information on deleting and restricting access to folders and images uploaded via the Image Manager.
- See “Performing Advanced Configuration Tasks via the iSupport Configuration Utility” on page 45 if you wish to use SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt all communications between your browser and an iSupport site via an HTTPS connection.

Agent and Database Functions

- Agents perform tasks in the background that are an integral part of iSupport functionality. See “Enabling and Scheduling Agents” on page 23 for more information.
- See page page 35 for information on backing up and restoring iSupport databases.
- See “Archiving and Database Maintenance” on page 42 for information on scheduling agents that maintain iSupport databases and move closed work items to archive databases.
- The iSupport Configuration Utility in the <*directory in which iSupport is installed*>\Utilities folder is used to perform advanced configuration tasks; see “Performing Advanced Configuration Tasks via the iSupport Configuration Utility” on page 45 for more information.

iSupport Licensing and Updates

- See “Managing Your iSupport License” on page 50 for information on administering the license for your iSupport application.
- See “Enabling iSupport Updates” on page 52 for information on enabling an automatic search for iSupport hotfix updates and automatic installation of available updates.

Troubleshooting

- See “Viewing the Event Log” on page 54 for information on displaying entries that reflect application errors and messages and the date and time that iSupport agents run.
- See “Generating iSupport Environment Reports” on page 60 for information on compiling a printable summary of configuration settings and information on the server on which the diagnosis is run.

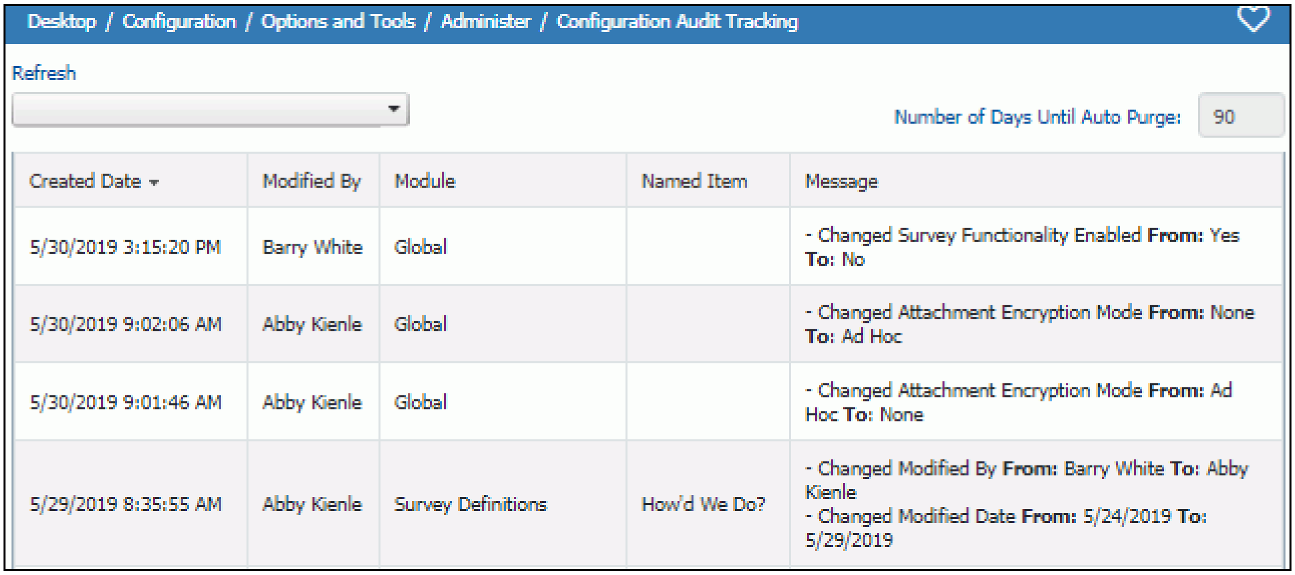
- Use the Notification Queue option under Options and Tools | Administer to display all notifications that have not been sent. You can use the checkboxes to restrict the notifications to appear in the screen, and delete any notifications that you do not wish to be sent.

Performance Best Practices and Recommendations

See page 61 for tips on increasing iSupport performance.

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.

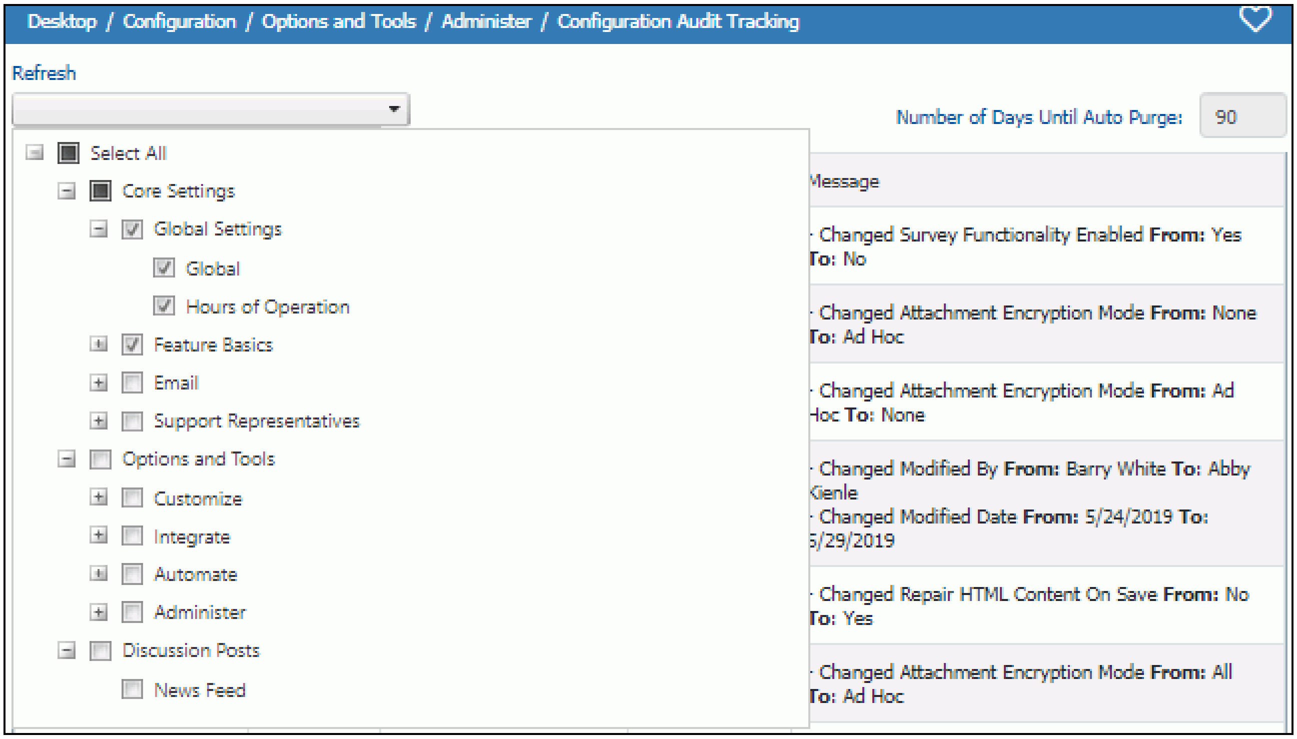


Desktop / Configuration / Options and Tools / Administer / Configuration Audit Tracking
Refresh

Number of Days Until Auto Purge: 90

Created Date ▾	Modified By	Module	Named Item	Message
5/30/2019 3:15:20 PM	Barry White	Global		- Changed Survey Functionality Enabled **From:** Yes **To:** No
5/30/2019 9:02:06 AM	Abby Kienle	Global		- Changed Attachment Encryption Mode **From:** None **To:** Ad Hoc
5/30/2019 9:01:46 AM	Abby Kienle	Global		- Changed Attachment Encryption Mode **From:** Ad Hoc **To:** None
5/29/2019 8:35:55 AM	Abby Kienle	Survey Definitions	How'd We Do?	- Changed Modified By **From:** Barry White **To:** Abby Kienle - Changed Modified Date **From:** 5/24/2019 **To:** 5/29/2019

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



Desktop / Configuration / Options and Tools / Administer / Configuration Audit Tracking
Refresh

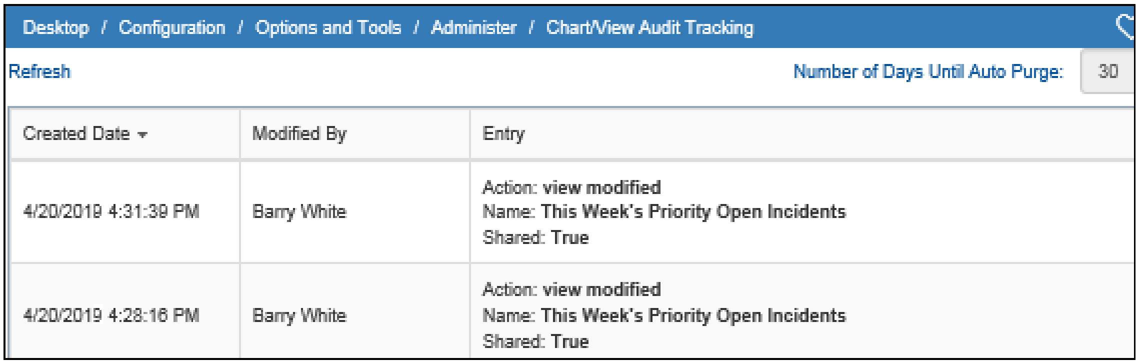
Number of Days Until Auto Purge: 90

- ■ Select All
  - ■ Core Settings
    - ☑ Global Settings
      - ☑ Global
      - ☑ Hours of Operation
    - ☑ Feature Basics
    - □ Email
    - □ Support Representatives
  - □ Options and Tools
    - □ Customize
    - □ Integrate
    - □ Automate
    - □ Administer
  - □ Discussion Posts
    - □ News Feed

Message
Changed Survey Functionality Enabled **From:** Yes **To:** No
Changed Attachment Encryption Mode **From:** None **To:** Ad Hoc
Changed Attachment Encryption Mode **From:** Ad Hoc **To:** None
Changed Modified By **From:** Barry White **To:** Abby Kienle Changed Modified Date **From:** 5/24/2019 **To:** 5/29/2019
Changed Repair HTML Content On Save **From:** No **To:** Yes
Changed Attachment Encryption Mode **From:** All **To:** Ad Hoc

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.

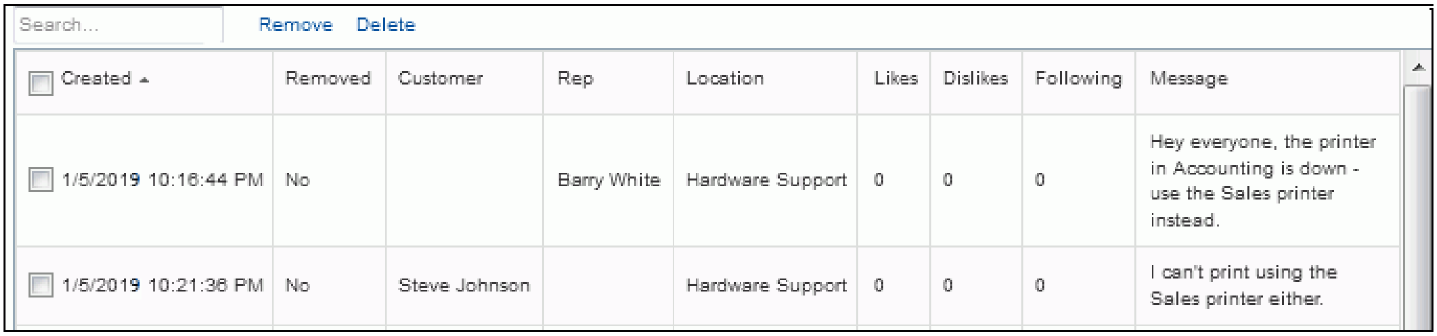

Desktop / Configuration / Options and Tools / Administer / Chart/View Audit Tracking
Refresh

Number of Days Until Auto Purge: 30

Created Date ▾	Modified By	Entry
4/20/2019 4:31:39 PM	Barry White	Action: view modified Name: This Week's Priority Open Incidents Shared: True
4/20/2019 4:28:16 PM	Barry White	Action: view modified Name: This Week's Priority Open Incidents Shared: True

Discussion Post Management

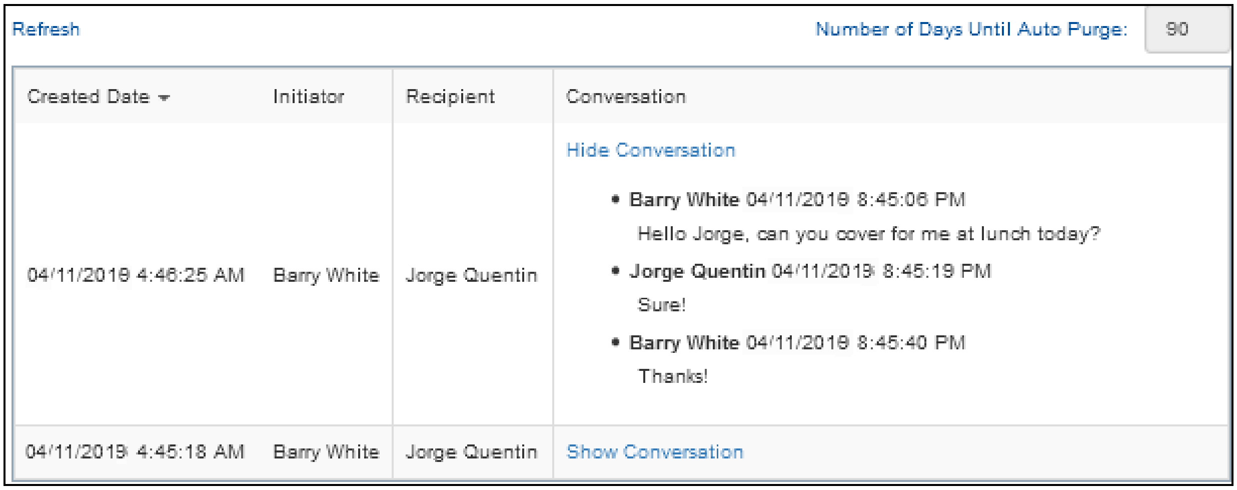
Use the Options and Tools | Administer | Discussion Post Management screen to view, remove, or delete discussion post entries that have been posted via a dashboard news feed, mySupport news feed, or knowledge entry on the mySupport portal. When an entry is removed, the text "This post has been removed 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.



□ Created ▲	Removed	Customer	Rep	Location	Likes	Dislikes	Following	Message
□ 1/5/2019 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.
□ 1/5/2019 10:21:36 PM	No	Steve Johnson		Hardware Support	0	0	0	I can't print using the Sales printer either.

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.



Number of Days Until Auto Purge: 90

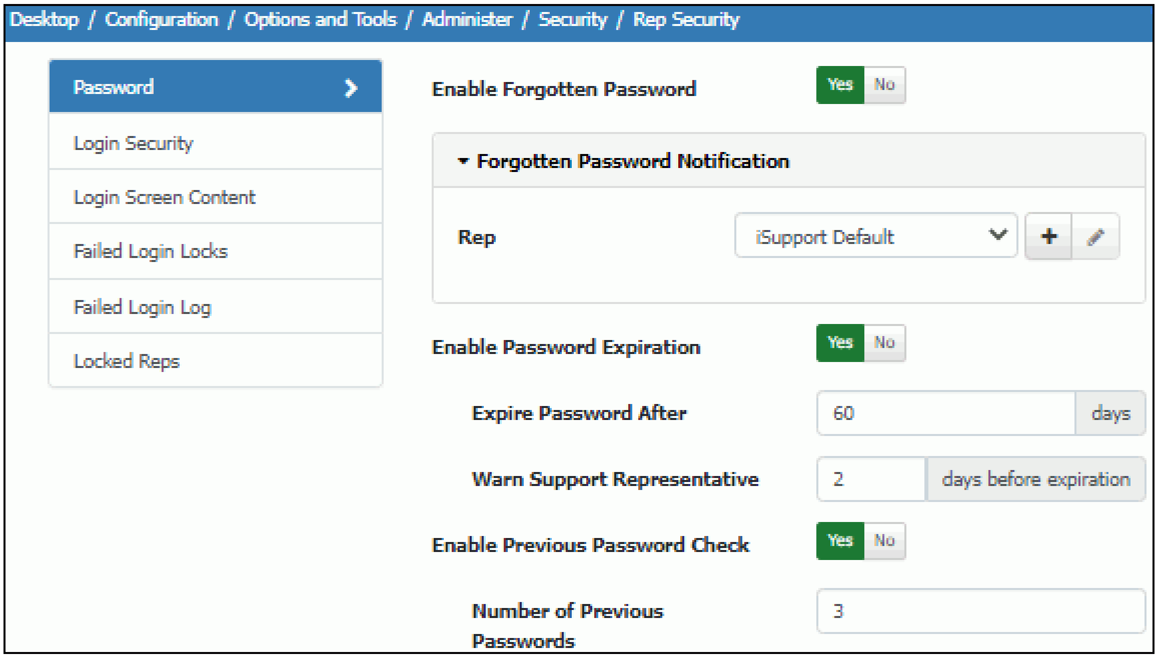
Created Date ▾	Initiator	Recipient	Conversation
04/11/2019 4:46:25 AM	Barry White	Jorge Quentin	Hide Conversation • **Barry White** 04/11/2019 8:45:06 PM Hello Jorge, can you cover for me at lunch today? • **Jorge Quentin** 04/11/2019 8:45:19 PM Sure! • **Barry White** 04/11/2019 8:45:40 PM Thanks!
04/11/2019 4:45:18 AM	Barry White	Jorge Quentin	Show Conversation

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

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

Configuring Password Complexity and Expiration

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


Desktop / Configuration / Options and Tools / Administer / Security / Rep Security
Password
Login Security
Login Screen Content
Failed Login Locks
Failed Login Log
Locked Reps
Forgotten Password Notification
+

Enable Forgotten Password: [✓ Yes] No

Rep: iSupport Default

Enable Password Expiration: [✓ Yes] No

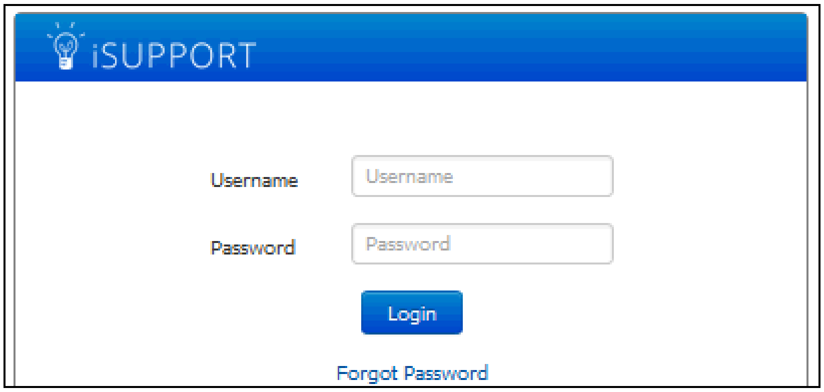
Expire Password After: 60 days

Warn Support Representative: 2 days before expiration

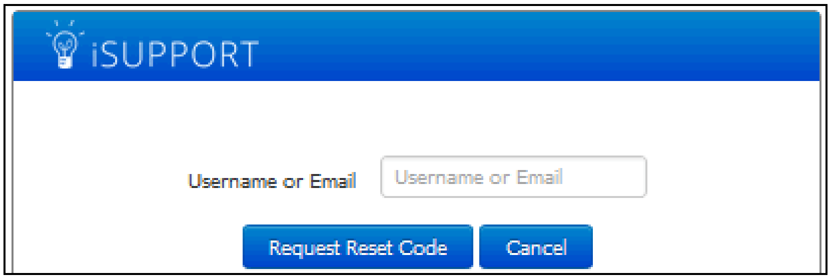
Enable Previous Password Check: [✓ Yes] No

Number of Previous Passwords: 3

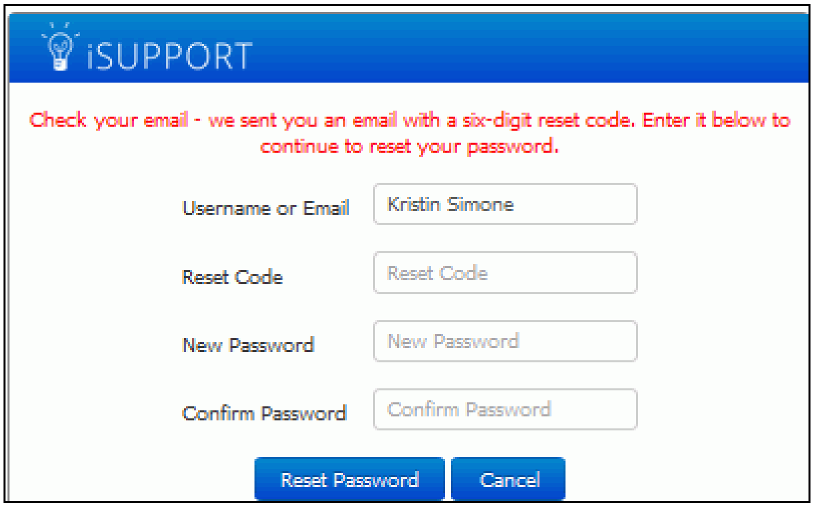
Enable Forgotten Password - Select Yes to include a Forgot Password link in the login dialog and send an email to a support representative with a password reset code. In the Notification field, select iSupport Default to use iSupport's default Forgotten Password notification or use the + Create New and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



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.



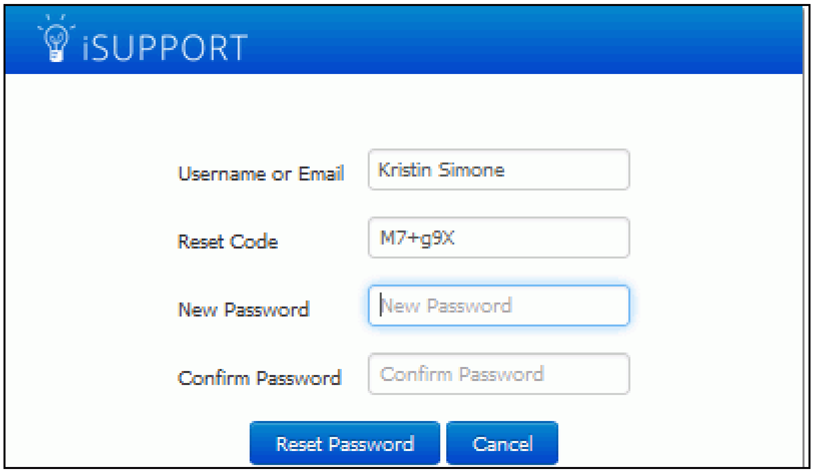
After an existing username or email address has been entered, the following dialog will appear:



Check your email - we sent you an email with a six-digit reset code. Enter it below to continue to reset your password.

Username or Email: Kristin Simone

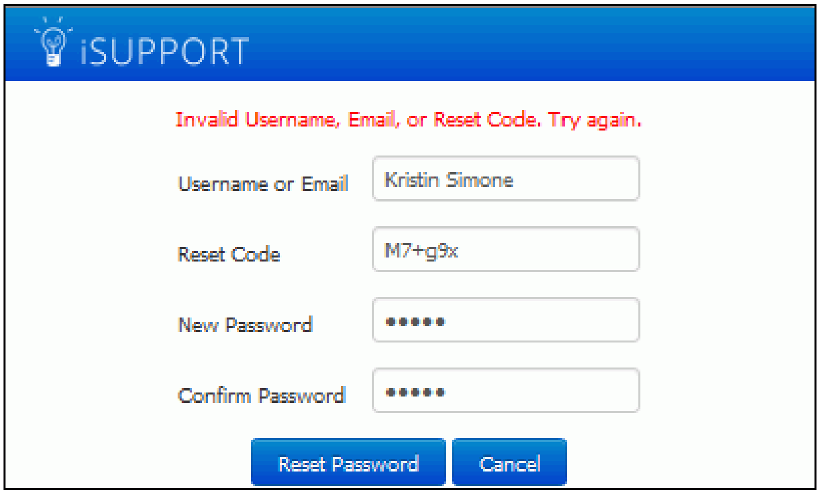
The selected notification will be sent to the support representative with a six-digit reset code and a link to the Desktop login screen. When the link is clicked, a dialog with a Reset Code field will appear.



Username or Email: Kristin Simone

Reset Code: M7+g9X

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.



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

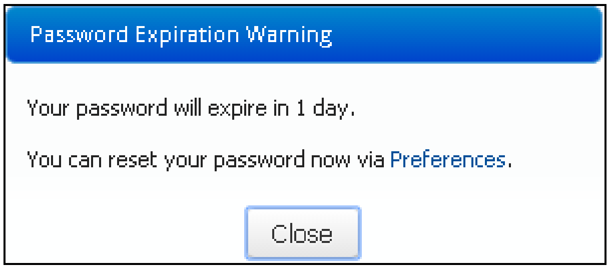
Username or Email: Kristin Simone

Reset Code: M7+g9x

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.



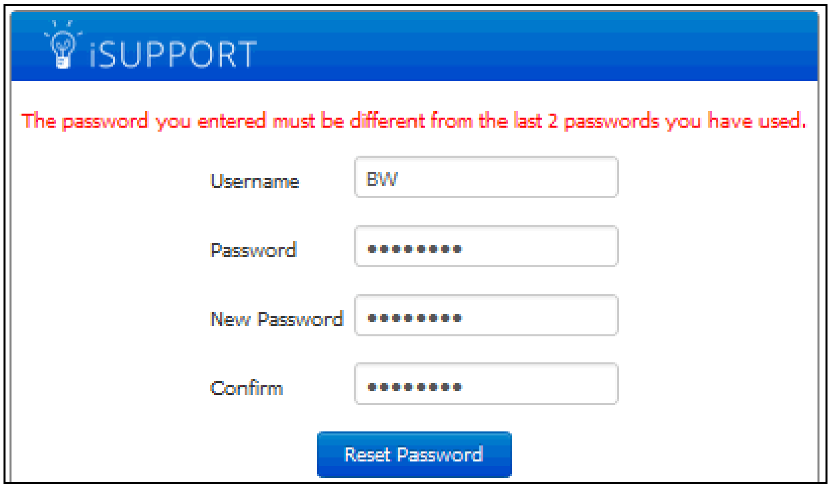
Your password will expire in 1 day.

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.



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

Username: BW

Password: ••••••••

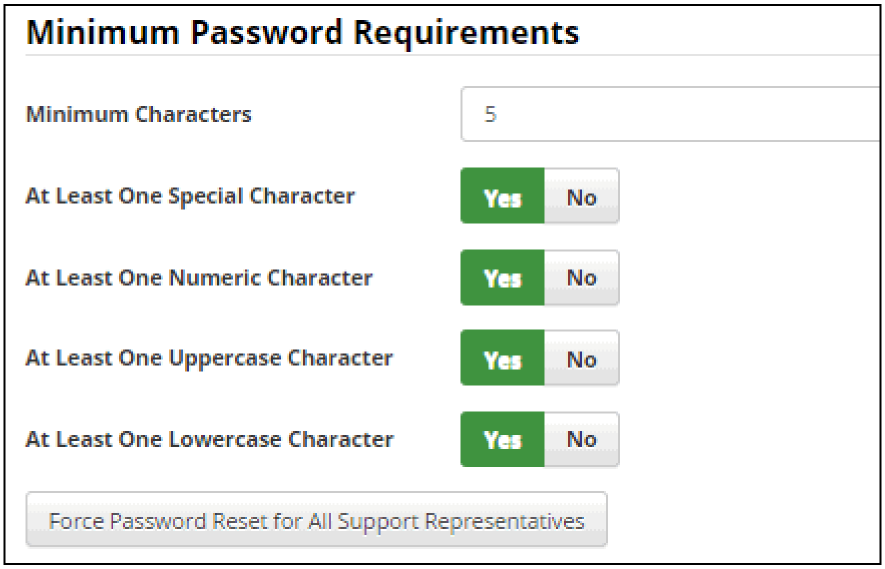
New Password: ••••••••

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.



Minimum Password Requirements

Minimum Characters: 5

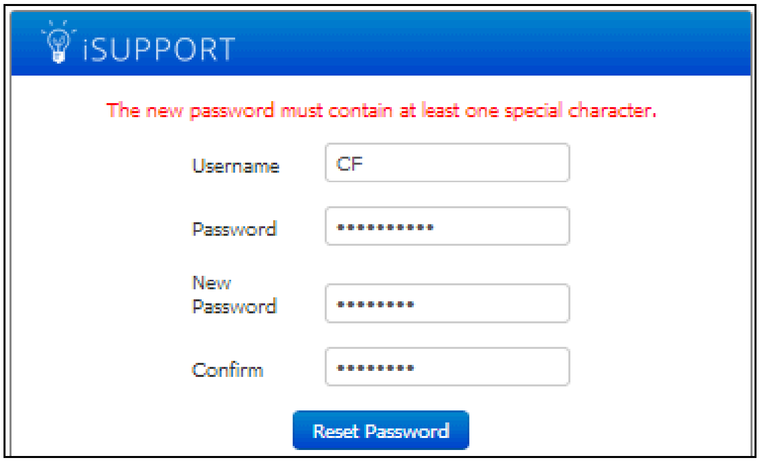
At Least One Special Character: [✓ Yes] No

At Least One Numeric Character: [✓ Yes] No

At Least One Uppercase Character: [✓ Yes] No

At Least One Lowercase Character: [✓ Yes] No

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



The new password must contain at least one special character.

Username: CF

Password: •••••••••••

New Password: ••••••••

Confirm: ••••••••

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 last one special character that is not a number or letter.

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

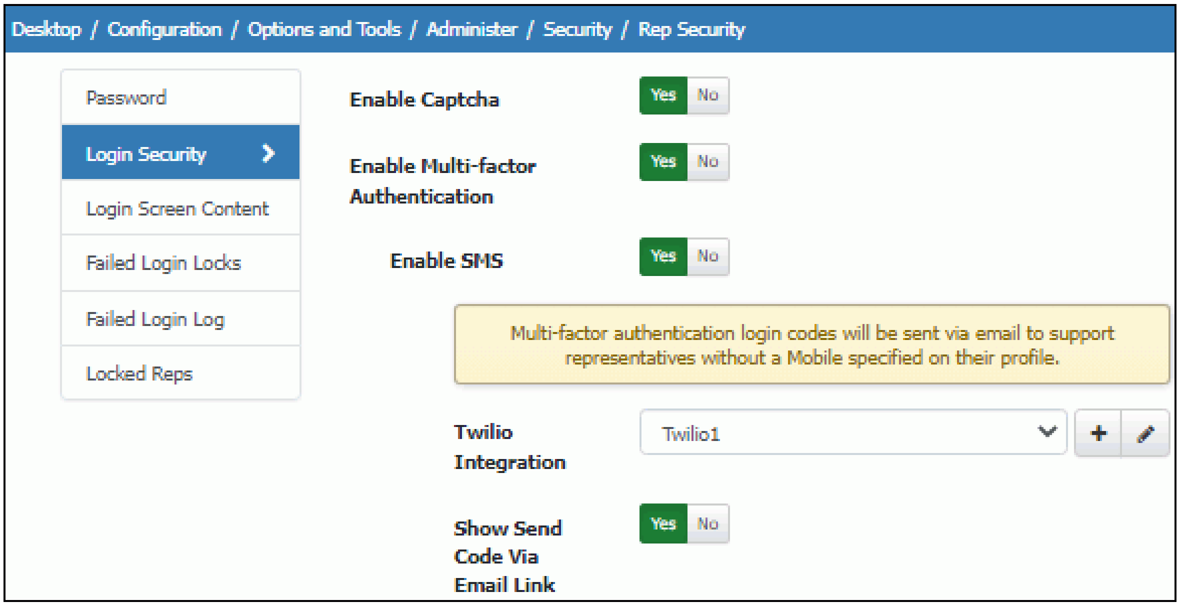
At Least One Uppercase Character - Select Yes to require a support representative’s newly entered password to contain at least one capital letter.

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

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

Configuring Login Security

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



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

- Password
- Login Security
- Login Screen Content
- Failed Login Locks
- Failed Login Log
- Locked Reps

Enable Captcha: Yes No

Enable Multi-factor Authentication: Yes No

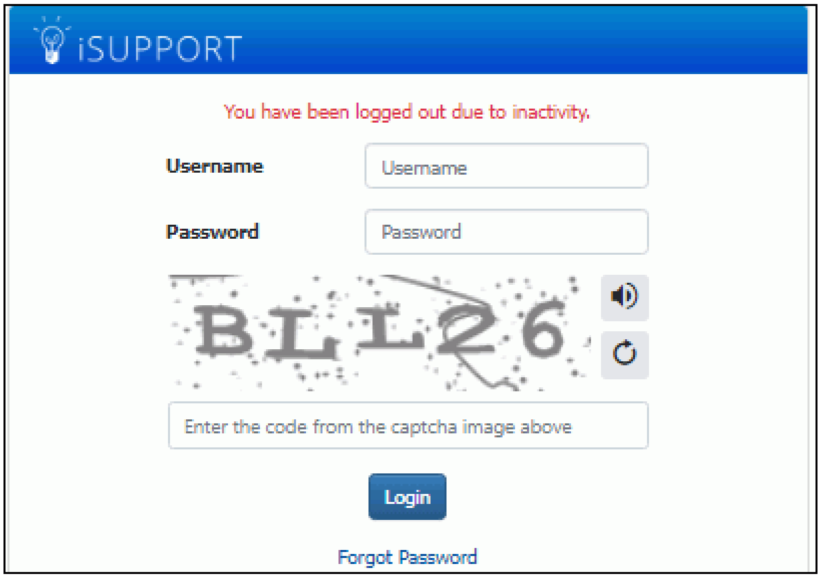
Enable SMS: Yes No

Multi-factor authentication login codes will be sent via email to support representatives without a Mobile specified on their profile.

Twilio Integration: Twilio1

Show Send Code Via Email Link: Yes No

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



iSUPPORT

You have been logged out due to inactivity.

Username: Username

Password: Password

Enter the code from the captcha image above

Login

Forgot Password

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

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

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

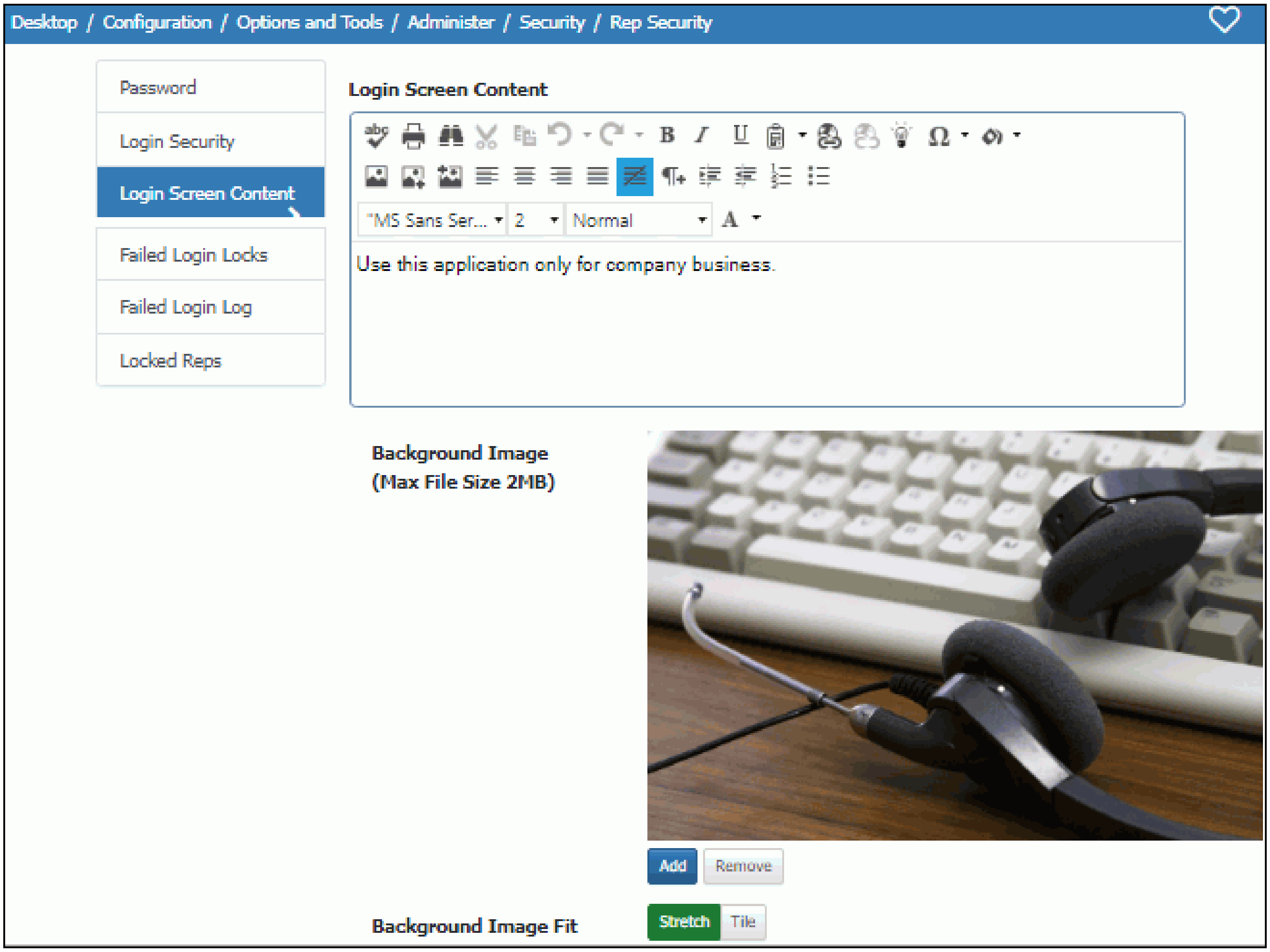
- If SMS **is not** enabled, the code is sent to the email address in the rep's Profile record.

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

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

Configuring Login Screen Content

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



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

- Password
- Login Security
- Login Screen Content
- Failed Login Locks
- Failed Login Log
- Locked Reps

Login Screen Content

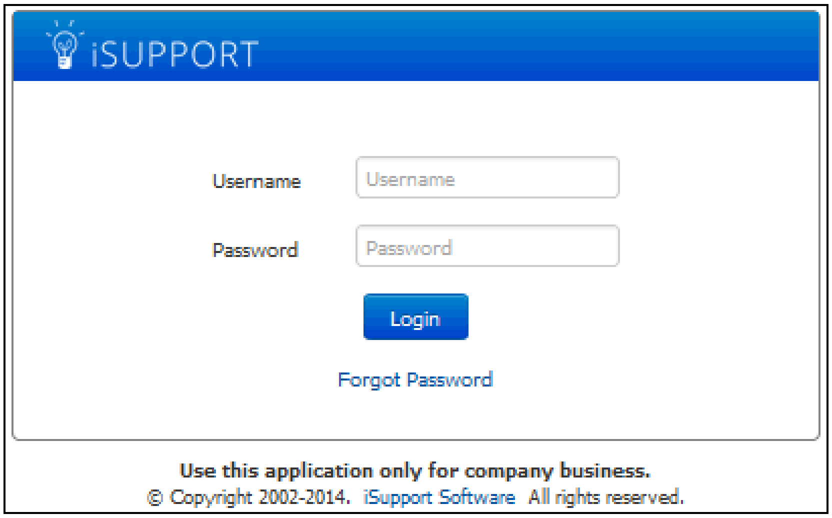
"MS Sans Ser... 2 Normal

Use this application only for company business.

Background Image (Max File Size 2MB)

Background Image Fit: [✓ Stretch] Tile

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



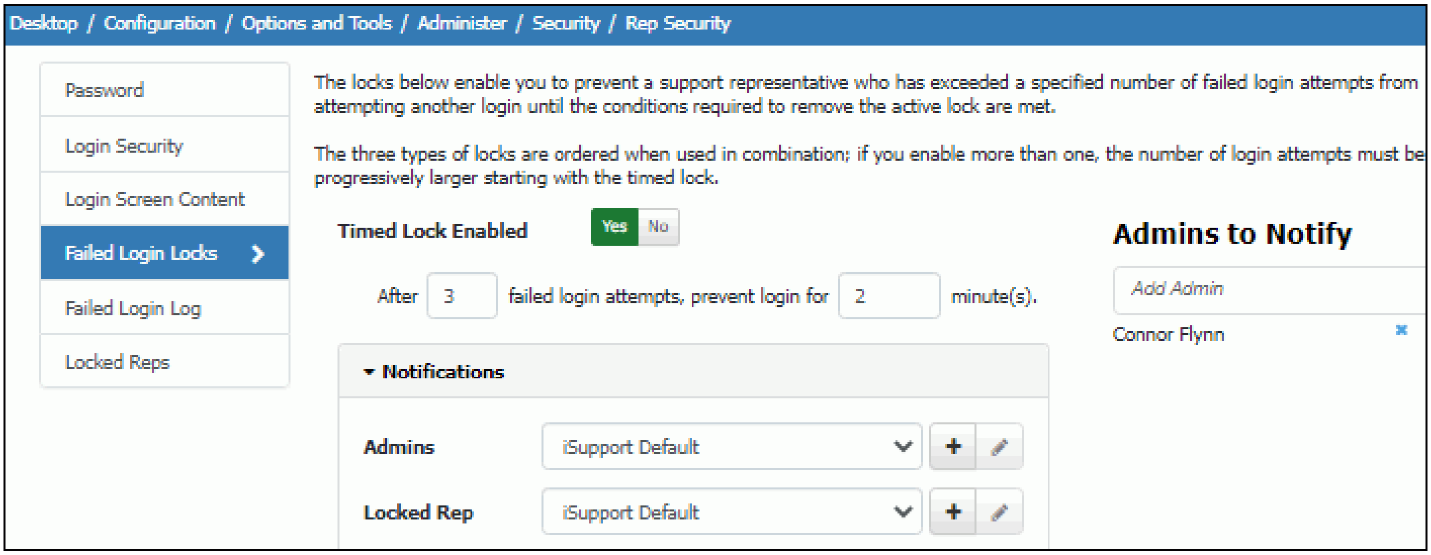
Use this application only for company business.
© Copyright 2002-2014. iSupport Software All rights reserved.

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

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

Configuring Failed Login Locks

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



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 3 failed login attempts, prevent login for 2 minute(s).

Admins: iSupport Default

Locked Rep: iSupport Default

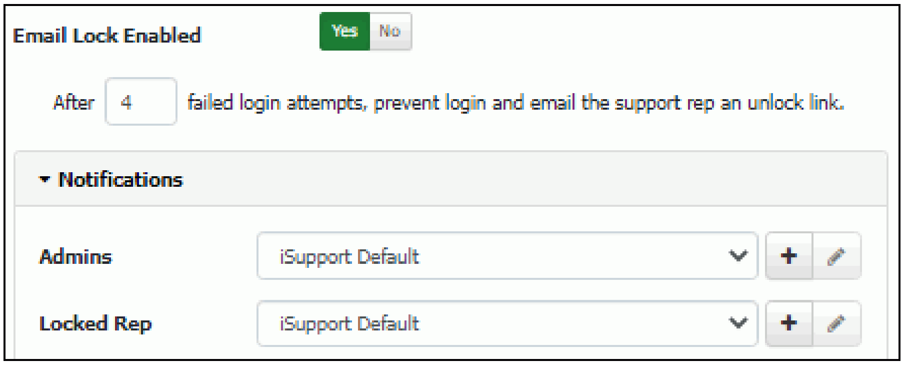
Admins to Notify: Connor Flynn

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

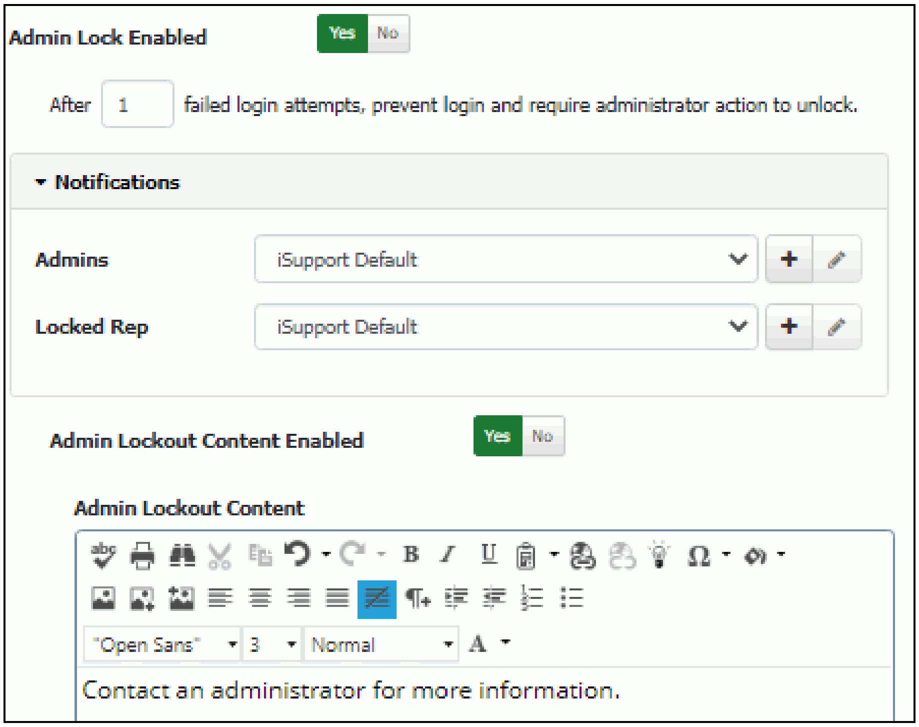
After 4 failed login attempts, prevent login and email the support rep an unlock link.

▾ Notifications

Admins: iSupport Default

Locked Rep: iSupport Default

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

▾ Notifications

Admins: iSupport Default

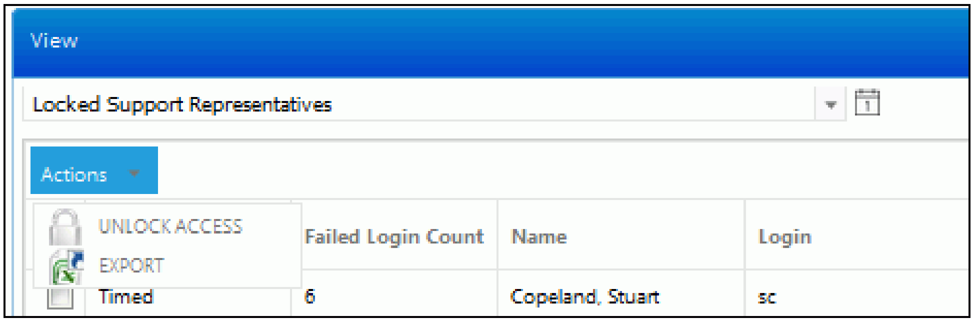
Locked Rep: iSupport Default

Admin Lockout Content Enabled: Yes No

Admin Lockout Content

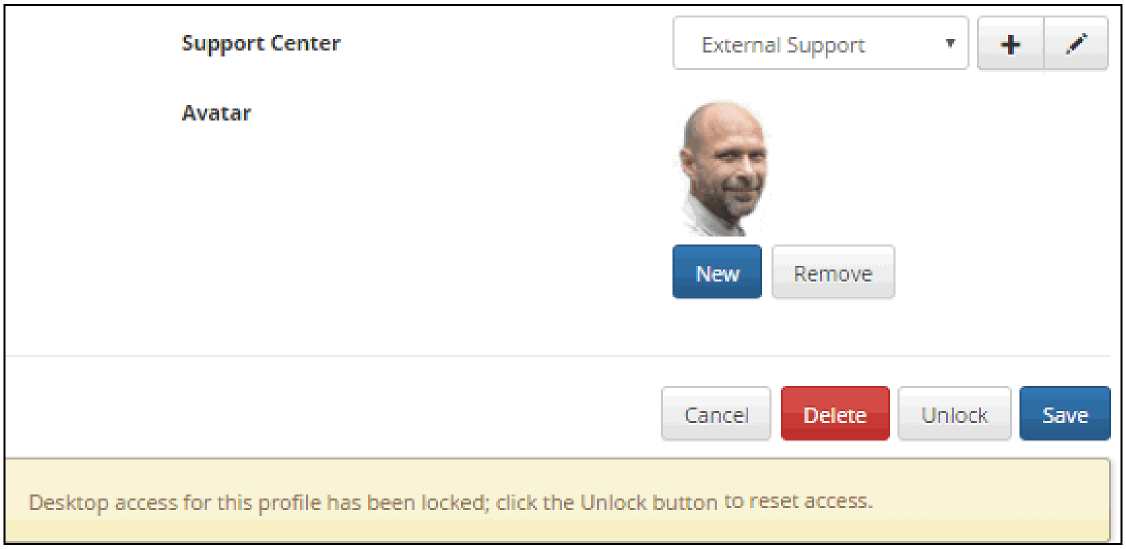
Contact an administrator for more information.

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



	Failed Login Count	Name	Login
□ Timed	6	Copeland, Stuart	sc

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



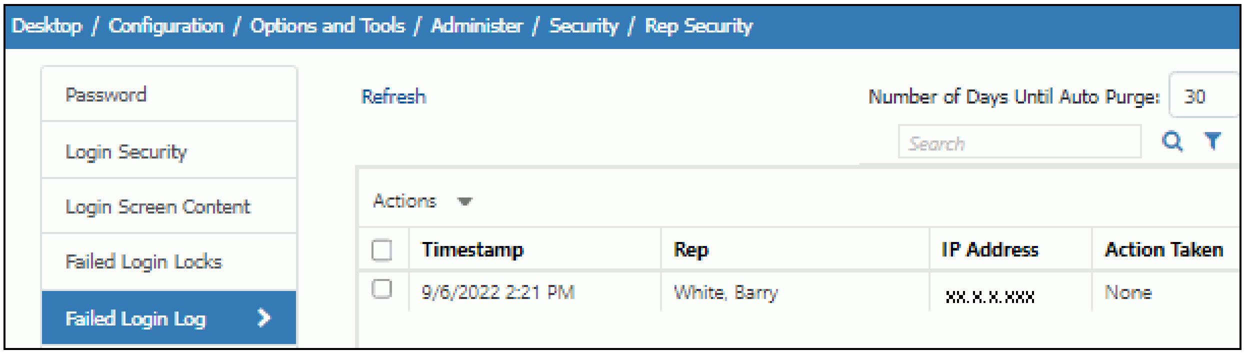
Support Center: External Support

Avatar

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

Viewing the Failed Login Log

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



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

Number of Days Until Auto Purge: 30

□	Timestamp	Rep	IP Address	Action Taken
□	9/6/2022 2:21 PM	White, Barry	xx.x.x.xxx	None

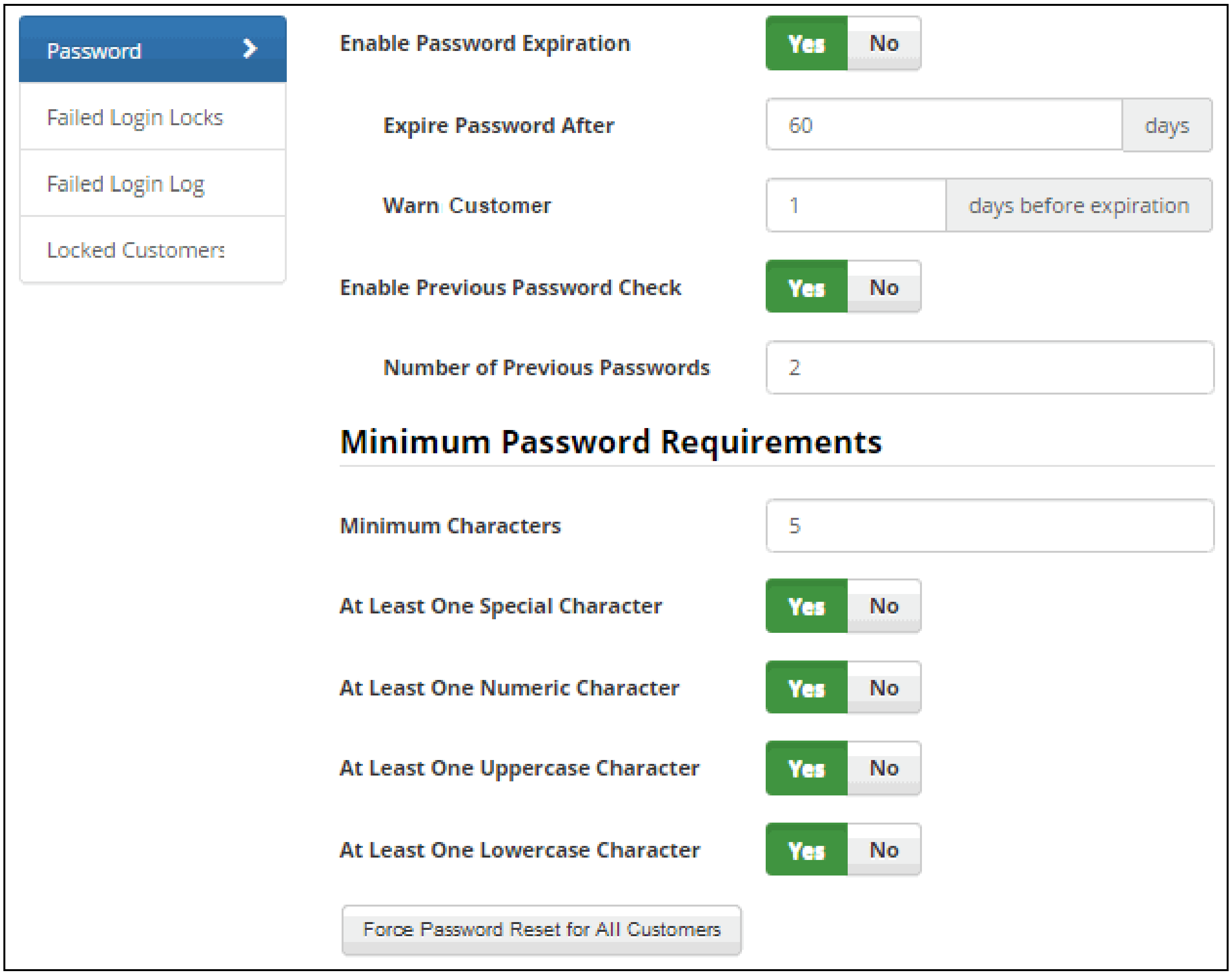
Configuring Password Complexity, Expiration, and Login Locks for Customers

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.

Note that CAPTCHA and multi-factor authentication can be enabled for a mySupport portal via the Login tab in the mySupport Options configuration screen; see the online help for more information.

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.



Enable Password Expiration [✓ Yes] No

Expire Password After 60 days

Warn Customer 1 days before expiration

Enable Previous Password Check [✓ Yes] No

Number of Previous Passwords 2

Minimum Password Requirements

Minimum Characters 5

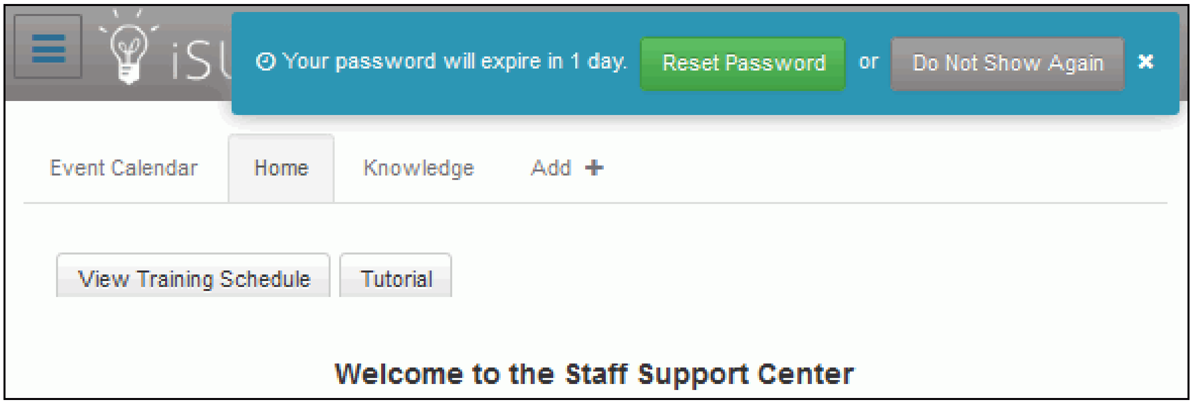
At Least One Special Character [✓ Yes] No

At Least One Numeric Character [✓ Yes] No

At Least One Uppercase Character [✓ Yes] No

At Least One Lowercase Character [✓ Yes] No

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.



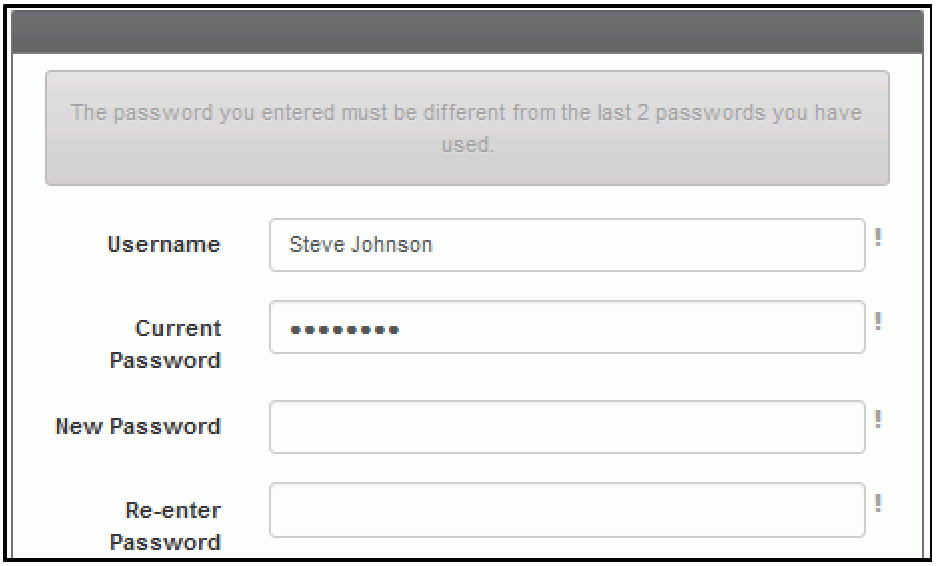
Your password will expire in 1 day.

Welcome to the Staff Support Center

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.



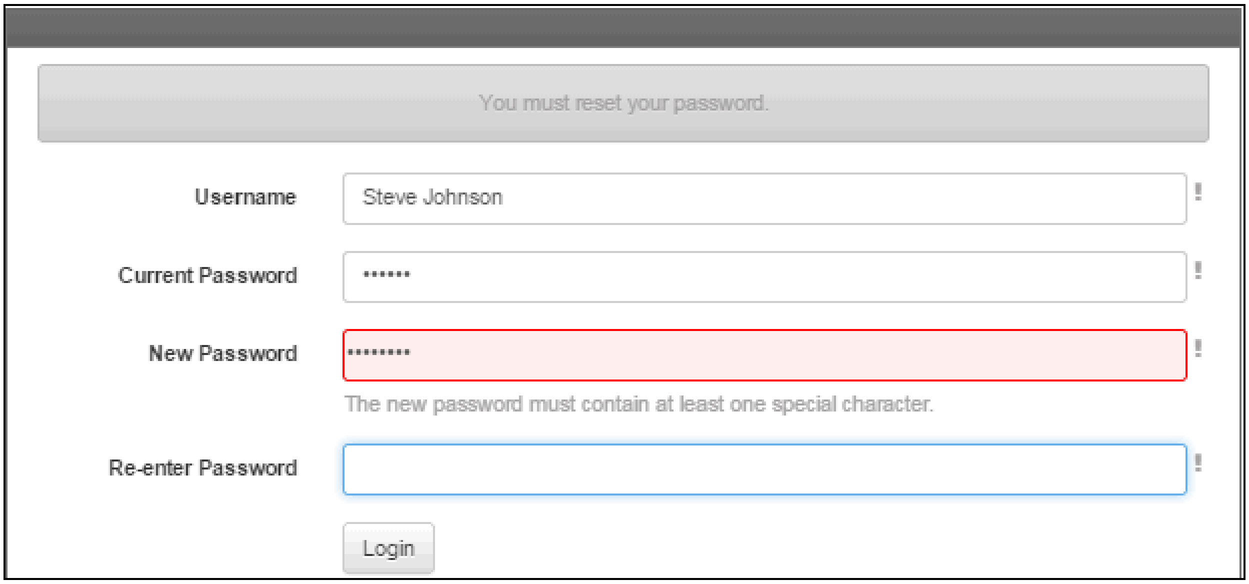
The password you entered must be different from the last 2 passwords you have used.

Username	Steve Johnson
Current Password	●●●●●●●●
New Password	
Re-enter Password	

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: Steve Johnson

Current Password: ••••••

New Password: ••••••••

The new password must contain at least one special character.

Re-enter Password:

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.

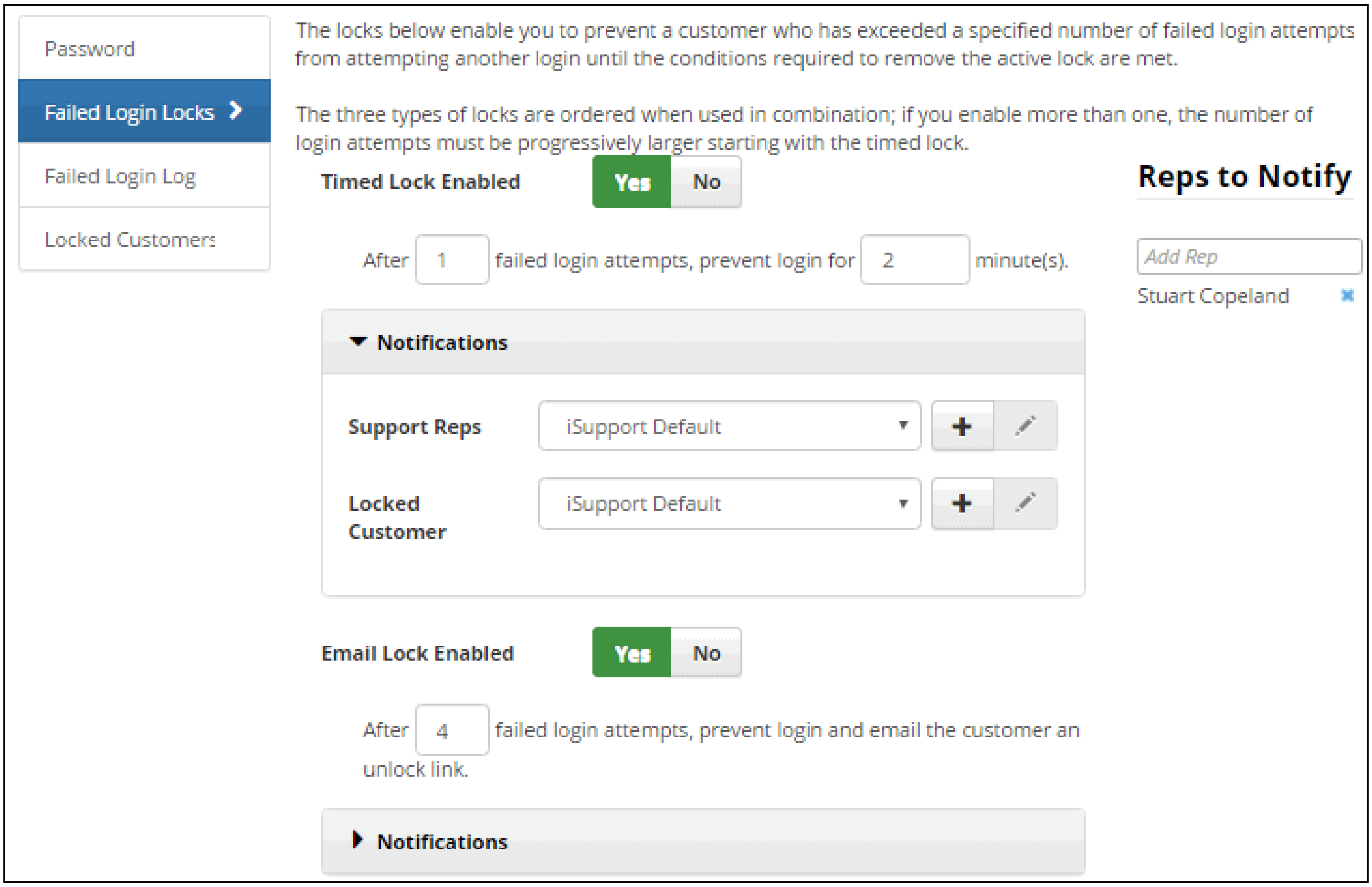
At Least One Uppercase Character - Select Yes to require a customer's newly entered password to contain at least one capital letter.

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 locks below enable you to prevent a customer 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 1 failed login attempts, prevent login for 2 minute(s).

Notifications

Support Reps: iSupport Default

Locked Customer: iSupport Default

Email Lock Enabled [✓ Yes] No

After 4 failed login attempts, prevent login and email the customer an unlock link.

Notifications

Reps to Notify: Stuart Copeland

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.

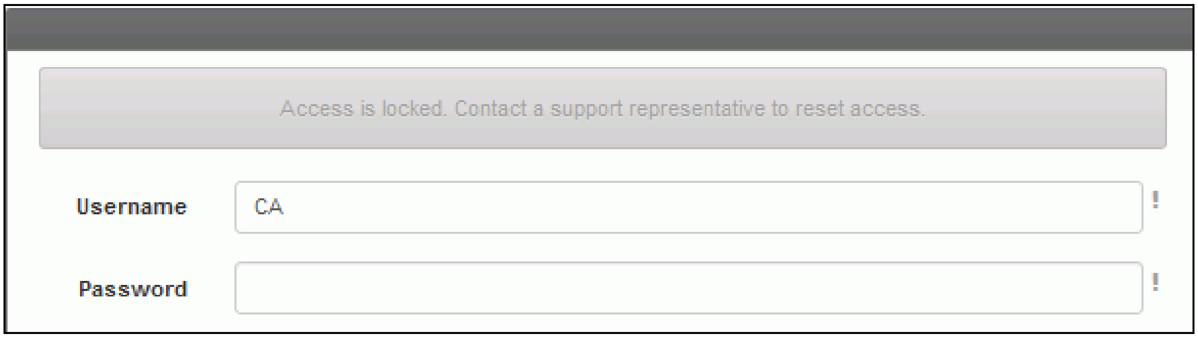
You can send notifications for each type of lock; support representatives selected in the Reps to Notify field will be notified for each notification selected for a lock. These notifications can be customized via the Custom Notifications screen. The three types of locks are ordered when used in combination; 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.

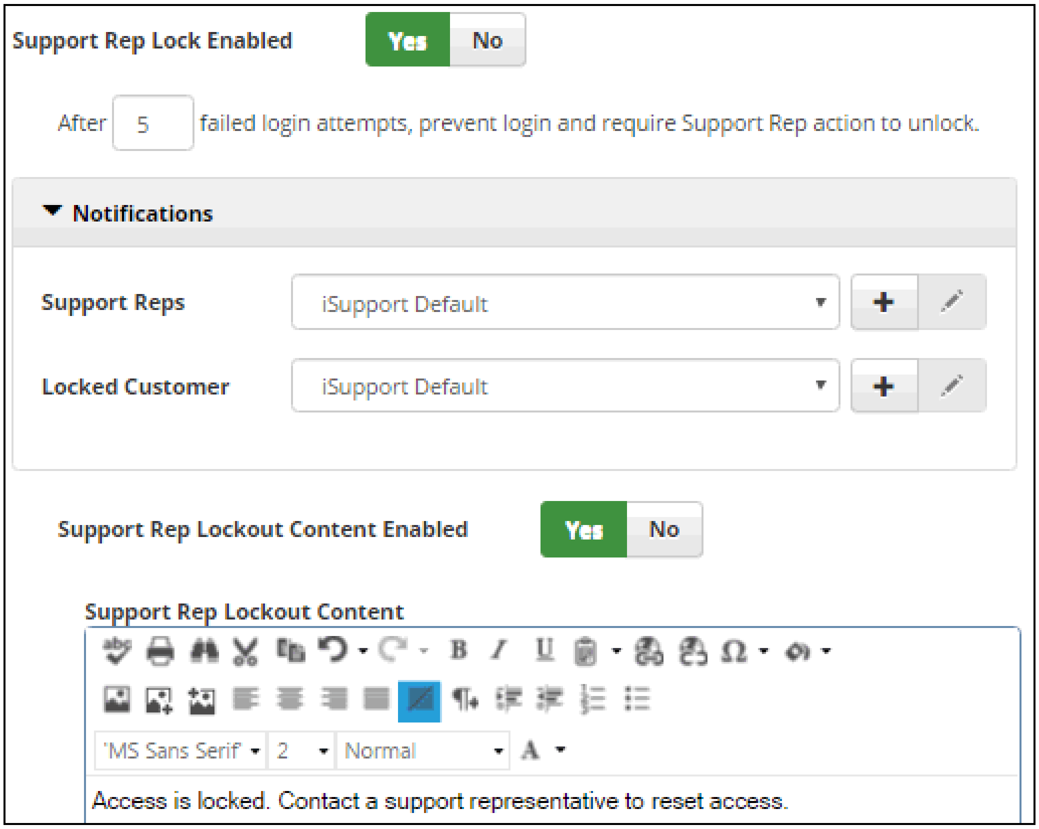


Access is locked. Contact a support representative to reset access.

Username: CA

Password:

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.



Support Rep Lock Enabled: Yes

After 5 failed login attempts, prevent login and require Support Rep action to unlock.

Notifications

Support Reps: iSupport Default

Locked Customer: iSupport Default

Support Rep Lockout Content Enabled: Yes

Support Rep Lockout Content

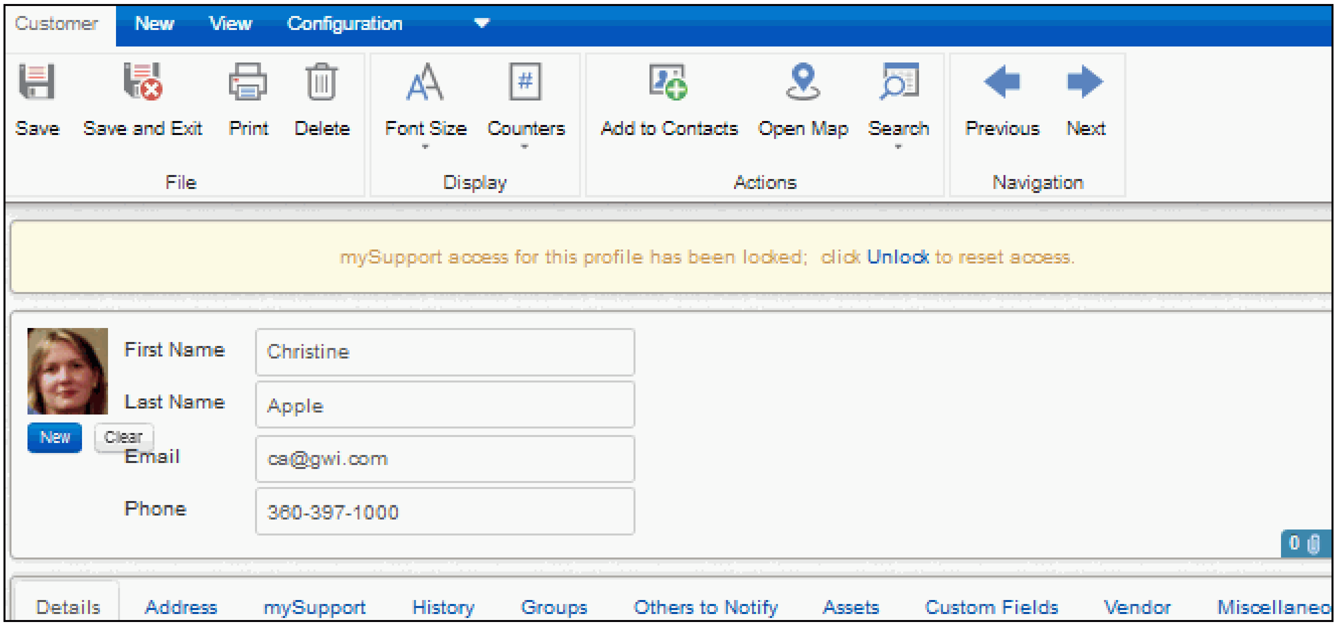
'MS Sans Serif' 2 Normal

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.



mySupport access for this profile has been locked; click Unlock to reset access.

First Name: Christine

Last Name: Apple

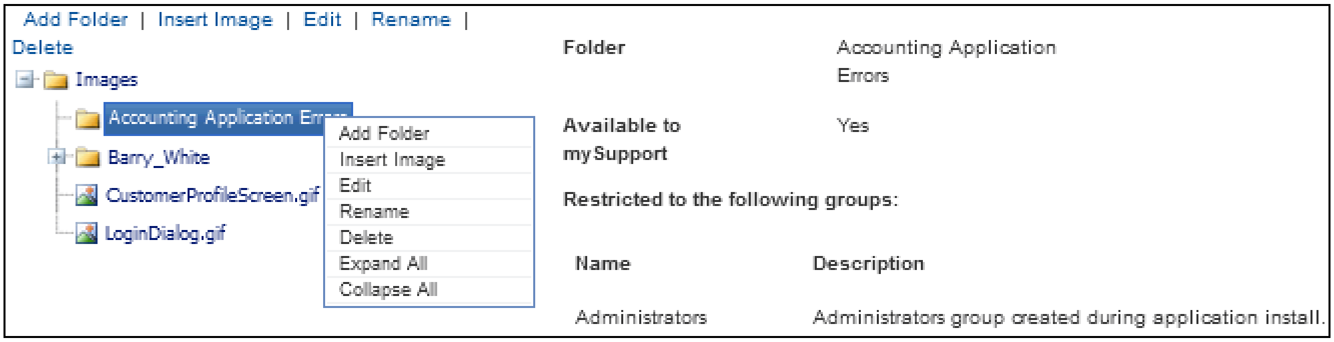
Email: ca@gwi.com

Phone: 360-397-1000

Managing Access to Images

In iSupport entry fields with a toolbar, you can select Image Upload 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.


Add Folder | Insert Image | Edit | Rename | Delete
Images
Accounting Application Errors
Barry_White
CustomerProfileScreen.gif
LoginDialog.gif
Add Folder
Insert Image
Edit
Rename
Delete
Expand All
Collapse All

Folder	Accounting Application Errors
Available to mySupport	Yes

Restricted to the following groups:

Name	Description
Administrators	Administrators group created during application install.

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.

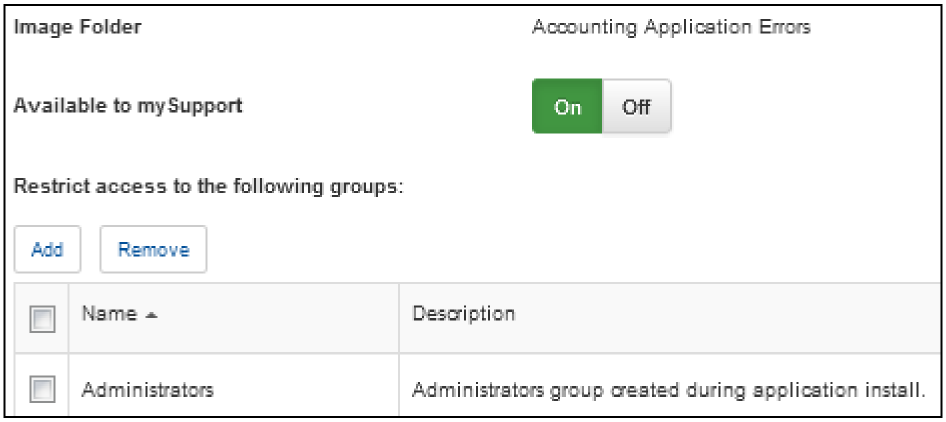


Image Folder	Accounting Application Errors
Available to mySupport	[✓ On] Off

Restrict access to the following groups:

☐	Name ▲	Description
☐	Administrators	Administrators group created during application install.

Note: In versions prior to Version 14, images added via email processing or uploaded by support representatives via the toolbar were added to the root of the Images folder; these images were unreferenced by iSupport. (iSupport started tracking references in Version 14 and added images into applicable folders, including the EmailProcessing and iSupport_Social_Client folders.) The Maintenance agent in this release searches pre-Version 14 installations for those images that were unreferenced and added prior to Version 14. Once the agent completes, an asterisk (*) will appear next to each unreferenced image for deletion if applicable. An email will be sent to support representatives designated as Administrators if the agent detects more than 100 unreferenced images.

You can delete unreferenced images in a folder and its subfolders by selecting the folder and clicking the Delete Unreferenced Images link.

Enabling and Scheduling Agents

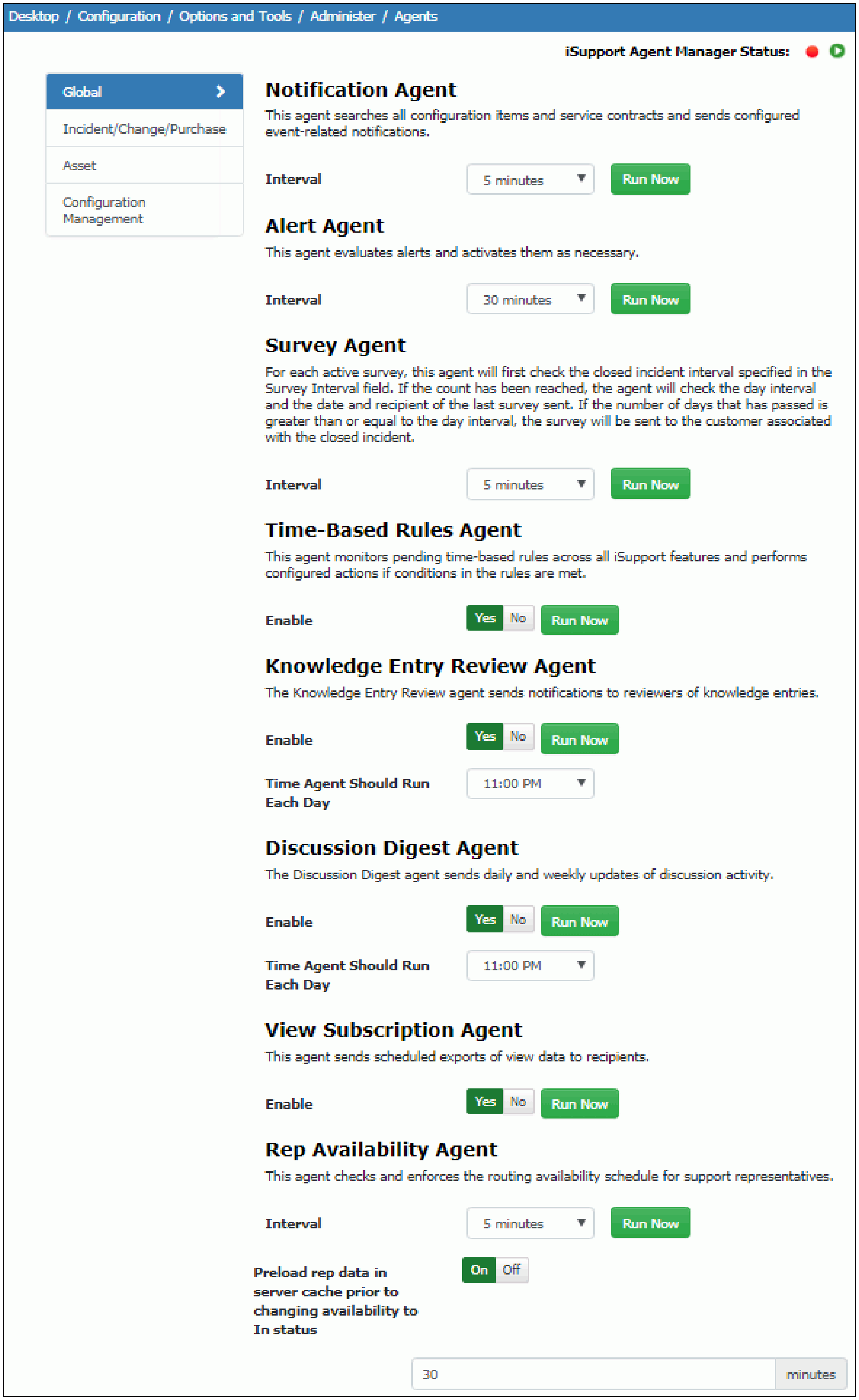
Agents perform tasks that are an integral part of iSupport functionality such as sending notifications. Agents run in the background; to verify that an agent has run, go to Options and Tools | Administer| Event Log. The iSupport Agent Manager service performs scheduled execution of iSupport agents, and 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 icon in the upper right corner of the screen indicates the status of the iSupport Agent Manager service; it is required to be running for normal operation of iSupport. If the indicator is red, use the icon next to the indicator to start it or go to Administration Tools | Services on the server that is hosting iSupport and start the service.

An ⚠ Alert will appear above the Desktop Configuration icon when the iSupport Agent service stops. Agent status is checked when the Desktop loads; it is updated when the agent starts or stops.

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.



Desktop / Configuration / Options and Tools / Administer / Agents
iSupport Agent Manager Status:
Global
Incident/Change/Purchase
Asset
Configuration Management

Notification Agent

This agent searches all configuration items and service contracts and sends configured event-related notifications.

Interval: 5 minutes — Run Now

Alert Agent

This agent evaluates alerts and activates them as necessary.

Interval: 30 minutes — Run Now

Survey Agent

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: 5 minutes — Run Now

Time-Based Rules Agent

This agent monitors pending time-based rules across all iSupport features and performs configured actions if conditions in the rules are met.

Enable: [✓ Yes] No — Run Now

Knowledge Entry Review Agent

The Knowledge Entry Review agent sends notifications to reviewers of knowledge entries.

Enable: [✓ Yes] No — Run Now

Time Agent Should Run Each Day: 11:00 PM

Discussion Digest Agent

The Discussion Digest agent sends daily and weekly updates of discussion activity.

Enable: [✓ Yes] No — Run Now

Time Agent Should Run Each Day: 11:00 PM

View Subscription Agent

This agent sends scheduled exports of view data to recipients.

Enable: [✓ Yes] No — Run Now

Rep Availability Agent

This agent checks and enforces the routing availability schedule for support representatives.

Interval: 5 minutes — Run Now

Preload rep data in server cache prior to changing availability to In status: [✓ On] Off

30 minutes

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, 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.

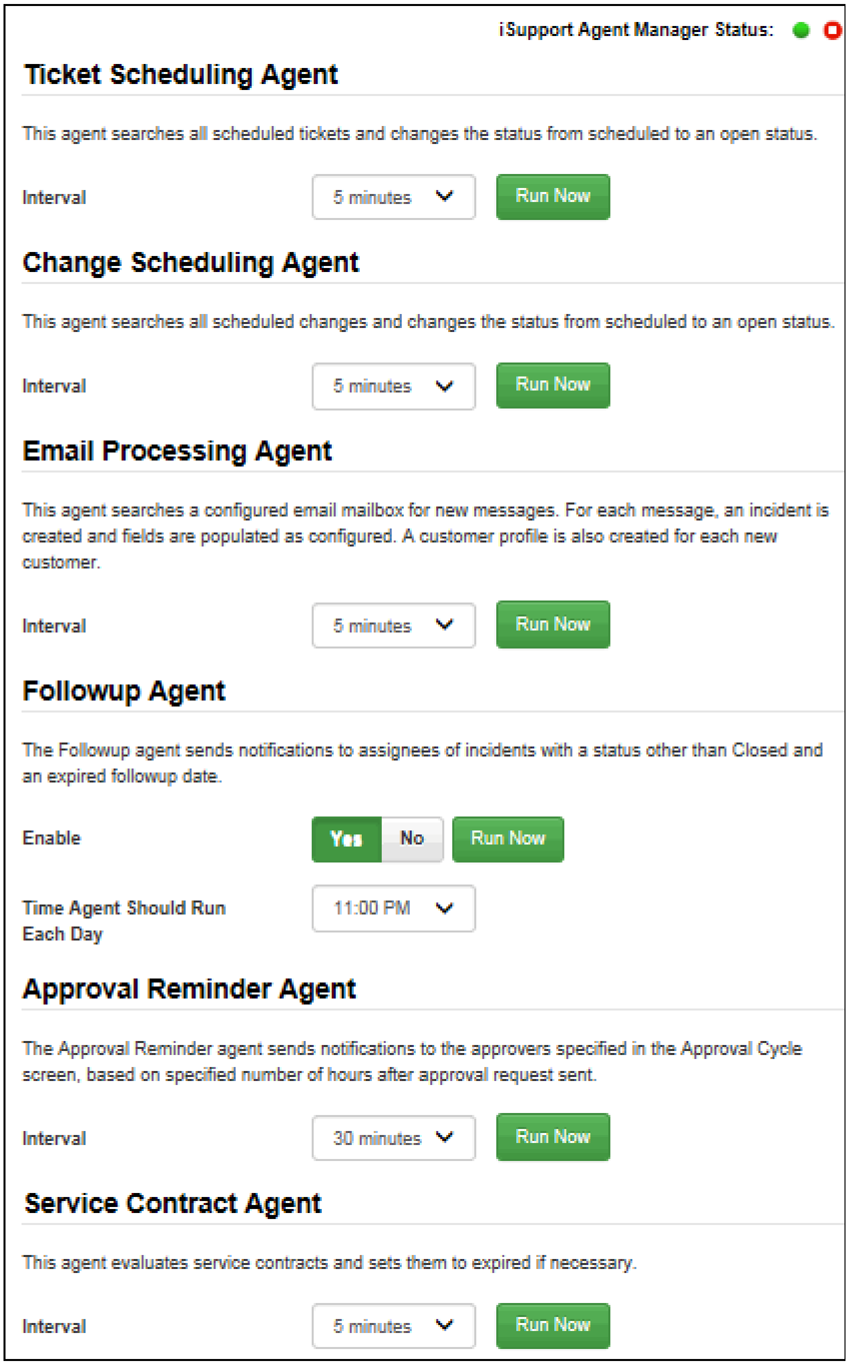
View Subscription Agent - Select Yes to enable the View Subscription agent, which sends scheduled view exports via email to recipients designated via the View component. This agent runs on a five minute interval.

Rep Availability Agent - Select the number of minutes in the interval for the agent to check and enforce the routing availability schedule for support representatives. Schedule routing availability via the Routing Availability tab in the Support Representative Profile screen.

Preload rep data in server cache prior to changing availability to In status - The iSupport Application Pool Startup agent initializes settings throughout the product in order to improve startup performance. Select On to enable this agent to monitor the availability schedule of support representatives and preload their settings for the specified number of minutes prior to any In status change.

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: 5 minutes

Change Scheduling Agent

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

Interval: 5 minutes

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: 5 minutes

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: 11:00 PM

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: 30 minutes

Service Contract Agent

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

Interval: 5 minutes

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.

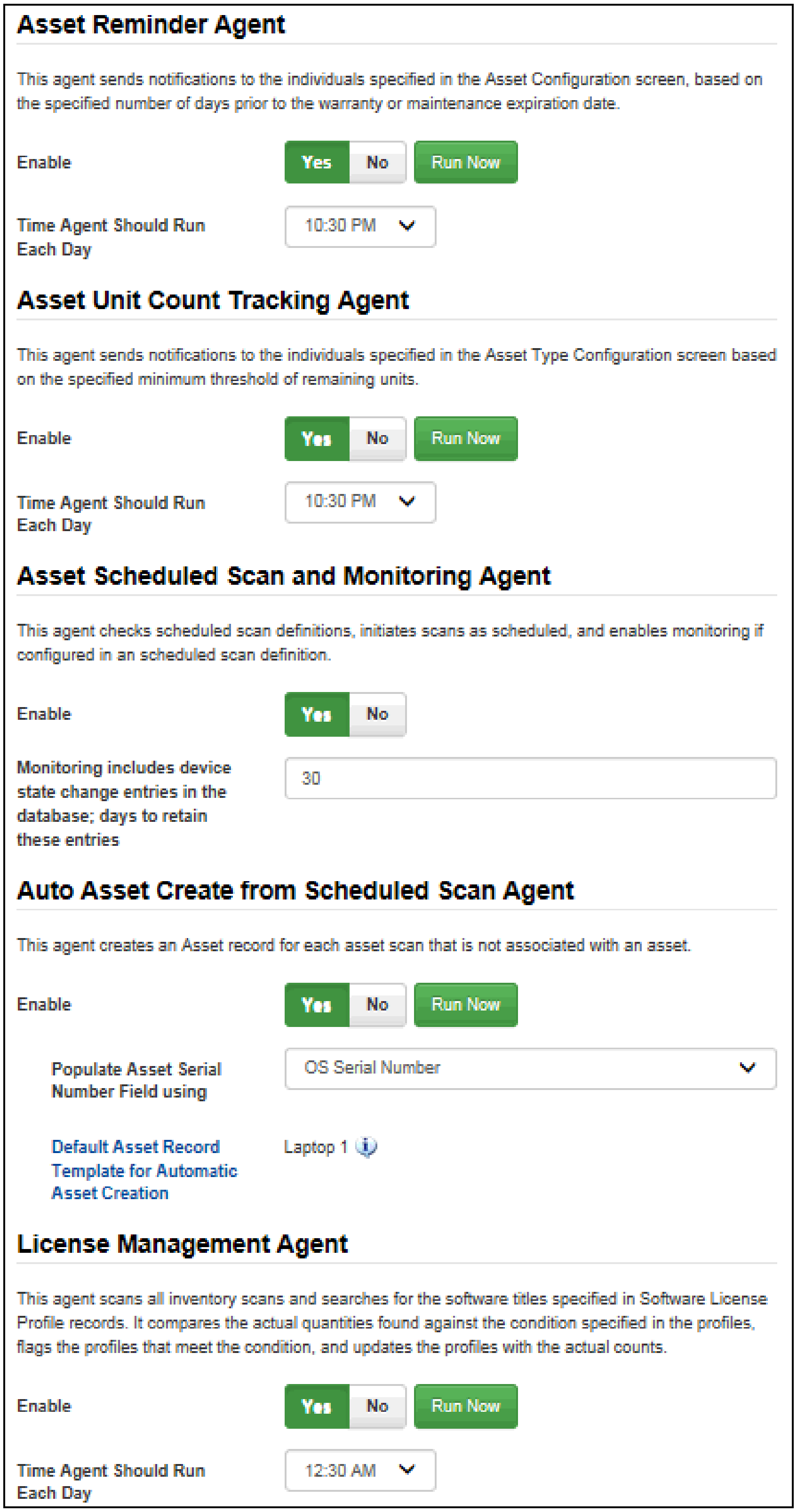
Followup Agent/Time the Followup Agent Should Run Each Day - Select Yes to enable the Followup agent that checks all incident followup dates. The agent sends email reminders to the incident assignees for each incident with an expired followup date and a status other than a Closed status. After selecting 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: 10:30 PM

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: 10:30 PM

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: 30

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: OS Serial Number

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: 12:30 AM

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.

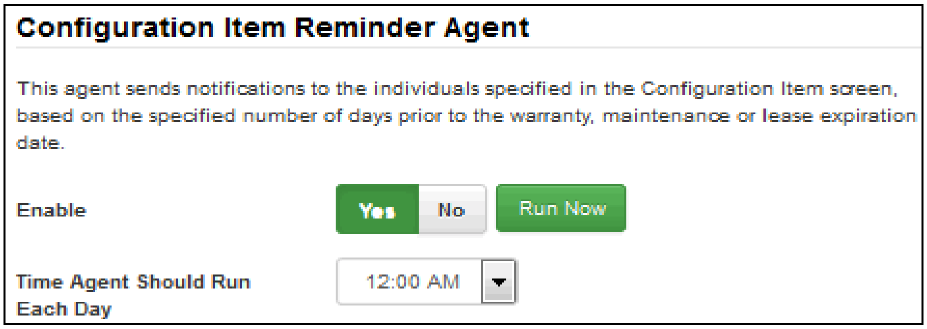
Populate Asset Serial Number Field With - Select Yes to populate the Asset Serial Number field with the operating system serial number when Asset records are created automatically for machines that are involved in scheduled scans but not associated with an existing record.

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.



Configuration Item Reminder Agent

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.

Enable: [✓ Yes] No

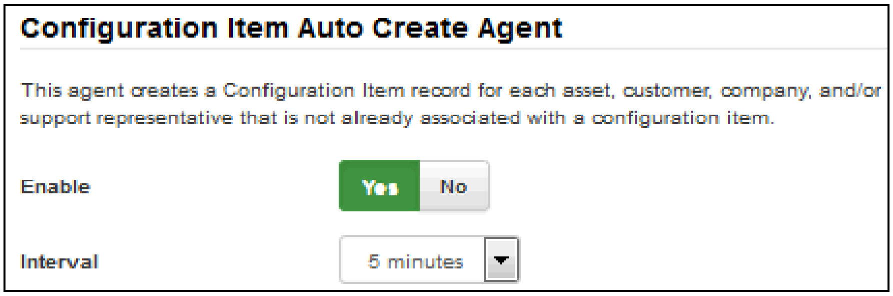
Time Agent Should Run Each Day: 12:00 AM

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.



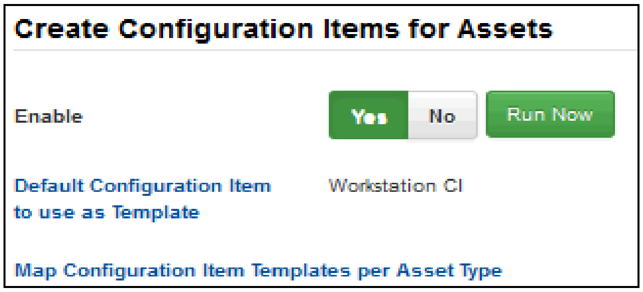
Configuration Item Auto Create Agent

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 5 minutes

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

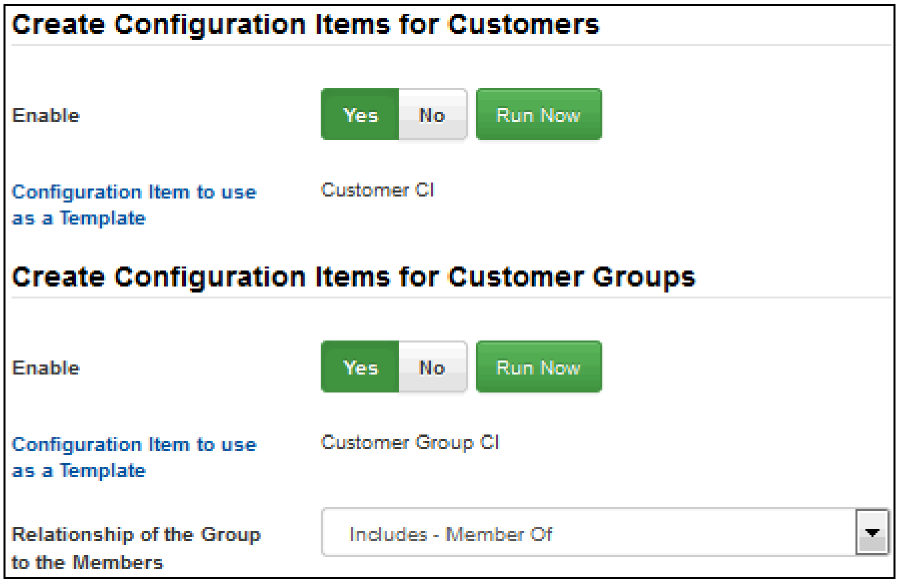
Map Configuration Item Templates per Asset Type

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.



Create Configuration Items for Customers

Enable: [✓ Yes] No · Run Now

Configuration Item to use as a Template: Customer CI

Create Configuration Items for Customer Groups

Enable: [✓ Yes] No · Run Now

Configuration Item to use as a Template: Customer Group CI

Relationship of the Group to the Members: Includes - Member Of

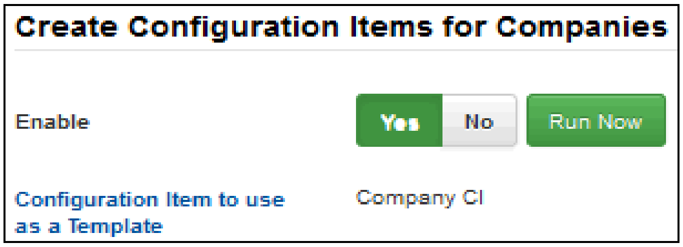
Use the Run Now button to run the agent immediately on a one-time basis. To create configuration items automatically for customers on an interval basis, enable the Configuration Item Auto Create Agent and select Yes in the Enable field in this section.

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.



Create Configuration Items for Companies

Enable: [✓ Yes] No · Run Now

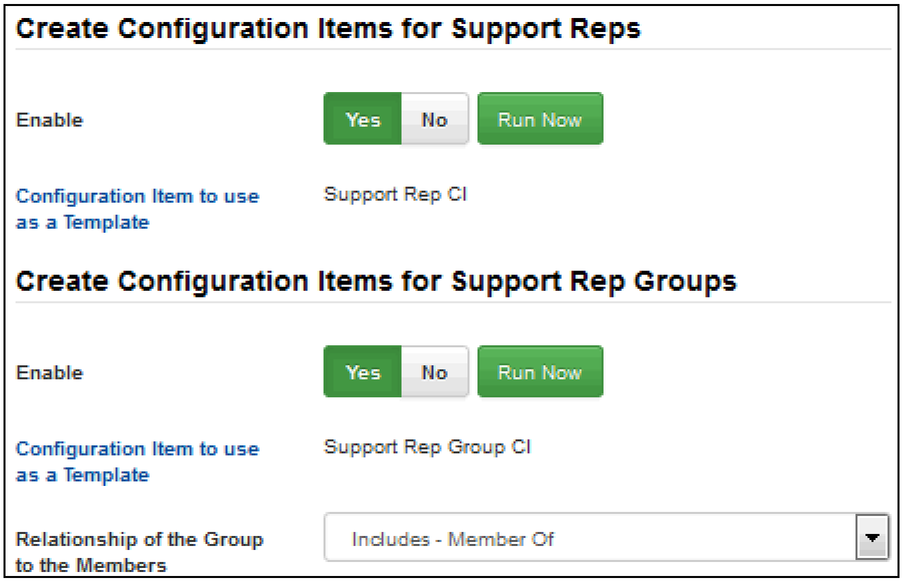
Configuration Item to use as a Template: Company CI

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.



Create Configuration Items for Support Reps

Enable: Yes No Run Now

Configuration Item to use as a Template: Support Rep CI

Create Configuration Items for Support Rep Groups

Enable: Yes No Run Now

Configuration Item to use as a Template: Support Rep Group CI

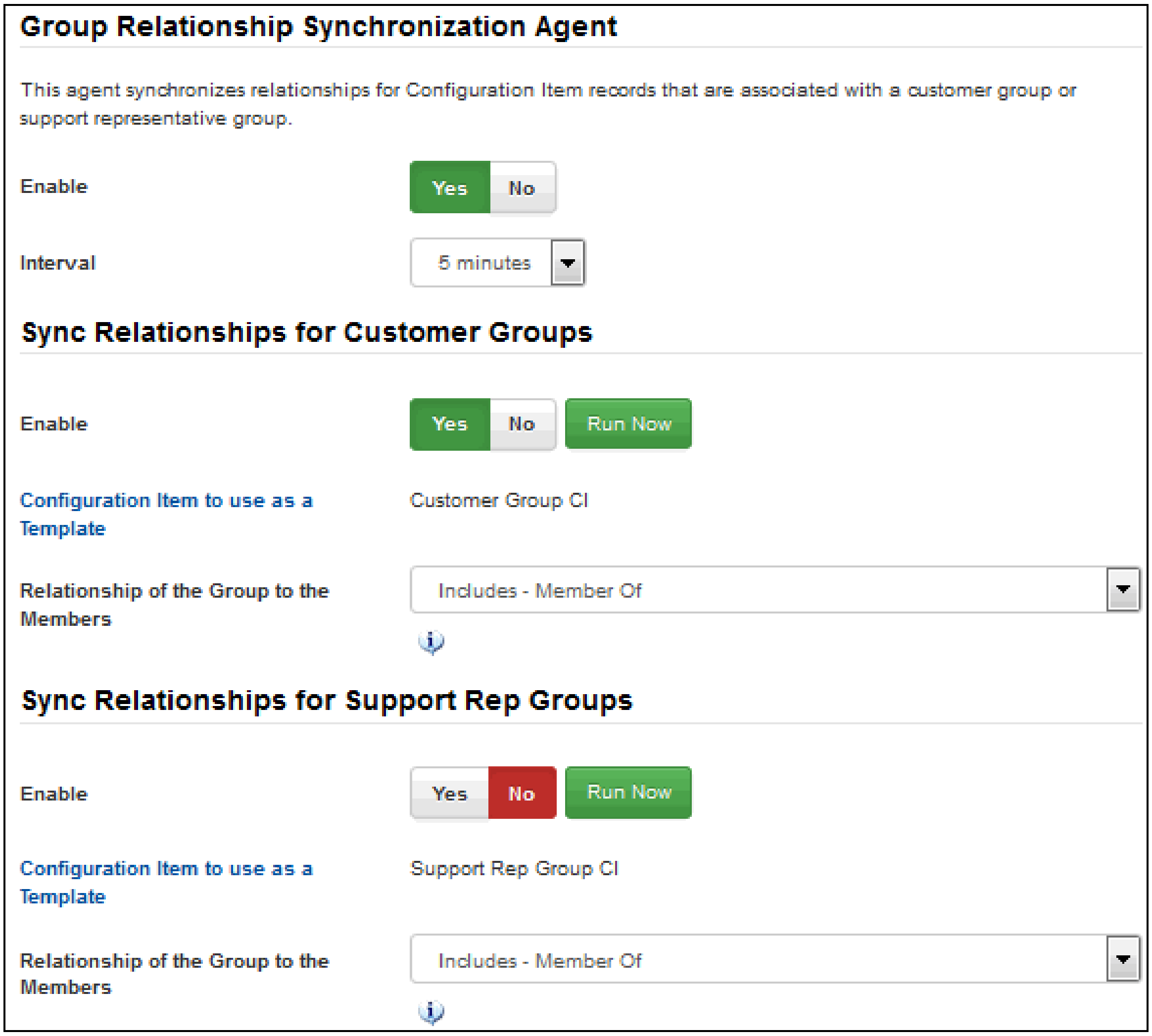
Relationship of the Group to the Members: Includes - Member Of

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

Interval: 5 minutes

Sync Relationships for Customer Groups

Enable: Yes

Configuration Item to use as a Template: Customer Group CI

Relationship of the Group to the Members: Includes - Member Of

Sync Relationships for Support Rep Groups

Enable: No

Configuration Item to use as a Template: Support Rep Group CI

Relationship of the Group to the Members: Includes - Member Of

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.

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, cSupportReporting, and cSurvey 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.
- **Important:** 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).
- **Important:** The Gwi.cSupport.Service.exe.config file in <*directory in which the Rep Desktop is installed*>\bin\.
- 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.

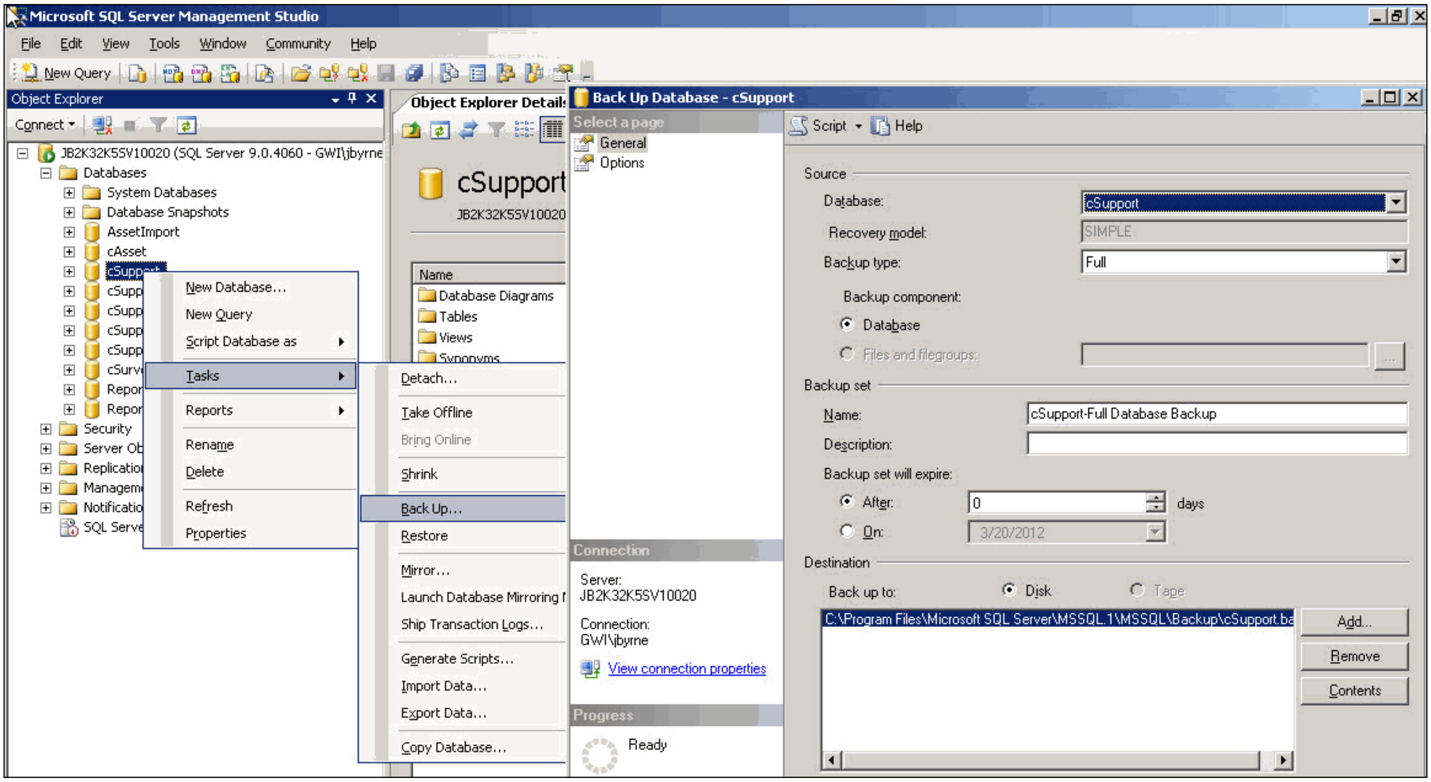
Method A - Backing Up SQL Server Databases using the SIMPLE Recovery Model

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.



Source

Database: cSupport

Recovery model: SIMPLE

Backup type: Full

Backup component: ● Database ○ Files and filegroups:

Backup set

Name: cSupport-Full Database Backup

Description:

Backup set will expire: ● After: 0 days ○ On: 3/20/2012

Destination

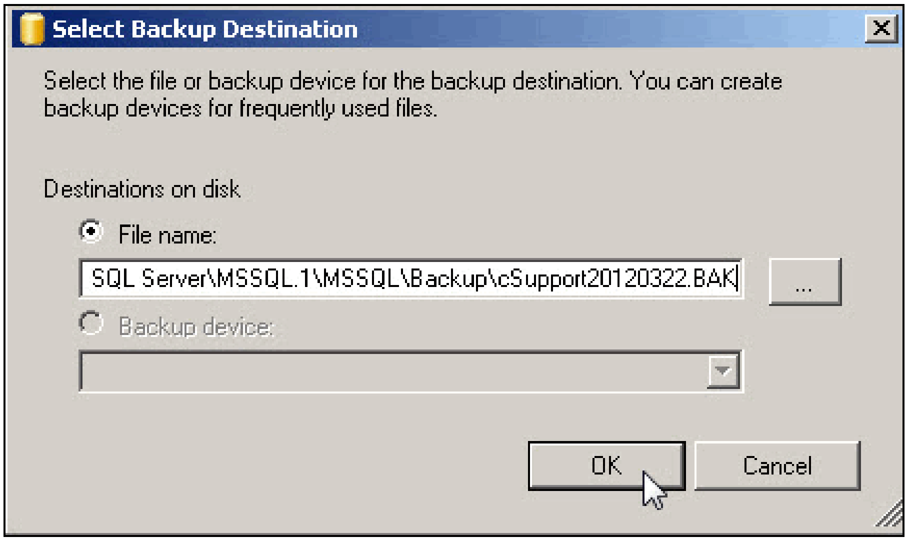
Back up to: ● Disk ○ Tape

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\cSupport.ba

Server: JB2K32K5SV10020

Connection: GWI\jbyrne

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.



Select the file or backup device for the backup destination. You can create backup devices for frequently used files.

Destinations on disk

● File name:

SQL Server\MSSQL.1\MSSQL\Backup\cSupport20120322.BAK

○ Backup device:

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

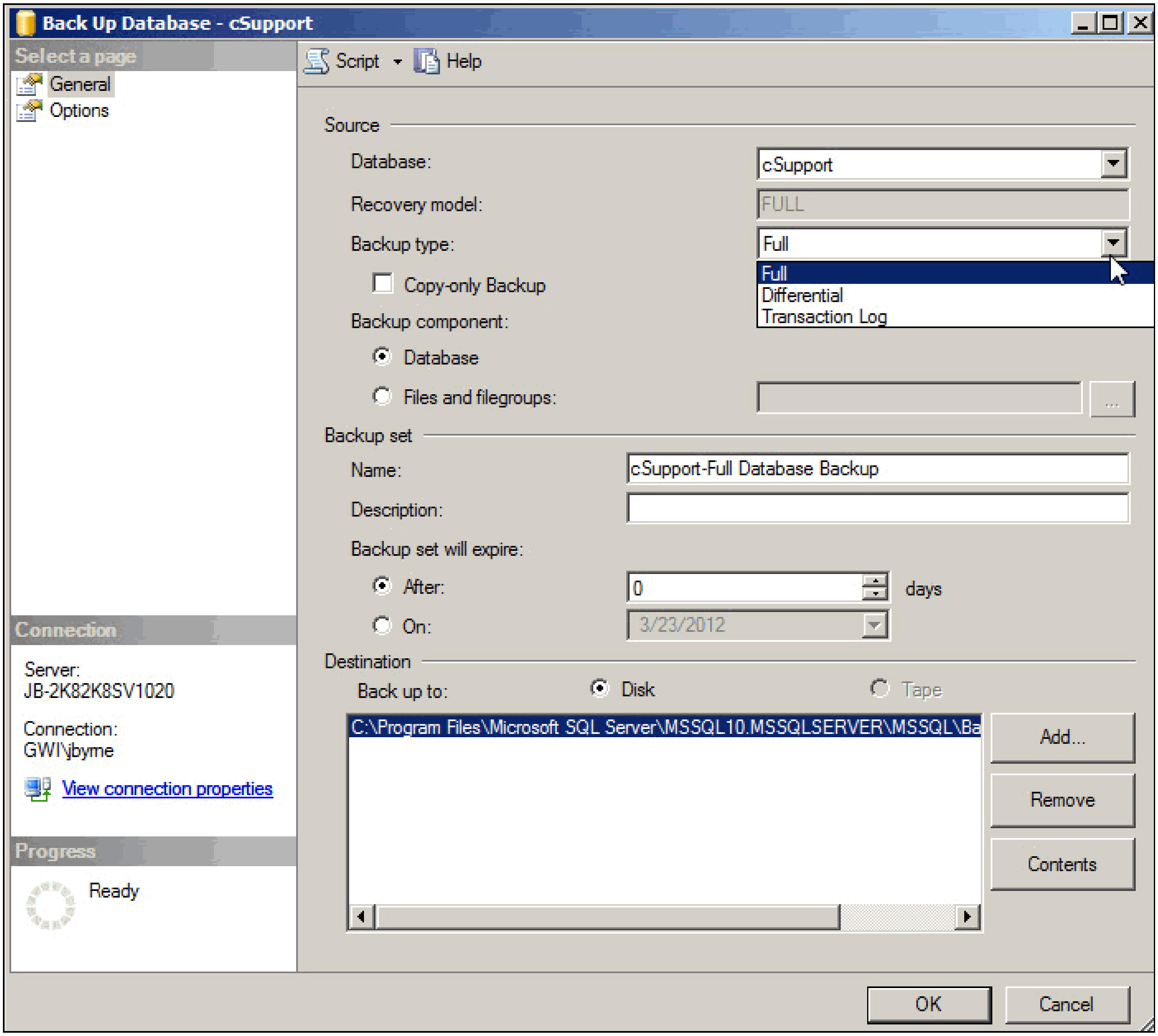
This method will require that you do two backups. The first will be a full backup of the cSupport database. The second will be a Transaction Log backup.

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.



Back Up Database - cSupport

Source

Database: cSupport

Recovery model: FULL

Backup type: Full

☐ Copy-only Backup

Backup component:

● Database

○ Files and filegroups:

Backup set

Name: cSupport-Full Database Backup

Description:

Backup set will expire:

● After: 0 days

○ On: 3/23/2012

Destination

Back up to: ● Disk ○ Tape

C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Ba

Connection

Server:
JB-2K82K8SV1020

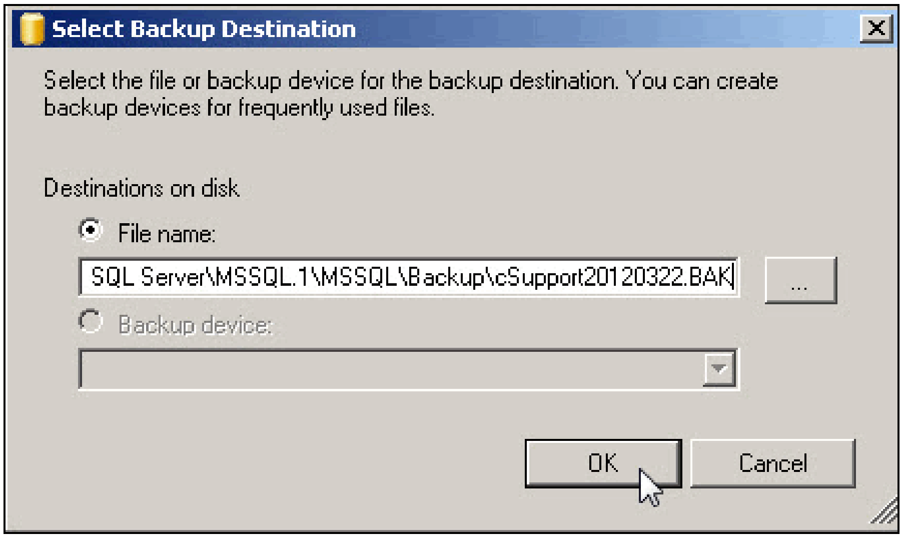
Connection:
GWI\jbyrne

Progress

Ready

- 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.



Select Backup Destination

Select the file or backup device for the backup destination. You can create backup devices for frequently used files.

Destinations on disk

● File name:

SQL Server\MSSQL.1\MSSQL\Backup\cSupport20120322.BAK

○ Backup device:

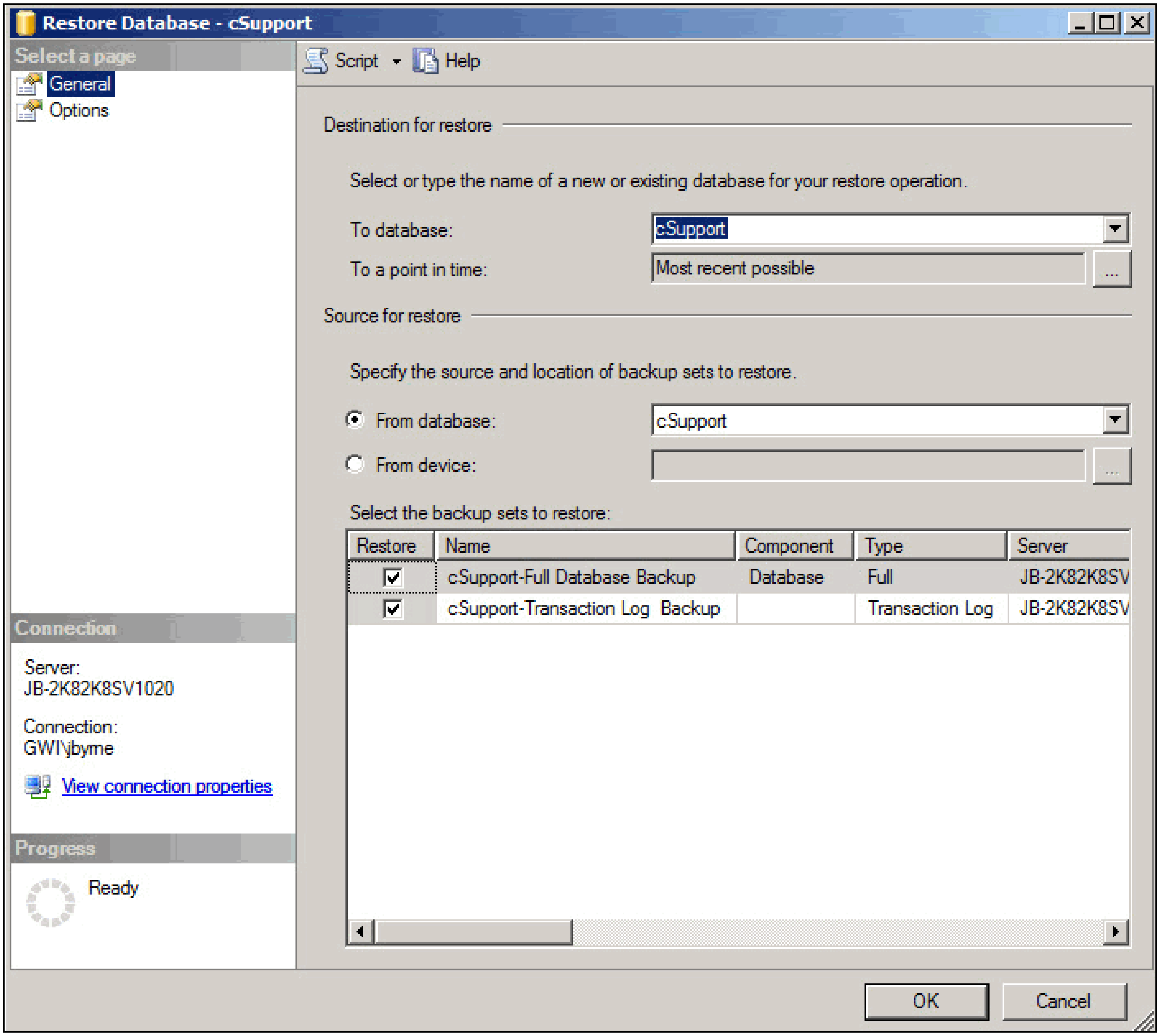
4 Click on Options to open this page. If you are creating a new backup set, the only additional options that you may want to select would be to Verify Backup When Finished, and Perform Checksum Before Writing to Media.

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.



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: cSupport

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

● From database: cSupport

○ From device:

Select the backup sets to restore:

Restore	Name	Component	Type	Server
☑	cSupport-Full Database Backup	Database	Full	JB-2K82K8SV
☑	cSupport-Transaction Log Backup		Transaction Log	JB-2K82K8SV

Server:
JB-2K82K8SV1020

Connection:
GWI\jbyme

View connection properties

Ready

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.

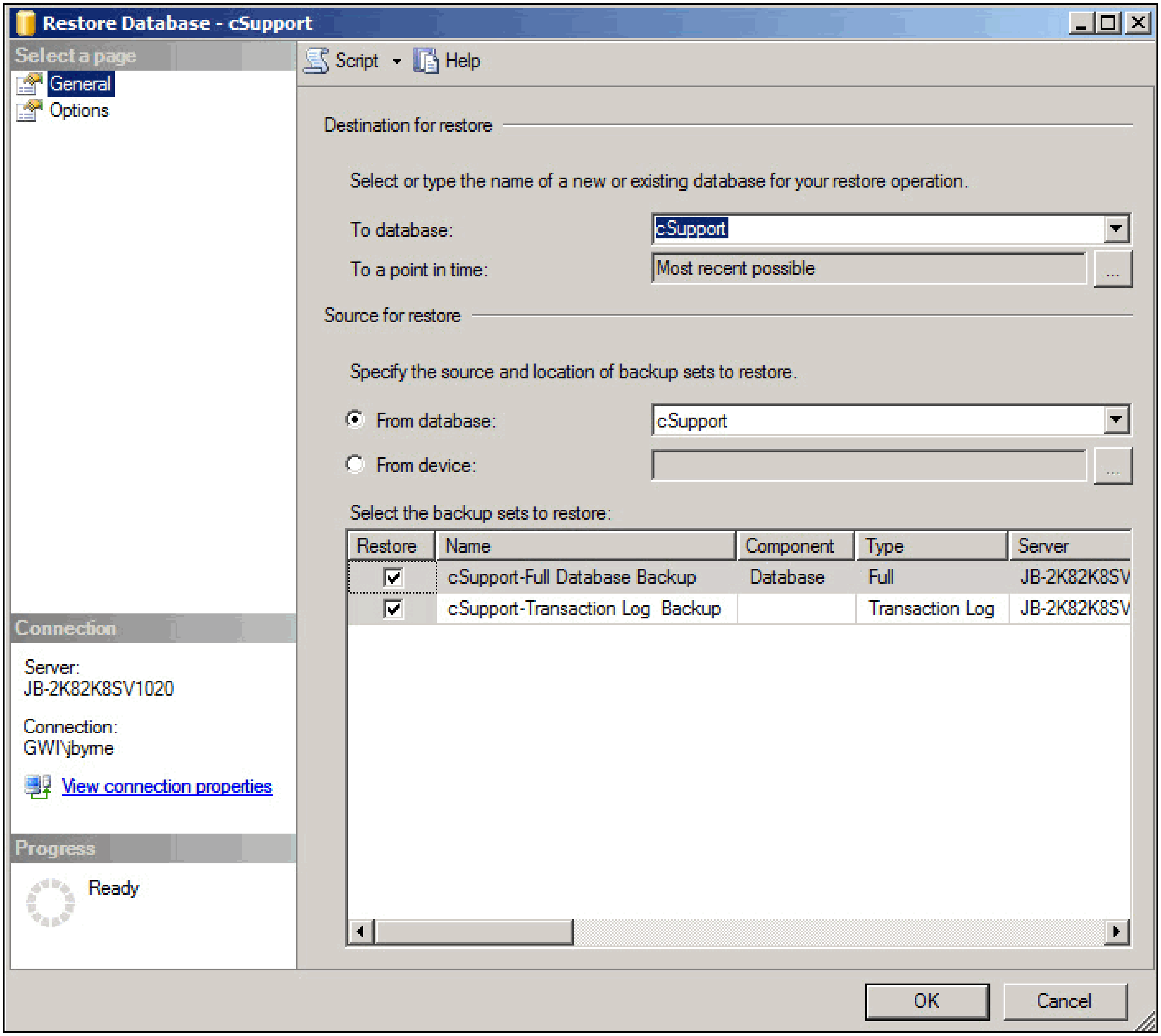
Note: All databases must be online and must have the same iSupport version number.

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.



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: cSupport

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

● From database: cSupport

○ From device:

Select the backup sets to restore:

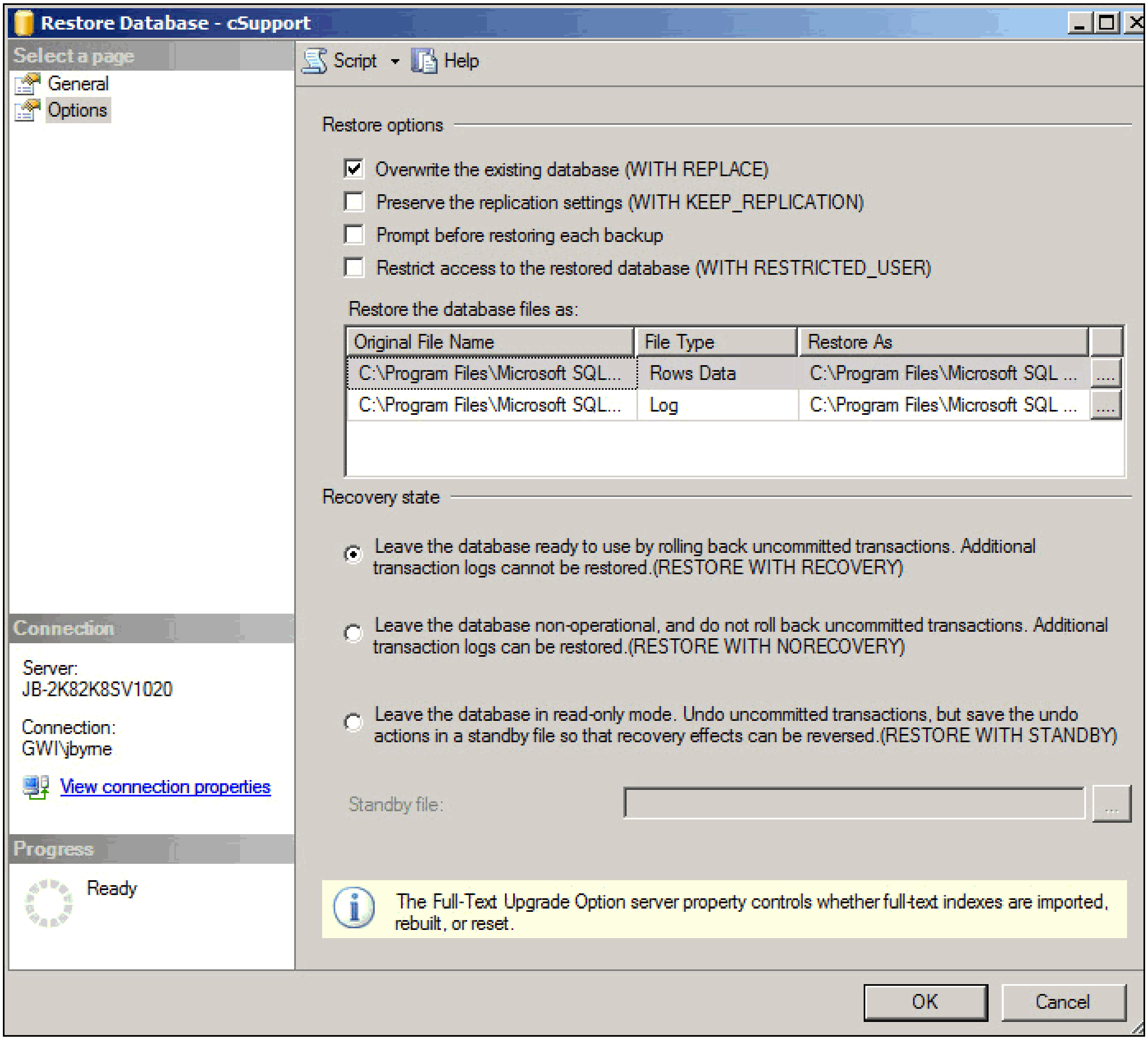
Restore	Name	Component	Type	Server
☑	cSupport-Full Database Backup	Database	Full	JB-2K82K8SV
☑	cSupport-Transaction Log Backup		Transaction Log	JB-2K82K8SV

Server:
JB-2K82K8SV1020

Connection:
GWI\jbyrne

Ready

4 Click Options to go to the Options page.



Restore options

☑ Overwrite the existing database (WITH REPLACE)

□ Preserve the replication settings (WITH KEEP_REPLICATION)

□ Prompt before restoring each backup

□ Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As
C:\Program Files\Microsoft SQL...	Rows Data	C:\Program Files\Microsoft SQL ...
C:\Program Files\Microsoft SQL...	Log	C:\Program Files\Microsoft SQL ...

Recovery state

● Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.(RESTORE WITH RECOVERY)

○ Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored.(RESTORE WITH NORECOVERY)

○ Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reversed.(RESTORE WITH STANDBY)

Standby file:

The Full-Text Upgrade Option server property controls whether full-text indexes are imported, rebuilt, or reset.

Connection

Server:
JB-2K82K8SV1020

Connection:
GWI\jbyrne

View connection properties

Progress

Ready

5 Check the first check box labeled Overwrite the Existing Database (WITH REPLACE).

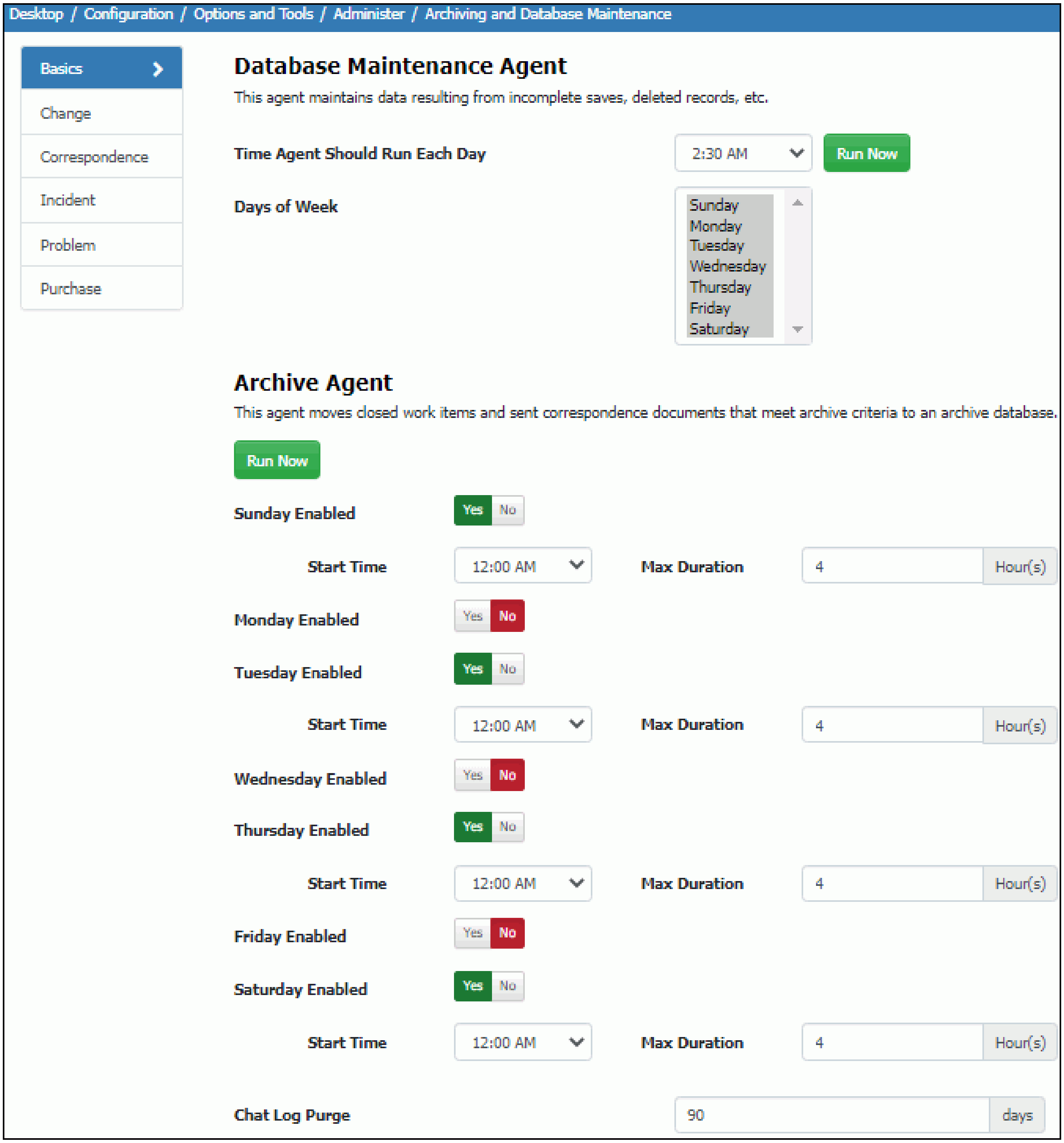
6 In the Restore the Database Files as option is only needed if you are also moving the database files to a new location, or if you are restoring backups from a different SQL Server.

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.

Archiving and Database Maintenance

Use the Options and Tools | Administer | Archiving and Database Maintenance screen to schedule agents that maintain iSupport databases. iSupport's Archive feature moves closed work items with a specified Closed status that are not marked for deletion to archive databases, and purges work items from archive databases. In order for an item to be archived, a specified number of days must have elapsed past the close date. Note that archived items cannot be edited, and support representative roles/permissions can apply to archiving activities.


Desktop / Configuration / Options and Tools / Administer / Archiving and Database Maintenance
Basics
Change
Correspondence
Incident
Problem
Purchase
Run Now
Run Now

Database Maintenance Agent

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

Time Agent Should Run Each Day: 2:30 AM

Days of Week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Archive Agent

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

Sunday Enabled	[✓ Yes] No		
Start Time	12:00 AM	Max Duration	4 Hour(s)
Monday Enabled	Yes [✓ No]		
Tuesday Enabled	[✓ Yes] No		
Start Time	12:00 AM	Max Duration	4 Hour(s)
Wednesday Enabled	Yes [✓ No]		
Thursday Enabled	[✓ Yes] No		
Start Time	12:00 AM	Max Duration	4 Hour(s)
Friday Enabled	Yes [✓ No]		
Saturday Enabled	[✓ Yes] No		
Start Time	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 days of the week and time at which the Database Maintenance agent should run each day.

Setting Time Frame Options for the Archive Agent

Use the settings in the Archive Agent section to set a start time and maximum run duration for each day of the week. Use the Run Now button to initiate the agent immediately; you will be prompted for a maximum runtime. In the Max Duration field, enter the amount of time (in hours) at which to terminate the archive agent if it is still running. This section is useful if you need to run the Archive agent for longer periods of time on weekends, particular days of the week, or times of lighter workloads.

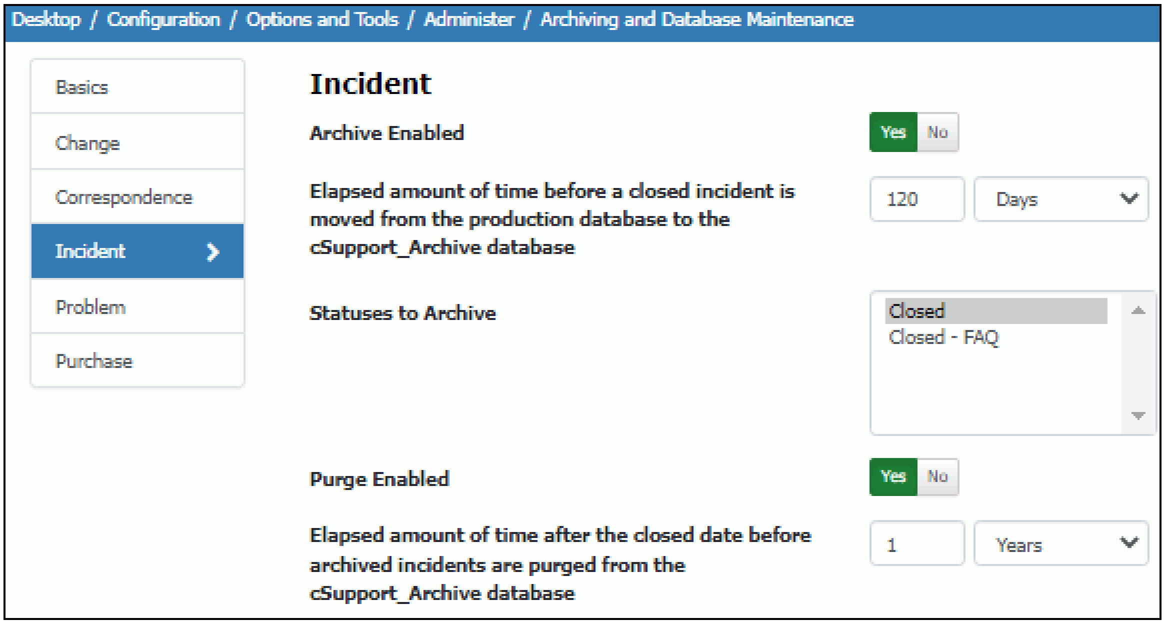
The Archive agent will do the following:

- 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.

When a customer request a chat, request details are logged; this log is available through the mySupport Chat Request view source in the View Designer.You can use the **Chat Log Purge** field to enter the number of days after which entries in the chat log will be deleted automatically by the Database Maintenance agent. Note that the Enable Features tab in the Core Settings | Feature Basics screen includes this field as well.

Setting Archive Options for Work Item Types

For each work item type, use the following fields to enable archiving, specify the status and elapsed amount of time before of items to archive, eligible for archiving or purging (which permanently deletes items from the applicable archive database after the specified number of days/years past the archive date).


Desktop / Configuration / Options and Tools / Administer / Archiving and Database Maintenance
Basics
Change
Correspondence
Incident
Problem
Purchase

Incident

Archive Enabled: Yes

Elapsed amount of time before a closed incident is moved from the production database to the cSupport_Archive database: 120 Days

Statuses to Archive: Closed; Closed - FAQ

Purge Enabled: Yes

Elapsed amount of time after the closed date before archived incidents are purged from the cSupport_Archive database: 1 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.

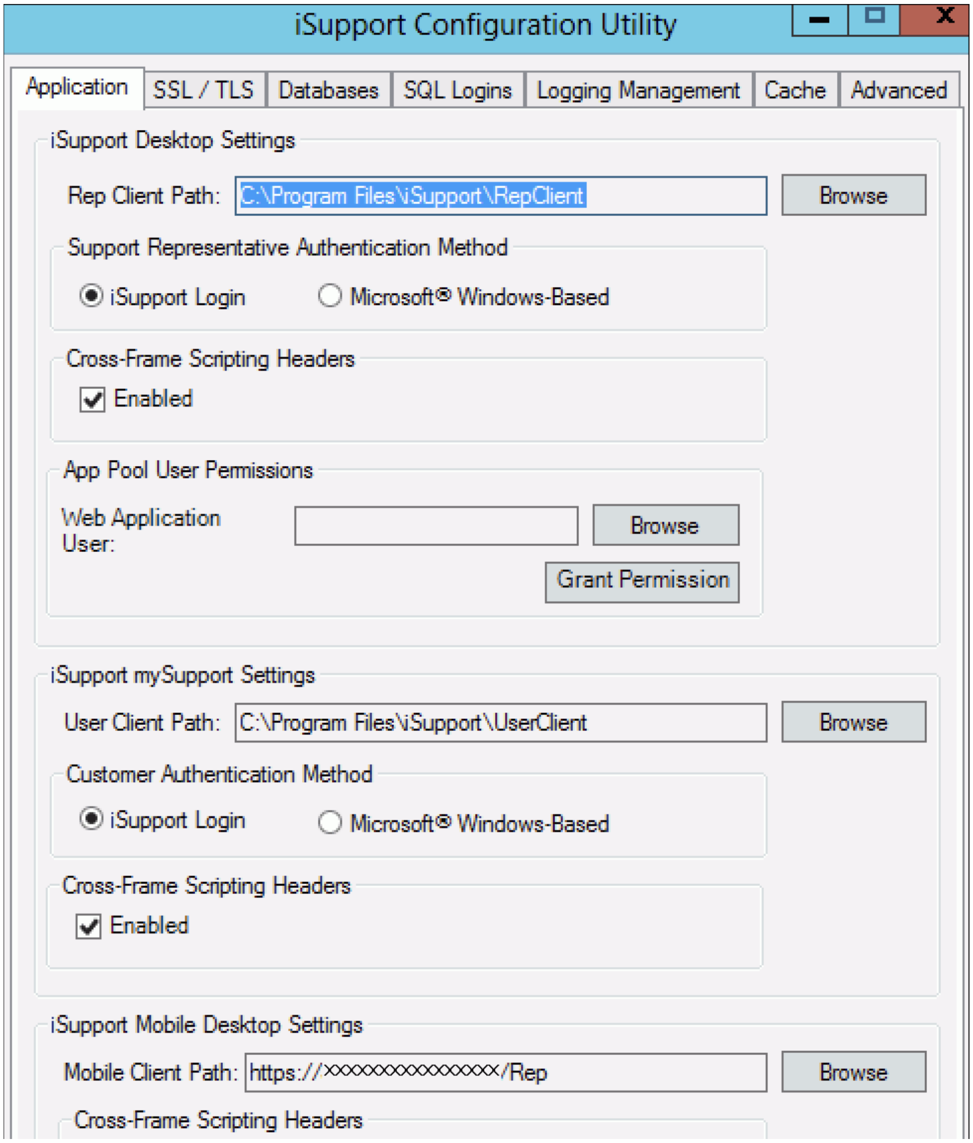
Statuses to Archive - Select one or more of the defined Closed statuses that will determine items eligible for archiving.

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.

Performing Advanced Configuration Tasks via the iSupport Configuration Utility

The iSupport Configuration Utility is used to perform advanced configuration tasks. It is located in the <*directory in which iSupport is installed*>\Utilities folder.

- Use the fields on the Application tab to select your authentication method for the Desktop and mySupport portals; iSupport Login is the default method. You can also enable/disable cross-frame scripting headers; to improve security, cross-frame scripting headers were added to the Rep, Mobile, and mySupport interfaces for new installs and upgrades. We recommend that you enable cross-frame scripting headers via the Application tab in the iSupport Configuration Utility after upgrading to v17.5. If you do load the Rep, Mobile, or mySupport interfaces from within an iFrame or you use the External mySupport Chat feature, you will need to add the site URLs for the interface (or from which external mySupport chat has been integrated) into the Approved Sites list.



iSupport Desktop Settings

Rep Client Path: C:\Program Files\iSupport\RepClient

Support Representative Authentication Method

● iSupport Login ○ Microsoft® Windows-Based

Cross-Frame Scripting Headers

☑ Enabled

App Pool User Permissions

Web Application User:

iSupport mySupport Settings

User Client Path: C:\Program Files\iSupport\UserClient

Customer Authentication Method

● iSupport Login ○ Microsoft® Windows-Based

Cross-Frame Scripting Headers

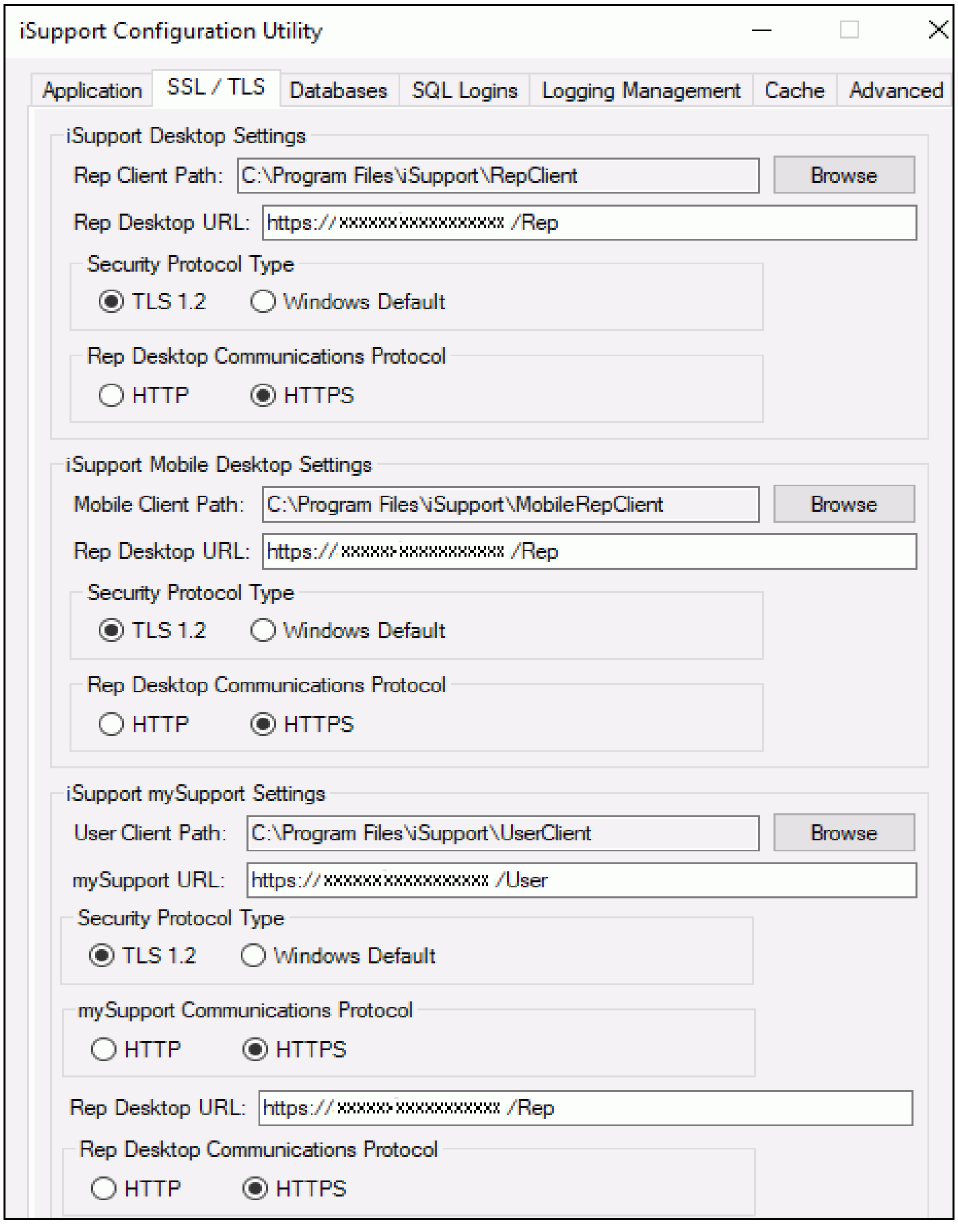
☑ Enabled

iSupport Mobile Desktop Settings

Mobile Client Path: https://xxxxxxxxxxxxxxxx/Rep

Cross-Frame Scripting Headers

- If you wish to use SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt all communications between your browser and an iSupport site via an HTTPS (the secure version of HTTP) connection, use the settings on the SSL/TLS tab. Note that IIS must be configured and a cert must be applied before making changes to these settings.



iSupport Desktop Settings

Rep Client Path: C:\Program Files\iSupport\RepClient [Browse]

Rep Desktop URL: https://xxxxxxxxxxxxxxxxxx /Rep

Security Protocol Type: ● TLS 1.2 ○ Windows Default

Rep Desktop Communications Protocol: ○ HTTP ● HTTPS

iSupport Mobile Desktop Settings

Mobile Client Path: C:\Program Files\iSupport\MobileRepClient [Browse]

Rep Desktop URL: https://xxxxxx xxxxxxxxxxxx /Rep

Security Protocol Type: ● TLS 1.2 ○ Windows Default

Rep Desktop Communications Protocol: ○ HTTP ● HTTPS

iSupport mySupport Settings

User Client Path: C:\Program Files\iSupport\UserClient [Browse]

mySupport URL: https://xxxxxxxxxxxxxxxxxx /User

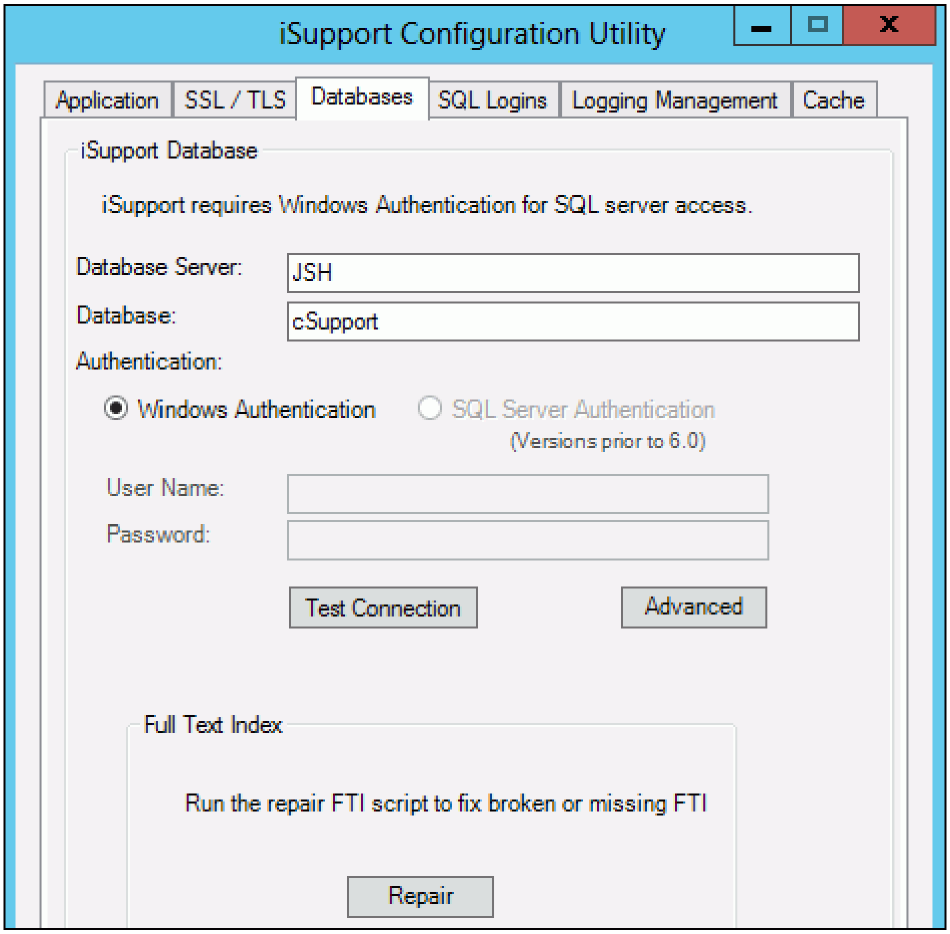
Security Protocol Type: ● TLS 1.2 ○ Windows Default

mySupport Communications Protocol: ○ HTTP ● HTTPS

Rep Desktop URL: https://xxxxxx xxxxxxxxxxxx /Rep

Rep Desktop Communications Protocol: ○ HTTP ● HTTPS

- Use the fields on the **Databases tab** to modify the SQL database, database server, and SQL login to the iSupport databases. The installation process initially populates these fields. Use the Repair button in the Full Text Index field under direction of iSupport Technical Support.



iSupport requires Windows Authentication for SQL server access.

Database Server: JSH

Database: cSupport

Authentication:

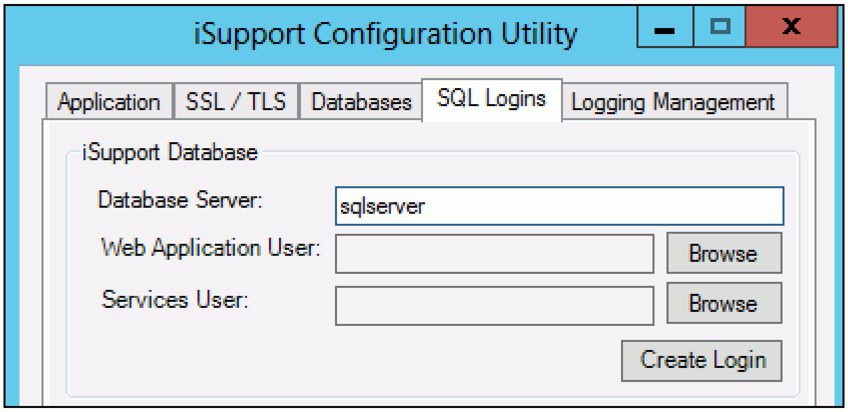
● Windows Authentication ○ SQL Server Authentication (Versions prior to 6.0)

User Name:

Password:

Run the repair FTI script to fix broken or missing FTI

- You can use the **SQL Logins tab** to create and set the proper db_owner permissions on the iSupport databases for the selected users in SQL. This requires SA access to the databases.

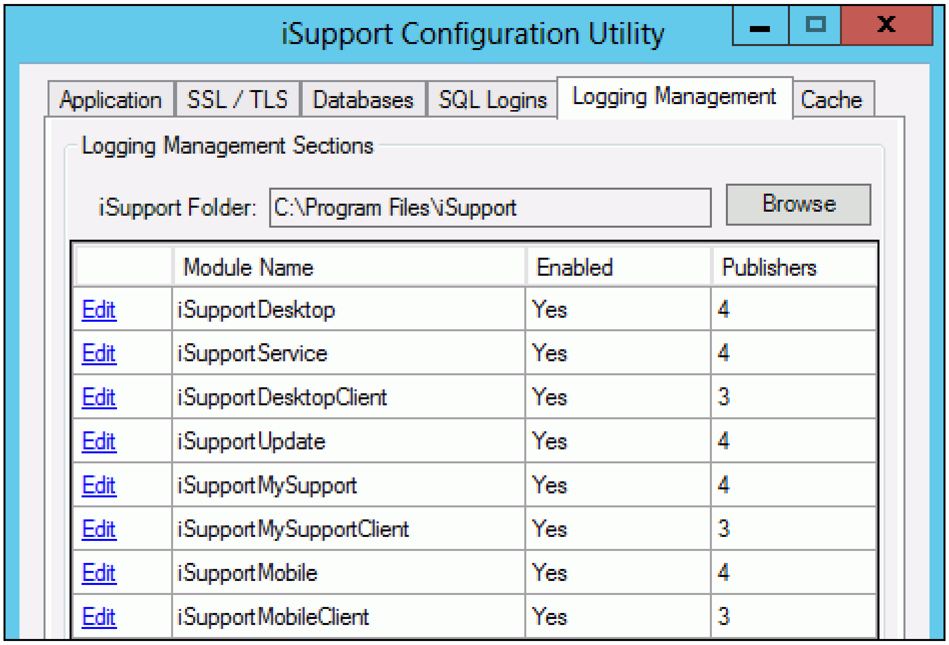


Database Server: sqlserver

Web Application User:

Services User:

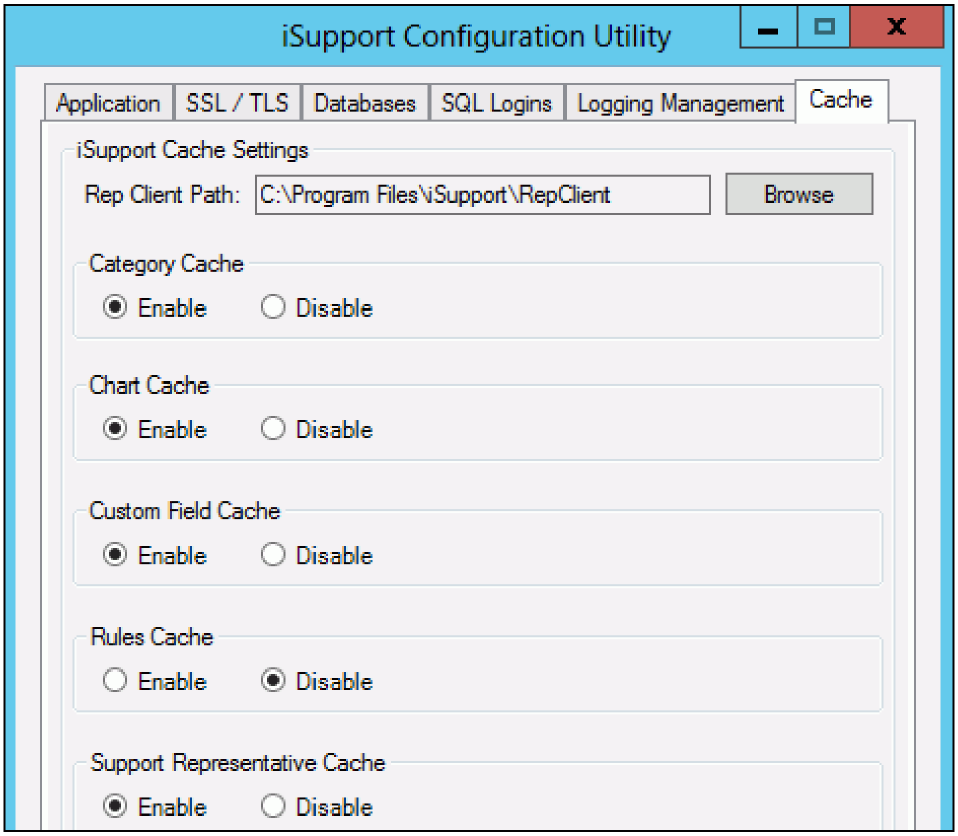
- You can use the **Logging Management tab** in the iSupport Configuration Utility to change variables to enable or disable logging to the SQL database on which iSupport is installed and the Windows Event Viewer, and specify the types of messages that are logged.



iSupport Folder: C:\Program Files\iSupport

	Module Name	Enabled	Publishers
Edit	iSupportDesktop	Yes	4
Edit	iSupportService	Yes	4
Edit	iSupportDesktopClient	Yes	3
Edit	iSupportUpdate	Yes	4
Edit	iSupportMySupport	Yes	4
Edit	iSupportMySupportClient	Yes	3
Edit	iSupportMobile	Yes	4
Edit	iSupportMobileClient	Yes	3

- The settings on the **Cache tab** are used when troubleshooting performance issues and display of categories, charts, custom fields, etc.



Rep Client Path: C:\Program Files\iSupport\RepClient

Category Cache
● Enable ○ Disable

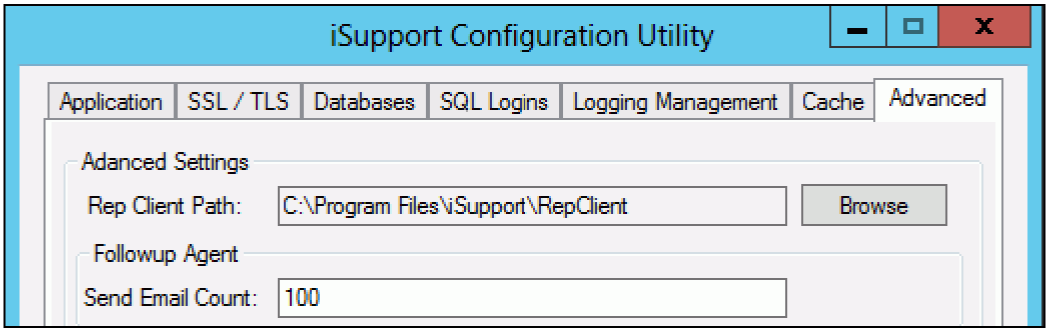
Chart Cache
● Enable ○ Disable

Custom Field Cache
● Enable ○ Disable

Rules Cache
○ Enable ● Disable

Support Representative Cache
● Enable ○ Disable

- Miscellaneous settings are included on the **Advanced tab**; all should be changed **only** under direction from iSupport Technical Support.



Adanced Settings

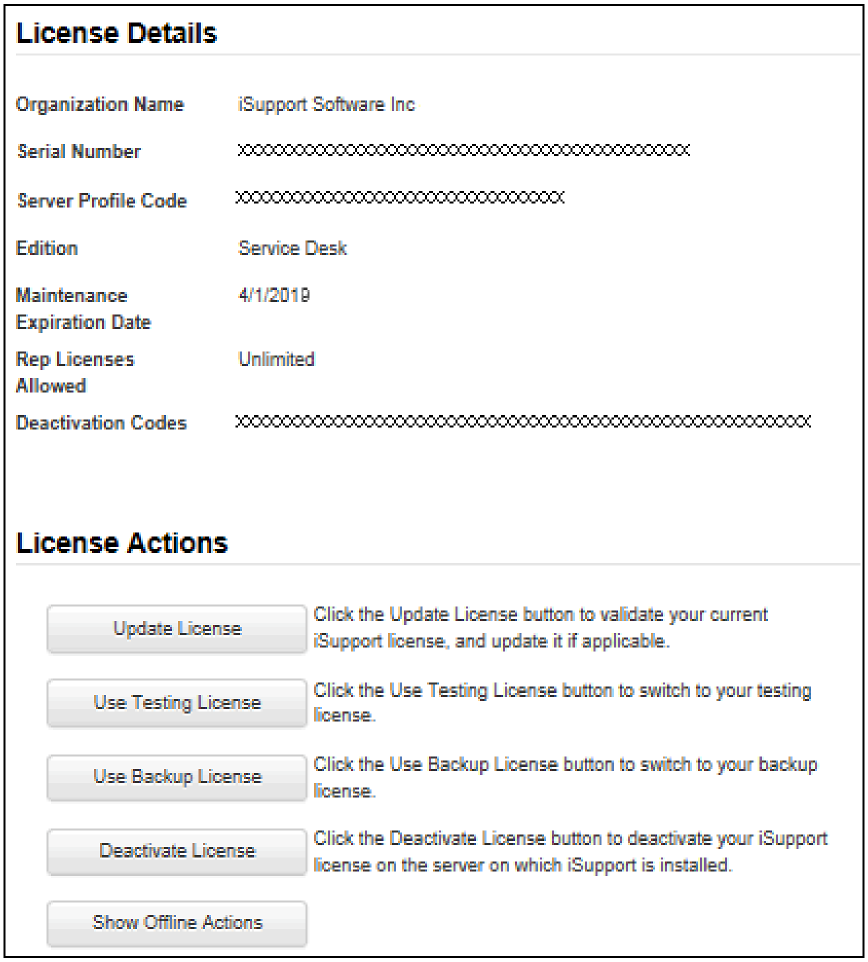
Rep Client Path: C:\Program Files\iSupport\RepClient

Followup Agent

Send Email Count: 100

Managing Your iSupport License

Use the Options and Tools| Administer | iSupport License Management screen to administer the license for your iSupport application. Note that there are three types of licenses: production, test, and backup. If your server is connected to the Internet, it will automatically validate your software and server configuration. If you are not connected to the Internet, you will be prompted for serial numbers and activation codes. These can be obtained by contacting iSupport Software Technical Support at 360.397.1099 or support@iSupport.com.



License Details

Organization Name	iSupport Software Inc
Serial Number	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Server Profile Code	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Edition	Service Desk
Maintenance Expiration Date	4/1/2019
Rep Licenses Allowed	Unlimited
Deactivation Codes	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

License Actions

Click the Update License button to validate your current iSupport license, and update it if applicable.

Click the Use Testing License button to switch to your testing license.

Click the Use Backup License button to switch to your backup license.

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

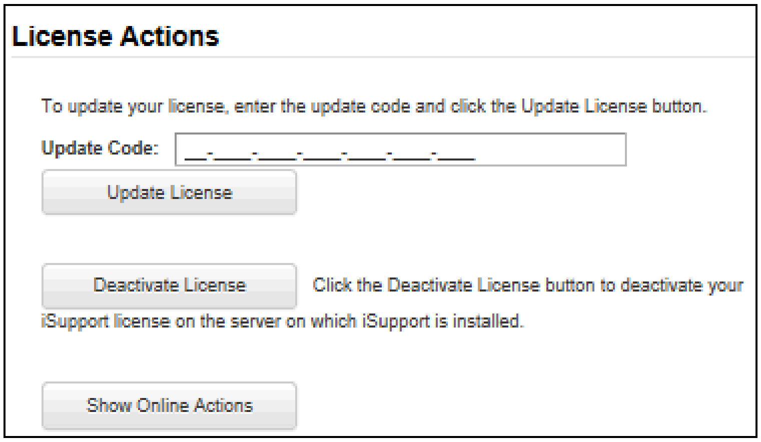
In the License Actions section:

- Use the **Update License** button to perform an immediate check to ensure that the software is running on the latest license parameters. The iSupport Installation will contact iSupport Software and acquire relevant information. This is typically done after purchasing additional iSupport support representative logins; you can use the additional logins after clicking this button to update your current license.
- Use the **Use Testing License** button to convert your installation license from a production license to a limited test license. This is typically done before installing iSupport onto a test server. After clicking this button, the button changes to Use Production License so you can convert the limited test license back to a production license.
- Click the **Use Backup License** button if you are using a disaster recovery or standby system. This is typically used for installation of iSupport onto a backup server.
- Use the **Deactivate License** button if the server is connected to the Internet and you are about to:
  - Uninstall iSupport
  - Decommission the server on which iSupport is installed
  - Make any changes to the server that will affect server profile code (for example, upgrading memory, increasing the number of processors, adding a new hard drive, swapping to a new hosting hard drive on a virtual server, or reinstalling iSupport onto a different server)

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

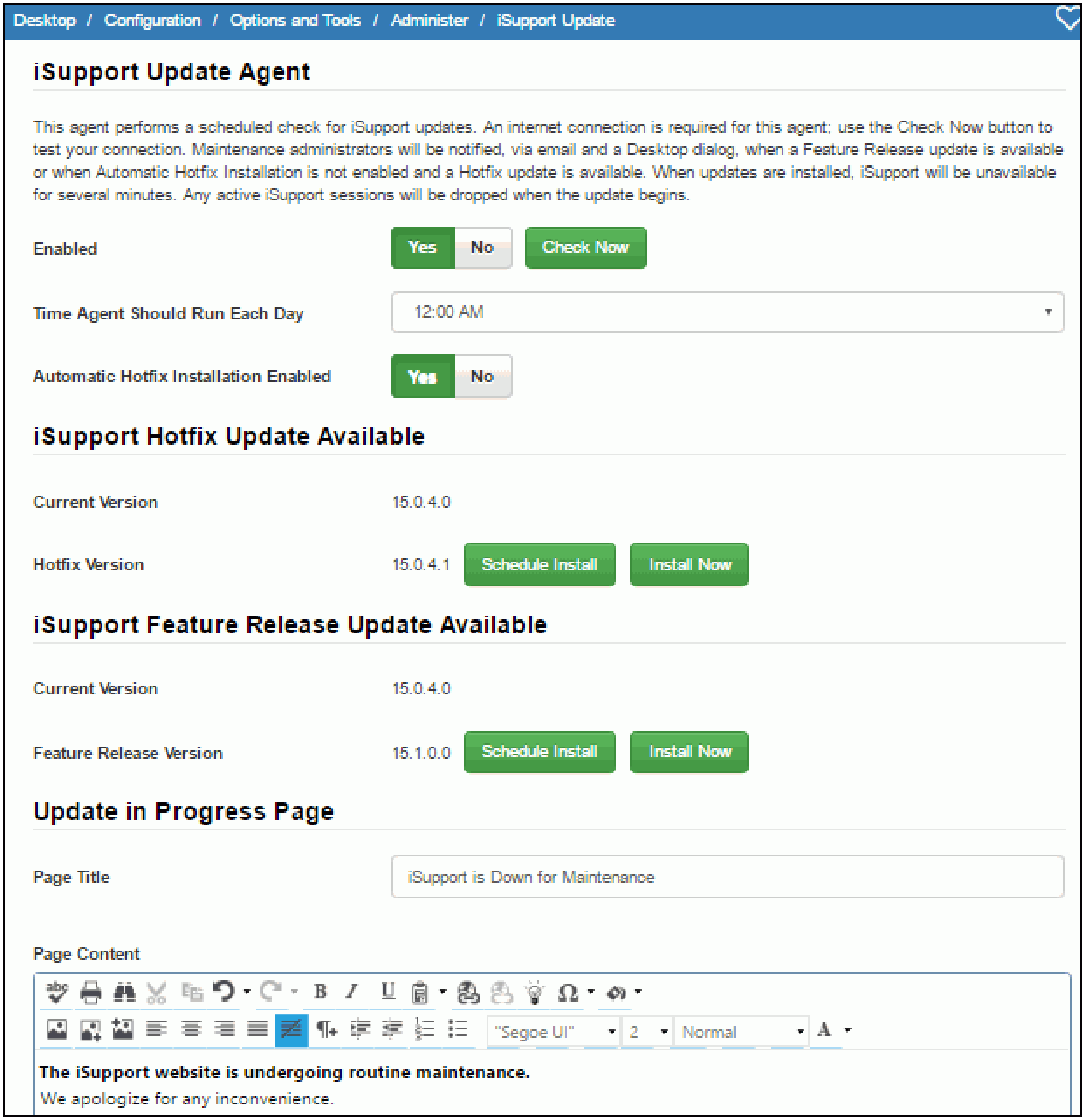
To update your license, enter the update code and click the Update License button.

Update Code: __-____-____-____-____-____-____

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

Enabling iSupport Updates

The iSupport Update agent performs a scheduled check for Feature Release and Hotfix updates to iSupport and notifies support representatives designated as Maintenance Administrators via email and a Desktop dialog when a Feature Release update is available. Use the Options and Tools | Administer | iSupport Update screen to enable and schedule this agent, enable automatic installation of Hotfix updates, schedule and install any available Hotfix and Feature Release updates, and configure the page that will appear when someone tries to access iSupport while an update is occurring.



Desktop / Configuration / Options and Tools / Administer / iSupport Update

iSupport Update Agent

This agent performs a scheduled check for iSupport updates. An internet connection is required for this agent; use the Check Now button to test your connection. Maintenance administrators will be notified, via email and a Desktop dialog, when a Feature Release update is available or when Automatic Hotfix Installation is not enabled and a Hotfix update is available. 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 — Check Now

Time Agent Should Run Each Day: 12:00 AM

Automatic Hotfix Installation Enabled: [✓ Yes] No

iSupport Hotfix Update Available

Current Version: 15.0.4.0

Hotfix Version: 15.0.4.1 — Schedule Install — Install Now

iSupport Feature Release Update Available

Current Version: 15.0.4.0

Feature Release Version: 15.1.0.0 — Schedule Install — Install Now

Update in Progress Page

Page Title: iSupport is Down for Maintenance

Page Content

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

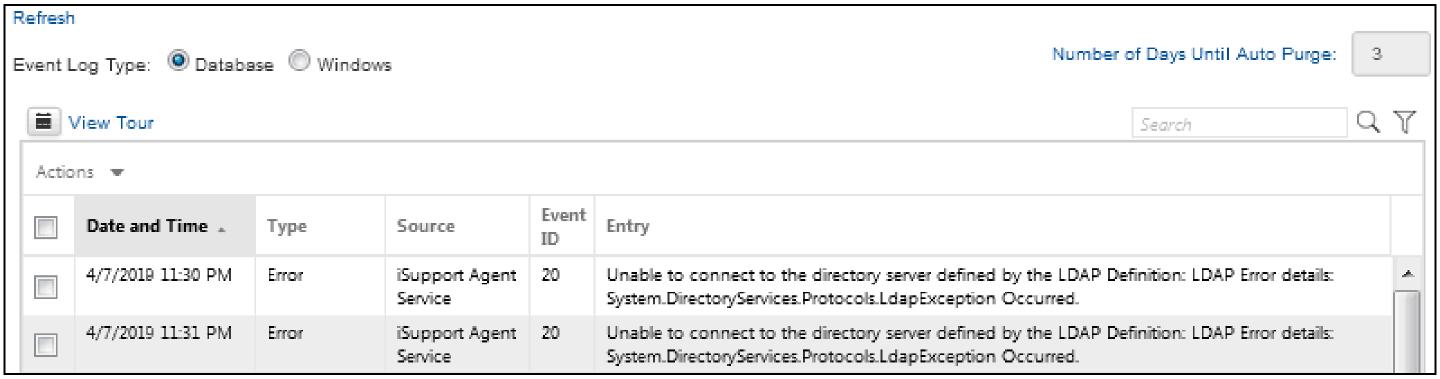
Select Yes in the Enabled field to enable an automatic search for Feature Release and Hotfix updates, and then select the time at which the agent should run each day. You can click the Check Now button to immediately perform a one-time search for an available Feature Release or Hotfix update; if found, the iSupport Hotfix Update Available and/or iSupport Feature Release Update Available sections will appear with the version numbers, a button to install the update immediately, and a button to display a dialog for scheduling the update installation.

The Automatic Hotfix Installation Enabled field will appear if the iSupport Update Agent is enabled; select Yes to automatically install any available Hotfix update. If you select No in this field, support representatives designated as Maintenance Administrators will be notified via email and a Desktop dialog when a hotfix is available.

Note that any active iSupport sessions will be dropped when the update begins, iSupport will be unavailable for several minutes while updates are installed. 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.

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.



Refresh

Event Log Type: ● Database ○ Windows

Number of Days Until Auto Purge: 3

View Tour

Search

Actions

□	Date and Time	Type	Source	Event ID	Entry
□	4/7/2019 11:30 PM	Error	iSupport Agent Service	20	Unable to connect to the directory server defined by the LDAP Definition: LDAP Error details: System.DirectoryServices.Protocols.LdapException Occurred.
□	4/7/2019 11:31 PM	Error	iSupport Agent Service	20	Unable to connect to the directory server defined by the LDAP Definition: LDAP Error details: System.DirectoryServices.Protocols.LdapException Occurred.

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 57 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.

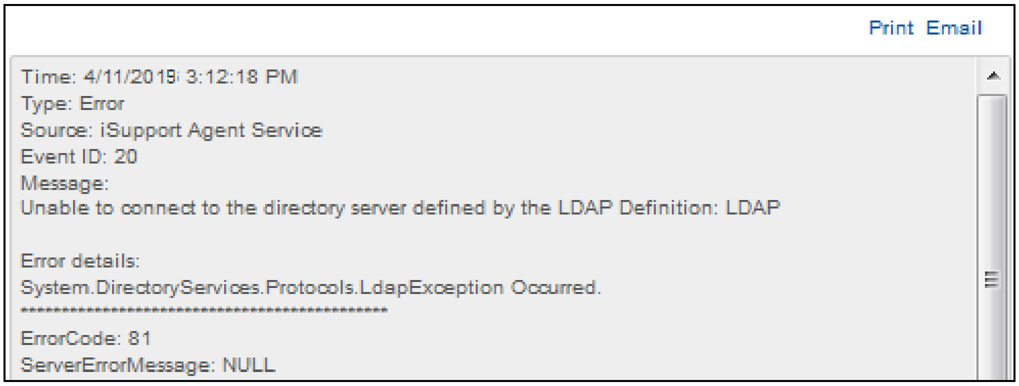
Database Logging Options

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 select 🔍 Quick Search. You can search for an incident number in an incident view, even if it doesn't exist in a displayed column.

Select ▼ **Advanced** Search 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 options to display and remove a *<field> <comparison method> <value>* search condition. Select ⊕ Add Condition 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. ★ Saved Searches 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 option 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.

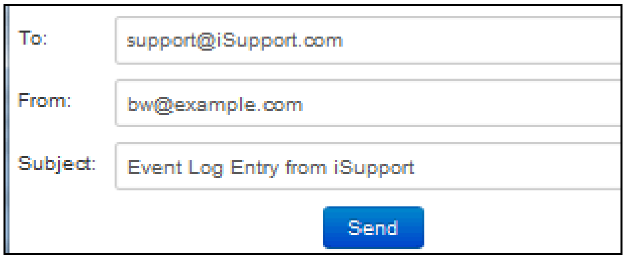
You can **export view data** in Microsoft® Excel (*.xls) format, Microsoft® Word (*.doc) format, Portable Document Format (*.pdf), or Comma Separated Value Format (*.csv). Comma Separated Value Format is usable with Microsoft Excel and other third party tools. Use the Export option on the Actions menu 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. 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.



```
Time: 4/11/2019 3:12:18 PM
Type: Error
Source: iSupport Agent Service
Event ID: 20
Message:
Unable to connect to the directory server defined by the LDAP Definition: LDAP

Error details:
System.DirectoryServices.Protocols.LdapException Occurred.
**************************************************
ErrorCode: 81
ServerErrorMessage: NULL
```

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.



To: support@iSupport.com

From: bw@example.com

Subject: Event Log Entry from iSupport

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	• Creates or updates an incident for each message. • Processes defined rules. • Creates a customer profile for each new customer.

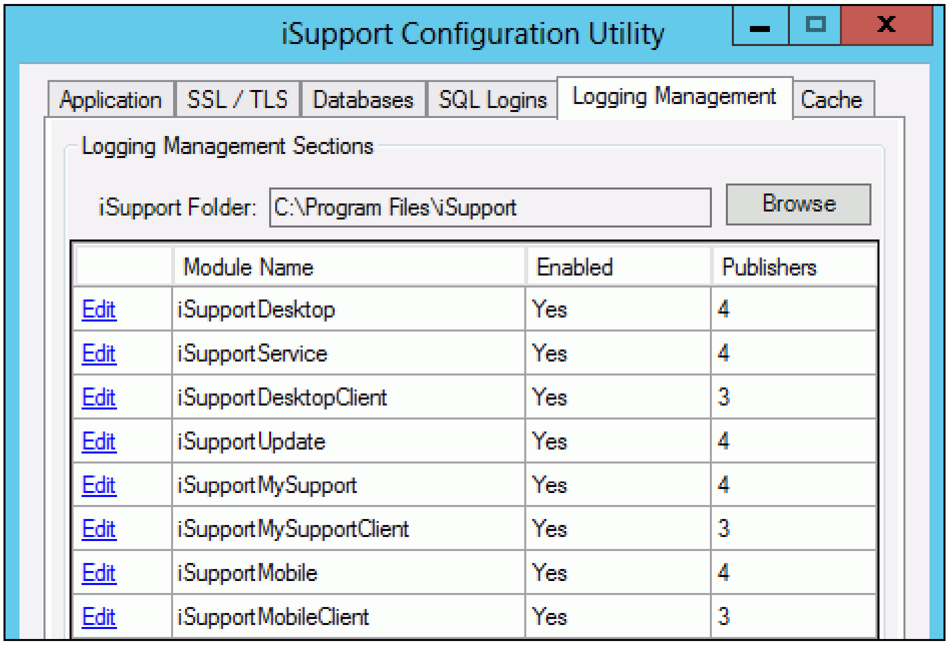
Event ID	Agent	Agent Description
8	Followup Reminder Agent	Checks all incident followup dates; sends email reminders to the incident assignees for all incidents with an expired followup date and a status other than Closed.
9	Database Maintenance Agent	Maintains data resulting from incomplete saves, deleted 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, 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.

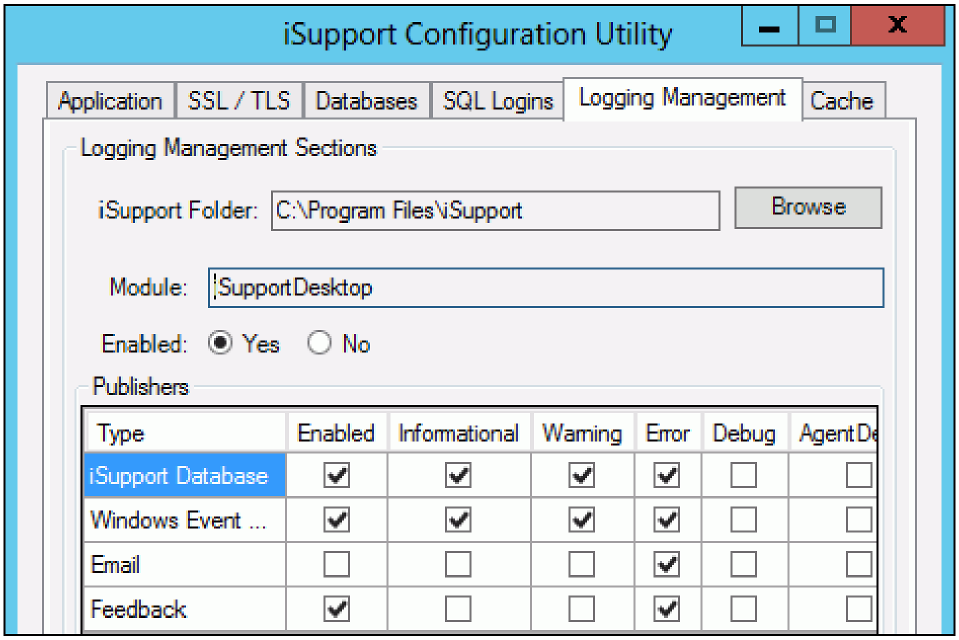
You can use the iSupport Configuration Utility to change variables to enable or disable logging to the SQL database on which iSupport is installed and the Windows Event Viewer, and specify the types of messages that are logged. The iSupport Configuration Utility is located in the <*directory in which 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.



iSupport Folder: C:\Program Files\iSupport

	Module Name	Enabled	Publishers
Edit	iSupportDesktop	Yes	4
Edit	iSupportService	Yes	4
Edit	iSupportDesktopClient	Yes	3
Edit	iSupportUpdate	Yes	4
Edit	iSupportMySupport	Yes	4
Edit	iSupportMySupportClient	Yes	3
Edit	iSupportMobile	Yes	4
Edit	iSupportMobileClient	Yes	3

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



Logging Management Sections

iSupport Folder: C:\Program Files\iSupport

Module: SupportDesktop

Enabled: ● Yes ○ No

Publishers

Type	Enabled	Informational	Warning	Error	Debug	Agent De
iSupport Database	☑	☑	☑	☑	□	□
Windows Event ...	☑	☑	☑	☑	□	□
Email	□	□	□	☑	□	□
Feedback	☑	□	□	☑	□	□

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 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 is installed (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="GWICommon" 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:

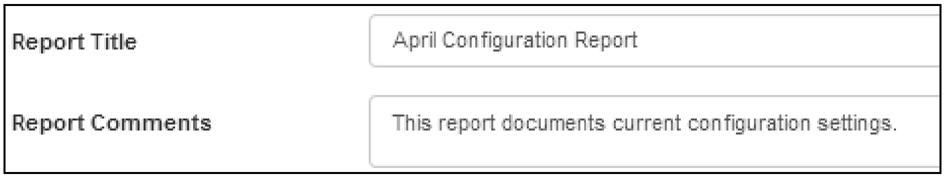
```
 <publisher mode="on" assembly="GWICommon" type="Gwi.LoggingManagement.SmtpEmailPublisher"
smtpServer="mailserver" emailFromAddress="fromAddress" emailToAddress="toAddress"
emailSubject="iSupport Desktop" includeServerNameInSubject="true" includeFirstLineInSubject="true"
supportedLogLevels="*" emailPriority="high"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

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.

Performance Best Practices and Recommendations

The response time you experience is dependent on hundreds, if not thousands, of many very small factors that can compound and cumulatively impact the perception of performance.

Here's how it works behind the scenes. Starting with your local computer, factors include speed and memory, other software running, and security and virus programs monitoring the system to make you safe. The data then exits through your network connection, wired or wirelessly through a switch or collection of switches (usually through a router), and then through some more switches onto the server which is hosting the Microsoft Internet Information Services (IIS) where the iSupport web presence resides.

All of that might be wrapped in a protective Secured Sockets Layer (SSL) which must be encrypted and decrypted with authentication checked. The IIS server may be dedicated to iSupport, or it may also serve other programs and applications...each vying for processor time and memory allocation. That server might be a virtual server that is residing on a virtual host whose processors are supporting not only the virtualizing software, but all the other processor and memory demands of the systems it hosts. The iSupport web code then authenticates and communicates with the collection of iSupport databases stored on the Microsoft SQL server. This SQL server also resides on a Windows server; it could be co-located with the IIS server, dedicated, or otherwise hosted or virtualized.

Configuration choices also come into play. After authentication, numerous items are checked: support representative permissions, customer and their other requests, customer's group, company, service contract, custom fields, selected category and any associated custom fields, conditional custom fields, priority, urgency, and impact. Rules are evaluated and applied. Individual data variations are considered, compared, looked up, and analyzed every time...and the data is then persisted. The process then repeats, in reverse, back to your local computer where the HTML web page and its containing data is then extracted and presented by the browser which is monitoring content and checking it for external suggested content. We are touching on some of the highlights here; the set of processes in your environment may vary.

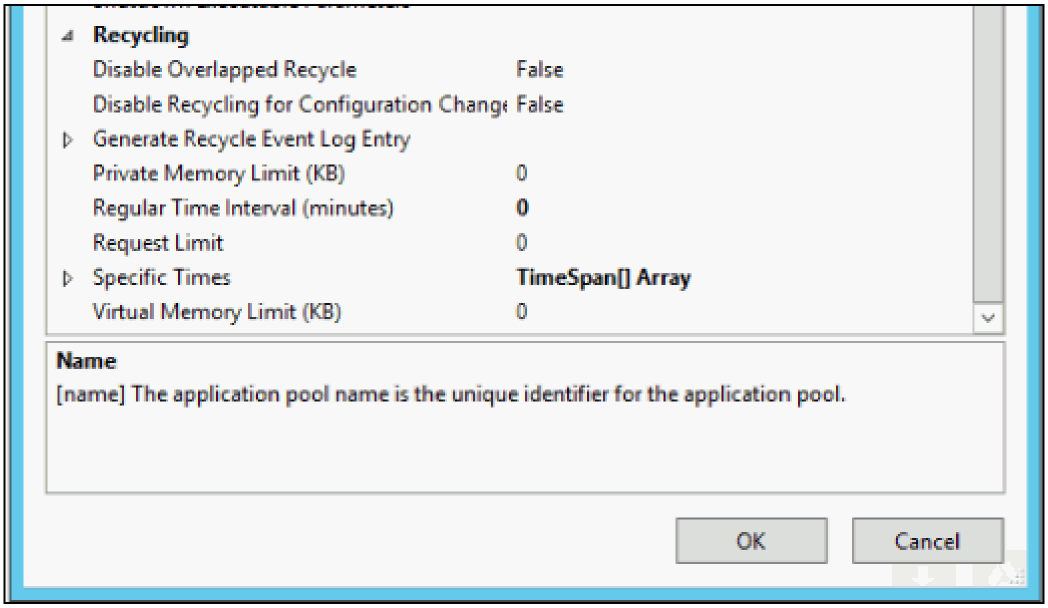
Typically each program, application, and website has its own unique set of challenges...and even though many of the factors are the same, there is rarely a fair comparison between two products, applications, services, etc. Ultimately it’s always matter of trade-offs: the power and dedication of the computing environment, security standards, network traffic, local computer, iSupport configuration selections, etc. All of these choices and more cumulatively impact perceived performance and must be considered to find the right balance for your environment.

The following recommendations from our Technical Support department can help to increase performance in your environment.

Environment

- Use the most current version of iSupport as we are constantly working to improve performance.
- Co-locate the iSupport Web Server (IIS) and the SQL Server on the same server; the key reason for this is so that you can use local accounts for your iSupport application pool account and your iSupport service account. This will minimize network traffic and load on your Active Directory servers, and may improve security as the credentials are only valid on the server.
- Verify that the following are set in the Advanced Settings for the iSupport application pool:
  - Process Model
  - Idle-Timeout (minutes) - 0
  - Maximum Worker Process - 1

- Match the following for the Recycling settings:



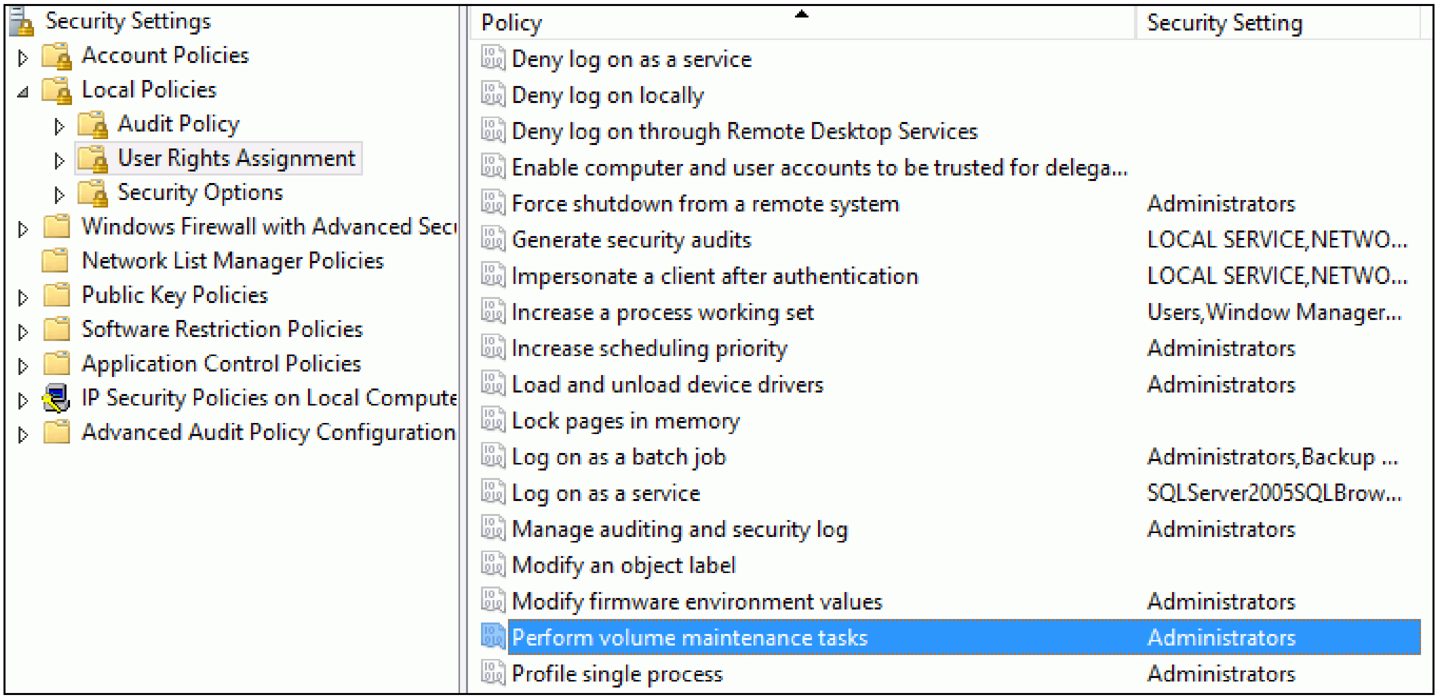
Recycling

Disable Overlapped Recycle	False
Disable Recycling for Configuration Chang	False
Generate Recycle Event Log Entry	
Private Memory Limit (KB)	0
Regular Time Interval (minutes)	**0**
Request Limit	0
Specific Times	**TimeSpan[] Array**
Virtual Memory Limit (KB)	0

Name

[name] The application pool name is the unique identifier for the application pool.

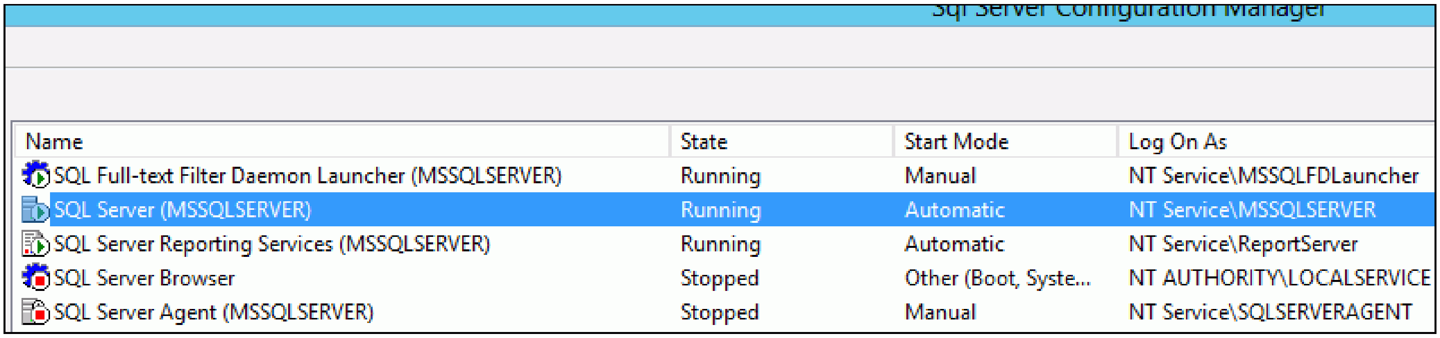
- Disable the Enable 32-Bit Applications setting for the application pool associated with iSupport.
- Use a dedicated server for iSupport rather than a virtual machine. If you must run on a virtual machine environment, the memory must be allocated and reserved (not configured to be used on demand). Do not rely on recommendations from optimization utilities.
- Enable instant file initialization. In the Security Policies Windows component (from Run, type secpol.msc), open Local Policies – User Rights Assignment and edit the Perform Volume Maintenance Tasks properties.



Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be trusted for delega...	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWO...
Impersonate a client after authentication	LOCAL SERVICE,NETWO...
Increase a process working set	Users,Window Manager...
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators,Backup ...
Log on as a service	SQLServer2005SQLBrow...
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators

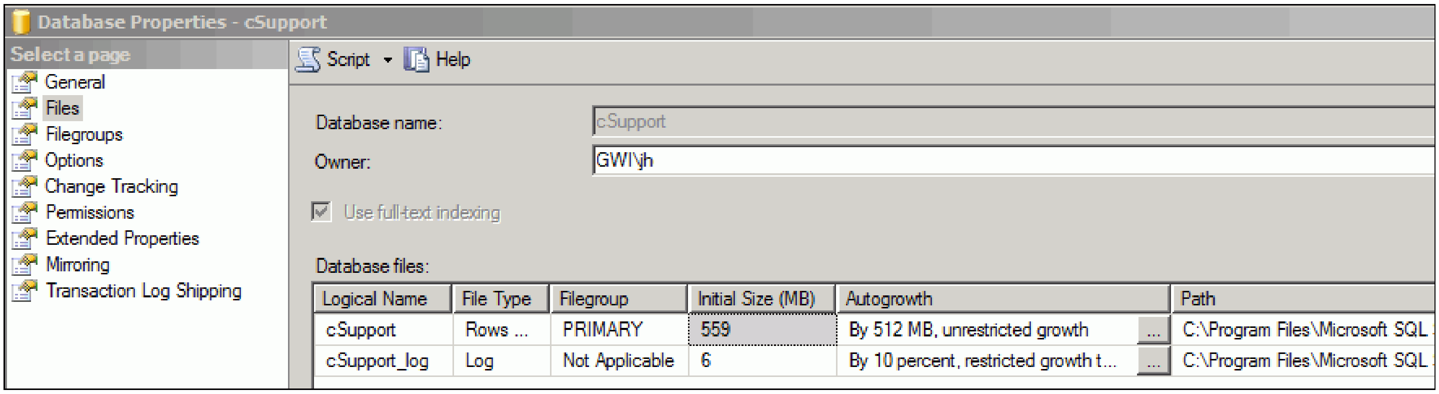
Add your SQL service, iSupport service, and iSupport application pool accounts to this policy (unless you SQL account is already part of a group that has access to it). If you are not sure of your account, verify it by going to SQL Server Configuration Manager and check the Log On As column.



Sql Server Configuration Manager

Name	State	Start Mode	Log On As
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Running	Manual	NT Service\MSSQLFDLauncher
SQL Server (MSSQLSERVER)	Running	Automatic	NT Service\MSSQLSERVER
SQL Server Reporting Services (MSSQLSERVER)	Running	Automatic	NT Service\ReportServer
SQL Server Browser	Stopped	Other (Boot, Syste...	NT AUTHORITY\LOCALSERVICE
SQL Server Agent (MSSQLSERVER)	Stopped	Manual	NT Service\SQLSERVERAGENT

- Tune the automatic growth of the log files via the properties of the cSupport database. For databases under 1GB, set it to between 20MB and 100MB. For databases in the GB sizes, set it to between 500MB and 1GB. Create only one transaction log file.



Database Properties - cSupport

Database name: cSupport

Owner: GWI\jh

☑ Use full-text indexing

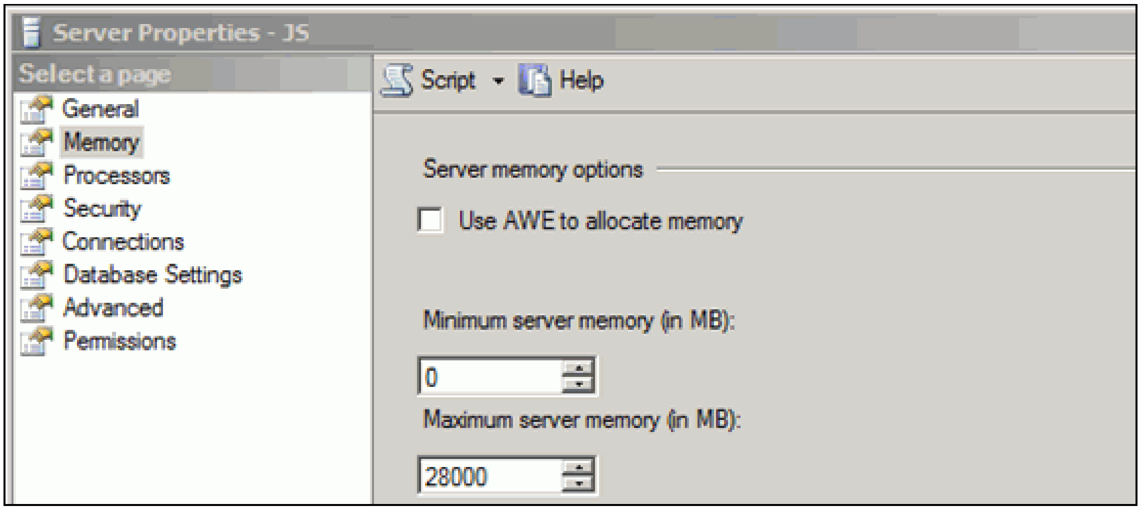
Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth		Path
cSupport	Rows ...	PRIMARY	559	By 512 MB, unrestricted growth	...	C:\Program Files\Microsoft SQL
cSupport_log	Log	Not Applicable	6	By 10 percent, restricted growth t...	...	C:\Program Files\Microsoft SQL

- Use at least three hard drives: one for the operating system, one for your MDF files, and one for your LDF files. (The Temp database should not be on an operating system drive.) Your Temp tables and databases should be pointing to the locations of the MDF and LDF files (which are the storage/log files of your SQL databases). A fast drive (for example, an SSD drive) is preferable for the Temp and cSupport databases. Network drives are not recommended.

- Include more than one processor on the machine; four is desired. Provide enough memory and processor power to handle the load. As a rule of thumb, use the sum of the size of all of your iSupport databases plus another 8-16 GB of ram for your operating system and IIS. Take into consideration how fast your databases are growing as well; for example, if you have had iSupport for four years and the size of your iSupport databases is currently 40GB, it averages to approximately 10GB per year. The recommended maximum SQL memory size would be 50GB, and when you add memory for the operating system the final system recommendation would be 64GB of memory.

- Set the attributes for maximum server memory (in MB) on the SQL Server. (This value should be at least 4GB less than maximum operating system memory; for example, if your server has 32GB of physical memory, you would set this attribute to 28GB. The reason for this is that SQL will consume all available memory, so we are reserving the minimum memory required for the operating system to continue functioning.



□ Use AWE to allocate memory

Minimum server memory (in MB): 0

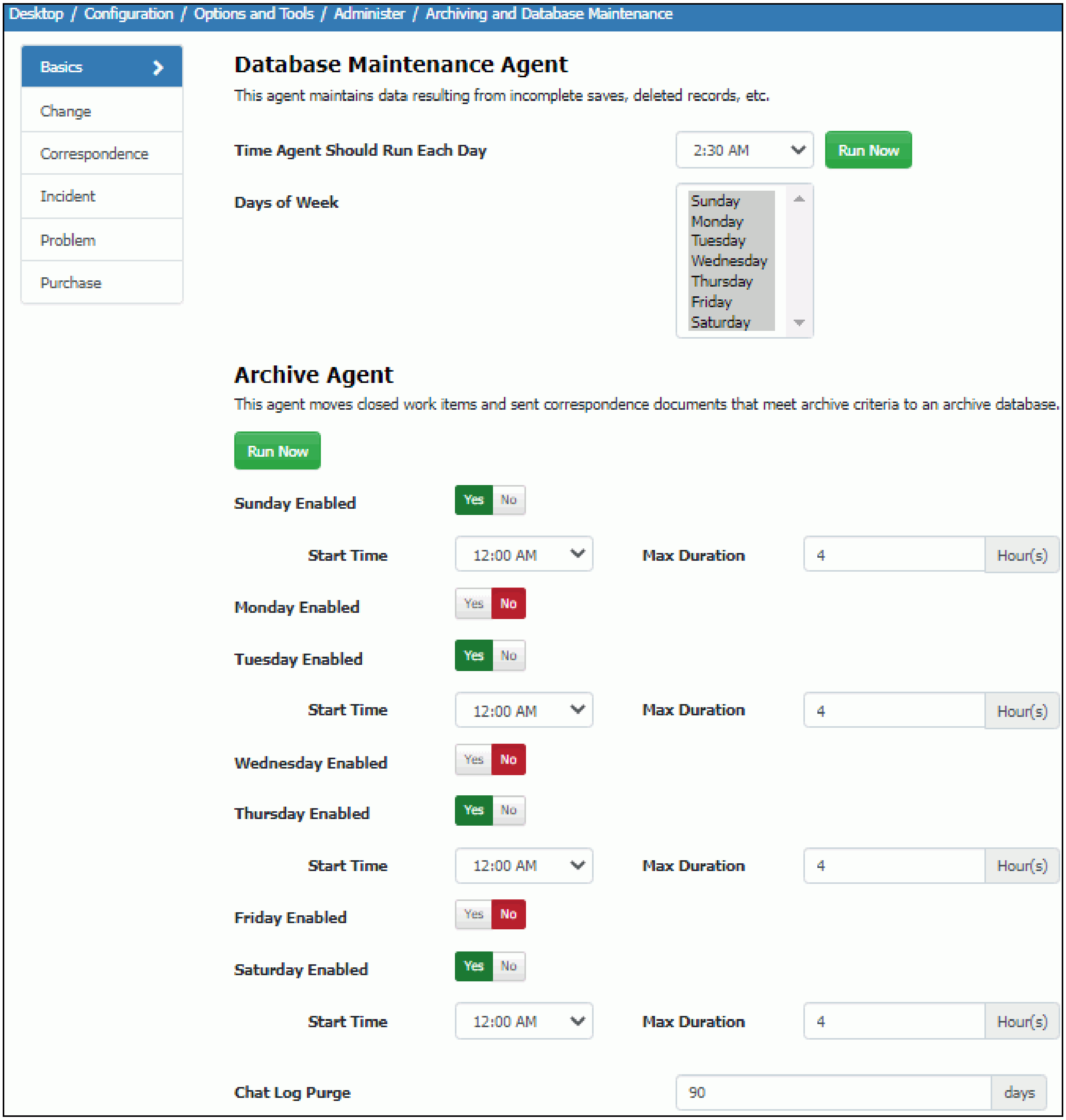
Maximum server memory (in MB): 28000

- If your databases are in full mode, ensure that full backups (databases and transaction logs) are performed daily and transaction logs are backed up every 15 minutes. Use SQL Management Studio jobs to back up your database in addition to your third party applications to ensure that the logs are committed and shrunk.

iSupport Application Usage

- Global searches can be taxing and inefficient when searching databases; search views instead. Try to avoid views that have large amounts of custom fields.
- The asset scanning process can be taxing, so run asset scans after hours or during periods of down time.
- Be efficient with your use of rules and rule groups. One well-written rule is better than many singular valuation/ action rules; try to keep the number of rules in a rule group to 8-12.
- Analyze your use of hierarchy templates; two or more hierarchies is better than one massive hierarchy.
- Be concise with your use of custom fields, customer and support representative groups, and roles.
- Evaluate the email accounts that you utilize and the frequency of checking for new messages.
- Archive your data via the Archiving and Database Maintenance feature under Options and Tools in the Configuration module. Set a maximum execution timer on the Archive agent, and ensure that the Archive agent

and Database Maintenance agent are not overlapping each other. For example, if you start the Archive agent at 12:00AM and run it for two hours, ensure that the Database Maintenance agent is scheduled for 2:30AM.


Desktop / Configuration / Options and Tools / Administer / Archiving and Database Maintenance
Basics
Change
Correspondence
Incident
Problem
Purchase

Database Maintenance Agent

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

Time Agent Should Run Each Day: 2:30 AM | Run Now

Days of Week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Archive Agent

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

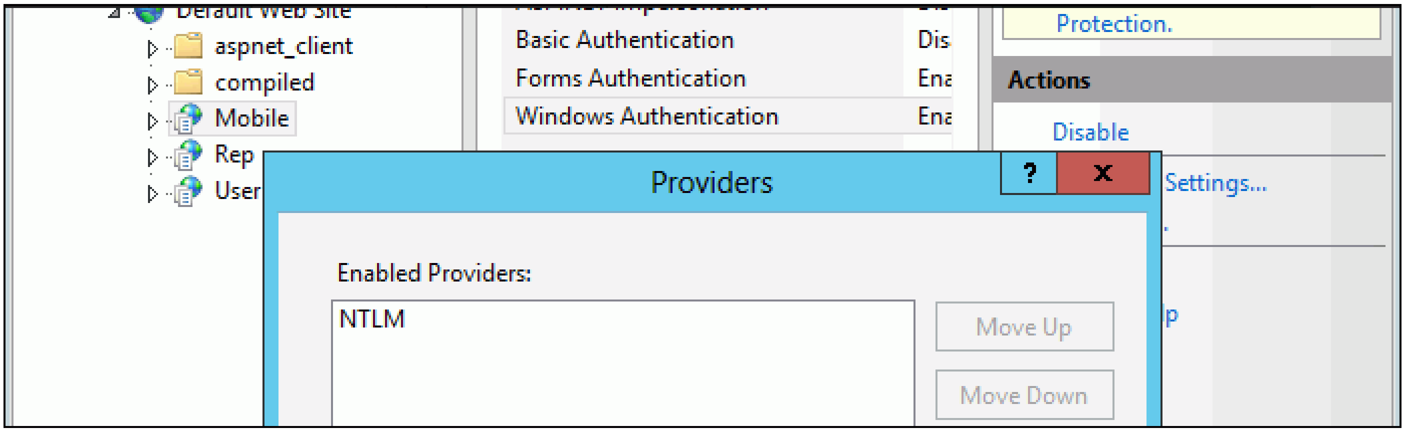
Run Now

Sunday Enabled	Yes		
Start Time	12:00 AM	Max Duration	4 Hour(s)
Monday Enabled	No		
Tuesday Enabled	Yes		
Start Time	12:00 AM	Max Duration	4 Hour(s)
Wednesday Enabled	No		
Thursday Enabled	Yes		
Start Time	12:00 AM	Max Duration	4 Hour(s)
Friday Enabled	No		
Saturday Enabled	Yes		
Start Time	12:00 AM	Max Duration	4 Hour(s)

Chat Log Purge: 90 days

- Subscriptions could tax the system; analyze any subscriptions you are running and the amount of data searched. Schedule subscriptions to run after hours if possible.
- If using the API, analyze how it could be affecting performance. (Note that iSupport doesn't support the API or correct any issues it may cause in your environment.)

- If using Windows Authentication for the Desktop and mySupport portals, ensure that only the NTLM is listed as an enabled IIS provider.



Enabled Providers:

NTLM