



MOTOROLA

E CARE 5.2 RELEASE NOTES

RELEASE NOTES FOR SELF-HOSTED INSTALLATIONS, VERSION 5.2.1 JUNE 2008

This document contains important information about eCare version 5.2. If you have additional questions, consult the eCare documentation and FAQs at the eCare Resource Page:

<http://www.netopia.com/support/software/ecare/>

WHAT'S NEW IN E CARE 5.2.1

NEW FEATURES AND ENHANCEMENTS

CAPABILITIES AND DEPLOYABLES

eCare version 5.2.1 includes several new *deployables*— the objects that manage the eCare components and controls that are downloaded to customer and Support Agent Web browsers. The deployable model allows for greater flexibility and control over the installation and use of eCare components; you can control when (and if) specific eCare components are installed on the computers that use your eCare service.

The key deployables in eCare 5.2.1 control the installation and use of the eCare remote-control component and the ScriptRunner applet, which executes Managed Scripts on the remote computer.

You can configure eCare deployables with your *ecare.xml* or overrides file. See chapter 4, “Configuring eCare Deployables,” in the *eCare Server Manual* for more information.

NEW JAVA-BASED REMOTE-CONTROL COMPONENT

eCare version 5.2.1 introduces a new Java-based remote-control component. The new Java component offers easy installation and a more modern look and feel.

With the default eCare configuration, the Java remote-control component is installed preferentially if the computer has the correct version of Java installed. As with the native-platform components in earlier versions of eCare, the Java remote-control component is installed automatically the first time a Support Agent signs in to eCare, or when a customer loads the trouble-ticket submission page in their Web browser.

If a computer does not have the correct version of Java installed, the default eCare configuration automatically installs the appropriate native-platform remote-control component instead (an ActiveX control for Windows, and a plugin for Macintosh computers).

You may also configure your eCare service to use only the Java-based remote-control component or only the native-platform components.

SYSTEM REQUIREMENTS

The Java-based remote-control component requires Java version 1.4.2_09 or later. In addition, it has the following system requirements.

- For Windows computers, Windows Vista, Windows XP, or Windows 2000.
- For Macintosh computers, MacOS X version 10.4 or later and Safari version 2.0.4 or later.

Note that the Managed Scripts feature also uses a Java component, and has the same Java and system requirements.

DEFERRED COMPONENT INSTALLATION

eCare version 5.2.1 includes the ability to defer the installation of the eCare remote-control component (as well as the Managed Scripts Java component) on the customer's computer until the Support Agent launches a service that requires it.

You can configure deferred installation with your *ecare.xml* or overrides file. See chapter 4, "Configuring eCare Deployables," in the *eCare Server Manual* for more information.

THE CONTROL AS ADMIN SERVICE

In many organizations, security concerns mandate that many Windows users do not have Administrator privileges on the computers they use. On Windows Vista, users without Administrator privileges are limited in the tasks they can perform. These limitations prevent Support Agents from making full use of eCare's Control service when they control Windows Vista computers.

The new Control As Admin service allows your Support Agents to launch a Control session *with Administrator privileges* on a remote Windows Vista computer. Running with Administrator privileges allows the eCare remote-control component far greater control over the Windows Vista computer.

ACCESS REQUIREMENTS

The Control As Admin service is supported only when your customers and Support Agents are on the same network—for example, if your Support Agents are part of your organization's internal help desk and your customers are other employees of your organization. It cannot be used if your customers are on an external network.

To use the Control As Admin service, Support Agents must have Remote Admin credentials on the customer's computer. If your Support Agents have Domain Admin credentials, they will have the correct access privileges automatically. However, you may also configure your Windows domain so that members of a domain group such as "Tech Support Technicians" are granted local administrator privileges on all domain computers. If your Support Agents belong to this domain group, they will be granted sufficient access privileges to use the Control As Admin service.

The Control As Admin service is available only when the customer's computer is running Windows Vista. In addition, only Support Agents with Premium Agent privileges assigned in their eCare profiles can use the Control As Admin service.

When the Control As Admin service is available, it appears on the *Share* menu in the Support Agent's eCare session window.

ENABLING THE CONTROL AS ADMIN SERVICE

You can enable the Control As Admin service with your *ecare.xml* or overrides file. See the *eCare Server Manual* for more information.

In addition, to allow your organization's Windows Vista computers to accept incoming Control As Admin sessions, open the computer's Windows Firewall control panel and enable the *File and Printer Sharing* exception.

CUSTOM MESSAGE DISPLAY

You can now configure a custom message that will appear at the top of the session transcript panel in the eCare session window. The content and appearance of this message can be changed by editing or replacing a file in the *custom* directory.

The custom message can be displayed to either the Support Agent or the customer, or to both. (The message will be different for Support Agents and customers unless you create identical message files.)

For information about how to configure custom messages, see the *eCare Server Manual*.

OTHER CHANGES

- Support Agents no longer require Premium Agent privileges to use the Transfer a File from the Server service.
- eCare now supports a login-failure URL. When a user attempts to sign in to eCare, but the attempt fails due to an invalid user name or password, eCare can redirect or forward the user to a specified URL.
- The eCare Reporting Center now includes the Privilege Audit Export report, which allows you to export a CSV file listing all Support Agent and administrator profiles on your eCare service and their eCare access privileges. The Privilege Audit report provides an online report of the same information in tabular format.

UPGRADING FROM eCARE 5.2 TO eCARE 5.2.1

To upgrade an eCare 5.2 service to eCare 5.2.1, use the following procedure.

Note: If you are upgrading your eCare service from eCare 5.0.1, follow the procedure [“Upgrading from eCare 5.0.1 or 5.1 to eCare 5.2” on page 4](#). Then upgrade from eCare 5.2 to eCare 5.2.1.

1. Shut down the eCare service you wish to upgrade.
2. Run the `UpgradeServiceInstall.sh` script in your Resin directory.
3. Run the `UpgradeOverrides.sh` script against the eCare service’s overrides file.
4. Restart your eCare service. eCare will update the database to complete the upgrade.

KNOWN ISSUES IN eCARE 5.2.1

- Computers running Windows Vista will not accept CTRL+ALT+DELETE commands from the remote computer during incoming remote-control sessions.
- If a customer on a Macintosh computer running Safari 2.0.4 enters eCare without submitting a trouble ticket—for example, by responding to an email invitation—the System Information service will not return the system profile to the Support Agent.
- When a Support Agent is controlling a customer’s Macintosh computer, and the customer’s computer is using the Java-based remote-control component, the computer may behave as if one of its modifier keys (SHIFT, COMMAND, or OPTION) is stuck down when the Support Agent clicks a mouse button. If this occurs, pressing the “stuck” modifier key several times may reset it. Pressing the ESCAPE key may also reset the modifier key.
- When a Support Agent uses the Java-based remote-control component to control or observe a remote Macintosh computer, and enables the Shrink to Fit function in the screen-sharing window, the remote desktop may not display correctly. If this occurs, minimize and restore the screen-sharing window.
- If a Support Agent or customer using a Macintosh computer shuts down the eCare remote-control component application in the dock, the user will not be able to use screen-sharing services for the remainder of their eCare session. To re-enable screen-sharing services, close and reopen the eCare Web browser window.
- If a customer’s computer is running Internet Explorer version 7 and Java 1.5 or earlier, a Support Agent attempts to execute a Managed Script on the customer’s computer, and the customer does not respond to the Java Applet Security dialog box before it times out, the customer’s trouble ticket is lost.
- When a computer connects to your eCare service and Java components are loaded, the screen may flash briefly as command windows open and close. This behavior is normal.
- When a Support Agent uses a screen-sharing service to control or view a Windows Vista computer, the Ask for Permission dialog box may open *behind* the active window on the customer’s computer. The customer must grant permission before the session can proceed. Support Agents should use the text-chat area to let their customers know what to expect.
- If you delete a Closed Action that is currently assigned to a weekly schedule (on the *Operating Hours* tab in the eCare Administrator window), it may cause a servlet exception when customers and Support Agents attempt to sign in to your eCare Service Center. Before you delete a Closed Action, be sure it is not in use by any of your weekly schedules.

UPGRADING FROM eCARE 5.0.1 OR 5.1 TO eCARE 5.2

eCare 5.2 runs on newer versions of Java and Resin than did eCare 5.0.1 and 5.1. These new versions require major changes to the Resin configuration file. As a result, the eCare 5.2 upgrade process is similar to that of a new installation. However, the upgrade script will move most information from your existing Resin container to the new one. (Certain exceptions may require you to make manual changes.)

In addition, the **securityevent** table must undergo extensive processing to prepare it for the new security event validation feature. If you have a large **securityevent** table, you may wish to archive most or all of the table before you perform the upgrade. This will streamline the upgrade process.

Note: During the upgrade process, the eCare 5.0.1 or 5.1 Resin directory will not be modified. When the upgrade is complete, your eCare 5.0.1 or 5.1 server will still function normally.

TO UPGRADE eCARE 5.0.1 OR 5.1 TO eCARE 5.2

1. **Back up your existing eCare installation, including the database.**
2. Change to the directory that contains the expanded eCare distribution.
3. Run the `UpgradeECareInstall_5_0_1_and_5_1_to_5_2.sh` script. This script uses four parameters in the following order:
 - The path to the Resin directory in which you installed eCare 5.0.1 or 5.1 (for example, `/usr/local/resin-2.1.17`)
 - The name of the overrides directory (not the full path; the name is `ecare4overrides` unless you manually changed it after installing eCare 5.0.1 or 5.1)
 - The name of the primary eCare service—the service name you used when you ran the original installation script for eCare 5.0.1 or 5.1 (for example, `helpdesk`)
 - The path to the new Resin directory in which you will install eCare 5.2 (in most cases, `/usr/local/resin-3.1.2`)

For example,

```
UpgradeECareInstall_5_0_1_and_5_1_to_5_2.sh /usr/local/resin-2.1.17 ecare4overrides
helpdesk /usr/local/resin-3.1.2
```

4. The script will prompt you to specify whether you changed the `resin.conf` file after you installed eCare 5.0.1 or 5.1.

```
Was the resin configuration file changed after the last install of eCare? (y/n)?
[n]:
```

- If you respond **no**, the upgrade script will collect information from the `install.record` file in the eCare 5.0.1 or eCare 5.1 overrides directory and transfer it to the new `resin.conf` and `wtp.conf` files.

If you changed any values in the `resin.conf` file without updating the `install.record` file, answer **yes**. The upgrade script will then prompt you to provide the values it needs for the new `resin.conf` and `wtp.conf` files.

After it creates the new `resin.conf` and `wtp.conf` files, the upgrade script will copy your overrides file to the new Resin directory and upgrade it to the new format. The upgrade preserves any portals or custom configuration specified in the overrides file.

The new eCare 5.2 installation will also include certain information from your previous eCare service, including the ticket archive, localization settings, and current ticket number, as well as any customizations you made with the `custom` directory.

5. You may need to manually copy certain changes to the `resin.conf` file. Such changes include new JNDI database definitions you added manually, which may have occurred if you added additional eCare services that use different databases.

If you performed any additional customization outside the `custom` and overrides directories, copy your customizations to the corresponding location in the eCare 5.2 Resin directory.

- If you added additional eCare services to your original eCare 5.0.1 or 5.1 installation with the `addServiceInstall.sh` script, copy the new database references from the original `resin.conf` file to the new eCare 5.2 `resin.conf` file. Then run the `UpgradeServiceInstall_5_0_1_and_5_1_to_5_2.sh` script for each service.

This script uses the same four parameters as the original upgrade script. For the third parameter, provide the name of the additional eCare service that you are upgrading. The upgrade script will copy and upgrade the service's configuration files in the same way that it copied the primary eCare service's files.

When you start the upgraded eCare server, the database for each service you upgraded will be updated. Because of the new fields in the `securityevent` table, this processing may take several minutes (or longer if your `securityevent` table is extremely large). The database upgrade process will be detailed in the `start.log` file for each eCare service you upgrade.

WHAT'S NEW IN ECARE 5.2

MANAGED SCRIPTS

The new Managed Scripts feature in eCare 5.2 permits knowledge, both diagnostic and remedial, to be encapsulated in a script, uploaded to the eCare server, and made instantly available to your Support Agents. You can maintain a repository of scripts at the server, and your Support Agents can securely execute these scripts on the remote Windows computer with a minimum of difficulty. (Managed Scripts are not supported on remote Macintosh computers.) The script results are automatically captured and returned to the eCare server, where they are both displayed to the Support Agent and logged for future reference.

With Managed Scripts, you can expand eCare's capabilities to run your own custom diagnostic scripts, tools, and functions. Managed Scripts can provide or support a wide variety of functionality. They can automate many different tasks: comprehensive diagnostic sweeps, installations, configurations, and more. They can also be used for specific individual needs. For example, your Support Agents may examine the remote file system, check for the presence of certain software, configure browser settings to meet the customer's needs, and install or execute applications on demand.

Note: To run a Managed Script, the customer's computer must have Java version 1.4 or later installed in the Web browser. Only the Java runtime, version 1.4.2 or later, is required; the full Java SDK is not needed. The Java runtime is approximately 16 MB in size, and it can be downloaded from <http://www.java.com/en/download/>. There are no special requirements for the Support Agent's computer.

For more detailed information about eCare's Managed Scripts feature, see the *eCare Administrator's Guide* and the *eCare Managed Scripts Technical Guide*.

ECARE INTEGRATION SERVER

Motorola now offers the new eCare Integration server. This eCare add-on supports integration with your existing external systems, such as CRMs. As part of the integration, eCare now supports secure handoffs of both customers and Support Agents from the external system to a provisioned eCare session. This integration allows your existing ticket management system to function as the "secure front door" to eCare without requiring users to sign in separately to eCare or enter redundant information in the eCare trouble-ticket form.

In addition, the Integration Server offers a publishing function that can return eCare session results for provisioned tickets to the external ticketing system. The eCare session record becomes an integrated part of the external system's account record.

For more information about the eCare Integration Server and its capabilities, see the *eCare Integration Guide*.

COMPONENT TRUST

eCare 5.2 supports *component trust*, a feature that improves the security of eCare components that are deployed to a remote computer. Component trust ensures that the component will accept commands only from a server that can be trusted—a server that the component can verify is a valid licensed server from Motorola.

To achieve component trust, eCare uses certificates—a set of information that is signed by a private key. The signing can then be verified to ensure that the data within has not been changed. eCare's component trust requires two artifacts: a Trust Certificate and a Signing Key. Motorola will provide you with your unique certificates.

See the *eCare Administrator's Guide* for more information.

NEW ADMINISTRATOR USER INTERFACE

The entire eCare Administrator Center has been redesigned with a new look and feel and improved functionality. See the *eCare Administrator's Guide* for more information.

TICKET QUEUE ENHANCEMENTS

The eCare administrator can now customize the eCare trouble-ticket queue in a number of ways. With the eCare Configuration Manager in the eCare Administrator center, you can control the amount and type of information that is displayed in the queue, apply several default ticket-sorting options, and allow your Support Agents to view only tickets that have already been assigned to them through an email invitation or eCare integration. To set your preferences, choose the **Configure** tab in the eCare Administrator Center. From the *Configure* menu, choose the *Options* page.

Support Agents can use the *My Tickets* option on the *View* menu to display only their own assigned trouble tickets.

See the *eCare Administrator's Guide* for more information.

SERVER-BASED FILE TRANSFER

With the new Transfer a File from the Server service, you use your eCare server to store files that your Support Agents can select and transfer directly to the customer. Using the eCare server for file storage makes it easier for you to control the files your Support Agents can send and keep them updated with the latest versions. To upload and manage files, choose the **Configure** tab in the eCare Administrator Center. From the *Configure* menu, choose the *Server Based File Transfers* page.

The Transfer a File from the Server feature is in addition to the Send a File service; it does not replace it. Your Support Agents may still use the Send a File service to transfer files from their local computers to the customer's computer. You may also choose to disable the Transfer a File from the Server service, the Send a File service, or both services.

See the *eCare Administrator's Guide* for more information.

SECURITY EVENT TABLE VALIDATION

The eCare database includes a table called **securityevent**, which records activities that may be relevant to the security of your eCare server. eCare can now check the **securityevent** table for tampering every time eCare starts up, daily at a specified time, or both.

See the *eCare Server Manual* for information about configuring **securityevent** table validation.

OTHER CHANGES AND ENHANCEMENTS

This version of eCare includes many refinements and enhancements to the features introduced in eCare 5.0. Some of these enhancements include

- The *View* menu in the Support Agent's eCare session window now displays a check mark next to the currently selected option.
- The *Share* menu at the top of the Support Agent's eCare session window now indicates the current color-depth selection.
- The Email Invite template has been updated.
- The Message of the Day on the trouble-ticket form now appears in a more prominent location. (If desired, you may use custom style sheets to change the appearance and location of the Message of the Day.)
- When you create a new Closed Action with a custom URL on the **Operating Hours** tab in the eCare Administrator Center, eCare now assumes the HTTP protocol if you do not enter one.
- When a customer is ready to submit a trouble ticket, they may now press ENTER instead of clicking the *Submit* button.
- Trouble tickets that were submitted through an email invitation are can now be displayed in an administrator-defined color in the trouble-ticket queue.
- The Agent Tool Shortcut feature now accepts long URLs.

BUG FIXES IN ECARE 5.2

- When a customer enters your eCare Service Center by responding to an email invitation, after a Support Agent reboots their computer, or by using the reconnect desktop shortcut after a session interruption, the trouble ticket is now correctly assigned to the Support Agent who sent the email invitation or was previously assisting the customer.
- When a Support Agent deletes a trouble ticket in the View All Tickets window, the ticket listing is now refreshed automatically.
- When eCare reboots a customer's computer, customer information (such as the customer's name and email address) is now retained correctly.
- All clients are notified of any link drop acceptance.
eCare session transcripts no longer display "Client accepted Link Drop request" for other eCare sessions that are active at the same time as the current session.
- Trouble tickets that were re-submitted after the remote computer was rebooted are now correctly displayed in an administrator-defined color in the trouble-ticket queue.
- In the Ticket Session report in the eCare Reporting Center, the *Ticket Duration* is now displayed correctly in hours, minutes, and seconds.
- When an eCare user changes their password and presses *Enter*, eCare no longer displays the 403: Direct Linking Not Allowed error page.
- When pop-up blocker options are set correctly in Internet Explorer version 7, the ActiveX warning bar no longer appears when eCare attempts to install the eCare ActiveX control. Previously, right-clicking the ActiveX warning bar to allow pop-ups caused the eCare session to fail.
- When a customer closes their Web browser during an eCare entry survey, the trouble ticket they submitted is no longer added to the queue.
- The *Click Here to Learn More* link on the Support Agent and Administrator portal pages now correctly opens a window with more information about the importance of avoiding actions that will reload the eCare window.
- eCare now displays an error message when a Support Agent enters an incorrect file name or path when attempting to transfer a file with the Send a File service.

- The Reboot Remote System option is no longer available when the customer is using a Macintosh computer. Rebooting the remote computer is not supported on Macintosh computers.
- The cursor no longer appears incorrectly in certain situations.
- Long text-chat messages are no longer obscured by the *Send* button.
- When a customer using Mac OS X version 10.5 receives a file with the Send a File service, the file is no longer saved with extra characters in the file name.
- The Ticket Export report now correctly uses the CSV file extension.

KNOWN ISSUES IN ECARE 5.2

- If you do not install the Email Invite and Reconnect portals with your eCare server, the options to enable these portals will still appear in the eCare Administrator Center's Configuration Manager. Enabling or disabling these options will have no effect.
- The default reconnect timeout—the time after which the unique URL the customer can use to reconnect to eCare after a reboot or session interruption—is set with the `<user-reconnect-time-out>` element in the `client-login` portal configuration, not the `reconnect-login` portal configuration. If this optional element does not appear in the `client-login` portal configuration, the default timeout is 1200 seconds (20 minutes).
- If a Support Agent signs in to the Support Agent portal on a computer with Windows Media Player version 9 or later, and the computer does not yet have the eCare ActiveX control installed, the Support Agent may be prompted to install the Windows Media Player Shim in addition to the eCare ActiveX control. The Windows Media Player Shim allows certain sounds to be played in the Web browser.
If the Support Agent declines the request, Support Agent audio alerts will not occur.
- Display of the trouble-ticket status may be truncated in the *My Tickets* area in the Support Agent's eCare session window.
- When a customer whose Web browser does not have Java installed submits a trouble ticket, the `RemoteScripting` probe causes Internet Explorer to display a message that the Web page requires Java. In addition, when the customer closes the message window, there may be a delay before the eCare session window appears.
Disabling the `RemoteScripting` probe will prevent this message from appearing. However, it will also disable all Managed Scripting. See chapter 4, "Configuring eCare Deployables," in the *eCare Server Manual* for information about the `RemoteScripting` probe and how to disable it.
- Certain characters, including question marks (?), ampersands (&), and quotation marks, may cause errors when you use them to name files you upload for use with the Transfer a File from the Server feature. Please limit file names for the Transfer a File from the Server feature to alphanumeric characters, periods (.), underscores (_), and hyphens (-).

WHAT'S NEW IN ECARE 5.0.1

- eCare support for Windows Vista has been improved. See ["eCare 5.0.1 and Windows Vista" on page 10](#).
- Mac OS X version 10.5, Leopard, is now supported.

NEW FEATURES AND ENHANCEMENTS

WINDOWS VISTA DETECTION

As in eCare 5.0, the eCare server will automatically detect when an eCare customer's computer is running Windows Vista and whether the eCare server is marked as an Internet Explorer Trusted Site in the customer's Web browser. If eCare is not marked as a Trusted Site, the customer is now prompted to allow the eCare server to

automatically download and run a script that applies the correct settings. (The customer is given the opportunity to decline this action. If the customer declines the script, their eCare session will continue, but remote-control services will not be available.)

Once the script has run, the customer's browser will automatically restart and return to the correct eCare service.

Please see [“eCare 5.0.1 and Windows Vista” on page 10](#), as well as the *Running eCare on Windows Vista* PDF document (available on the eCare Resource Page) for additional information, requirements, and limitations.

E CARE RECONNECT COMPONENT IMPROVEMENTS

The eCare reconnect component has been improved.

- The eCare server now prompts the customer to activate the reconnect component after the customer has submitted their trouble ticket and before they are placed in the trouble-ticket queue. In addition, the Activate dialog box is now more prominent. These changes may reduce the number of eCare sessions in which the reconnect component is not activated.

Note: If the customer declines the Activate dialog box, the Reboot Remote System service will not be available during their eCare session. The *Reboot Remote System* option will be disabled on the *Tools* menu.
- When a Support Agent attempts to reboot a customer's computer, eCare now displays a warning message that allows the customer to decline the reboot request. Previously, eCare displayed the reconnect component's Activate dialog box.
- The eCare reconnect component is now supported on Windows Vista.

REQUIRED POST-UPGRADE CONFIGURATION

If your eCare service uses an overrides file, and it defines specific versions of the eCare remote-control component for Windows 2000 or later, you must manually update the overrides file after you upgrade to eCare 5.0.1. The `<class-id>`, `<min-version>`, and `<download-file>` entries for each Windows version should be updated to match the entries in the default *ecare.xml* file.

Previous versions of the eCare remote-control component will not work correctly with the new version of the eCare server.

CONFIGURATION FILE CHANGES

The `<entry-portals>` section in the *ecare.xml* file now includes the `<default-visible-host>` entry. This entry specifies the domain name of your eCare server, and it is used when the eCare server sets itself as an Internet Explorer Trusted Site on a customer's Windows Vista computer.

You will specify the `<default-visible-host>` setting during the installation process; the installation script will prompt you for it. However, if you later change the URL of your eCare service, you must manually update this setting in your *ecare.xml* or overrides file.

BUG FIXES

- Shortcut URLs in the *Reference* menu are now loaded correctly on the Support Agent's computer.
- When the Support Agent uses the System Information service, the link to the System Information data now appears correctly in the session transcript.
- When the Support Agent uses the System Information service to generate a report for a Macintosh computer, the System Information window was previously difficult to read. Its appearance has been improved.
- The *Sort Newest First* option on the *View* menu in the trouble-ticket queue now works correctly.

ECARE 5.0.1 AND WINDOWS VISTA

Windows Vista is a radically different version of the previous Microsoft Windows OS. When eCare version 5.0.1 runs on Windows Vista, certain Internet Explorer settings are required to allow remote-control functionality. In addition, there are a number of known issues.

For full installation and configuration instructions, and a discussion of limitations and known issues with Windows Vista and eCare, see the *Running eCare on Windows Vista* document. In addition, please visit the eCare Resource Page, where updated information will be posted as it becomes available.

<http://www.netopia.com/support/software/ecare/>

ECARE CUSTOMERS AND WINDOWS VISTA

- eCare customers running Windows Vista must use Internet Explorer version 7 as their Web browser. Other versions of Internet Explorer and other Web browsers are not supported.
- When a customer whose computer is running Windows Vista visits your eCare Service Center for the first time, the eCare server will prompt the customer to download and install the appropriate version of the eCare ActiveX control. (Customers may also pre-install the ActiveX control as described in the *Installing the eCare Remote-Control Component* PDF document, available from the eCare Resource Page.)
- Once the eCare ActiveX control has been installed, the customer is prompted to download and run a registry-edit script, which is offered only to customers whose computers are running Windows Vista. The script will set the eCare server as a Trusted Site in Internet Explorer (the script will run automatically when download is complete). After the script runs, Internet Explorer will restart and return to your eCare Service Center automatically.

The customer is given the option to decline the Trusted Site script. If the eCare server is not set as a Trusted Site in the customer's Web browser, the customer will still be able to use eCare. However, remote-control services will not be available.

- If the customer pre-installed the eCare ActiveX control with the MSI installer before visiting your eCare Service Center, the eCare server will not attempt to download it again. It will automatically proceed to the Trusted Site script.

ECARE SUPPORT AGENTS AND WINDOWS VISTA

- eCare Support Agents running Windows Vista must use Internet Explorer version 7 as their Web browser. Other versions of Internet Explorer and other Web browsers are not supported.
- When the Support Agent visits your eCare Service Center for the first time, the eCare server will detect that the Support Agent's computer is running Windows Vista. It will prompt the Support Agent to download and install the eCare ActiveX control. (You may also pre-install the ActiveX control as described in the *Installing the eCare Remote-Control Component* PDF document, available from the eCare Resource Page.)
- Before the Support Agent can allow the customer to use the Give User Control service to control the Support Agent's computer, the eCare server must be set as a Trusted Site in the Support Agent's Web browser. The simplest way to make the eCare server a Trusted Site is to add it to the browser's Trusted Site list. See the *Running eCare on Windows Vista* PDF document for details.

If the eCare server is not set as a Trusted Site in the Support Agent's Web browser, they will still be able to use eCare. However, the Give User Control service will not be available.

KNOWN ISSUES IN ECARE 5.0.1

The following issues are known to exist in eCare 5.0.1. Note that some of these issues may have been resolved in later versions.

SCREEN-SHARING SESSION TIMEOUT

Your eCare server is configured to close eCare sessions after a certain amount of time has elapsed without data transfer. During a long screen-sharing session in which you do not use the mouse or keyboard (for example, if you are occasionally monitoring a long process on the remote computer), the remote computer's screen-saver may activate or its monitor may power off, even though onscreen activity is continuing. Depending on your operating system, these events may cause the remote computer to stop transmitting data. Once data transmission stops, the default eCare session timeout begins. If the full timeout period is reached without mouse or keyboard activity, your screen-sharing session will close before you are finished.

To avoid inadvertent screen-sharing session timeouts, configure your screen-saver and monitor settings as needed for your operating system.

Note: You may also change the default timeout period by editing the `<request-timeout>` tag in the `resin_wtp.conf` file.

WINDOWS COMPUTERS

If the Windows screen saver is set to *Blank*, screen-sharing data is no longer sent when the screen saver is activated. When the data flow stops, the default eCare session timeout will begin.

To avoid this type of timeout, use any screen saver other than Blank. Or configure the computer to power down the monitor instead of blanking the screen.

MACINTOSH COMPUTERS

If the *Power Off Monitor* setting is enabled on your Macintosh, screen-sharing data is no longer sent when power to the monitor is disabled—even if the computer uses a moving screen saver. When the monitor is powered off, the default eCare session timeout will begin.

To avoid this type of timeout, do not use the Power Off Monitor setting on a Macintosh that you will need to control or observe for long periods.

OTHER ISSUES

- When a Support Agent deletes a trouble ticket in the View All Tickets window, the ticket listing does not automatically refresh. The trouble ticket is deleted correctly, but it will still appear in the ticket listing for all Support Agents. If any Support Agent subsequently attempts to delete the same trouble ticket, they will be signed out of eCare.
However, if a Support Agent manually refreshes the View All Tickets window, any deleted trouble tickets will no longer appear in their window. Therefore, before deleting trouble tickets, Support Agents should manually refresh the View All Tickets window to ensure that only active tickets are present.
- eCare surveys are not presented when the Support Agent signs out, even when eCare is configured to present them.
- If the customer uses the Close button to close their eCare window while the Activate dialog box is present, Internet Explorer may crash.
- When Support Agent uses the Request a File service, and both the Support Agent and customer's computers are running Windows XP, the Support Agent must have the eCare server set as a Trusted Site in Internet Explorer. In addition, Trusted Sites must be assigned a security level of Medium-low or lower. If the eCare server is not a Trusted Site, or if Trusted Sites have a higher security level, the Support Agent's eCare session will fail when the Agent attempts to download the file.
- The Support Agent user interface no longer supports Internet Explorer 5.5 or computers running Mac OS X 10.3.9. However, this limitation is not enforced when the Support Agent signs in to eCare.

WHAT'S NEW IN ECARE 5.0

NEW FEATURES

eCare 5.0 includes an entirely new Support Agent portal with an enhanced appearance and functionality.

The new Support Agent portal also provides the ability to work on multiple trouble tickets at the same time. The Support Agent can quickly switch between trouble tickets for optimum support efficiency.

BUG FIXES

- Macintosh computers no longer experience occasional failure of active remote-control sessions.
- The remote-control component is now more reliable.
- Surveys are now presented and saved correctly.

© Copyright 2007-2008 Motorola, Inc. All rights reserved.