



# eControl 3.5

## for Novell eDirectory & GroupWise Installation & Update Guide

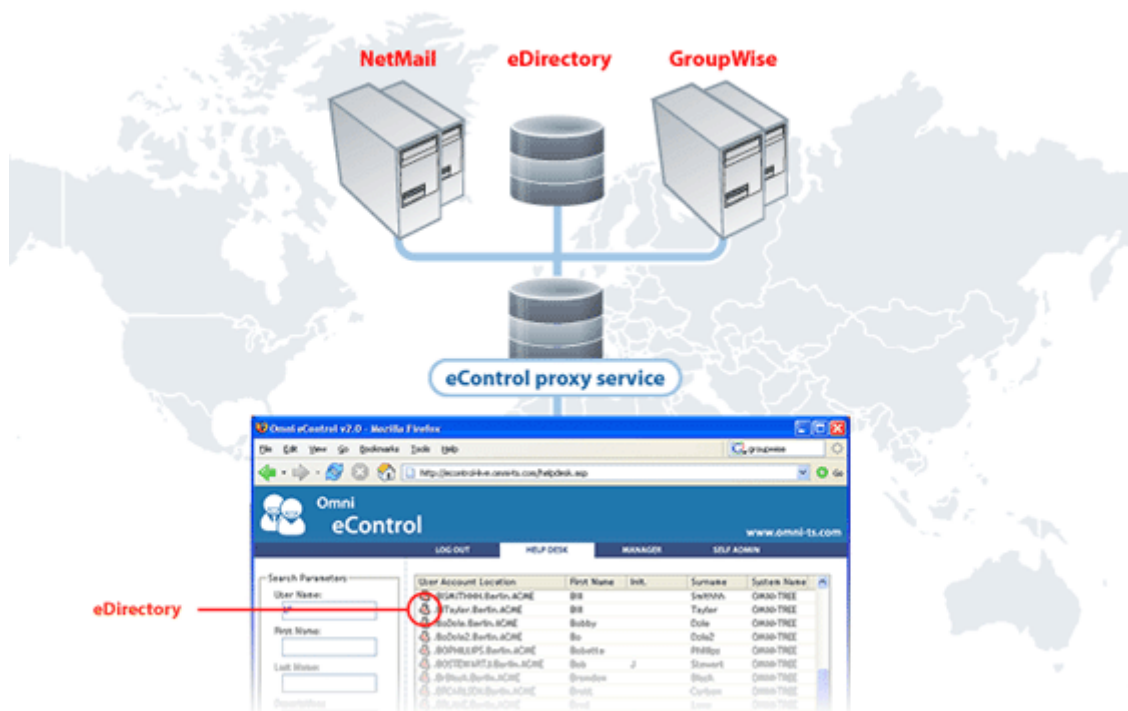
### This Guide

Welcome to the “**eControl 3.5 Installation and Update Guide**” for Novell eDirectory and GroupWise management. This guide covers eControl 3 system requirements, installation, initial sign-on, and upgrading or updating the eControl system.

Other guides in this series includes:

- “**eControl 3.5 Requirements Checklist for eDirectory and GroupWise**”
- “**eControl 3.5 for eDirectory and GroupWise Administrator Guide**”
- “**eControl 3.5 for eDirectory and GroupWise Operator Guide**”
- “**eControl 3.5 for eDirectory and GroupWise Self-Service Guide**”

**eControl 3.5 for eDirectory and GroupWise** delivers a simplified, web-based management, provisioning, self-service and audit application designed for non-technical users. eControl empowers junior administrators, help desk operators, HR staff, department managers, support staff and even end-users to perform common user account management tasks in eDirectory and GroupWise – from a web browser, with NO security permissions and NO access to Novell ConsoleOne or iManager.



## Table of Contents

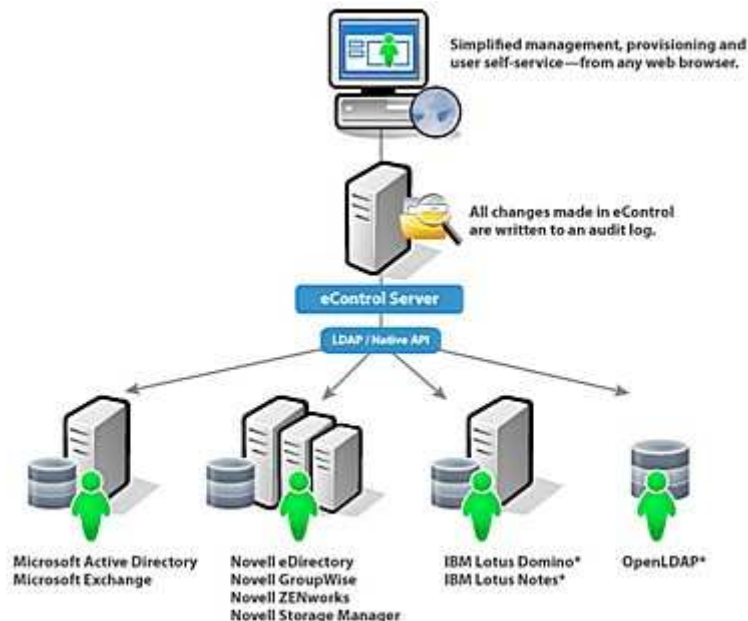
<b>How eControl Works .....</b>	<b>3</b>
<b>Planning for eControl .....</b>	<b>5</b>
Planning for the eControl Environment .....	5
Typical eControl Scenarios .....	5
<b>Preparing for eControl .....</b>	<b>6</b>
Certified Novell Systems .....	6
eControl Service Accounts .....	6
eControl Host Server - System Requirements .....	6
eDirectory - System Requirements .....	8
Requirements for Novell "Home Directory" Support .....	8
Requirements for GroupWise .....	8
Firewall Requirements for eControl in eDirectory and GroupWise .....	9
<b>Install and Configure eControl .....</b>	<b>9</b>
Step 1 - Install eControl .....	9
Step 2 - Create the Target eDirectory Tree Connection(s) .....	12
Step 3 - Create the Target GroupWise Connection .....	15
Step 4 - Confirm the eDirectory Connection(s) .....	19
Step 5 - Confirm and Configure the GroupWise Connections .....	20
Step 6 - Install and Configure the eControl Remote Agent Server .....	23
Install the eControl Remote Agent Server .....	24
Configure "Remote Agent" Support on the eControl Host Server .....	24
Configure "Remote Agent" Support on the eControl Remote Agent Server .....	25
Step 7 - Restart IIS .....	26
<b>Initial Sign-on .....</b>	<b>26</b>
<b>License eControl .....</b>	<b>32</b>
Request a License .....	32
Upload the License .....	34
<b>Assign Delegated Administration .....</b>	<b>35</b>
<b>Upgrading eControl .....</b>	<b>35</b>
Upgrade eControl 2.5 to eControl 3 .....	36
Update eControl to the Latest Release .....	36
Confirm the eControl Installation .....	36
Backup eControl Configuration and License Files .....	36
Uninstall the Omni eControl Connection Agent Service .....	37
Uninstall eControl .....	37
Reinstall eControl .....	37
Reinstall Omni eControl Connection Agent Service .....	37
Restore the eControl Configuration and Licenses Folders .....	38
<b>Support for eControl .....</b>	<b>39</b>
Reporting a Technical Issue .....	39
Upgrade and Maintenance Support Agreements .....	40
Contacting Support .....	40
Online Resources .....	41

## How eControl Works





eControl 3.5 provides a web-based directory and email service management system with special features designed to empower non-IT staff with the ability to manage users without requiring **SUPERVISOR or ADMINISTRATOR** rights! With eControl, concerns such as WAN bandwidth, distance, time-zones, training of IT staff, improving helpdesk effectiveness, costs, and security are overcome.



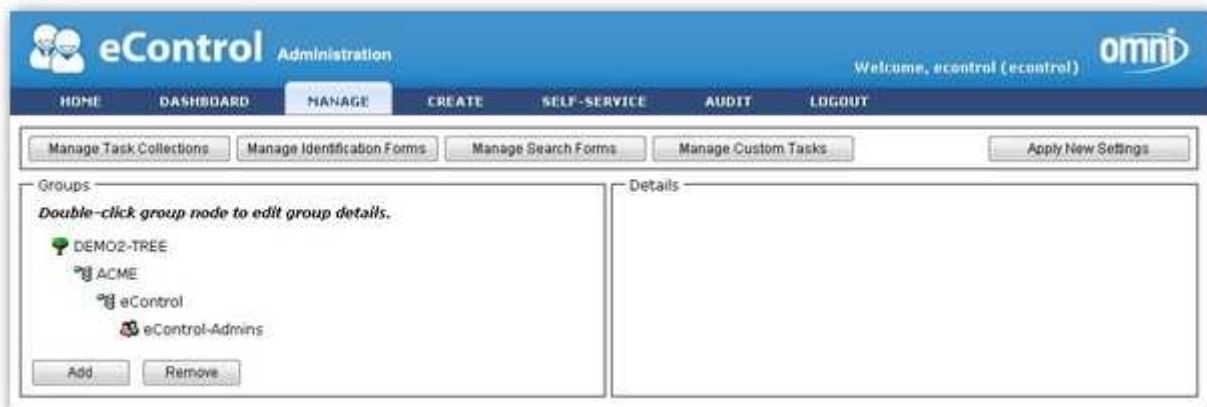
eControl installs as a Windows service that can connect directly to the configured mail and directory systems via **native API, SOAP and/or LDAP calls**. This enables support staff to manage mixed and multiple Active Directory, Exchange, eDirectory and GroupWise systems from a single web interface. eControl 3.5 now supports 3<sup>rd</sup> Party Extensions integrating SQL database systems.



eControl comprises four feature modules that are enabled through the licensing process and provisioned in the administration panel:

 <b>eControl Manage</b>	Provide simplified, role-based management of user accounts, email lists, groups and other directory objects to support staff. eControl Manage allows you to control users' search and task authority. NO special permissions required.
 <b>eControl Create</b>	Use eControl Create to empower HR and office staff to provision user accounts, email lists and groups based on pre-configured profiles. Simplify and standardise your provisioning processes and ensure compliance with naming standards and password requirements.
 <b>eControl Self-Service</b>	Deliver user self-service functions for Active Directory, Exchange, eDirectory and GroupWise. These functions include password changes, "forgot-my-password" challenge phrases, subscriptions to distribution lists and the ability to update demographic information.
 <b>eControl Audit</b>	All changes made in eControl are written to an audit log for administrator oversight. eControl Audit Viewer and Reporting enhances compliance and security audits.

Provisioning eControl is performed by logging into the eControl portal using the eControl service account credentials and clicking the "Administration" option in the tool bar. This is the only account that can configure how eControl works and can provision management task collections, create profiles, self-service assignments, and audit file access to other users in the environment.



## Planning for eControl

### Planning the eControl Environment:

eControl integrates into a large number of systems using a wide variety of different programming interfaces (APIs) to communicate with each system. Windows is the required operating system for eControl because many of the APIs required to manage and provision user accounts in Novell-only, Microsoft-only and mixed and multiple GroupWise, eDirectory, Active Directory and Exchange environments are only available on the Windows platform. Support is now included for 3<sup>rd</sup> Party extensions enabling integration to SQL based systems.

### Typical eControl Scenarios

There are three typical eControl scenarios:

- **eControl managing eDirectory only:**
  - "eControl Host Server" - a Windows 2003 or 2008 server that will host the eControl website:
    - Windows server that meets system requirements
    - Windows Novell client
    - Installation of eControl
    - Configure Active Directory Connections
    - License the eControl installation
  - "eDirectory Tree" - each eDirectory tree that eControl will manage must be configured with an eControl master service account.
  - "Home Directory Servers" - eControl can only manage user home directories hosted on NSS volumes (NetWare or Linux).
- **eControl managing eDirectory with GroupWise** - All requirements for "eControl managing Active Directory only" and add:
  - "**eControl Host Server**" - a Windows system that will host the eControl website. GroupWise client must be installed, or if GroupWise system is running on another Windows server, or on Linux (non-NSS volumes) then install an empty secondary domain on this server.
  - "**eControl Remote Agent Server**" - if an empty GroupWise domain cannot be installed on the eControl Host Server, then the eControl server and the "Omni eControl Connection Agent" windows service must be installed and configured on Windows server that hosts one or more GroupWise domains in a "GroupWise on Windows server(s) only" environment.

## Preparing for eControl

### Certified Novell Systems

eControl 3 can connect to:

- **Certified Directory:** any eDirectory tree, 8.5 or higher on NetWare, SLES OES or Windows server
- **Certified Email System:** any GroupWise system, 5.5 EP or higher (7.0.3 HP1+ with SOAP enabled on PO Agents to support all eControl management tasks).

### eControl Service Accounts

eControl service accounts will need to be created. Pay close attention to this requirement throughout the system requirements below. It is highly recommended that the same common name (SAM account logon name) and password be used for all eControl service accounts created. Ensure that the service account name is not the same as the computer name of the Windows system hosting eControl, e.g. if the eControl host server is named **eControl** then use a different name for the eControl service account like **ecadmin**.

### eControl Host Server - System Requirements

eControl must be installed and connections must be configured and licensed on a eControl host server that meets the following requirements:

- Windows Server 2003 or 2008
  - Standard or Enterprise server and R2 supported
  - x86 and x64 server platforms are both supported
  - 500 MB available disk space (in addition to server requirements)
  - 256 MB RAM (in addition to server requirements)
  - Full support for VMware, Microsoft Virtual Server, Xen, and other virtualization technologies
  - Can be stand alone or member server

*eControl 3.x cannot be installed on Windows 2000.*
- Apply the latest Service Packs and applicable Microsoft Updates.
- Install Microsoft .NET 3.5 SP1
- **Webserver on Windows 2003:** IIS 6 is installed. Ensure that ASP .NET v2.0.50727 web service extension is enabled in IIS Manager.
- **Webserver on Windows 2008:** IIS 7 is installed. Ensure that the following 'Role Services' are installed (in addition to the standard IIS roles):
  - Under 'Application Development' – 'ASP .NET' is installed.
  - Under 'Security' – the applicable 'Authentication' role for your environment is installed.
  - Under 'Management Tools' – 'IIS 6 Management Compatibility' and all child roles are installed.

- Install Windows Powershell 1.0 - available through Microsoft Update as an optional update or from:  
<http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.msp>
- Install Windows Silverlight (optional to support the Dashboard) download from:  
<http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx>
- Disable IE Enhanced Security (recommended)
  - for **Windows Server 2003**:
    1. Open "Control Panel" > "Add or Remove Programs".
    2. Select "Add/Remove Windows Components".
    3. In the "Windows Components Wizard" window uncheck the "Internet Explorer Enhanced Security Configuration" option and click "Next" and "Finish".
  - for **Windows Server 2008**:
    1. Open "Server Manager".
    2. Under the "security information section, click on the Configure IE ESC" link.
    3. Change the Administrators setting to "Off".
    4. Click "OK".
- Configure Data Execution Protection (DEP) for the GroupWise client or disable DEP:
  - To disable DEP on **Windows Server 2003**:
    1. Open "Control Panel" > "System". Select the "Advanced" tab and "Settings" button under "Startup and Recovery".
    2. Under "System Startup" click "Edit".
    3. Change the "/noexecute=optout" to read "/noexecute=AlwaysOff" and save the boot.ini file.
    4. In the "Startup and Recovery" window, click "OK".
    5. In the "System Properties" window click "OK".
    6. You will have to restart the system for the settings to take effect.
  - To disable DEP on **Windows Server 2008**:
    1. Launch an elevated command prompt shell with administrative privileges and credentials.
    2. Then execute the following command:  
  
**bcdedit.exe /set {current} nx AlwaysOff**

## eDirectory - System Requirements

- eDirectory 8.5+ running on any Novell supported platform (including NetWare, SuSE (Linux), Windows).
- An LDAP enabled server for access to eDirectory.
- For simple/universal password support, SSL must be enabled on the LDAP server (enabled by default).
- eControl Host Server **does not** need eDirectory locally installed.
- Create an "eControl" service account in each eDirectory tree and grant it supervisor rights to the root of the tree. Set the password to not expire.

## Requirements for Novell "Home Directory" Support

- Not required if Novell Storage Manager is used (all version supported).
- Home directories must be located on network available NSS volumes (NetWare or OES2 Linux) or OES2 Linux NCP mount share.
- Requires Novell client 4.91.5+ must be installed on the eControl host server.

## Requirements for GroupWise Support

- All versions of GroupWise 5.5 EP+ are supported.
- GroupWise 7.0 SP3 + and SOAP enabled on the post offices is required to support all eControl management tasks.
- GroupWise Client (should match server version) must be installed on the eControl Host Server.

Three different configurations are supported:

1. GroupWise Domain on a network accessible NSS volume (hosted on either Netware or Linux) requires a Novell Client version 4.9+ installed and GroupWise client to be installed on the eControl host server. No "Omni eControl Connection Service" is required.
2. For GroupWise system installed on a Windows server:
  - Option 1 - install an empty secondary domain on the eControl host server (recommended), or
  - Option 2 - install the "Omni eControl Connection Service" on the Windows server hosting a GroupWise domain.
3. For GroupWise hosted on a Linux server (installed on non-NSS volume):
  - Option 1 - install an empty secondary domain on the eControl host server (recommended), or
  - Option 2 - install an empty secondary domain on a NSS volume on a Netware or Linux server, or
  - Option 3 - install an empty secondary domain on a Windows server and install the "Omni eControl Connection Service".

## Firewall Requirements for eControl in eDirectory and GroupWise

Ensure that any firewalls between the eControl host server and the all servers that the eControl host server will connect with are open for:

- TCP Port 636 In/Out to support SSL (if required).
- TCP Port 7xxx In/Out to support connection between the eControl host server and the GroupWise SOAP ports enabled on GroupWise POAs.
- TCP Port 16xx In/Out ports to support GroupWise connection between the eControl host server and the GroupWise POs.

## Install and Configure eControl

There are 8 steps to install and configure the eControl host server:

- Step 1 – Install eControl
- Step 2 – Create the target eDirectory tree connection(s)
- Step 3 – Create the target GroupWise connections
- Step 4 – Confirm the eDirectory tree connection(s)
- Step 5 – Confirm and configure the GroupWise connections.
- Step 6 – Install and configure the Omni eControl Remote Agent Server (if required)
- Step 7 – Restart IIS

### Step 1 - Install eControl

#### Downloading eControl

Prior to installing the eControl host server, ensure that the server meets the system requirements. Download the **econtrol.setup-latest.zip** file from the download link provided by the eControl download email.

The recommended best practise is to create a **C:\Download-Omni\Control** folder and extract the the **econtrol.setup-latest.zip** file to that folder. This should create a **C:\Download-Omni\Control\3.x.xx.xxxx** eControl setup folder that is specific to the release version contained in the **econtrol.setup-latest.zip** file.

**IMPORTANT NOTE:** Do not delete or remove the folder containing the eControl installation files. You can use those files to upgrade or uninstall eControl in the future.

#### Where to install eControl

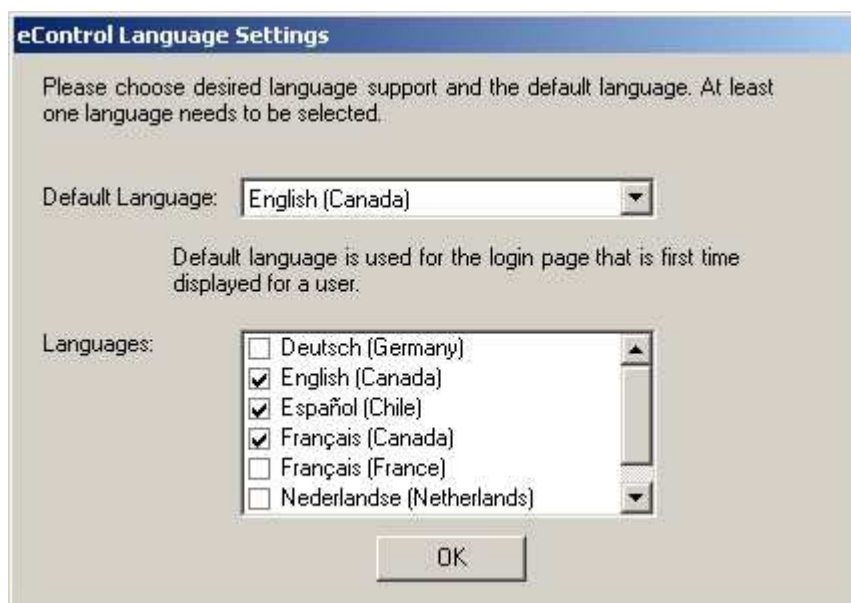
Prior to installing eControl, ensure that each target server meets the system requirements. Run the eControl installation on the following host servers:

- On the Windows server that will host the eControl Host Server.
- On the Windows server that will host the eControl Remote Agent Server.

## Run the eControl Installer

The eControl **setup.exe** file will ensure that Windows installation and .Net framework requirements are met, then install eControl and Riva on the host Windows system:

1. Execute the **setup.exe** file in the **C:\Download-Omni\Control\3.x.xx.xxxx** eControl setup folder.
2. If you see the EULA license agreement page for **Windows Installer 3.1** click **Accept**. This indicates that the Windows Installer 3.1 application is not installed and you agree to install it.
3. If you see the EULA license agreement page for **.NET Framework 3.5 SP1** click **Accept**. This indicates that the required .Net Framework components are not installed and you agree to install it. Clicking **Accept** will start the installing the installation of the Windows 3.1 installer software.
4. When you see a window indicating that **Setup must reboot before proceeding** click the **Yes** button to allow the host Windows system to reboot.
5. After the Windows system reboots, login and the installation of the .Net Framework 3.5 SP1 components will automatically continue. This may take some time so please be patient.
6. When you see a window indicating that **Setup must reboot before proceeding** click the **Yes** button the host Windows system reboot.
7. At the **Welcome to the Omni eControl Setup Wizard** window click **Next >**.
8. At the **License Agreement** window, ensure that **Agree** is selected and click **Next >**.
9. At the **Select Installation Folder** window you can make the necessary adjustments and click **Next >** to continue.
10. At the **Confirm Installation** window click **Next >**.
11. At the **eControl Language Settings** window, select the default language and add the checks to the languages that you want installed.



eControl has been localized to support English, French, Spanish, German, Dutch, and Polish in the eControl web portal. Click **OK** to continue.

12. At the **eControl Web Component Configuration Window** window:



- Click **Yes** if installing on to the eControl Host Server and the eControl Portal will be the default web site.
  - Click **No** if this server hosts another website in the default website folders. You can always configure the eControl website manually in IIS manager. Contact Omni support for additional information.
  - Click **No** if installing on the server that will host the eControl Remote Agent Server.
13. At the **Installation Complete! eControl Web Server restart required** window, click **Yes** (this window will not appear if you selected **No** in the previous step)



14. At the **Installation Complete** window click **Close**.

**IMPORTANT NOTE:** The next two steps will create the eDirectory tree and GroupWise connections. The GroupWise connection requires file system access to the **wpdomain.db** file hosted on an NSS volume on a NetWare or Linux server, or on a local drive. If an eControl Remote Agent Server is being installed, run steps 2 and 3 on the eControl Remote Agent server first to create the GroupWise trusted application key.

## Step 2 - Create the Target eDirectory Tree Connection(s)

The next step involves running an "eDirectory Connection" wizard to create an eControl connection to a target eDirectory tree. This procedure needs to be repeated for each target eDirectory tree that will be managed using eControl. Connections need to be created for each instance where eControl has been installed in Step 1 (eControl Host Server and eControl Remote Agent Server).

Prior to running the eDirectory connection wizard, ensure that an eControl service account has been created in each target eDirectory tree, that this account uses the same username, e.g. "econtrol" or "ecadmin", that each account uses the same password and that the password is set to never expire, and that each account has been made a supervisor trustee of the root of the eDirectory tree.

To create an Active Directory connection:

1. From the windows desktop of the Windows system where eControl is installed click "Start" > "All Programs" > "Omni" > "eControl" > "Configure Connections". This will open the Riva Application.



2. Select "Setup" and click on the "Novell eDirectory" link in the "Connection Wizards" box. This will start the eDirectory connection wizard.
3. At the "Welcome to Novell eDirectory Connection Wizard" windows click **Next >** to continue.
4. At the "Target Information" window provide the information for the eDirectory authentication server (which server do the users authenticate to):



**New eDirectory Connection Wizard**

**Target Information**  
Enter the connection information for the eDirectory Server.

eDirectory Ldap Host :  Port :

Enable SSL

- Specify the DNS name (preferred) or IP address for the eDirectory LDAP authentication server.
  - Ensure that the "Enable SSL" option is checked (recommended). Click **Next >** to continue.
5. In the "Authentication Information" window, specify the LDAP context name of the eControl master service account that has supervisor rights to the root of the eDirectory tree.



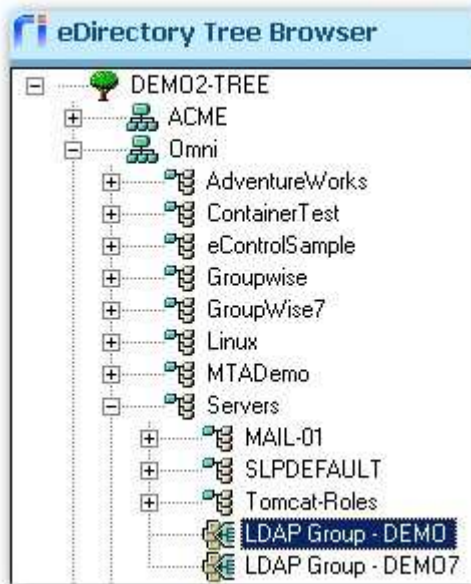
**New eDirectory Connection Wizard**

**Authentication Information**  
Enter credentials to connect to the eDirectory server.

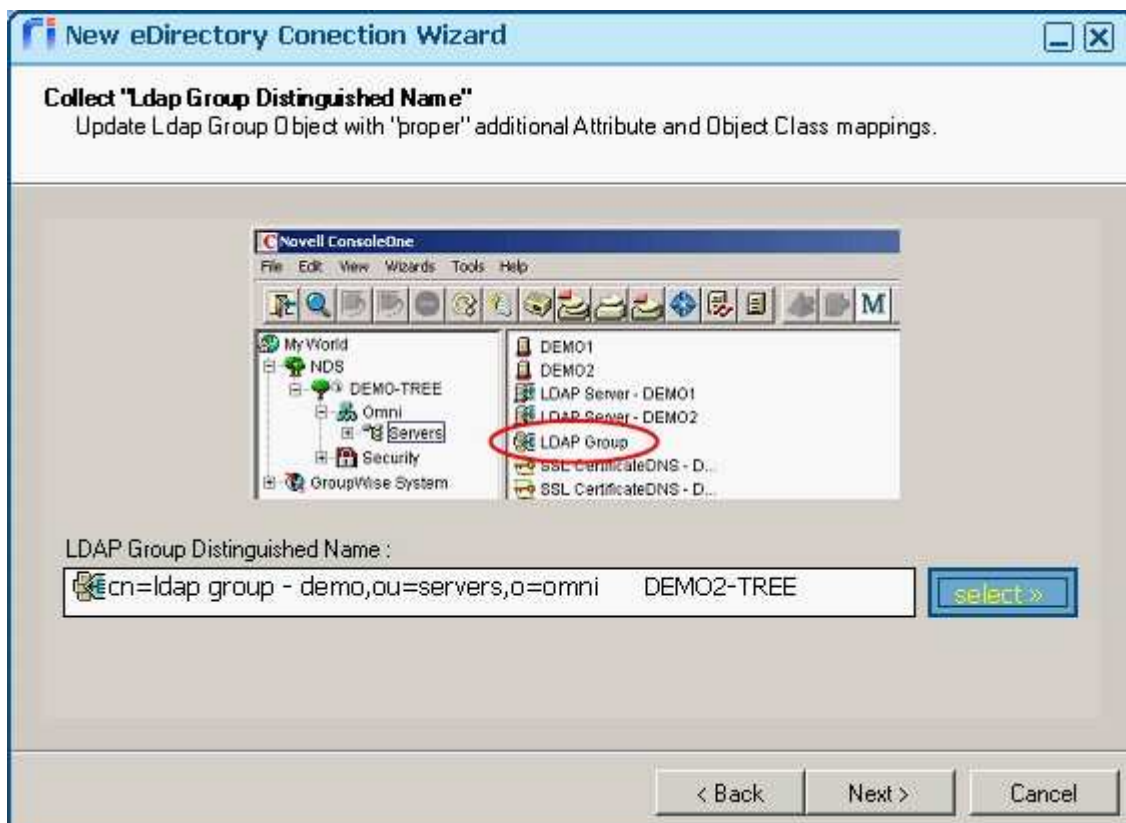
User Name :   
example: cn=admin,ou=users,o=omni

Password :

6. In the "Collect "Ldap Group Distinguished Name" window, click the **select >>** button.
7. In the "eDirectory Tree Browser" window, browse to and select the LDAP Group for the server that you authenticated to in Step 4. Click the **OK** button.



8. In the "Collect "Ldap Group Distinguished Name" window, click the **Next >>** button.



9. In the "Results for matched/Not Matched Attribute List and map" window, ensure that the "Skip Mapping Step" option is not checked and click **Next >**.

10. In the "Results for matched/Not Matched Class List and map" window, ensure that the "Skip Mapping Step" option is not checked and click **Next >**.
11. In the "Refresh eDirectory LDAP Server" window, click **Next >**.
12. In the "eDirectory connection successful" window, click **Finish**. This should auto start the GroupWise Connection Wizard.

### Step 3 - Create the target GroupWise Connections

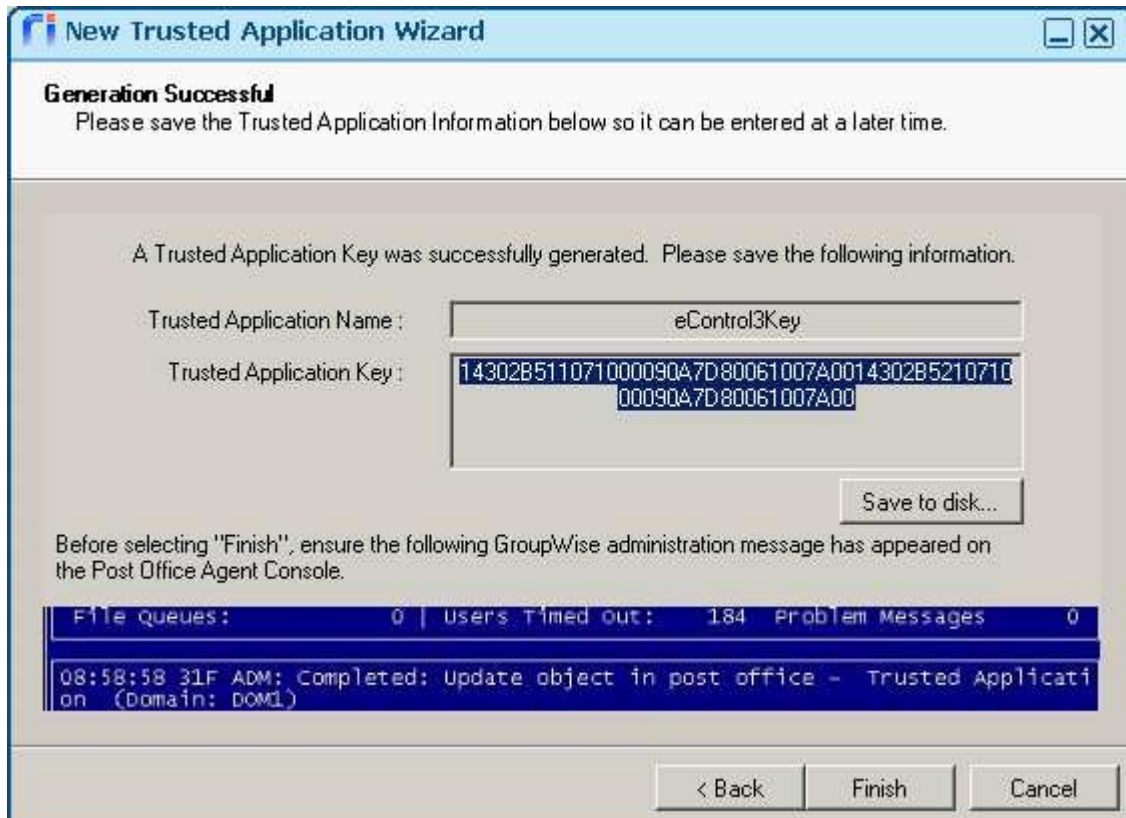
The next step involves running the "GroupWise Connection" wizard to create connection to GroupWise domains and post offices that will be managed by eControl:

1. At the "Welcome to the GroupWise Wizard" window, ensure that the "Enterprise Connection" option is selected and click **Next >**.

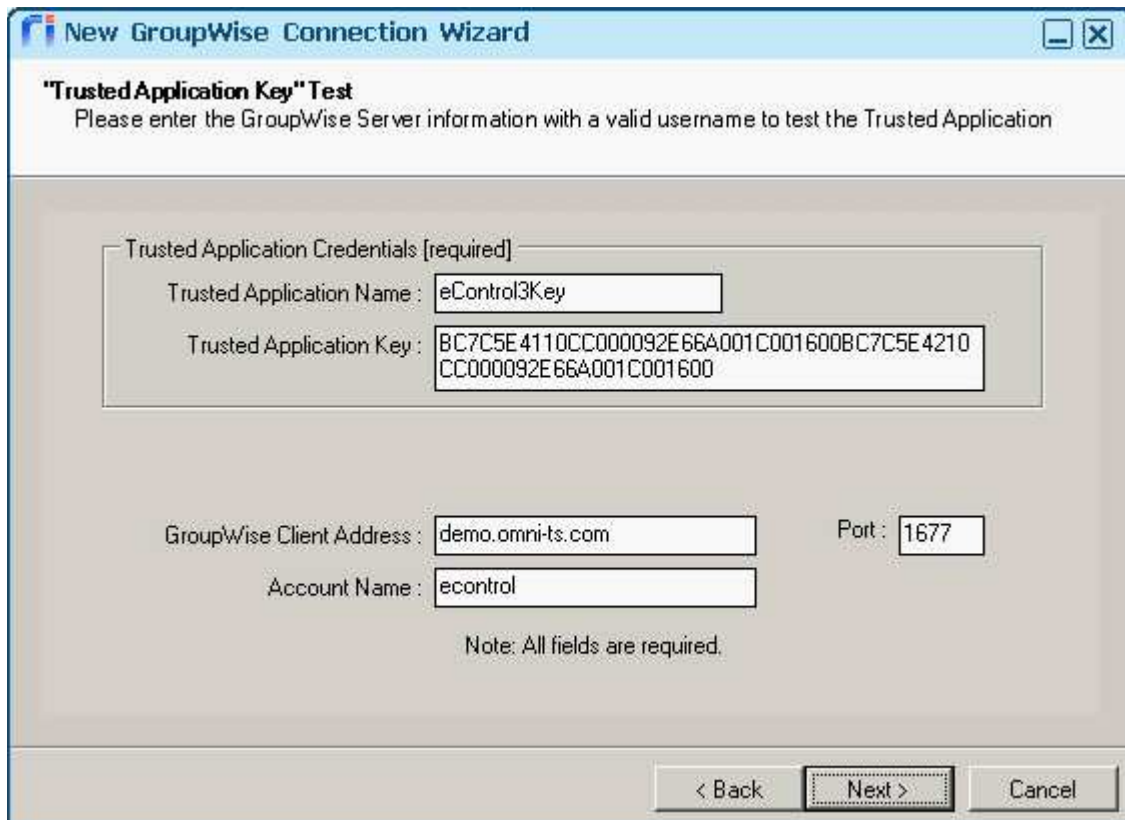


2. At the "Trusted Application Key" window:
  - Select "Create a new Trusted Application Key" if this is the first installation of eControl and a trusted application key has not been created before (proceed to step 3), or
  - Select "Manually Provide an existing Trusted Application Key" option if a trusted key has been created and you have the key information (proceed to step 7).
3. At the "Welcome to the Trusted Application Wizard" window, click **Next >**.

- At the "Collect Trusted Application Parameters" window, specify the path to the wpdomain.db file for the GroupWise domain that Riva will connect to (can be a mapped drive or UNC path to a GroupWise domain hosted on a NSS volume, or a NCP mount share, or a local drive) and the desired Application Name for the trusted key.
- At the "Collect Trusted Application Options" window, ensure that "Overwrite a Trusted Application Key with the same name as this one?" is selected and click **Next >**.
- At the "Generation Successful" window, click "**Save to disk ...**" and save a copy of the trusted key information. Click **Finish**.



- At the "Trusted Application Key Test" window, specify the Trusted Application Name and Trusted Application Key (if not automatically provided ... this can occur if you chose to "Manually Provide an existing Trusted Application Key" in step 2).



**New GroupWise Connection Wizard**

**"Trusted Application Key" Test**  
Please enter the GroupWise Server information with a valid username to test the Trusted Application

Trusted Application Credentials [required]

Trusted Application Name : eControl3Key

Trusted Application Key : BC7C5E4110CC000092E66A001C001600BC7C5E4210  
CC000092E66A001C001600

GroupWise Client Address : demo.omni-ts.com Port : 1677

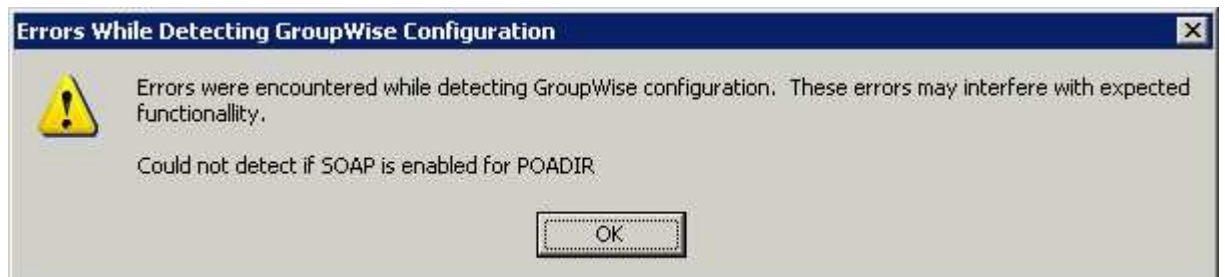
Account Name : econtrol

Note: All fields are required.

< Back Next > Cancel

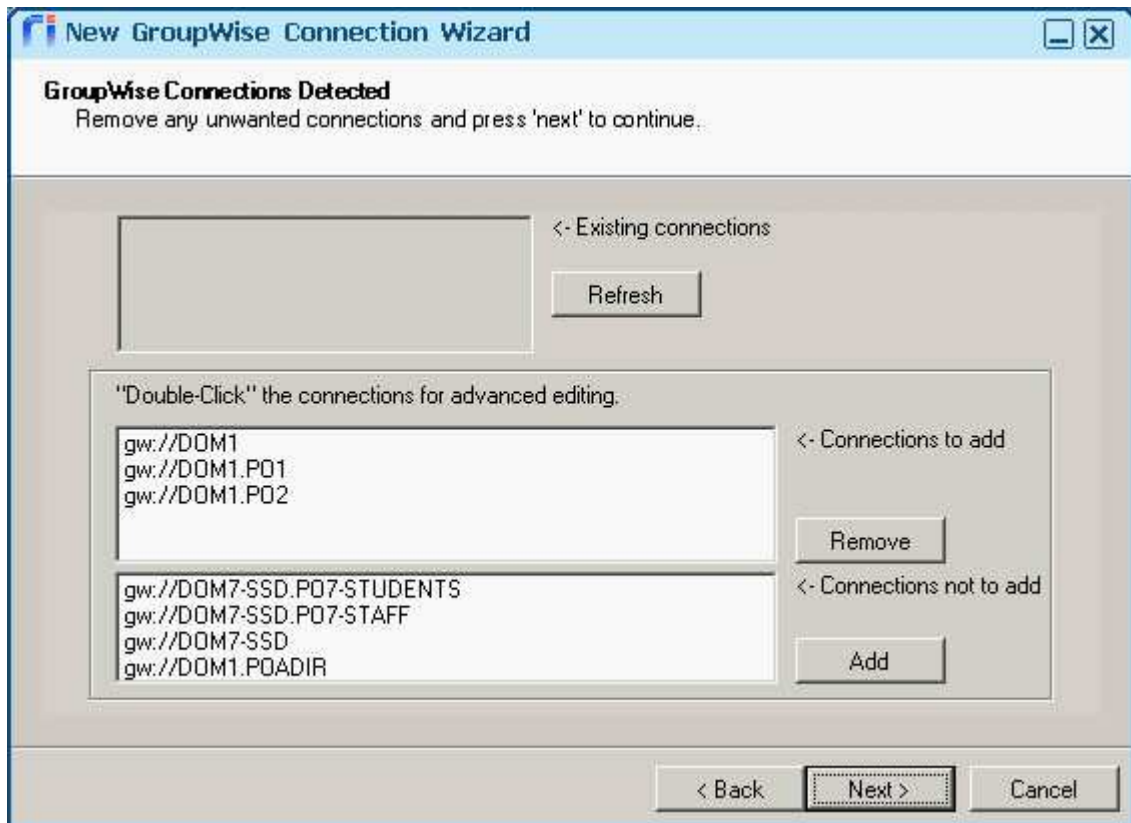
Add the GroupWise Client Address (IP address or DNS name) and Port number of the post office hosting the GroupWise account for the eControl master account, and the corresponding GroupWise account name, and click **Next >**.

- At the "Choose detection type" window, select **Automatic GroupWise Configuration Detection** and click **Next >**.
- At the "Choose an eDirectory Connection" window, select the eDirectory tree that hosts the GroupWise system and click **Next >**.
- If there are GroupWise post offices that are not configured for SOAP, an "Errors While Detecting GroupWise Configuration" window will open.



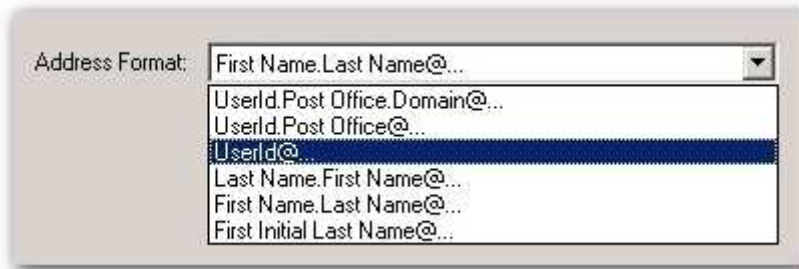
Click **OK**.

- In the "GroupWise Connection Detected" window, click the GroupWise domain and post office objects that will not be managed by eControl and click **Remove**. This will move those objects to the "Connections not to add" text box.



Click **Next >**.

12. In the "Internet Addressing" window, select the applicable Address Format from the drop-down list for the primary internet email address domain and click **Next >**.



13. In the "Automatic Configuration Results" window, click **Finish**.

The eDirectory and GroupWise connections will be visible in Riva "Setup".



- Repeat steps 1 to 13 for each additional GroupWise system being managed by eControl.

### Step 4 - Confirm the eDirectory Connection(s)

This step is necessary to confirm each eDirectory tree connection created in Step 2:

- Open "Configure Connections" (Riva application) and open the eDirectory tree connection under "Setup" by double-clicking the connection object.
- Under the "General" tab, confirm that the correct account details are recorded:



- Ensure that the appropriate LDAP Group is listed for the "Distinguished Name".
  - Ensure that the full LDAP context name of the eControl master service account is displayed in the "Username" field.
3. Under the "Connection Targets" tab, click the ldap:// connection and click the **"Test the connection target"** link. Click the **"OK"** button.



## Step 5 - Confirm and Configure the GroupWise Connections

This step is necessary to confirm and configure the GroupWise post office and domains connections created in Step 3:

1. Open "Configure Connections" (Riva application) and open the primary GroupWise Post Office connection under "Setup" by double-clicking the connection object.
2. Under the "General" tab, confirm that the correct account details are recorded:



Confirm that the GroupWise trusted application key name is displayed as the "Username".

- Under the "Options" tab, ensure that the correct "Address Format" option is selected and:



- **GroupWise on Remote NSS Volume:** If the entire GroupWise system is installed on one or more remote NSS volumes or NCP Mount Shares, specify the UNC path to the **wpdomain.db** file of the primary GroupWise Domain.
  - **GroupWise on Local Drive:** If the entire GroupWise system is on the local drive(s), specify the local drive path to the **wpdomain.db** file of the primary GroupWise Domain.
  - **GroupWise Empty Domain on the Local Drive:** If an empty GroupWise Domain is installed on the local drive, specify the local drive path to the **wpdomain.db** file of the empty GroupWise Domain.
4. Click the **Save** button to save the Options settings.
  5. Re-open the GroupWise Primary Post Office connection object.
  6. Under "Options" select all of the GroupWise Post Offices and Domain in the list box and click **Save**. This will copy the settings to all of the rest of the GroupWise connection objects.



7. Re-open the GroupWise Primary Post Office connection object.
8. Under "Test Trusted Key", ensure that "This connection already has the Trusted Key" line exists. Type in the name for a GroupWise account and click the **Test Key** button.



In the "Success" window, click the **OK** button. In the "Connection Edit" window, click the **Save** button.

## Step 6 - Install and Configure the eControl Remote Agent Server

**Note:** Do not perform the tasks associated with this step unless an eControl Remote Agent Server is required.

An eControl Remote Agent Server will need to be installed and configured if one of the following conditions exists:

- **GroupWise is not hosted on a NSS volume or NCP mount share on Linux** – and an empty GroupWise Domain cannot be installed on the eControl Host Server.

OR

- **GroupWise is installed on a Windows Server** – the eControl Host Server cannot be hosted on the GroupWise server, and an empty GroupWise Domain cannot be installed on the eControl Host Server.

Under either of these circumstances, the GroupWise connection wizard on the eControl Host Server will not be able to create a GroupWise trusted application key. Steps 1 through 5 should be performed on the designated eControl Remote Agent Server first, and then on the eControl Host Server.

## Install the eControl Remote Agent Server

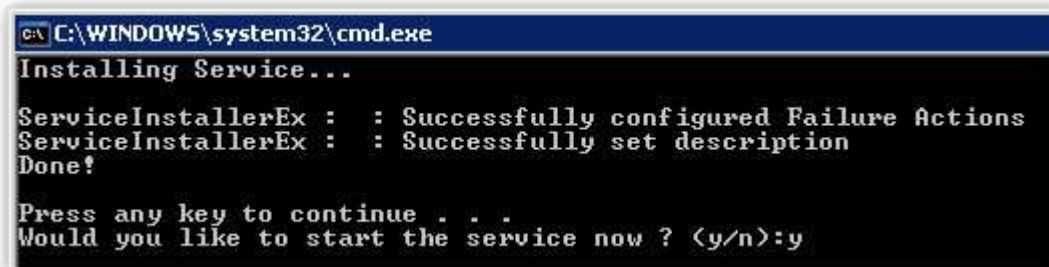
To install the eControl Remote Agent Server:

1. If eControl has not been installed on this server, ensure that the server meets system requirements for eControl and following the procedure detailed in **STEP 1 – Install eControl** (see pages 10-13). At the **eControl Web Component Configuration Window** window



click **No, Skip or Configure Manually**.

2. Complete the procedures detailed in **STEP 2** to **STEP 5** (see pages 12-23).
3. To install the eControl Connection Agent service, run the **InstallAgent.bat** file located in C:\Program Files\Omni\eControl\Omni.Services.Connection



Answer **y** to complete the installation of the service.

## Configure “Remote Agent” Support on the eControl Host Server

To configure the eControl Host Server to connect to the eControl Remote Agent server:

1. Open “Configure Connections” (Riva application) and open the AD domain connection under “Setup”.
2. Under the “Remote Agent” tab, specify the **Host** that is running the eControl Connection Agent service.



3. Click **Save >>** to save the settings and close the Connection Edit window.

### Configure "Remote Agent" Support on the eControl Remote Agent Server

To configure the Remote Agent server to connect to the eControl host server:

1. Open "Configure Connections" (Riva application) and open the AD domain connection under "Setup".
2. Under the "Remote Agent" tab, specify the **eControl Server IP** that is running the eControl website.



3. Click **Save >>** to save the settings and close the Connection Edit window.

## Step 7 - Restart IIS

Once all eDirectory and GroupWise connection settings have been configured and tested, IIS on the eControl Host Server must be restarted by performing an **iisreset /restart**.

## Initial Sign-on

The first time that an eControl Login is performed is important because there are some initialization tasks that get completed. The first login should use the credentials of the eControl master service account configured in the eDirectory Tree connection.

The initial login will provide an option to create a sample eControl configuration which can be used for training and evaluation.

You can access the eControl login from:

- <http://localhost> on the eControl host server
- <http://<eControl host server IP address or DNS name>> from any supported browser on any desktop.

eControl has been optimized to work best with Internet Explorer 7.0 or higher, but would work with most browsers that support AJAX. Please be patient as it may take a few moments before the eControl login page appears for the first time.



**eControl Login:**

Username:

Password:

Language:

- English (Canada)
- Español (Chile)
- Français (Canada)

- **Username** – provide the login name configured to the Active Directory connection configured during the installation. If there are multiple AD connections, choose the domain where you want to host the eControl management accounts from.
- **Language** – This will appear if eControl was installed with multiple language support. The visible language of the eControl web pages will be localized to the language selected during the login.

To properly initialize the eControl web portal:

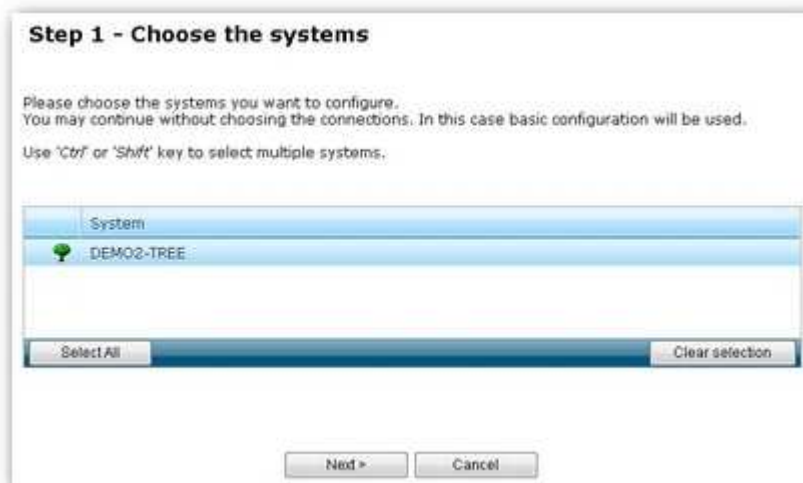
1. Login as the primary eControl administrator configured in the Active Directory connection during the installation.

2. At the "Welcome to eControl" page:

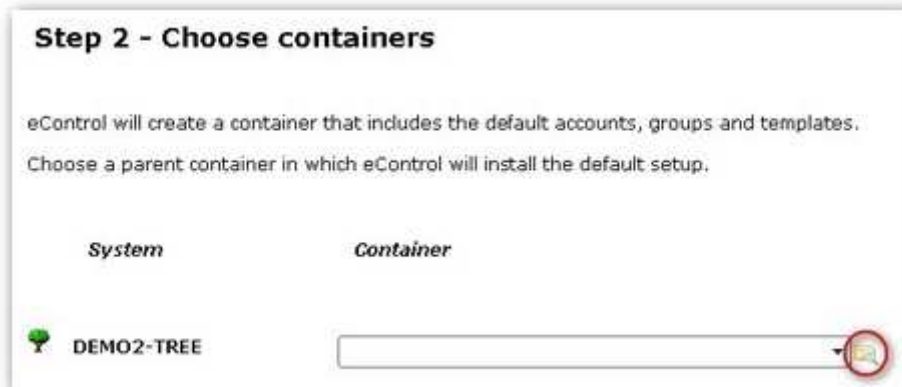


- Choose **START** to run the basic configuration wizard, or
- Choose **Skip wizard** to skip the wizard

3. Assuming that **START** is selected, Step 1 will present a list of Active Directory domains that connections have been created during the eControl installation. If you want sample eControl objects created in all the domains, click "**Select All**", otherwise, select the domain(s) from the list and click **Next >**.



- In **Step 2 – Choose Containers**, click on the ellipsis beside the empty text box



to open an eControl Directory Browser window. Navigate the Active Directory domain and select the container to act as the parent for the eControlSample container and sample objects.

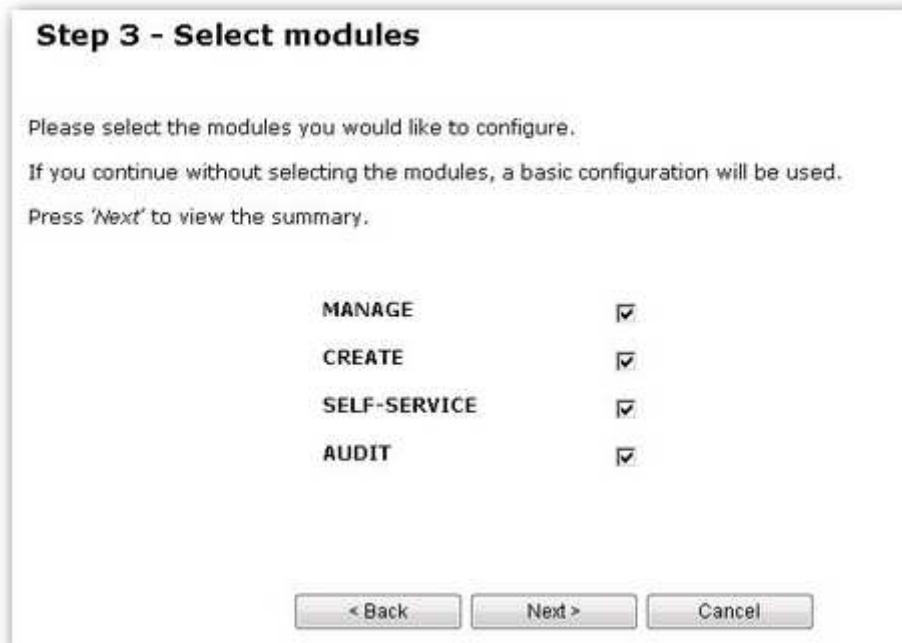


Click **OK** to close the eControl Directory Browser window. The selected container will appear in the text box.

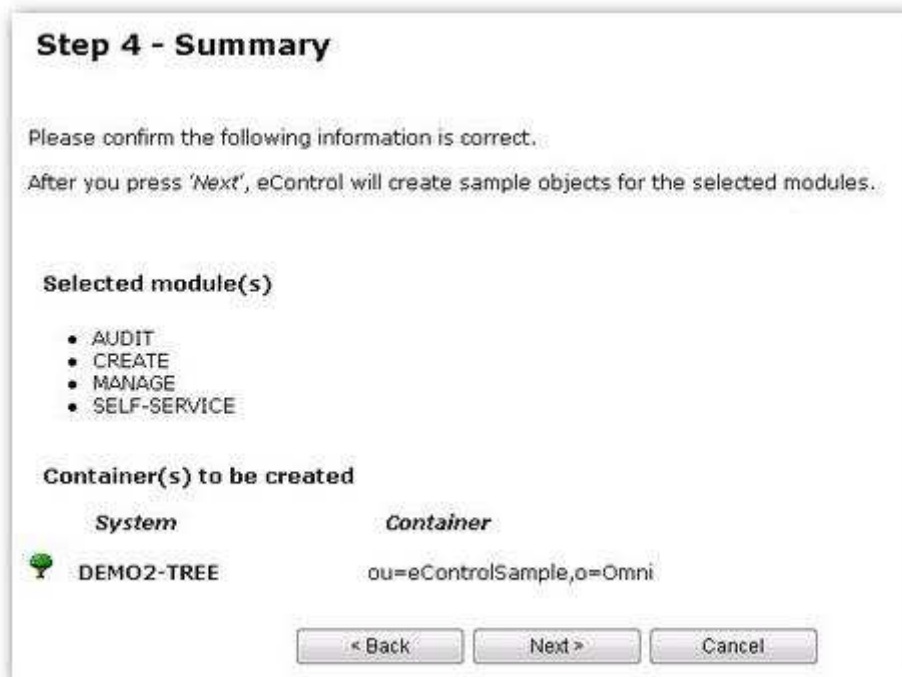


- In the **Step 2 – Choose Containers** window, click **Next >** to continue.

6. In the **Step 3 – Select modules** window click **Next >**.



7. In the **Step 4 – Summary** window, click **Next >**.



8. In the **Save configuration to disk** window, click **Next >**.



9. In the "Wizard Complete!" window, click **Apply Settings**.



## License eControl

### Request a License

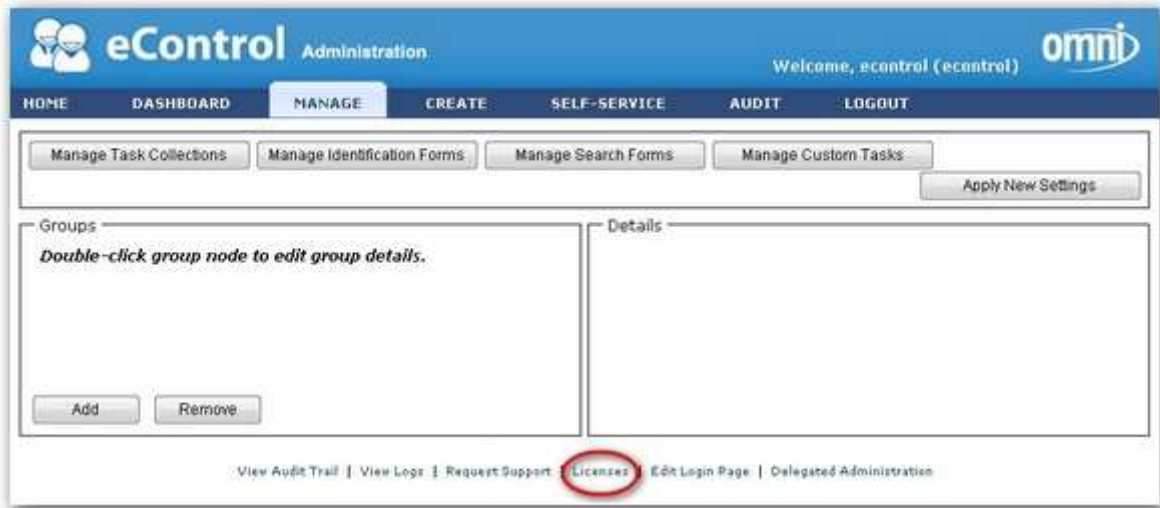
eControl is licensed from the "Administration" panel in the eControl portal website. You must first request a license:

1. In the eControl portal, notice that the footer indicates that eControl is running in DEMO mode.

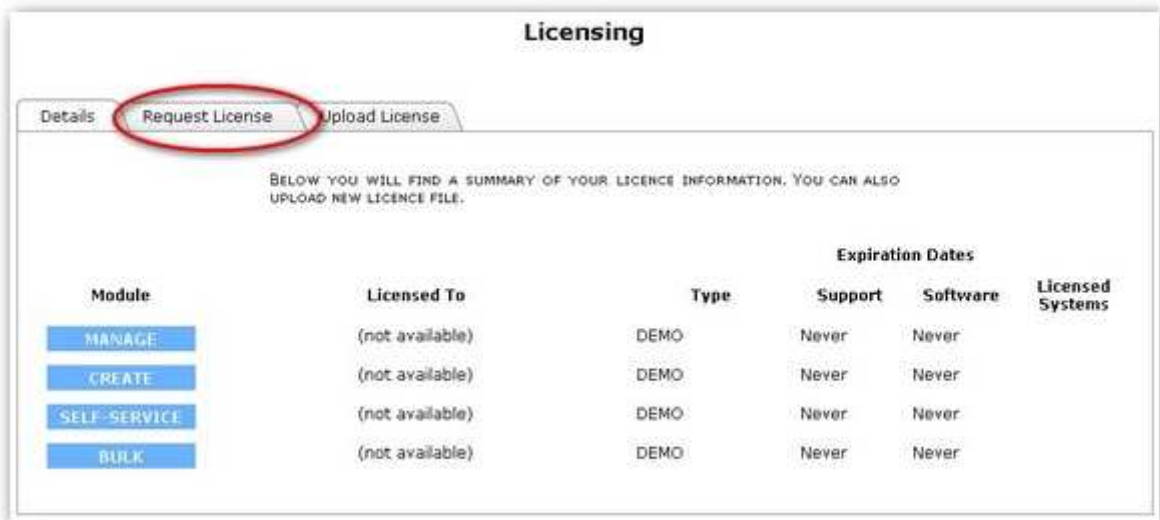


Click on the **Administration** in the menu bar.

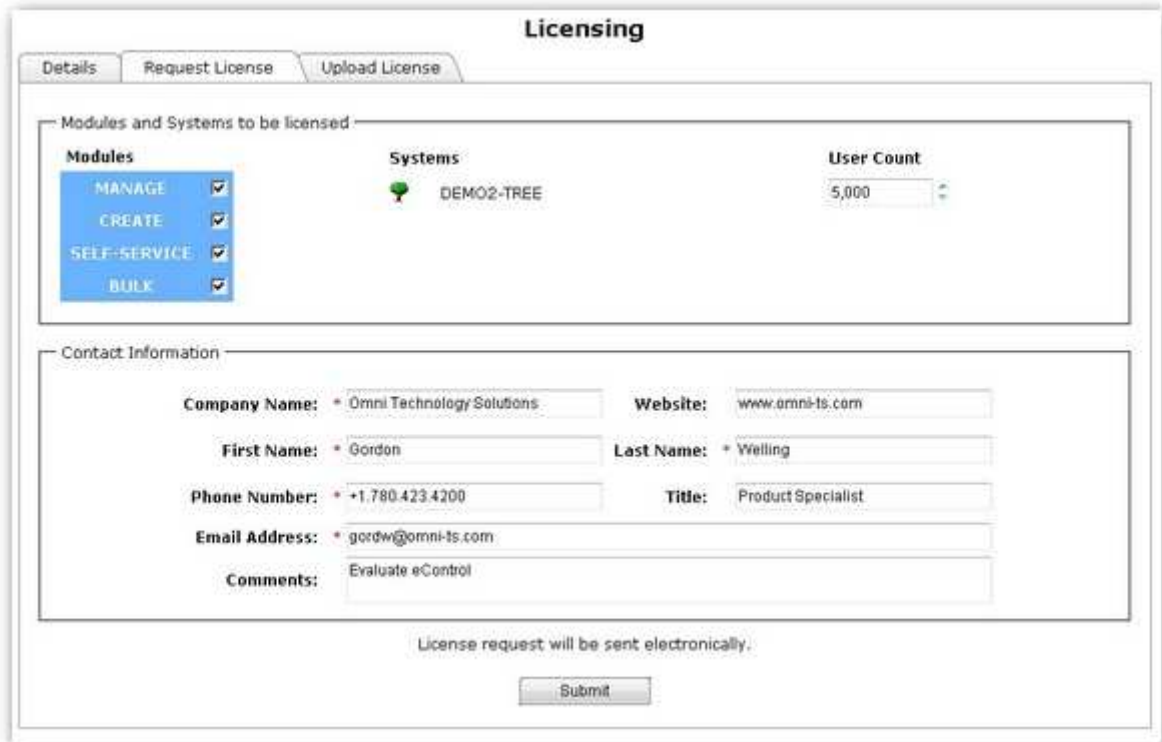
2. In the "Administration – Manage" page, click on the **Licenses** link in the footer.



3. In the “Licenses - Details” page, click on the **Request License** tab.



4. In the “Licenses – Request License” page, select modules to license, specify the desired license count and complete the contact information. The ‘\*’ next to a field indicates information must be provided.



Click **Submit** to continue. A successful upload will be indicated.

### Upload the License

A .license file will be sent by email within 24 working hours. Save a copy of the .license file locally and complete the following steps:

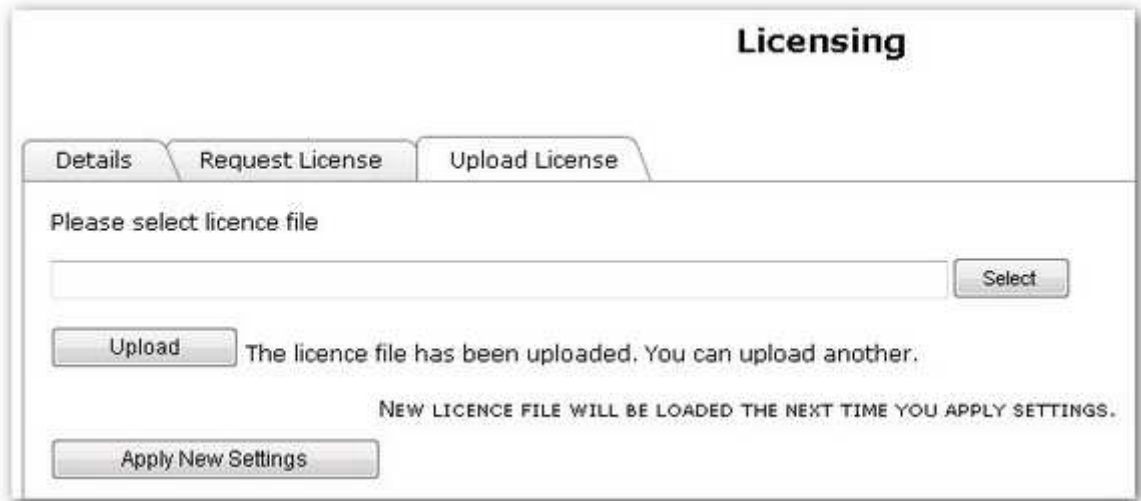
1. Login in eControl as the eControl service account.
2. Select **Administration** from the menu bar and click on the **Licenses** link in the footer.



3. To apply the license file, click the **Upload License** tab. Click the **Select** button, navigate to and select the .license file and click **Upload**.



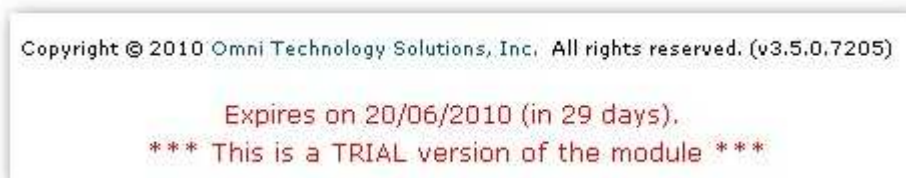
- If the license file upload is successful, click **Apply New Settings**.



- License details can be verified under the **Details** tab.



- Once the license has been applied, the license status in the footer should change.



**Note:** If the footer information does not reflect the new license information, logout of eControl and close the browser. Perform an **IISRESET /RESTART**. Open a browser and logon into eControl and check the footer information.

## Assign Delegated Administration

Access to the eControl "Administration" pages is limited to the account configured in the eDirectory connection (or an Active Directory connection in a mixed Directory environment), and to members of the group that is assigned "Delegated Administration."

To assign "Delegated Administration":

1. Create a group in eDirectory (e.g. *eControl-Admins*) and add members that should be provided access to the eControl administration panel.
2. Login to eControl as the eDirectory connection user.
3. Click on "Administration" in the menu bar.
4. Click on the "Delegated Administration" link in the footer of any "Administration" panel page.
5. Click **Add**. Navigate to and select the desired group for eControl Delegated Administrators.
6. Navigate to the "Manage" page and click the **Apply Settings** button.
7. Logout and login as a Delegated Administrator.

## Upgrading eControl

There are 2 types of upgrading for eControl:

- **Upgrade** – upgrade an existing installation of eControl to a new major release, e.g. from eControl 2.5 to eControl 3.x
- **Update** – update an existing eControl installation to a newer minor release, e.g. from eControl 3.4 to 3.5

### Upgrade eControl 2.5 to eControl 3.x

Upgrading eControl 2.5 to the latest release of eControl 3.x is a two step process:

- Upgrade eControl 2.5 to eControl 3.0. This usually involves migrating eControl 2.5 from a Windows 2000 server platform to eControl 3.0 on a Windows 2003 or 2008 server platform.
- Update the eControl 3.0 installation to the latest 3.x release.

Upgrading eControl requires direct intervention and assistance from Omni technical support. Customers must contact Omni to schedule an eControl 2.5 to 3.x upgrade.

### Update eControl to the Latest Release

Updating eControl 3.x to the latest release can be performed by the customer without assistance from Omni technical support.

### Confirm the eControl Installation

It is important to upgrade all related installations of eControl. Confirm the following information:

- On the **eControl host server**:
  - Is the Omni Connection Service Agent installed?
    - Open Windows Manage > Services and confirm if there is an **Omni eControl Connection Agent** service installed and "Started".
    - View the properties of this agent and under "Log On" confirm how the agent is configured to log on as. If the "Local System account" is not selected, record the account being used as this will have to be reconfigured after the agent is reinstalled (see below).
- **On the eControl remote agent server** hosting the Omni eControl Connection Agent:
  - Open Windows Manage > Services and confirm if there is an **Omni eControl Connection Agent** installed and "Started".
  - View the properties of this agent and under "Log On" confirm how the agent is configured to log on as. If the "Local System account" is not selected, record the account being used as this will have to be reconfigured after the agent is reinstalled (see below).

### Backup eControl Configuration and License Files

On the **eControl host server**, use Windows explorer make a copy of the following folders:

- On a Windows 2003 server:
  - C:\Program Files\Omni\Riva\Configuration
  - C:\Program Files\Omni\Riva\Licenses
- On a Windows 2008 server:
  - C:\Program Files (x86)\Omni\Riva\Configuration
  - C:\Program Files (x86)\Omni\Riva\Licenses

On the **eControl remote agent server**, use Windows explorer make a copy of the following folders:

- On a Windows 2003 server - C:\Program Files\Omni\Riva\Configuration
- On a Windows 2008 server - C:\Program Files (x86)\Omni\Riva\Configuration

### Uninstall the Omni eControl Connection Agent Service

Uninstall the eControl Connection Agent service from the eControl Remote Agent Server where the Agent is installed (*Note: the path will vary depending on the release of eControl currently installed*). Run the **UninstallAgent.bat** file from one of the following locations:

- C:\Program Files\Omni\eControl\Agents\Omni.Services.Connection\
- C:\Program Files\Omni\eControl\Agents\Omni.Services.Connection.Agent\
- C:\Program Files (x86)\Omni\eControl\Agents\Omni.Interop.Agent\
- C:\Program Files (x86)\Omni\eControl\Agents\Omni.Services.Connection\
- C:\Program Files (x86)\Omni\eControl\Agents\Omni.Services.Connection.Agent\

### Uninstall eControl

Uninstall eControl from the eControl host server and the eControl remote agent server where the Omni eControl Connection Agent is installed. This can be done in one of two ways:

- Use **Windows Control Panel > Add or Remove Programs** to remove "Omni eControl" **OR**
- Run the eControl **setup.exe** installer for the version of eControl currently installed and select "**Remove Omni eControl**"

### Reinstall eControl

Reinstall eControl on the eControl host server and the eControl remote agent server where the Omni eControl Connection Agent needs to be installed.

1. Download and extract the latest release of eControl
2. Run the **setup.exe** file and install eControl in the same manner and in the same locations that it was previously installed.
  - on the eControl host server first
  - on the eControl remote agent server

### Reinstall Omni eControl Connection Agent Service

Reinstall the Omni eControl Connection Agent on the eControl Remote Agent Server, wherever it was installed previously:

1. Run the **InstallAgent.bat** file on the eControl server and on the Exchange servers where the Omni Services Connection Agent is installed:
  - Run the **InstallAgent.bat** file from  
C:\Program Files\Omni\eControl\Agents\Omni.Services.Connection
  - Answer **Y** to the question to start the service.
  - Using Windows Manage > Services configure the Log On properties of the Omni Services Connection Agent to match those credentials confirmed before starting the update process and restart the agent service.
2. Run **iisreset /restart**

### Restore the eControl Configuration and Licenses Folders

(Optional) After the update is completed, if eControl does not appear to connect to the configured AD domains and Exchange Mailbox servers, or if the eControl website appears to be running in "DEMO" mode, restore the backup copies of the \Configuration and \Licenses folders:

1. Close the Riva application.
2. Using Windows Task Manager, end the process for the **Omni.Services.Connection.exe** process.
3. Restore the backup files as required:
  - Copy the backup \Licenses folder to C:\Program Files\Omni\Riva\Licenses
  - Copy the backup \Configuration folder to C:\Program Files\Omni\Riva\Configuration
4. Run **iisreset /restart**

## **eControl 3.5 for eDirectory & GroupWise Installation & Update Guide**

---

5. Open a browser and login into the eControl portal. A new **Omni.Services.Connection.exe** process should launch in Windows Task Manager.
6. Confirm that the eControl web portal is behaving as expected.
7. Close Windows Task Manager.

## Support for eControl

### Reporting a Technical Issue

The eControl "Administration" pages include a "Request Support" link in the footer.



Complete the form and click **Submit**. The eControl server will send the issue and a copy of the application logs and config files to our technical support team.

### eControl - Request Support

THANK YOU FOR TAKING TIME TO SUBMIT AN ISSUE REPORT. YOUR FEEDBACK IS INVALUABLE TO HELPING IMPROVE ECONTROL AND INCREASE YOUR SATISFACTION.

YOUR ISSUE WILL BE ASSIGNED TO A CASE MANAGER FOR RESOLUTION. PLEASE EXPECT TO BE CONTACTED WITHIN TWO BUSINESS DAYS.

First Name:	* Gordon	Last Name:	* Welling
Company Name:	* Omni Technology Solutions		
Phone Number:	* +1.780.423.4200	Severity:	* Normal
Email Address:	* gordw@omni-ts.com		
Issue Type:	* Application Error		
Problem Title:	* Licensing not working		
Problem Description: (Note: Please include steps to reproduce)	* I applied the license file provided and eControl website is still working in "DEMO" mode		

### Upgrade and Maintenance Support Agreements

Customers who have current upgrade and support contracts are eligible to receive full email and telephone support Monday to Friday between 9:00 a.m. and 5:00 p.m. Mountain Time during regular working days. Limited email support may be available during extended hours. Email and telephone support is also available to customers who are evaluating Riva. 365x7x24 support is available for optional purchase.

## Contacting Support

You can contact support by phone, email or fax.

Email: support@omni-ts.com  
Phone: +1-780-423-4200  
Fax: +1-780-423-4711

You can also use the "Contact Us" link in the upper right-hand corner of our web site. Please include as many details as possible when requesting support:



The screenshot shows a web-based contact form titled "contact form". It contains several input fields: "Topic" (dropdown menu with "Technical Support" selected), "Subject" (text box with "License not working"), "Product" (dropdown menu with "Management - eControl" selected), "Your Name" (text box with "lan"), "Your Email" (text box with "Sample"), and "Contact Number" (text box with "+1.234.567.8901"). Below these fields is a CAPTCHA section with the image "Which hallowed" and a text box containing "which hallowed". To the right of the CAPTCHA is a ReCAPTCHA logo with the text "stop spam. read books.". Below the CAPTCHA is a "Message" text area containing the text: "I have applied the .license file but eControl indicates that it is still running in "Demo" mode.". At the bottom of the form is a "Send »" button.

### Online Resources

Online resources for Riva include:

- Product Documentation: Go to [www.omni-ts.com](http://www.omni-ts.com) select **Support**, follow the link for **Documentation** and select **eControl and EMU Documentation**
- eControl Flash Tutorials: will be added to [www.omni-ts.com/quicktours](http://www.omni-ts.com/quicktours)
- Support Forum: Go to [www.omni-ts.com/Forum](http://www.omni-ts.com/Forum) and:
  - Select the **eControl ~ Installation, Management and Support** forum.
  - "**eControl Tips**" available at <http://www.omni-ts.com/forum/post--2124--page-1.html> is a collection of forum articles to provide troubleshooting and advanced management steps for eControl.
- Product FAQ: Go to <http://www.omni-ts.com/web-management> and select **Frequently Asked Questions**