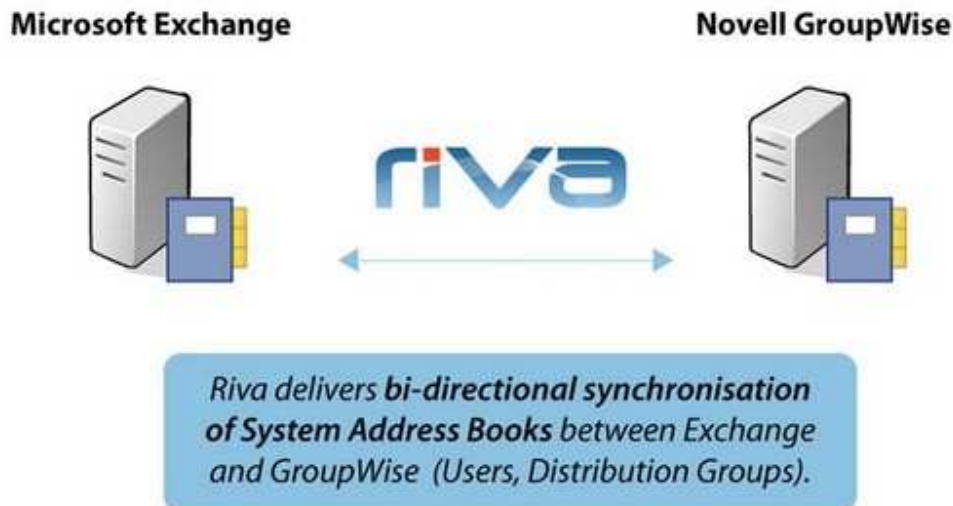


This Guide

Welcome to the Administrator Guide for Omni's Riva Identity Integration "Managed External Domains".



Riva Managed External Domains is designed for those environments that host both Microsoft Exchange 2007 or 2010 and GroupWise 7 or 8 and need a replacement for the Novell GroupWise Gateway to Exchange.

How Riva Identity Integration "Managed External Domains" Works

Riva "Managed External Domains" is actually composed of two Riva identity integration policies:

- **GroupWise External Domain Integration Policy** - synchronizes Active Directory (AD) users and contacts as GroupWise users in a GroupWise external domain.
- **Exchange Global Address List Integration Policy** - synchronizes the eDirectory user objects as AD contacts in an AD container.

Although administrators can choose to configure contact synchronizing in only one direction, e.g. from eDirectory to Active Directory, this guide presumes that bi-directional synchronization will be configured. This configuration allows both systems' users to be available in both system address books.

Table of Contents

How Riva Identity Integration “Managed External Domains” Works	1
System Requirements	3
Riva Host Windows System	3
Preparing Target Systems	4
Setup and License the Riva Identity Integration Server	4
Step 1 – Install Riva the Identity Integration Server	4
Step 2 – Setup the Riva Connection to the eDirectory and GroupWise Systems	4
Step 3 – Setup the Riva Connection to the Active Directory System	8
Step 3 – License Riva	10
Create Managed External Domain Policies	12
Create the “Exchange Global Address List Integration” Policy	12
Create the “GroupWise External Domain Integration” Policy	13
How to Execute and Schedule Riva Policies	15
Support for Riva	19
Reporting a Technical Issue	19
Upgrade and Support Maintenance Agreements	19
Free Support	20
Contacting Support	20
Online Support	20

System Requirements

Riva Host Windows System

Riva Identity Integration Server makes use of the Riva application which must be installed and configured on a host Windows system that meets the following system requirements:

- **Riva Host System OS:** Windows XP, Windows server 2003, 2003R2
- **Software Requirements:**
 - Windows .NET Framework 2.0 or higher must be installed.
 - Novell Windows client for eDirectory
 - Novell Windows client for GroupWise
- **Minimum Processor (CPU):** Intel P4 / AMD Athlon XP (supports x86 and x64 architectures)
- **Minimum Memory (RAM):** 256 MB (in addition to host system requirements)
- **Minimum Disk Space:** 500 MB
- **Certified Messaging Systems:**
 - Microsoft Exchange 2010, 2007 SP1 with Rollup 1, 2003 SP1+
 - GroupWise 7.0.x or 8.0.x
- **Protocols:** Standard TCP/IP on applicable ports to connect to GroupWise, and standard non-secure (port 389) or secure (port 636) LDAP connections to eDirectory and Active Directory must be available for communication between the Riva server and the target servers.

Preparing Target Systems

Requirements vary depending on which Riva policy is being utilized:

- For the **GroupWise External Domain Integration Policy** ensure that:
 - A GroupWise external domain and external post office(s) must be created in the target GroupWise system,
 - Identify an eDirectory/GroupWise user that has supervisor rights to create new user objects in the target external post office and has supervisor rights to the wpdomain.db file of the GroupWise domain that the external domain will link to,
 - Identify the source parent container in Active Directory that contains user and contact objects to synchronize to the target GroupWise external post office.
 - Riva requires the creation and configuration of Active Directory, eDirectory and GroupWise connections.
- For the **Exchange Global Address List Integration Policy** ensure that:
 - Identify an Active Directory account that has permissions to create contacts in the target Active Directory container.
 - Identify the source eDirectory parent container to synchronize to Active Directory. This policy will synchronize all users in the source and corresponding child eDirectory containers to the target Active Directory container.
 - Create or identify a target Active Directory container dedicated to holding the contacts synchronized from eDirectory.
 - Configure a Global Address List recipient policy (Exchange 2003) or an Address List recipient filter (Exchange 2007/2010) to ensure that the contacts synchronized from the source eDirectory system are published in the target Exchange system.
 - Riva requires the creation and configuration of Active Directory and eDirectory connections.

Setup and License the Riva Identity Integration Server

There are four steps to install and configure Riva Identity Integration Server on a Microsoft Windows system:

- Step 1 - Install the Riva Identity Integration Server
- Step 2 - Setup the Riva connection(s) to the target eDirectory and GroupWise system(s)
- Step 3 - Setup the Riva connection(s) to the target Active Directory domain(s)
- Step 4 - License Riva

Step 1 - Install Riva Identity Integration Server

To install Riva, create a **C:\Program Files\Omni\Riva** folder. (Note: If you are an eControl customer, create a Riva2 folder to be used for Riva Integration Server.) Extract the riva-latest.zip file and copy the contents of the **riva-latest** folder to the **C:\Program Files\Omni\Riva** folder. Make a shortcut of the Riva.exe file to your desktop and label it as "Launch Riva".



Double-click the **Launch Riva** desktop icon, or double-click the **Riva.exe** file in the Riva installation directory.

The next requirement is to ensure that the latest release of Riva is installed:

1. Run **Riva** and click on **Check for Updates** in the menu bar. Follow the update wizard to download and apply the latest release files as applicable.
2. Close and restart **Riva**.

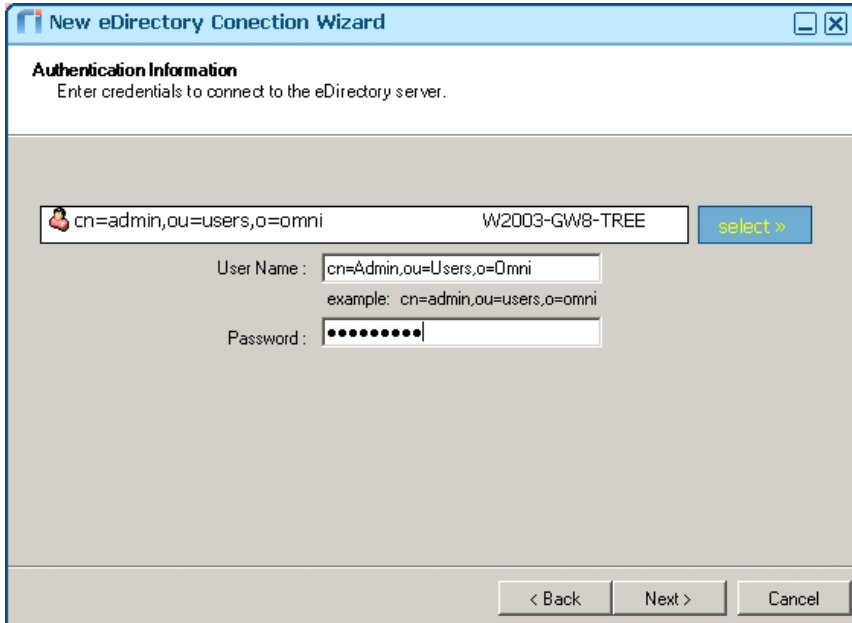
Step 2 - Setup the Riva Connections to the eDirectory and GroupWise Systems

To add and configure the target eDirectory and GroupWise system connections:

1. Select the **Setup** tab and click "Novell eDirectory" in the **Connection Wizards** list to run the applicable eDirectory Connection wizard.
2. At the **Welcome** window click **Next >**.
3. At the **Target Information** window, enter the IP address or DNS name of the eDirectory LDAP server. Choose to enable SSL (port 636) or disable SSL (port 389). Click **Next >**.
4. At the **Authentication Information** you can manually provide the LDAP context-based user name, e.g. **cn=admin,ou=users,o=omni** or if the LDAP server supports anonymous binds, click the **select >>** button, browse the eDirectory tree and select the desired user and click the **Ok >>** button.

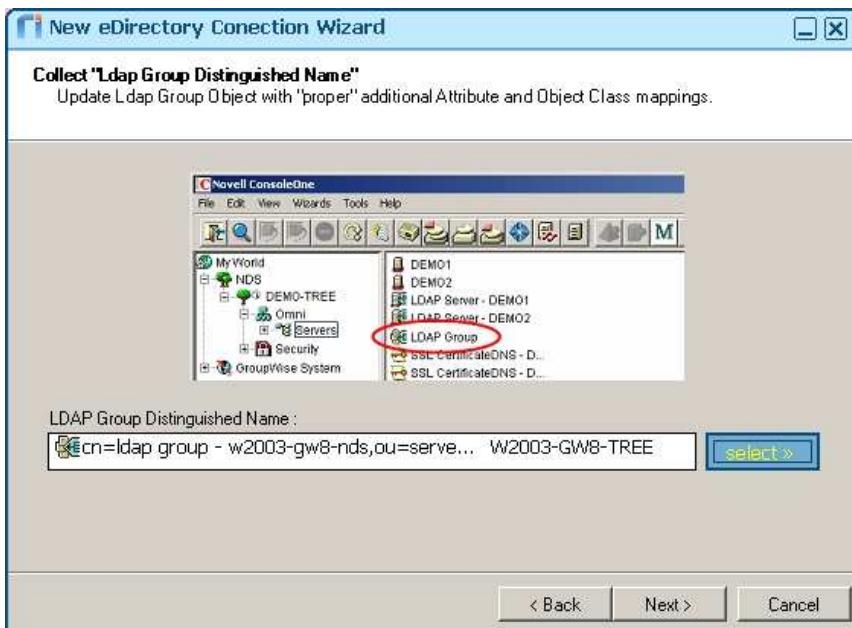
Note: For the "GroupWise External Domain Integration" policy provide credentials for a user with supervisor rights, otherwise credentials for a user with normal rights can be used.





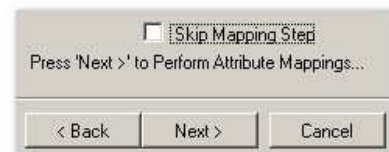
Provide the password and click **Next >**.

- At the **Collect "Ldap Group Distinguished Name"** window, click on the **select >>** button, navigate the eDirectory tree and select the LDAP group for the LDAP server identified in step 2 above.

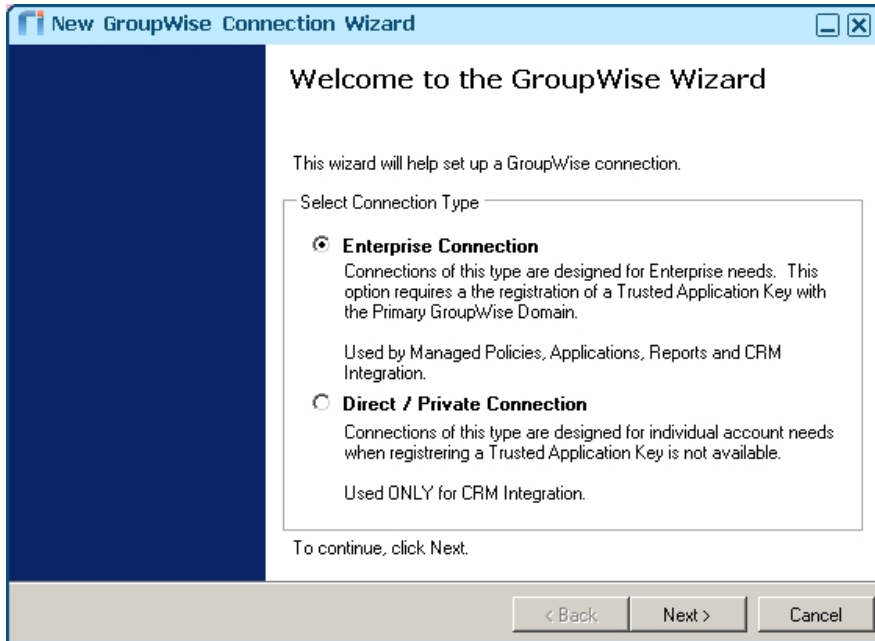


Click **Next >**.

- At the **Results for Matched/Not matched Attribute List and map** window, uncheck the **Skip Mapping Step** option and click the **Next >** button.
- At the **Results for Matched/Not matched Class List and map** window, uncheck the **Skip Mapping Step** option and click the **Next >** button.



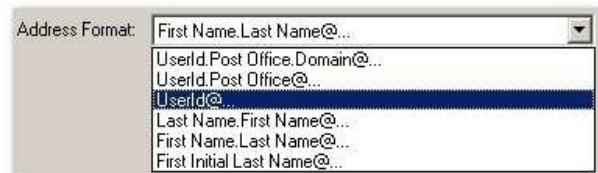
8. At the **Refresh eDirectory LDAP Server** window click the **Next >** button.
9. At the **eDirectory connection successful** window, click the **Finish** button. This will automatically start the GroupWise connection Wizard.
10. At the **Welcome to the GroupWise Wizard**, ensure that the **Enterprise Connection** option is selected and click the **Next >** button.



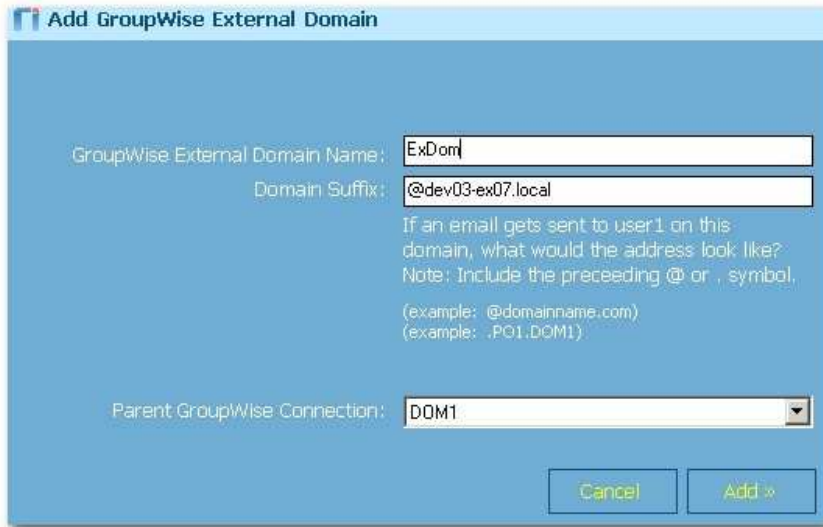
11. At the **Trusted Application Key** window, ensure that the **Skip Trusted Application Key creation** option is selected and click the **Next >** button.
12. At the **Choose detection type**, window click the **Next >** button.
13. At the **Choose an eDirectory Connection** window, ensure that the correct eDirectory tree is selected and click the **Next >** button.



14. At the **GroupWise Connections Detected** window, select any GroupWise domain or post office objects that do not need a connection (e.g. domains dedicated to GWIA or WebAccess) and click the **Remove** button. Click the **Next >** button to continue.



15. At the **Internet Addressing** window, select the preferred internet addressing set for these connections and click the **Next >** button.
16. At the **Automatic Configuration Results** window, click the **Manually add a GroupWise External Domain** button.
17. In the **Add GroupWise External Domain** window provide the details for the GroupWise external domain created to support the **GroupWise External Domain Integration** policy.

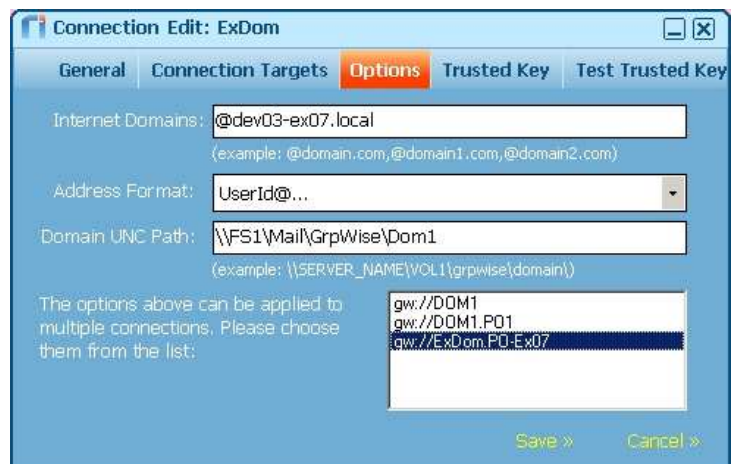


Click the **Add >>** button.

- In the **Add GroupWise External Domain** window, click the **Finish** button. This will create the eDirectory and GroupWise connections.



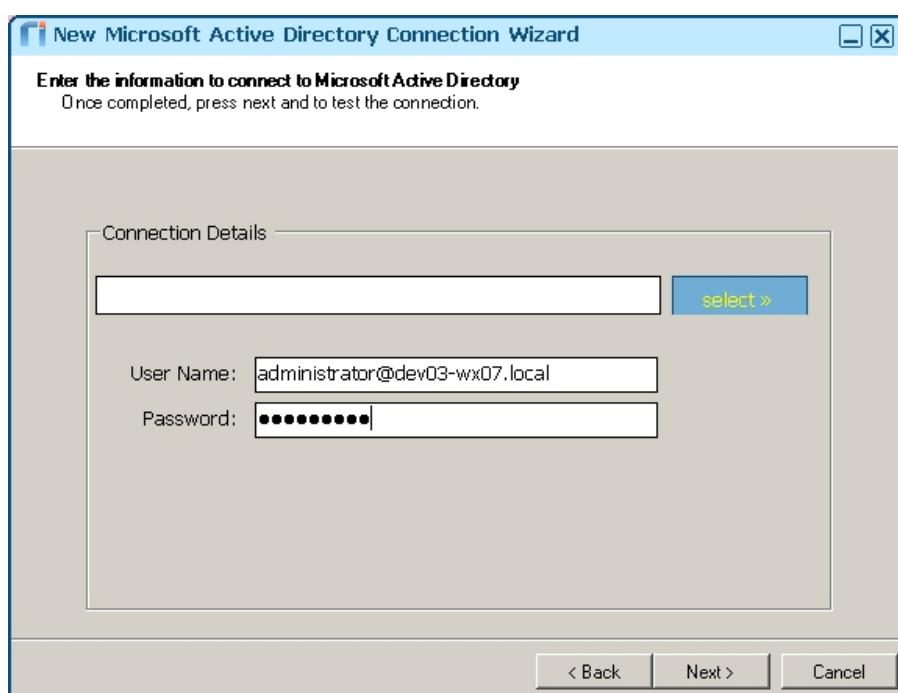
- Double-click the external domain connection and click on the **Options** tab. Verify that the Internet Domain name is correct. Set the “Address Format” to match the email address used in Active Directory. Specify the UNC or local path to the GroupWise domain that the external domain is supposed to link to. Highlight the external post office in the multiple connections list and click **Save >>**.
- Double-click the external post office connection, select the **Options** tab and confirm that these settings match those set in step 19 above.



Step 3 - Setup the Riva Connections to the Target Active Directory Domain

To add and configure the target Active Directory domain connection:

1. Select the **Setup** tab and click “Microsoft Active Directory” in the **Connection Wizards** list to run the applicable Active Directory domain connection wizard.
2. At the **Welcome to Microsoft Directory Connection Wizard** window click **Next >**.
3. At the **Target Information** window, enter the IP address or DNS name of the Active Directory LDAP server. Choose to enable SSL (port 636) or disable SSL (port 389). Click **Next >**.
4. At the **Enter the information to connect to Microsoft Active Directory** window, provide the Active Directory user name, e.g. **administrator@internet.domain** or if the LDAP server supports anonymous binds, click the **select >>** button, browse the Active Directory domain and select the desired user and click the **Ok >>** button.



Note: For the “**Exchange Global Address List Integration**” policy, provide credentials for a user with administrator rights, otherwise credentials for a user with normal rights can be used.

5. If you see a **Conflict Hostname Detected** window, this indicates that the Active Directory domain controller (LDAP server) responded with the DNS name of the server.
 - o If the Windows computer hosting the Riva application is joined to the Active Directory domain and is configured to use the DNS server for the Active Directory domain, select **Yes**,
 - o otherwise select **No**.
6. At the **Detected Available Services** window click **Next >**.



- At the **Microsoft Active Directory connection Wizard complete** window, uncheck the **Launch Exchange Connection Wizard** option and click the **Finish** button.



This should create the Active Directory domain connection.



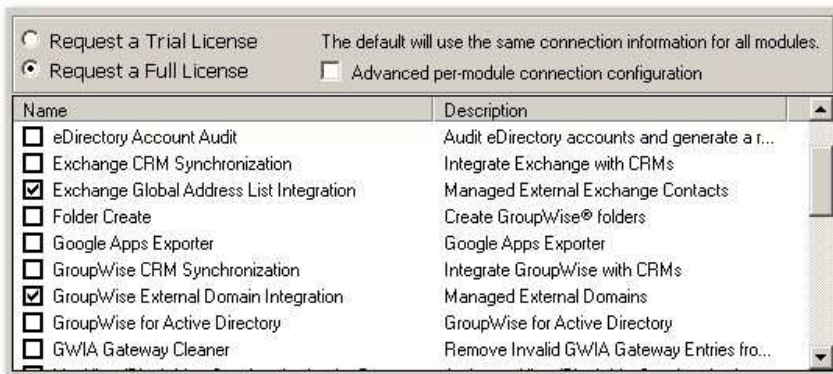
Step 4 - License Riva

Once the Exchange and CRM connections have been created, run the License Request Wizard to create a license request file and submit the request electronically or email the request file to Omni to receive the licence:

- On the Riva tool bar click the **Request License** link to start the license request wizard.

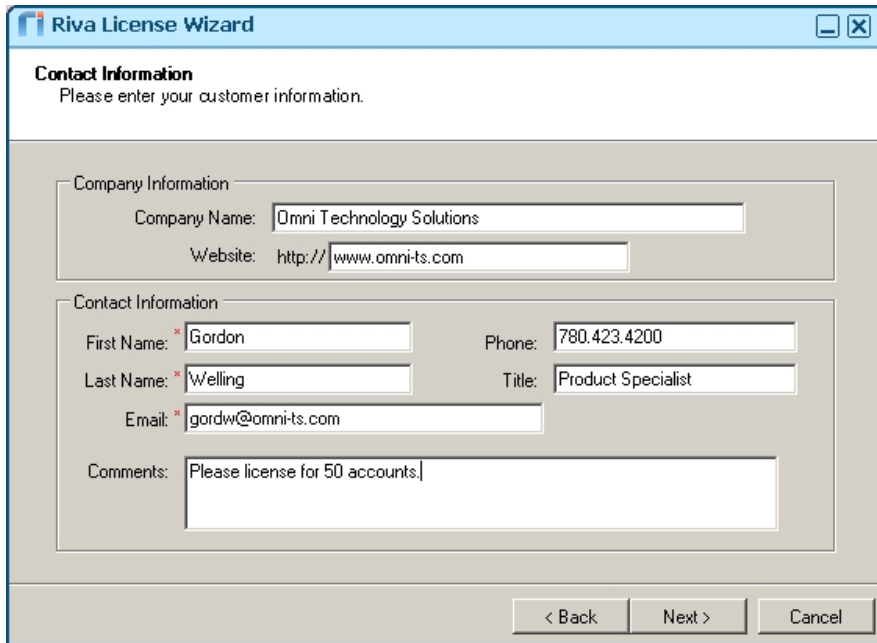


- At the “Welcome to the Riva License Wizard” window, click **Next >**.
- In the “Module Selection” window, select **“Request a Trial License”** or **“Request a Full License”** and check the **Exchange Global Address List Integration** and **GroupWise External Domain Integration** options.



Click **Next >** to continue.

4. In the **Riva License Configuration** window, click **Next >**.
5. In the **Configure Connections** window ensure that **Complete** is selected and click **Next >**.
6. In the **License Review Details** window, click **Next >**.
7. In the **Configuration Complete** window, click **Next >**.
8. In the **Contact Information** window, fill in the information and click **Next >**.



Riva License Wizard

Contact Information
Please enter your customer information.

Company Information

Company Name: Omni Technology Solutions

Website: http://www.omni-ts.com

Contact Information

First Name: * Gordon Phone: 780.423.4200

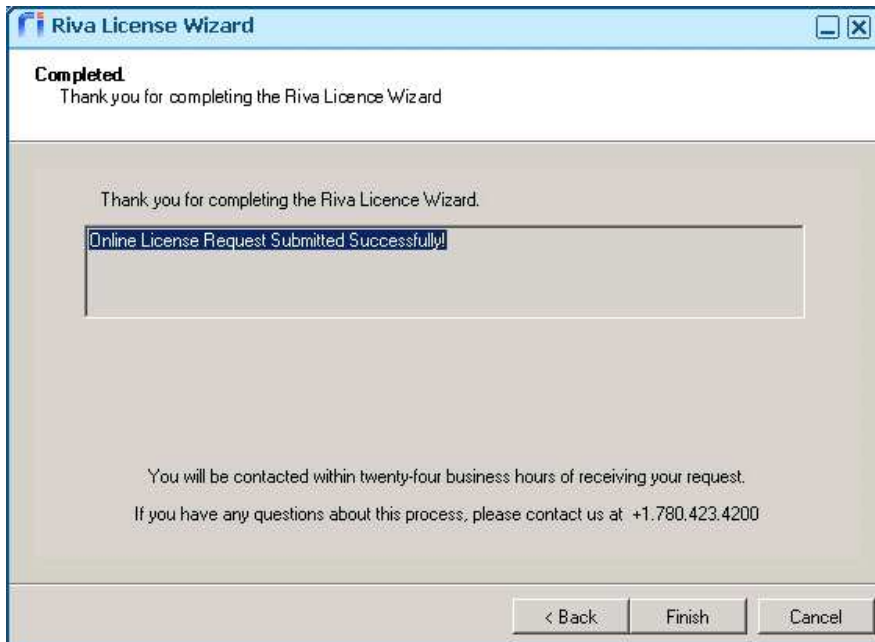
Last Name: * Welling Title: Product Specialist

Email: * gordw@omni-ts.com

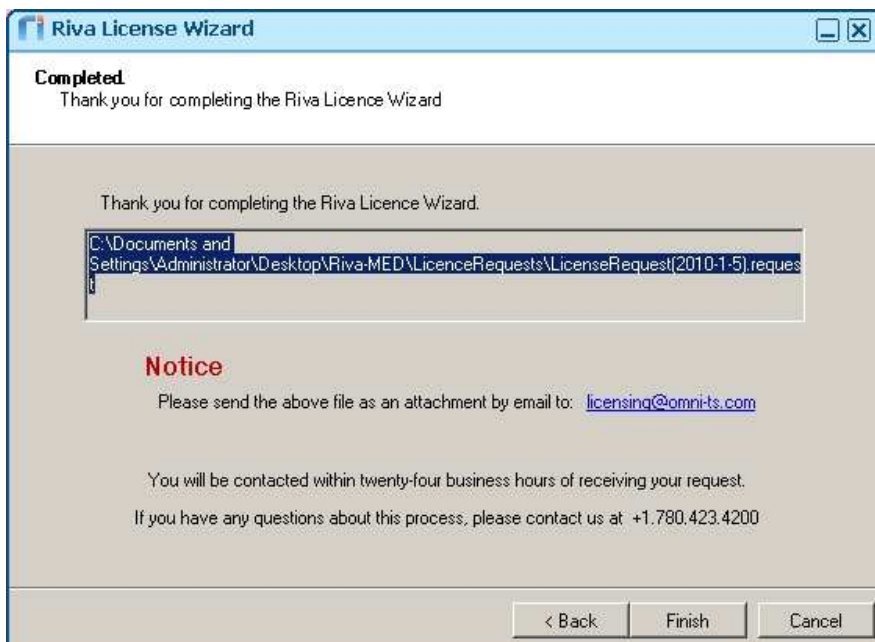
Comments: Please license for 50 accounts.

< Back Next > Cancel

9. In the “Submit Request Electronically?” window, click **Yes**. Riva will attempt to upload the license request to the Omni License Request server.
10. If the license request upload was successful, Riva will show a successful “Completed” window.



If the license request upload was not successful, Riva will open a “Completed” window to prompt you to send the file that was created to licensing@omni-ts.com. Note the path to the LicenseRequest(date).request file. You will receive a license file by email.



11. After you receive the license, save a copy of the Riva .license file to the **\\Licenses** folder inside your Riva installation directory. You will need to close and restart the Riva application for the license to take effect.

Create Managed External Domain Policies

Create the “Exchange Global Address List Integration” Policy

The **Exchange Global Address List Integration Policy** is used to synchronise eDirectory user objects from a source eDirectory container (including child containers) to an Active Directory domain as contacts in an AD container. To create and configure the policy:



- Under “Policies”, in the “Identity Integration” menu category, click on **Exchange Global Address List Integration** to open a new policy.
- Modify the values of the “Name:” and “Description” fields to properly identify the policy.



- Click on **select >>** for the “eDirectory Container” field and navigate the eDirectory tree and select the parent container that holds the user accounts to be synchronized as contacts to the target Active Directory domain. This selection will synchronize all user accounts contained in the parent and respective child containers. Click **OK** to select the parent container.



- Click on **select >>** for the “Active Directory” field, navigate the Active Directory domain and select the target container that will hold the contact objects synchronized from the source eDirectory container(s) specified in step 3. Click **OK** to select the target container.



- Ensure that the **Enabled** option is checked.
- (Optional) Ensure that the **Scheduled** option is checked if this policy will be scheduled using Windows task scheduler (see “Execute and Schedule Policies” below).

- (Optional) Click on the **Summary Report** tab. Check the **Send Execution Summary Report** option and complete the form to identify the email address that the Riva application will send a SMTP email to containing the policy execution summary report. This is a valuable optional setting if the policy is being scheduled. You will need to configure your SMTP server to accept relay requests from the IP address of the Riva server.



Edit Exchange Global Address List Integration

General | **Summary Report**

Send Execution Summary Report

Email Address:

SMTP Server

Host:

Port: (default SMTP port is 25)

- Click **Save** to save the policy.

Create the “GroupWise External Domain Integration” Policy

The **GroupWise External Domain Integration Policy** is used to synchronise Active Directory user and contact objects from a source Active Directory container (including child containers) to a GroupWise external post office as external accounts:

- Under “Policies”, in the “Identity Integration” menu category, click on **Exchange Global Address List Integration** which will open a new policy.
- Modify the values of the “Name:” and “Description” fields to properly identify the policy.




Edit GroupWise External Domain Integration

General | Options | Summary Report

Name:

Description:

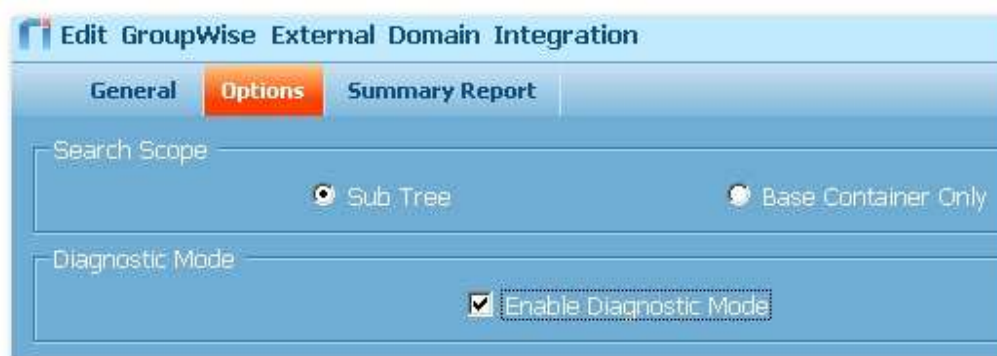
- Click on **select >>** for the “Active Directory Container” field, navigate the Active Directory domain and select the parent container that holds the user accounts and contacts to be synchronized as external users to the target GroupWise external post office. This selection will synchronize all user accounts contained in the parent and respective child containers. Click **OK** to select the parent container.



- Click on **add >>** for the “GroupWise Post Office” field and select the external post office that will host the external accounts synchronized from the Active Directory users and contacts (step 3 above). Click **OK** to select the target container.



- Ensure that the **Enabled** option is checked.
- (Optional) Ensure that the **Scheduled** option is checked if this policy will be scheduled using Windows task scheduler (see “Execute and Schedule Policies” below).
- Select the **Options** tab. Select the **Sub Tree** search scope to synchronize all users and contacts in the parent and child containers below the parent, otherwise select the **Base Container Only** search scope. Check **Enable Diagnostic Mode** to enable verbose logging (for trouble-shooting if required).



- (Optional) Click on the **Summary Report** tab. Check the **Send Execution Summary Report** option and complete the form to identify the email address that the Riva application will send a SMTP email to containing the policy execution summary report. This is a valuable optional setting if the policy is being scheduled. . You will need to configure your SMTP server to accept relay requests from the IP address of the Riva server.

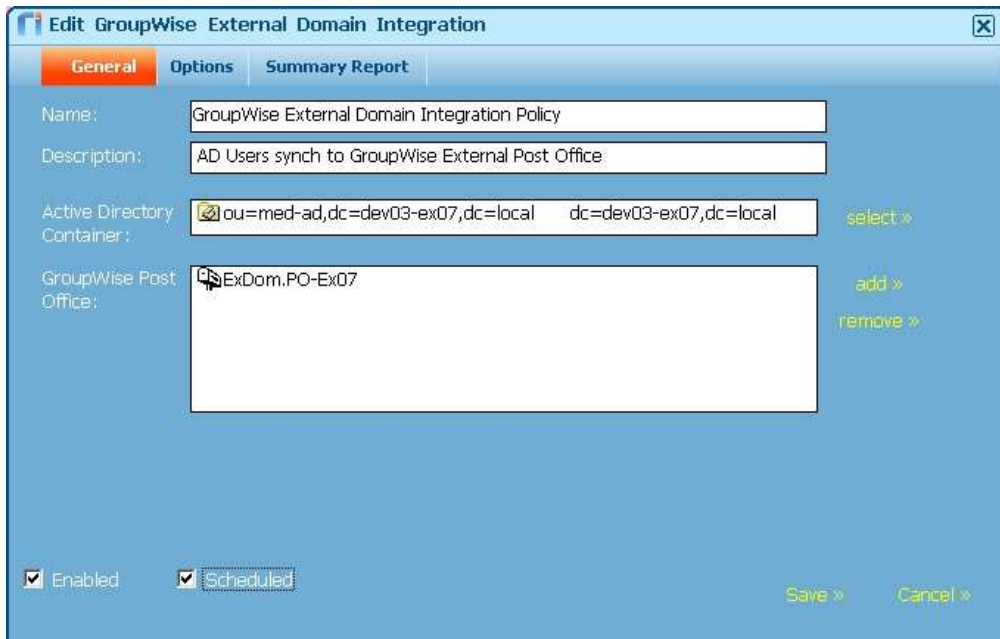


The screenshot shows a dialog box titled "Edit Exchange Global Address List Integration" with two tabs: "General" and "Summary Report". The "Summary Report" tab is active. It contains a checked checkbox for "Send Execution Summary Report". Below this is an "Email Address" field with the value "admin@w2003-gw8.local". Underneath is a "SMTP Server" section with a "Host" field containing "10.10.2.178" and a "Port" field containing "25" with a note "(default SMTP port is 25)".

- Click **Save** to save the policy.

How to Execute and Schedule Riva Policies

There are two global settings which affect policy execution:



The screenshot shows a dialog box titled "Edit GroupWise External Domain Integration" with three tabs: "General", "Options", and "Summary Report". The "Summary Report" tab is active. It contains a "Name" field with "GroupWise External Domain Integration Policy" and a "Description" field with "AD Users synch to GroupWise External Post Office". The "Active Directory Container" field shows "ou=med-ad,dc=dev03-ex07,dc=local" and "dc=dev03-ex07,dc=local" with a "select" button. The "GroupWise Post Office" field shows "ExDom.PO-Ex07" with "add" and "remove" buttons. At the bottom, there are checkboxes for "Enabled" and "Scheduled", both of which are checked. "Save" and "Cancel" buttons are also present.

- **Enabled** - this setting controls execution from within the Riva GUI.
- **Scheduled** - this setting controls execution when Riva.exe is run from the command line or using Windows Task Scheduler.

Enabled and **Scheduled** are not mutually exclusive. If both are selected, then the policy can be executed from within the Riva application and it can be run from the command line or by using Windows task scheduler.

There are four ways to execute Riva policies:

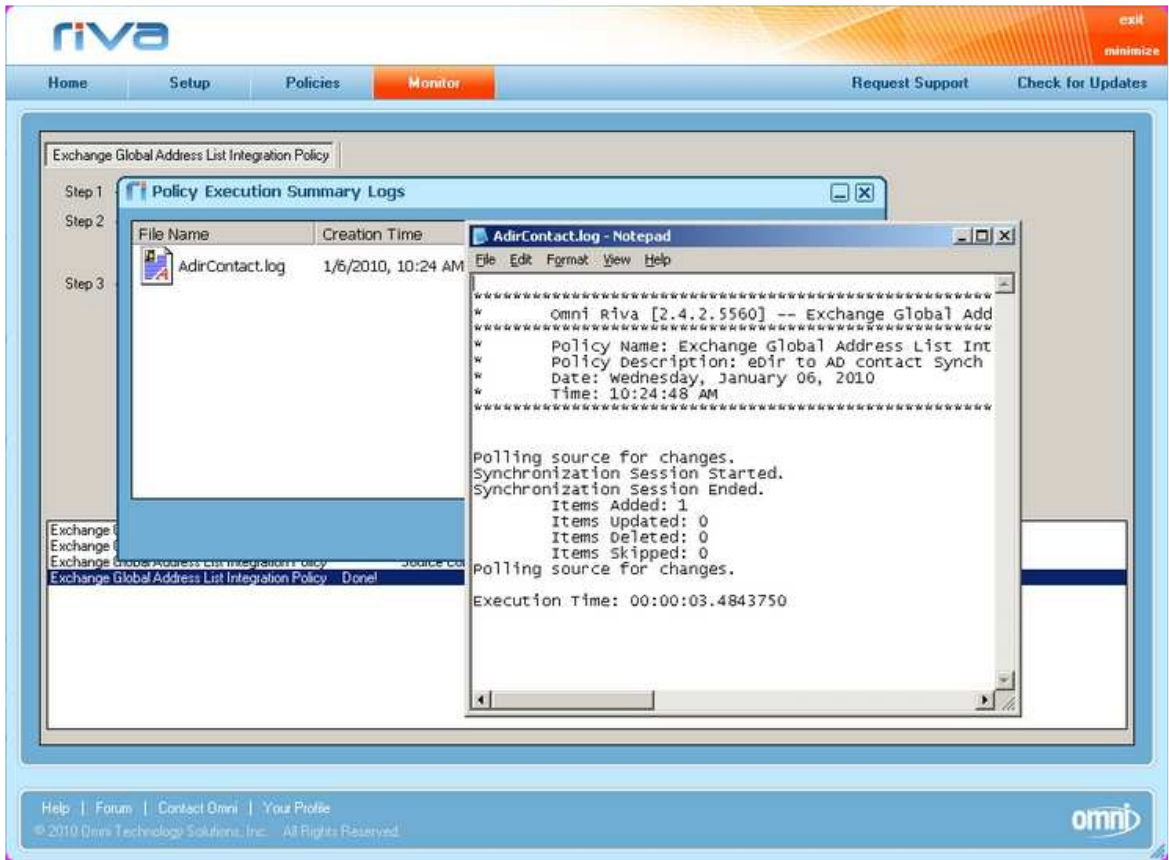
- **Execute All Policies** - click the “Execute All Policies” link in the **Actions:** tool bar. This will execute all enabled Riva policies.



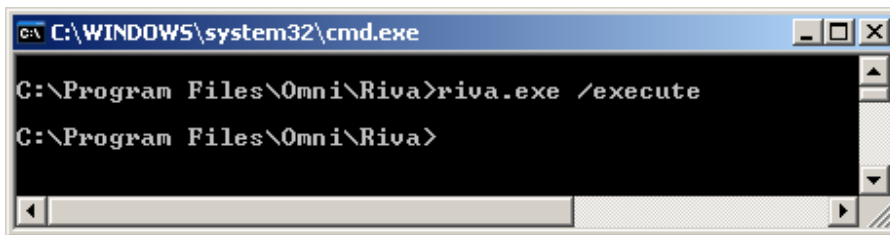
- **Execute Selected Policies** - use Ctrl+click to select one or more policies and click **Execute Selected Policies** in the **Actions:** tool bar. This will execute only those selected policies that are enabled. To execute a single policy, right-click the policy and choose **Execute**.



Note - When policies are executed from Riva interface, the Riva **Monitor** tab will automatically open and display the policy execution in real-time.

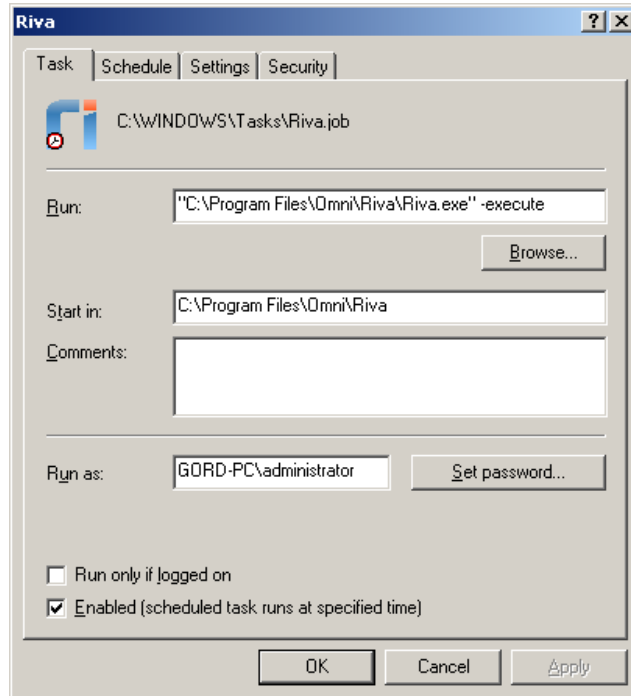


- **Command Line Execution** - You can run Riva from the command line for single execution or for scheduled updates: `c:\<path to file>\riva.exe /execute` will cause all scheduled policies to be executed.



- **Schedule a Policy** - You can schedule one or more Riva Policies using Windows Task Scheduler. To schedule Riva:
 1. Run the “Add Scheduled Task” wizard (Start > Programs > Accessories > System Tools > Scheduled Tasks). Click **Next >** and click **Browse . . .** to navigate to and select the RivaApp.exe file. Specify the frequency to run this task and click **Next >**. Complete the wizard.
 2. Open the task and modify the **Run:** value
 C:\Program Files\Omni\Riva\Riva.exe to read
 "C:\Program Files\Omni\Riva\Riva.exe" -execute

Place double-quotation marks around the path to the Riva.exe file and add -execute to the end of the line.

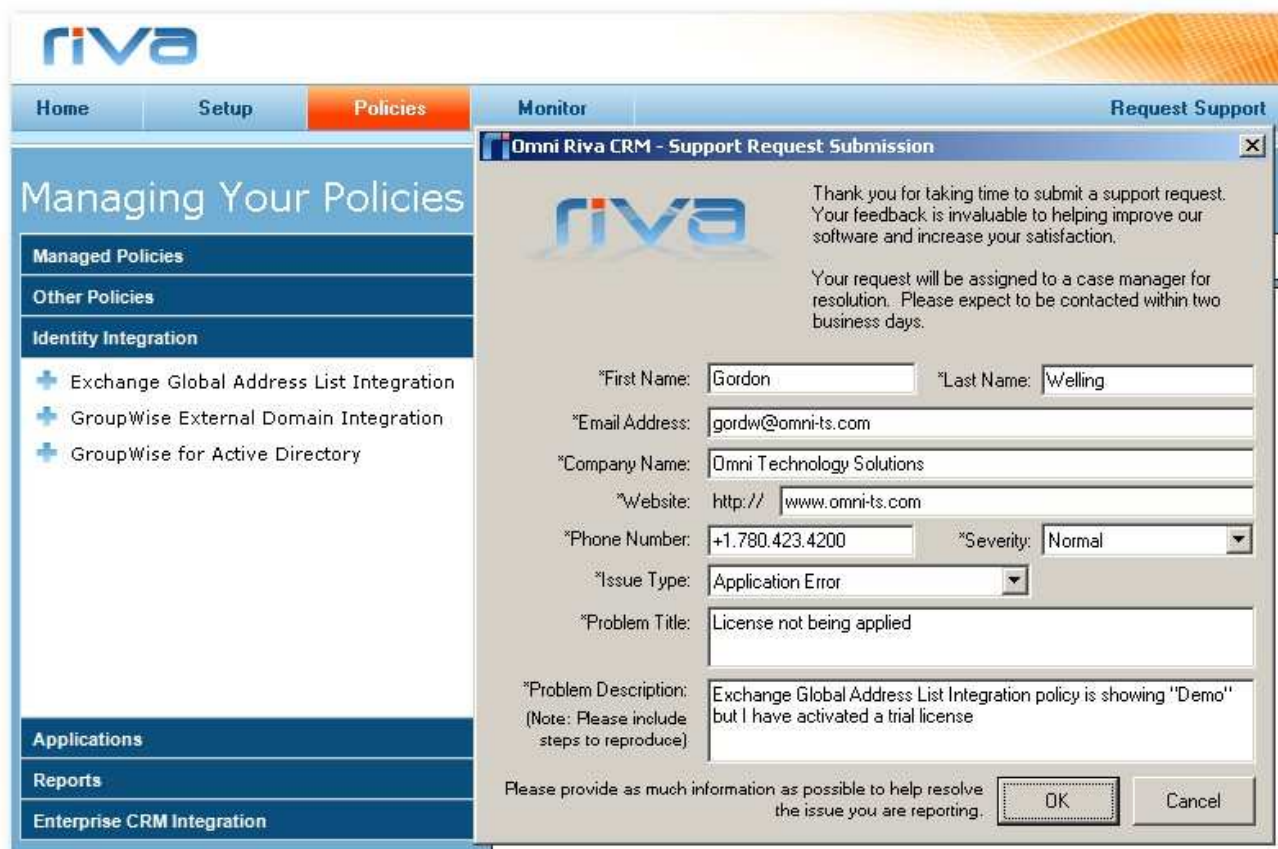


Click **OK** or **Apply** to save the changes to the task.

Support for Riva

Reporting a Technical Issue

Riva CRM Integration Server includes a “Submit Issue Report” feature in the program. If you experience a problem with the application, click the **Request Support** link and complete the form. Please ensure that you include the correct contact information. Once the **OK** button is clicked, Riva CRM Integration Server will send this issue and a copy of the application logs to our technical support team and create a support incident that will be tracked in our CRM.



The screenshot shows the Riva CRM interface with a 'Request Support' dialog box open. The dialog box is titled 'Omni Riva CRM - Support Request Submission' and contains the following information:

- Thank you for taking time to submit a support request. Your feedback is invaluable to helping improve our software and increase your satisfaction.
- Your request will be assigned to a case manager for resolution. Please expect to be contacted within two business days.
- *First Name: Gordon
- *Last Name: Welling
- *Email Address: gordw@omni-ts.com
- *Company Name: Omni Technology Solutions
- *Website: http://www.omni-ts.com
- *Phone Number: +1.780.423.4200
- *Severity: Normal
- *Issue Type: Application Error
- *Problem Title: License not being applied
- *Problem Description: Exchange Global Address List Integration policy is showing "Demo" but I have activated a trial license

Please provide as much information as possible to help resolve the issue you are reporting.

Buttons: OK, Cancel

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.

Free Support

Free support is limited to information available from our support forum, our web site and information contained in the user manual. Telephone and email support for customers who do not have a current support contract can be provided on a fee per-hour basis.

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:

contact form

Topic:

Subject:

Product:

Your Name:

Your Email:

Contact Number:

Message:

Online Resources

Online resources for Riva include:

- **Product Documentation:** Go to www.omni-ts.com select **Support**, follow the link for **Documentation** and select **Messaging Documentation**
- **Riva Flash Tutorials:** will be added to www.omni-ts.com/quicktours
 - **Support Forum:** Go to www.omni-ts.com/Forum
- **Product FAQ:** Go to <http://www.omni-ts.com/integration/questions.html>