

RIVA ON-PREMISES EDITION VO4.O2.2019

---

# Administrators Guide to Riva On-Premises Edition



# Riva CRM Integration On-Premises Management Guide for Administrator

04 – 02- 2019



## Contents

Foreword .....	6
Common Questions About Riva On-Premises Deployments .....	7
Manage Riva On-Premises.....	9
Upgrade Riva to the Latest Public Release:.....	9
To update Riva to the latest public release .....	9
Manually Upgrade Riva:.....	10
Requirements.....	10
Manually Upgrade:.....	10
How to Roll Back a Riva Installation: .....	12
Possible Challenges.....	12
Perform a Rollback of the Riva Installation: .....	12
Creating an App.Settings File to enable Advances Options .....	16
What is an App.Settings file? .....	16
Create an App.Setting File .....	16
Step 1: Make critical backups .....	16
Step 2: Locate the proper directory.....	17
Step 3: Create the App.Setting (.config) file .....	17
Step 4: Copy the default contents into the new file .....	18
Step 5: Insert specific contents.....	18
Step 6: Save and test your changes.....	18
Example of an App.Setting File with Four Advanced Settings .....	19
Moving Riva to a Different Windows System .....	20
Step 1: Prepare the Target Host Windows System.....	21
Step 2: Remove the Riva CRM Agent Synchronization Service from the Source Host Windows System.....	21
Step 3: Prepare the Riva Folder Structure for a Move.....	22
Step 4: Move (or Copy) the Riva Directory to the Target Windows System .....	23
Step 5: Upgrade Riva on the Target server .....	24
Step 6: Enable Riva on the Target Server.....	24
Step 7: Decommission the Previous Riva On-Premises Server .....	25
Move Riva to a Different Folder on the same Windows System .....	25

Procedure to Move Riva Folders .....	25
Determine the current parent folder holding the Riva server files.....	26
Stop the Riva CRM Agent Service .....	26
Move the Riva folders/files to the new parent folder .....	26
Reinstall the Riva CRM Agent Service .....	27
Reset Desktop shortcuts for Riva .....	27
Priority Support: .....	28
Priority Support Eligibility .....	29
Pricing.....	29
Change Management in Riva On-Premises: .....	30
How Change Entry Works .....	30
How Change Entries are Saved: .....	30
How to Configure Change Entries .....	31
To require a change entry after every change: .....	31
To use the same change entry for a series of changes (Configuration Mode): .....	31
To save changes without recording change entries .....	32
Two Primary Applications Used to Manage Riva On-Premises: .....	33
Managing Target User: .....	34
Disable or enable syncing for a single user: .....	34
Disable or Enable Syncing for All Target Users in a Sync Policy .....	34
Disabled data sync for a sync policy.....	34
Enable data sync for a sync policy.....	35
Remove User from a Riva Sync Policy and Reset License Count .....	35
Remove the user(s) to disable data sync to a user .....	36
Release the License .....	36
Remove the user(s) transaction data (OPTIONAL) .....	36
Remove the user(s) sync log files (OPTIONAL) .....	37
Add Users to an Existing Riva Sync Policy .....	37
Step 1: Prepare the Target Email and CRM Environments.....	38
Step 2: Adjust the Riva License .....	39
Step 3: Add New Target User(s) .....	39
Bulk Manage User Mailboxes Assigned to a Riva Sync Policy .....	40

Use Exchange Distribution Groups .....	40
Detecting changes to the members of distribution groups .....	42
Troubleshooting Changes to the members of distribution groups .....	43
Import Mailboxes from a.csv file.....	44
Manually Edit the Policy XML File .....	45
Move Target Exchange or Notes Users to another Sync Policy Using Identical Category Names. 46	
Step 1: Disable the “Source” and “Target: CRM Sync Policies .....	47
Step 2: Move the User to the “Target” Policy .....	47
Step 3: Enable to “Source” CRM Sync Policy .....	49
Step 4: Enable the “Target” CRM Sync Policy.....	49
Step 5: Inform Moved User(s) of Sync Changes.....	49
Move Target Exchange or Notes Users to another Sync Policy Using Different Category Names. 50	
Step 1: Clear the Synchronization Data for the Target User Accounts.....	51
Step 2: Move the Users from the Source Policy to the Target Policy .....	52
Step 3: Inform Moved User(s) of Sync Changes.....	53
Move Target Email User(s) to a Duplicate Sync Policy.....	53
Step 1: Duplicate a CRM Sync Policy.....	54
Step 2: Configure theNew Policy .....	54
Step 3: Move the Users to the New Policy .....	55
Step 4: Enable the “Source” CRM Sync Policy .....	56
Step 5: Enable the Duplicate CRM Sync Policy .....	56
Step 6: Instruct the Moved User(s) to Delete Unwanted Items .....	56
Managing Riva Sync Policies .....	57
Configure a sync policy for Exchange and IBM Notes .....	58
Configure a sync policy for Google’s G Suite .....	58
Configure a sync policyfor GroupWise.....	58
Set Advanced or Custom Options for Connection(s) or Sync Policy .....	58
The Way to Set an Option.....	58
Apply Advanced or Custom Options to a Sync Policy or Connection Object .....	59
Apply Advanced or Custom Options to Individual Target User(s) in the Riva Sync Policy .....	61
How the Changes to the Advanced or Custom Options Are Applied .....	63
What Data is Affected.....	63

How to Rename a Riva Sync Policy .....	63
Rename a Synchronization Policy.....	64
Rename the Policy File .....	65
How to Duplicate a Riva Policy .....	66
What Happens When a Sync Policy is Duplicated .....	68
Remove a Riva On-Premises Sync Policy or Connection .....	68
Ensure That You Are Working with the Correct Riva Files .....	69
Recommended: Make a Backup of the Riva Configuration Files.....	70
Remove a Synchronization Policy .....	71
What Happens When a Policy is Removed .....	72
Remove a Connection .....	73
What Happens When a Connection is Removed .....	74
How to Restore an Accidentally Removed Riva Sync Policy or Connection .....	74
Appendix – Corresponding KnowledgeBase Articles .....	76

## Foreword

Welcome to Riva's "Riva On-Premises Management Guide for Administrators". At Riva, we are proud of our client's and we are invested in your success. Therefore, we have put together to guide to assist us with that goal.

The purpose of this guide is to provide Riva Admins the ability to more effectively manage their Riva On-Premises instances and have the tools you need to be effective.

Each section of this guide is laid out with detailed steps. The headings of each section are hyperlinked to relevant or corresponding [Knowledge Base Articles](#) that can be found on our website and you will find additional links throughout this guide to further assist you.

At the end of this guide you will find an Appendix that list all the relevant [Knowledge Base Articles](#) that are relevant to this guide.

Finally, I would add, that this is only meant as a guide. If you are experiencing an issue or have any questions regarding the contents contained within this guide, please reach out to our Client Success Team via the [Riva Support Request form](#).

## Common Questions About Riva On-Premises Deployments:

Here are some common questions and answers related to deploying a Riva On-Premises server:

1. Question: How long does a typical "Riva deployment" take?

Answer: Provided that all preparations have been completed, a Riva On-Premises server can be installed, licensed, configured, enabled, and monitored for first time sync polls between 90 minutes to 3 hours. The length of time varies depending on the skill and experience of the individuals conducting the deployment.

2. Question: What is the difference between a "trial", "pilot", and "production" Riva deployment?

Answer: Any customer can be provided a no-cost "trial" license for 5 users that is good for 15 days to evaluate and confirm if Riva is a viable sync solution. Larger enterprise customers may want to deploy a "Pilot" environment to test a small group of users with real data before approving a full "production" deployment.

3. Question: What kind of support is provided during "trials"?

Answer: You have access to full levels of support during a "trial" period. Support includes access to online documentation, submitting support requests, and consultations with the Riva Success Team to confirm sync policy option settings.

4. Question: Is dedicated technical assistance available to deploy a Riva server?

Answer: Yes. The Riva Success Team offers a Get Started Bundle (GSB) for Riva On-Premises for Exchange, Google's GSuite, and GroupWise deployments. A GSB consists of up to three hours of dedicated technical assistance to guide you through all of the steps on the deployment checklist. At the present time, we offer a White Glove Session to Notes customers to assist with deploying Riva On-Premises for Notes. To schedule a Get Started Bundle or White Glove Session, contact the Riva Success Team.

5. Question: Is Riva On-Premises available for retail Gmail?

Answer: Riva On-Premises uses a concept of "user impersonation" that requires an admin level user to impersonate into other mailboxes in the same business email system. Retail Gmail is not designed for this concept. Customers who want to sync CRM data with their Gmail mailboxes can use our hosted Riva Cloud for Google service.

6. Question: Is there a document that describes the Riva On-Premises deployment model in more detail?

Answer: Yes. We invite you to read our online Knowledge Base article Overview of a Riva On-Premises Server deployment.



7. Question: Can I schedule a demo of Riva On-Premises before making a decision to deploy?

Answer: Yes. Contact the Riva Success Team to schedule a How Riva syncs my data demo.

8. Question: Are there any videos available that demonstrate data sync for different email clients and mobile devices?

Answer: Yes, we invite you to visit our YouTube channel and view the various playlist

## Manage Riva On-Premises

### Upgrade Riva to the Latest Public Release:

To use the procedure laid out below, the following requirements must be met:

- Riva 2.4.31 or higher is currently installed. (To know which version is installed, see [Determine which Riva On-Premises version is installed.](#))
- The Riva server has access to the internet.
- The [firewall allows communications with Check for Updates.](#)

If any requirement is not met, [contact the Riva Success Team](#), who will either

- Perform the upgrade for you or
- Provide you with the information to [manually update Riva.](#)

### To update Riva to the latest public release:

1. Start the **Riva Manager** application.
2. On the menu bar, select **Check for Updates**.  
**Note:** If you do not see **Check for Updates**, select **Tools** and then select **Check for Updates**. Either way, on the menu that appears, select **Automatic Update (Online)**.
3. If the update fails at this point or later in this procedure, see [What to do if the online update fails.](#)
4. In the **Internet Connection** window, select **Yes**.
5. If an **Update Available** window appears, select **Yes**.
6. In the **Download Successful** window, take note of the version number, and select **OK**.
7. Close and restart the **Riva Manager** application.
8. [Check the version of Riva currently installed](#), and verify that the version number matches the one you took note of.
9. Select **OK**.

## Manually Upgrade Riva:

### Requirements:

**Note:** This article applies **only**

- If the Riva Success Team, a Riva developer, or the Knowledge Base has advised you to manually update Riva On-Premises **and**
- If the Riva version currently installed is 2.4.31.13761 or higher.
  - To know which Riva version is installed, see [Determine which Riva On-Premises version is installed](#).
  - To manually upgrade Riva from a pre-2.4.31 version, [contact the Riva Success Team](#).

You can also [upgrade Riva to the latest public release](#) — without having to contact the Riva Success Team first — if some requirements are met.

### Manually Upgrade:

**To manually update Riva On-Premises version 2.4.31.13761 or higher from a ZIP file:**

1. Go to the URL that the Riva Success Team or a Riva developer has given you, select the file that you were advised to download, and download it. ([Contact the Riva Success Team](#).)
2. Save the .zip file to any folder outside the [Riva server folder structure](#).
3. Right-click the .zip file, and select **Properties**. In the window that appears, on the **General** tab, if the **Unblock** button exists, select it, and then select **OK**.
4. Start the **Riva Manager** application.
5. On the menu bar, select **Check for Updates**.

If you do not see **Check for Updates**, select **Tools** and then select **Check for Updates**.

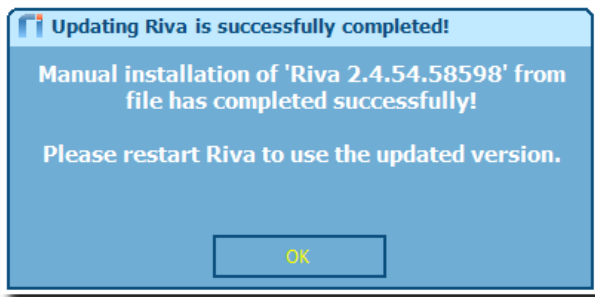
Either way, on the menu that appears, select **Manual Update (Offline from ZIP file)**.

6. In the **Open** window, browse to and select the Riva installation ZIP file, and select **Open**.

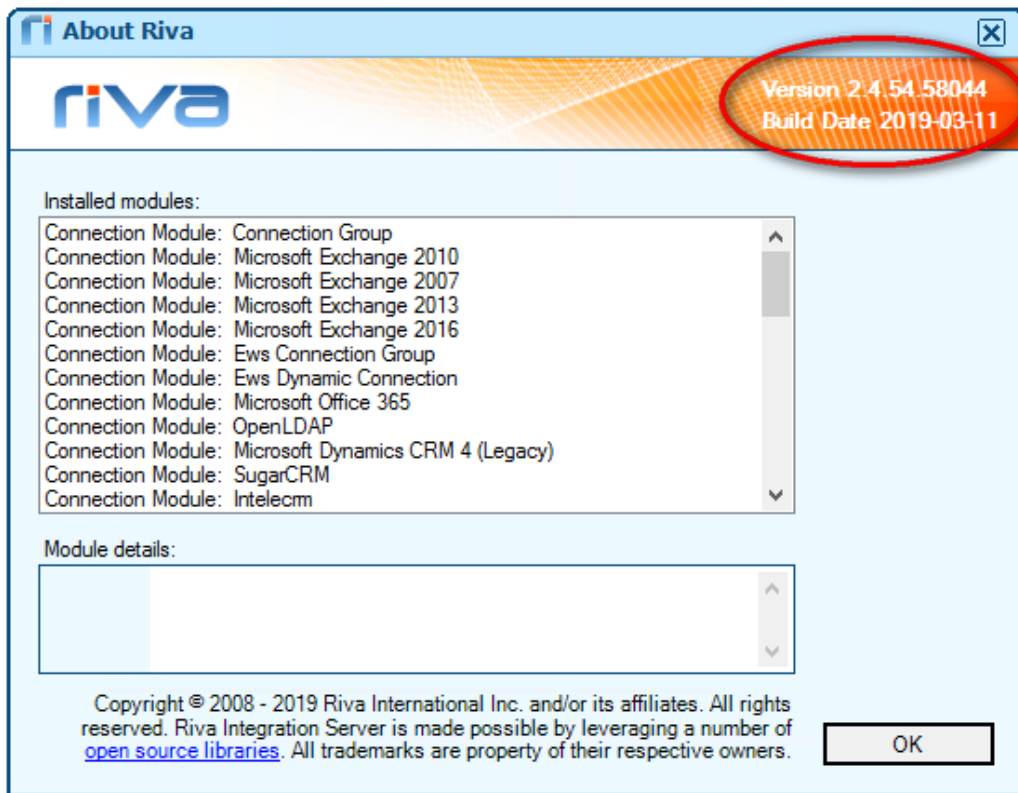
A "**Processing ...**" window appears while Riva runs the manual update process. Riva extracts the ZIP file, copies the files into the applicable Riva server folders, and re-installs any Riva windows services.

When Riva has finished the manual update process, an **Updating Riva is successfully**

**completed!** message box appears.



7. Take note of the version number, and select **OK**.
8. Close and restart the **Riva Manager** application.
9. In the top left, select the **Riva** logo, and confirm that Riva has been upgraded to the release version that you took note of.



10. Select **OK**.

## How to Roll Back a Riva Installation:

If after [upgrading Riva](#) you observe problems, you can restore the previous version of Riva without losing connection settings or policies.

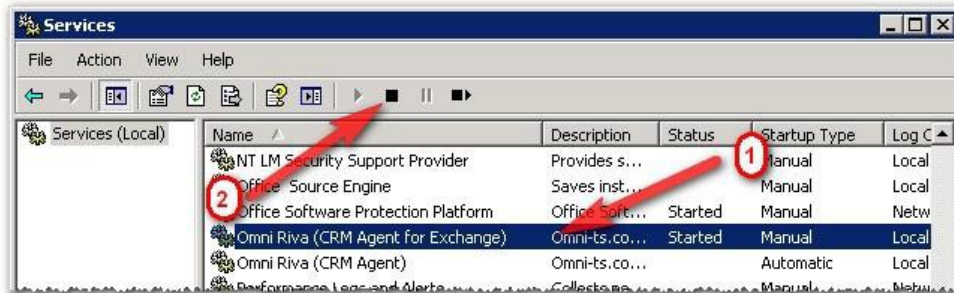
### Possible Challenges:

Riva performed properly before the upgrade, but afterwards, one or more of the following occurs:

- Riva does not start.
- A Riva policy does not execute properly — it displays errors in the logs.
- The update partially failed.
- Riva On-Premises fails to synchronize properly.
- Riva closes when I attempt to run a policy or perform a scheduled policy using Windows scheduler.

### Perform a Rollback of the Riva Installation:

1. Open **Windows Services**, and stop any **Omni Riva** services.



If a Riva service is stuck in a **Stopping** state, stop it manually. For instructions, see [Riva service is stuck "stopping"](#).

2. In **Windows Services**, for each Omni Riva service, open its properties, and confirm the path to the service executable file



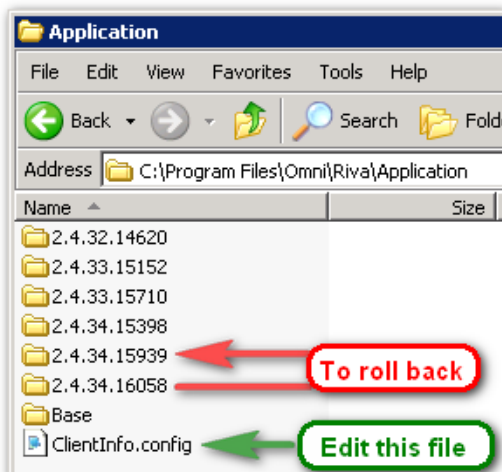


3. Start the **Riva Manager** application.
4. In the top-left corner, select the **Riva** icon. In the **About Riva** window that appears, confirm the version number, and double-click the version number.

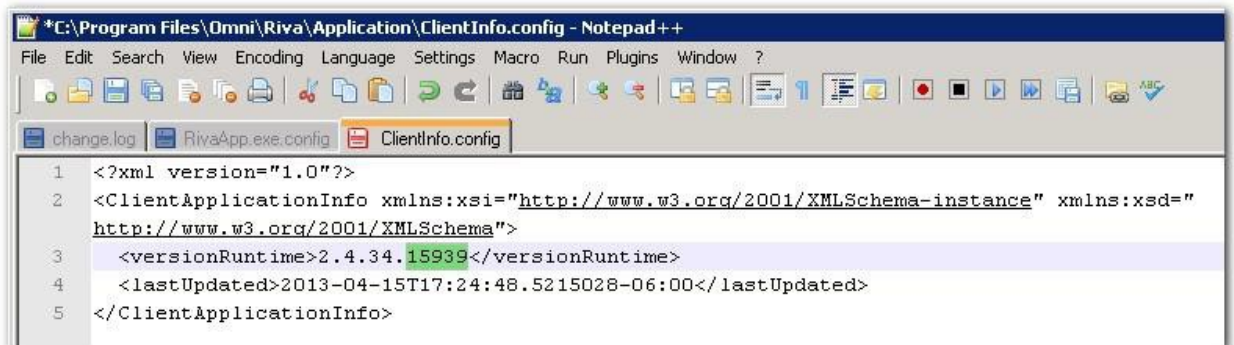


Windows Explorer displays the contents of the \Riva installation folder.

5. Close the Riva application windows.
6. In **Windows Explorer**, navigate to the **\Riva\Application** folder. Take a note of the previous version number.



7. Open the **ClientInfo.config** file in an ASCII-based text editor, and modify the **<versionRuntime>** value to reflect the version number of the previous Riva version to roll back to, for example, **2.4.34.15939**.

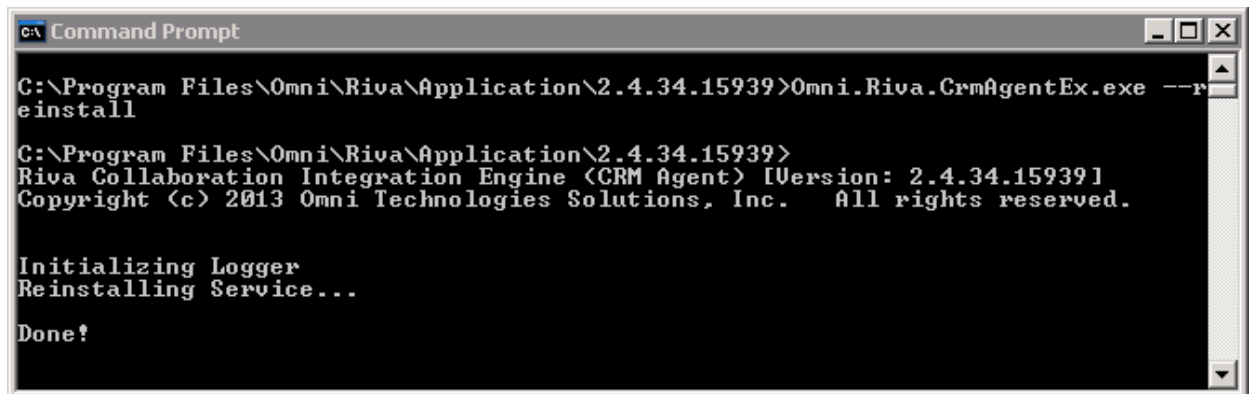


Save the file, and close the text editor application.

8. Close **Windows Explorer**.

**Note:** If performing a Riva rollback for Riva Policies and Reports, skip steps 9 to 12 and 14.

9. Open a CMD prompt with elevated privileges (Run as administrator).
10. CD to the path of the version to roll back to, for example  
**CD C:\Program Files (x86)\Omni\Riva\Application\2.4.34.15939 [enter]**
11. To reinstall the Omni sync service for Riva for Exchange, type **Omni.Riva.CrmAgentEx.exe --reinstall [enter]**



To reinstall the 64-bit sync service, type **Omni.Riva.CrmAgentEx64.exe --reinstall [enter]**

**Note:** The 64-bit Riva sync service is not available in Riva releases prior to 2.4.40. If you need to roll back to a release prior to 2.4.40, the 64-bit service must be uninstalled, and the 32-bit service must be installed. For assistance, [contact the Riva Success Team](#).

To reinstall the Omni sync service for Riva for GroupWise, type **Omni.Riva.CrmAgent.exe --reinstall [enter]**

### Services not related to CRM Sync

To reinstall the Omni Riva II Agent service for Riva IIS for GroupWise, type

**Omni.Riva.IIAgent.exe --reinstall[enter]**

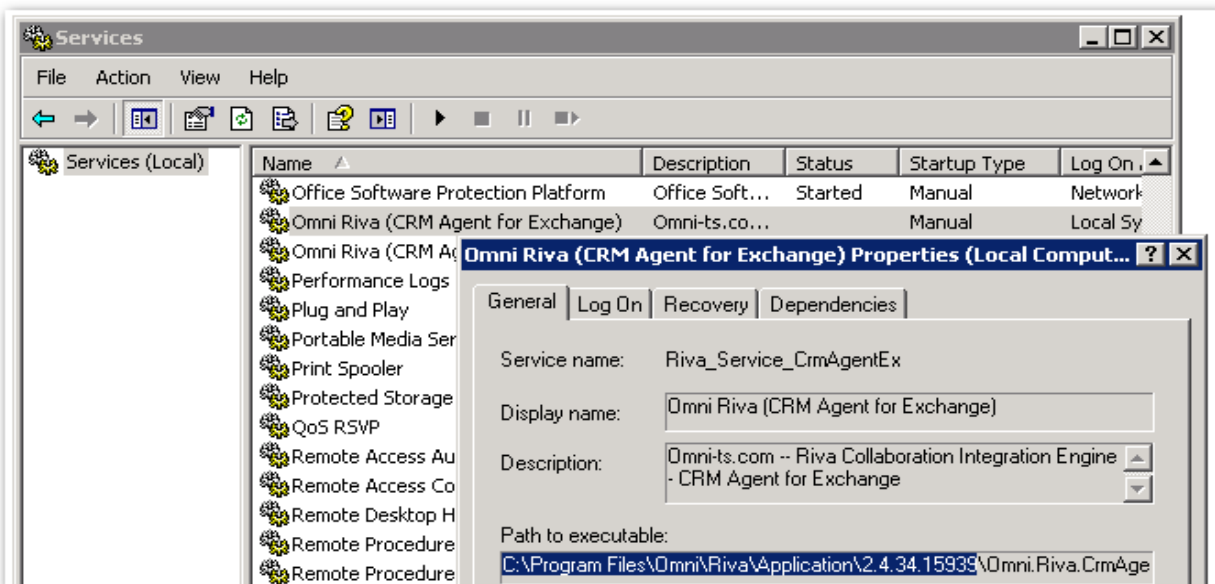
To reinstall the Omni Riva Monitor service for Riva for GroupWise SDL, type **Omni.Riva.Monitor.exe --reinstall[enter]**

For more information on Riva services not related to CRM sync, see [Expose Riva services to monitor software](#).

12. Close the CMD window.
13. Start the **Riva Manager** application. Select the **Riva** logo, and confirm that the version has been rolled back.



14. Open **Windows Services**, open the properties of the applicable Omni CRM Agent service, and confirm that the path is now set to the version that you rolled back to.



## Applies to

All installations of:

- Riva On-Premises server
- Riva Policies and Reports
- Riva Managed Applications
- Riva Identity Integration

## [Creating an App.Settings File to enable Advances Options:](#)

Many advanced options can be set to adjust how Riva and its components work together. In some cases, the use of an advanced option requires the creation of an App.Setting file, as described in this article. In other cases, you can enter advanced options into fields in the Riva Manager application

## What is an App.Settings file?

An App.Setting file is a file that contains code to set various advanced options for a specific part of Riva. Multiple App.Setting files can be created. These files have a predefined XML format that must be respected; otherwise, the specific component may not start.

## Create an App.Setting File

### To create an App.Setting file:

1. Make critical backups.
2. Locate the proper directory.
3. Create the App.Setting (.config) file.
4. Copy the default contents into the new .config file.
5. Insert specific contents.
6. Save and test your settings.

## Step 1: Make critical backups

- Create copies of the following:
  - The \Riva\Configuration folder.
  - All the .config files that reside in \Riva\Application\<version in use>.

**Tip:** Always back up your current Riva configuration and application before deleting or altering existing files.

## Step 2: Locate the proper directory

Locate the directory appropriate for your configuration. Every time Riva is updated and a new version is installed, a new "application" directory is created. This "application" directory contains executables, DLL libraries, and localization resources.

- \Riva\Application\Base\ for a new installation

Name	Date modified	Type	Size
Base	2011.05.09 11:40	File folder	
ClientInfo.config	2011.05.09 11:44	CONFIG File	1 KB

- Riva\Application\<latest version>\ for an updated installation. (Note: Always select the latest version or the currently running version.)

Name	Date modified	Type	Size
2.4.23.10972	2011.04.27 13:54	File folder	
2.4.23.10975	2011.04.27 14:03	File folder	
2.4.23.10976	2011.04.28 14:25	File folder	
2.4.23.10983	2011.04.29 19:00	File folder	
2.4.23.11001	2011.04.29 19:00	File folder	
ClientInfo.config	2011.04.29 19:00	CONFIG File	1 KB

## Step 3: Create the App.Setting (.config) file

1. In the directory identified at step 2, create a text file.  
Depending on the module for which you want to set the advanced options, the file name will be different.
2. In this table, find the appropriate file name:

To modify this	the file name is
Riva Manager application	RivaApp.exe.config
Riva CRM Service Monitor interface	Omni.Riva.CrmMonitor.exe.config
Riva CRM Agent for Exchange	Omni.Riva.CrmAgentEx.exe.config
Riva CRM Agent for IBM Notes	Omni.Riva.CrmAgentEx.exe.config
Riva CRM Agent for GroupWise	Omni.Riva.CrmAgent.exe.config



3. Save the file by using the appropriate name. Ensure that the extension is ".config" and NOT ".txt".

#### Step 4: Copy the default contents into the new file

Copy the contents of the default template into the new .config file. Default template of an "empty" App.Setting file

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="App.Setting1.Key" value="App.Setting1.Value" />
  </appSettings>
</configuration>
```

Take care to copy the contents exactly as they appear. The required format is the same for every Riva App.Setting file.

#### Step 5: Insert specific contents

In the default contents that you copied into the file, replace "App.Setting1.Key" and "App.Setting1.Value" respectively with the "key" and "value" that you have received from Riva support or found in another Knowledge Base article.

**Note:** Be sure to enclose the key and the value with double quotation marks ("), exactly as in "App.Setting1.Key" and "App.Setting1.Value" in the template.

#### Step 6: Save and test your changes

1. Save the file.
2. Restart the component that the file was created for.
3. Verify that the option is producing the desired effect.

## Example of an App.Setting File with Four Advanced Settings

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="LoggingLevel" value="DEBUG" />
    <add key="Web.Proxy.Username" value="administrator" />
    <add key="Web.Proxy.Password" value="mysecret" />
    <add key="Web.Proxy.Domain" value="AD_NT_DOMAIN" />
  </appSettings>
</configuration>
```

## Moving Riva to a Different Windows System

If required, Riva can be moved to a different Windows system. Most moves are required to satisfy one of two requirements:

- A corporate migration to the latest version of Windows and decommissioning of older Windows systems, or
- Moving Riva to a Windows system that can better meet the resource requirements of a larger enterprise deployment (100+ target user accounts).

For instructions if you need to relocate the Riva folder structure on the same Windows system, see [Move Riva to a different folder or volume on the same Windows system](#).

The steps in this article have been written to move the Riva On-Premises server, but they can be used to move any installation instance of Riva. For the list of Windows services that Riva can install, based on the policy or application configured for that instance of Riva, see [Expose Riva Services to monitoring software](#). If you are not dealing with Riva CRM integration, please disregard any steps or information that pertain specifically to Riva CRM Integration.

### **Terms used:**

For the procedure to move Riva to a different Windows system, refer to the following terms:

- **Source system or server:** The Windows server where Riva is currently installed. This instance of Riva will be decommissioned.
- **Target system or server:** The Windows server where Riva will be moved to. This instance of Riva will be deployed as the operational Riva server.

### **To move Riva to a different Windows system:**

1. Prepare the target host Windows system to meet the system requirements for Riva.
2. Remove the current Riva Agent service.
3. Prepare the \Riva folder structure for a move.
4. Move Riva from the source Windows system to the target Windows system.
5. Upgrade Riva on the target Windows system.
6. Enable Riva on the target server.
7. Decommission the current Riva server.

## Step 1: Prepare the Target Host Windows System

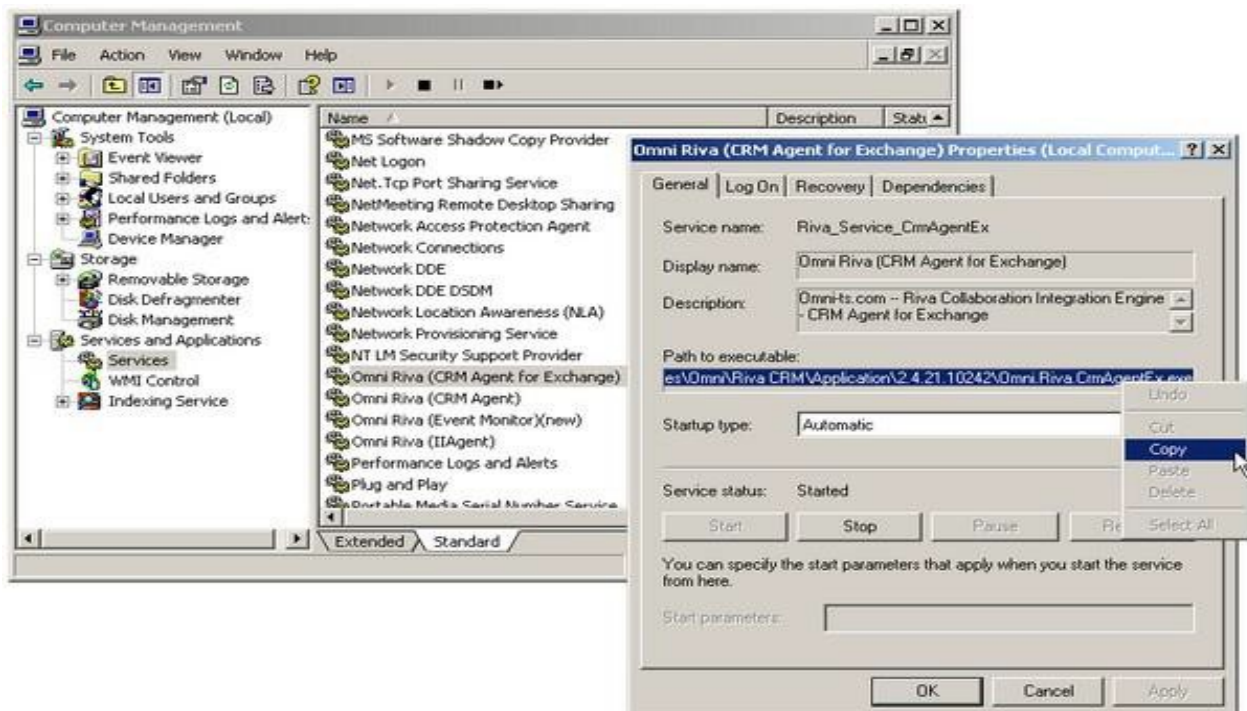
### To prepare the target host Windows system:

1. Ensure that the target host Windows system meets the [system requirements](#).
2. Configure connections to the target email and CRM systems. (Refer to the source Windows system.)

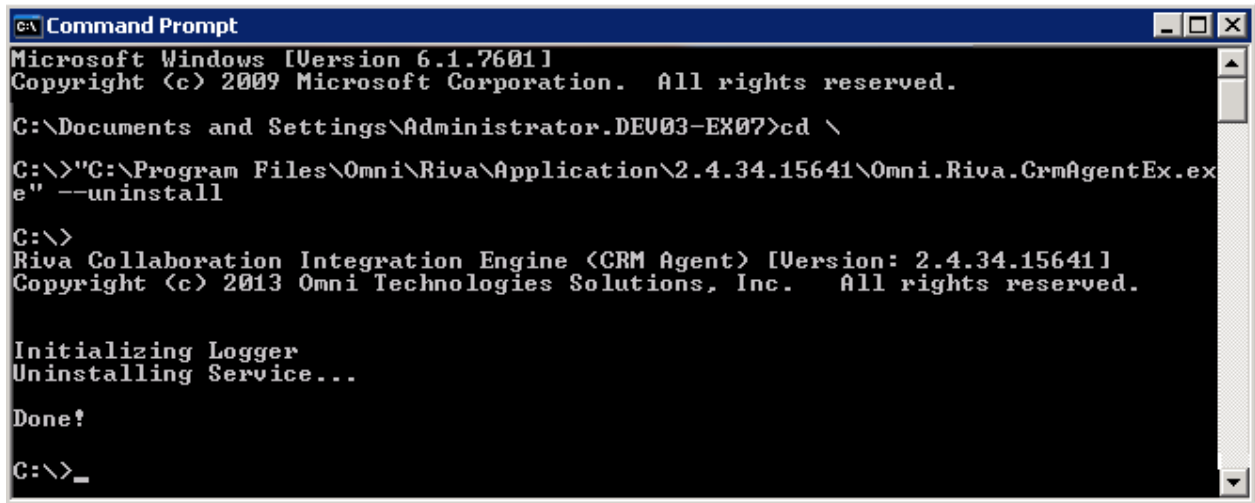
## Step 2: Remove the Riva CRM Agent Synchronization Service from the Source Host Windows System

It is critical to ensure that the Riva CRM synchronization service on the source Windows system be removed. This is necessary to prevent creating duplicate records in the CRM, which would occur if two instances of the Riva CRM synchronization service configured against the same targetsystems and users were running concurrently.

1. On the source Riva server, start the **Riva CRM Monitor** application, and stop the service.
2. Open **Windows Services**, and confirm that the Omni Riva (CRM Agent for Exchange) or the Omni Riva (CRM Agent) status is blank. If the status is displaying **Stopping**, see [Riva service is "Stopping..."](#) for steps to force the service to stop.
3. In **Windows Services**, open the properties of the Riva CRM Agent service, and copy the path to the service to the Windows clipboard.



4. Open a CMD prompt with elevated privileges (Run as administrator).
5. Enter **CD \** and press **ENTER**. Type a " (double quotation mark), then click in the CMD prompt window, right-click, and select **Paste**. After **\Omni.Riva.CrmAgentEx.exe**, add a " (double quotation mark), add a space, type **--uninstall**, and press **ENTER**.



```

C:\ Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Documents and Settings\Administrator.DEV03-EX07>cd \

C:\>"C:\Program Files\Omni\Riva\Application\2.4.34.15641\Omni.Riva.CrmAgentEx.exe" --uninstall

C:\>
Riva Collaboration Integration Engine (CRM Agent) [Version: 2.4.34.15641]
Copyright (c) 2013 Omni Technologies Solutions, Inc. All rights reserved.

Initializing Logger
Uninstalling Service...

Done!

C:\>_
  
```

6. When **Done!** appears, press **ENTER**, and close the CMD prompt window.
7. Refresh **Windows Services**, and confirm that the Riva CRM Agent service has been removed from the list of installed services.
8. Close **Windows Services**.

### Step 3: Prepare the Riva Folder Structure for a Move

In most circumstances, if Riva has been deployed for a significant period of time, the size of the \Riva folder can be substantial. It is best to remove non-essential files to reduce the size of the \Riva folder structure. This will reduce the amount of time it takes to move Riva to a new host Windows system, especially if the move is to a new data center.

Here are some suggestions for trimming non-essential files from the \Riva folder structure to minimize the size of the ZIP file:

1. Create a full backup of the \Riva folder structure, for example **Riva-2014.07.10- Backup.zip**.
2. In the **Riva Manager** application, on the menu bar, select **Policies**, and disable all of the sync policies.
3. In **Windows Explorer**, navigate to **\Riva\Application\**, and remove all the version folders older than the one you are currently using.
4. In **\Riva\Logs\**, remove all log files that are more than six days old.
5. In **\Riva CRM Integration Logs\**, remove the user folders that are no longer in sync policies. Optionally, you can remove log files from each user's folder that are more than



six days old.

6. Remove the **\Riva\Resources\** and **\Riva\LicenseRequests\** folders.
7. Remove any backup copies of folders under **\Riva** that were made earlier, for example **\Riva\Configuration.bak** or **\Riva\Copy - Configuration\**.

Additionally, you can trim some files from the sync policy transaction folders. You have to be careful with this to ensure that you do not remove the wrong files. (You can recover those folders from the backup created at step 1 if required.)

8. In the **Riva Manager** application, on the menu bar, select **Policies**. Edit a sync policy.
9. Select **General**, press the **CTRL** key, and double-click the **Name** label in the form beside the text box of the policy name.

Windows Explorer displays the contents of the transaction folder for that sync policy.

10. Navigate to the **\Lookup** folder.  
You will see a folder for each user, for example **USERNAME\$DOMAIN\$COM** for **username@domain.com**.
11. Remove the folders for users that have been permanently removed from the sync policy and will never be added back.
12. For each sync policy, repeat steps 1 to 4.

Create a ZIP file of the **\Riva** folder structure  
Archive the following folders into a **Riva.zip** file:

- \Riva\Application\**
- \Riva\Configuration\**
- \Riva\CRM Integration Logs\** (Older log files have been removed.)
- \Riva\Custom\**
- \Riva\Licenses\**
- \Riva\Logs\** (Older log files have been removed.)
- \Riva\Transactions\** (Folders of permanently inactive users have been removed.)

## Step 4: Move (or Copy) the Riva Directory to the Target Windows System

This is when you move or copy the installation instance of Riva from the source Windows system to the target Windows system:

1. On the **source Windows system**, start the **Riva Manager** application. On the menu bar, select **Policies**. For each sync policy, right-click, and select **Disable**.
2. On the **target Windows system**, create the desired **\Omni** folder structure on a local

drive. Mapped network drives cannot be used. Examples of valid folder structures:

**c:\Program Files\Omni** (For Windows 64-bit.)

**c:\Program Files(x86)\Omni** (For Windows 32-bit.)

**d:\Omni** (Example for secondary volume.)

3. Copy the **Riva.zip** file from the **source** Windows host to the **target** windows host, and extract it into the **\Omni** folder created at step 2.

## Step 5: Upgrade Riva on the Target server

[Manually upgrade Riva to the latest public release.](#)

## Step 6: Enable Riva on the Target Server

**To prepare the Riva instance on the target Windows system:**

1. On the **source Windows system**, ensure that you have [removed the CRM Agent service](#).
2. On the **target Windows system**, perform the following steps.
3. In **Windows Explorer**, locate the **\Riva** folder.
4. Create a shortcut to the desktop for the Riva.exe and Riva CRM Monitor application.
5. Start the **Riva CRM Monitor** application.
6. Start the **Riva Manager** application. On the menu bar, select **Setup**.
7. In the right pane, for every **email connection** that is used by a CRM synchronization policy, open the email connection, and perform a test connection to a target user specified in the CRM synchronization policy. Ensure that the test connections work.
8. In the right pane, for every **CRM connection** that is used by a CRM synchronization policy, open the CRM connection, and perform a test connection to a target user specified in the CRM synchronization policy. Ensure that the test connections work.
9. On the menu bar, select **Policies**. Ensure that all sync policies are disabled.
10. Edit one of the sync policies. Make any desired changes, and save the policy. When prompted to save the policy and install the CRM Agent service, select **Yes**. If all of the sync policies are disabled, Riva cannot yet sync any data.
11. Ensure that the CRM Agent service is configured properly. See [Configure the properties of the CRM Agent Service](#).
12. Select the sync policy that is configured for the smallest number of users, and enable the policy. In the **Riva CRM Monitor** application, confirm that the target user accounts appear to be synchronizing correctly.
13. Enable the rest of the sync policies, and continue to monitor data sync.

### Troubleshooting

If the target connection tests do not work, or if you notice errors in the CRM Monitor after installing and starting the CRM Agent service on the target Windows system, review the Knowledge Base to find the answer to the errors, or use the [Request support](#) procedure to obtain technical assistance from the Riva support staff.

## Step 7: Decommission the Previous Riva On-Premises Server

1. Archive or store the backup Riva folder ZIP file created.
2. On the **source** host Windows system, remove the **\Riva** folder structure.

## Move Riva to a Different Folder on the same Windows System

If required, Riva can be moved to a different folder on the same Windows system. Most moves are required to satisfy one of two requirements:

- The system drive (C:\) that Riva is installed on is running out of disk space. Moving Riva to a different volume will free disk space.
- Riva is being run from a user's personal desktop or other non-system folder which is creating UAC and file/folder permissions errors.

The steps in this article do not apply to moving a Riva installation to a different Windows system. Refer to "[Move Riva to a Different Windows System](#)" for the correct steps.

## Procedure to Move Riva Folders

For this procedure, refer to the following terms:

- **Current parent folder** - refers to the Windows folder where Riva is currently installed.
- **New parent folder** - refers to the Windows folder where the Riva folders structure will be moved to.

The proper procedure to move Riva to a different Windows system is:

1. Determine the current parent folder holding the Riva server files.
2. Stop the Riva CRM Agent service.

3. Move the Riva folders/files to the new parent folder.
4. Reinstall the Riva CRM Agent service.

### Determine the current parent folder holding the Riva server files

To determine the source parent folder currently holding the Riva folder structure:

1. Logon to Windows using the user normally used to run the Riva Manager application.
2. Open the Riva Manager application.
3. Click the "Riva" logo in the top left corner.
4. In the About Riva window, double click on the Riva version number in the top right corner.
5. Windows explorer will open to the \Riva folder where Riva is installed. The parent folder above the \Riva folder is the source parent folder, e.g. **C:\Documents and Settings\<Username>\Desktop\riva-latest\Riva**
6. Open Windows Services applet (**Start > Run > services.msc**).
7. Open the properties for the Omni Riva CRM Agent (for Exchange). Check the path for the service. It should match the path determined in step 5.
8. Verify which user the service logon uses.

### Stop the Riva CRM Agent Service

- Use the Windows services applet (services.msc) to STOP and DISABLE the Omni CRM Agent service.

OR

- Use the Riva CRM Monitor application to STOP the service.

### Move the Riva folders/files to the new parent folder

1. Using Windows explorer, move the \Riva folder to the new target location, e.g. **D:\Riva**.
2. Right-click the D:\Riva folder and select **Properties**.
3. Under the **Security** tab, click the **Advanced** button.
4. Ensure the local **Administrators** group has **Full Control** permissions assigned to **This folder, subfolders and files**. Ensure that the **Allow inheritable permissions from the parent to propagate to the object and child objects** is checked.
5. Click **OK** and **OK**.

## Reinstall the Riva CRM Agent Service

1. Edit the D:\Riva\Application\ClientInfo.config file and confirm the version that Riva is configured to run.
2. Open a CMD prompt window and go to the D:\ directory.
3. CD to the D:\Riva\Application\<version> folder.
4. Type **Omni.Riva.CrmAgentEx.exe --reinstall** [Enter]. This will reinstall the Riva CRM Agent service so that it runs from the new folder location and retain the properties previously configured including the logon settings.

## Reset Desktop shortcuts for Riva

1. Remove the existing desktop shortcuts for Riva Manager and the CRM Monitor applications.
2. Create corresponding desktop shortcuts from D:\Riva for the Riva Manager and the CRM Monitor applications.
3. Using the desktop shortcut, start the Riva Manager application. Confirm that you can see the Email and CRM connections, and the sync policies.
4. Using the desktop shortcut, start the Riva CRM Monitor application. START the service and confirm that you can see the users appear in the user list. Open a few user monitor activity windows and confirm that Riva is syncing users correctly.



## Priority Support:

Priority support is available as a paid service for critical issues that occur outside Riva's standard support hours. Critical issues are defined as P1 and P2 priority levels in the following chart. Priority support does NOT apply to P3, P4, or P5 issues.

Priority Level	System State	Support Call-Back	Fix Expectation	Fix Method
P1 – Priority Support	Riva software causing invalid data to be synchronized and/or causing data corruption such that the CRM or email platform are unusable for the majority of users	Within one hour	Emergency fix for specific customer as soon as practicable	Specific patch files
P2 – Priority Support	Major functions of Riva software not available for all users	Within one hour	Emergency fix available on a priority basis	Packaged fix
P3	Major functions of Riva software not available for some users	Does not qualify for after hours support. Response: next business day.	Interim release available, typically in 1 to 3 months	Interim Release
P4	Minor Riva software functions not fully available	Does not qualify for after hours support. Response: next business day.	Next release, minimum twice per year	New release
P5	Enhancement or documentation issue with Riva software	By end of next business week	Possible in future releases	New release

## Priority Support Eligibility:

Priority support applies only to new P1 and P2 issues brought forward by a qualified individual in the organization (Riva administrator).

Priority support applies to new issues, not for existing or ongoing issues/tickets.

Priority support is available during these hours:

Standard support hours, weekdays:

5 am – 5 pm (Pacific North America).

8 am – 8 pm (Eastern Americas).

2 pm – 2 am (Central Europe).

10 pm – 10 am (Eastern Australia).

Closed Saturday and Sunday.

Outside regular support hours:

5 pm – 5 am (Pacific North America).

8 pm – 8 am (Eastern Americas).

2 am – 2 pm (Central Europe).

10 am – 10 pm (Eastern Australia).

Saturday and Sunday (available for 24/7 priority support option only).

Clients will receive a priority phone number to call outside Riva's standard support hours.

## Pricing:

Priority Support Options	Cost
24hour/5daysperweek(MondaytoFriday)	20% of the license list price
24hour/7daysperweek(SundaytoSunday)	30% of the license list price

## Change Management in RivaOn-Premises:

Keeping track of—and documenting—the changes that are made to Riva sync connections, policies, advanced options, and/or custom options is very important.

Built-in change management tracking is available in Riva 2.4.43 or higher. A Change Entry window is available to record the reason for a change made to a connection, policy, or advanced options or custom options. It is also possible to record one explanation that will apply to multiple subsequent changes. The information entered in the Change Entry window is persisted with the same document that stores the connection, policy, or external settings.

Many organizations use a source code repository like Git or SVN. Those repositories can track changes as well as display changes between revisions. By placing the Riva\Configuration and Riva\Custom folders in a repository, changes to Riva can be maintained under change control. **Note:** The Change Entry window is not available to record changes made in app.settings files. What

is an [app.setting file](#)? This limitation is effective whether the app.setting file is edited with an external editor (for example, Notepad) or by means of the Riva Manager application.

### How Change Entry Works:

Every change entry can record

- a technical support issue number related to the change;
- the author or team that is making the change;
- a reason for the change; and/or
- a more detailed, multi-line description of the change.

### How Change Entries are Saved:

The change entries are saved to the modified connection, policy, or advanced settings.

**Example:**

This example is at the top of a sync policy file named "CRM Synchronization Policy.policy"

```

1  <?xml version="1.0" encoding="utf-8"?>
2  <!--##### Change Entry Notice :: Start #####
3  Last Change by Riva Fri, 31 Mar 2017 14:15:41 GMT
4
5  <?xml version="1.0" encoding="utf-16"?>
6  <ChangeEntry xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
7  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
8    <Author>phrodeur</Author>
9    <IssueNo>n/a</IssueNo>
10   <Reason>Removed some calendar clutter.</Reason>
11   <Description>Calendar &gt; Exchange Calendar: Advanced Options &gt;
12   Selected "Ignore 'All Day Events' with 'Show as Free'".</Description>
13   <FileHash>8880a5e88182605d2512eb3a49835bda</FileHash>
14   <ChangeHash>f4730af88206fe771f82140ecd594078</ChangeHash>
15   </ChangeEntry>
16   ##### Change Entry Notice :: End ##### -->
17   <CrmModule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
18   xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="{mid_crm}" enabled=

```

## How to Configure ChangeEntries:

By default, changes are saved without recording change entries.

### To require a change entry after every change:

1. Start the **Riva Manager** application.
2. On the menu bar, select **Tools**, and then choose **Change Entry Configuration**.
3. In the window that appears, select the **Require change entry on all changes** checkbox, and select **OK**.

Result: Every time a connection or policy is saved, the Change Entry window appears for recording an Issue #, Reason, and/or Description.

### To use the same change entry for a series of changes (Configuration Mode):

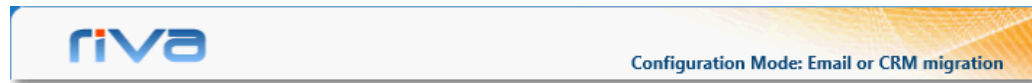
1. Start the **Riva Manager** application.
2. On the menu bar, select **Tools**, and then choose **Change Entry Configuration**.
3. In the window that appears, within the **Configuration Mode** area, select **Start**, and select **OK**.
4. In the **Global Change Entry** window that appears, enter the details that will be automatically recorded for multiple subsequent changes, and select **OK**.

Results:

- Configuration Mode becomes effective. Every time a connection or policy is saved, the change entry made in the Global Change Entry window is automatically saved with the connection or policy.

**Note:** In Riva 2.4.48.48681 or higher, the Configuration Mode becomes inoperative if you exit from the Riva Manager application.

- At the top of the Riva Manager application, a constant reminder displays the Reason that was entered or selected in the Global Change Entry window.



5. When you no longer want that change entry to be saved with changes (in other words, when you want Configuration Mode to become inoperative), do as follows:
  - a) On the menu bar, select **Tools**, and then choose **Change Entry Configuration**.
  - b) In the window that appears, within the **Configuration Mode** area, select **Stop**, and select **OK**.

**Results:**

- The reminder that displayed the Reason for the change disappears.
- The change entry made in the Global Change Entry window will no longer be saved with connection or policy changes.

### To save changes without recording change entries:

1. Start the Riva Manager application.
2. On the menu bar, select **Tools**, and then choose **Change Entry Configuration**.
3. In the Configure Change Entry window, clear the **Require change entry on all changes** checkbox, and select **OK**.

## Two Primary Applications Used to Manage Riva On-Premises:

The **Riva Manager** application is used to carry out the following operations:

- Set up the email system and CRM system connection accounts;
- License your installation;
- Create, configure, and enable or disable your sync policies.

The **Riva Service Monitor** is used to provide

- a real-time view of the sync operations for one or more or all users;
- the ability to stop, start, or restart the service; and
- the ability to review the sync error count and review the specific data sync errors by selecting the **Errorstab**.

## Managing Target User:

### Disable or enable syncing for a single user:

To temporarily stop syncing to a specific user, remove the user from the assigned sync policy. On the first sync cycle after the policy is saved, Riva stops syncing data to the removed user.

1. Start the **Riva Manager** application. On the menu bar, select **Policies**.
2. Right-click the policy for the desired target user, and select **Edit**.
3. Select the **General** tab. On the email user list, select the user to disable, and click **remove >>**.
4. Save the sync policy.

On the next sync cycle, the Riva CRM Agent service stops syncing data to the removed user.

5. In the **Riva CRM Monitor** application, confirm that data sync to the target user has ceased.

**Note:** *The removed user remains visible in the user queue in the CRM Monitor application until the service is stopped/started or restarted.*

To re-enable sync to a target user previously removed, re-assign them to the sync policy. On the first sync cycle after the policy is saved, Riva starts syncing data to the re-enabled target user.

1. Start the **Riva Manager** application. On the menu bar, select **Policies**.
2. Right-click the policy for the desired disabled target user, and select **Edit**.
3. Select **add >>**, and follow the steps to [add the previously removed user](#) to the target user list.
4. Save the sync policy.

On the next sync cycle, the Riva CRM Agent service resumes syncing data to the re-enabled user.

5. In the **Riva CRM Monitor** application, confirm that data sync to the user has restarted.

### Disable or Enable Syncing for All Target Users in a Sync Policy:

#### Disabled data sync for a sync policy:

Disable a sync policy to stop data sync to all target users of that policy. On the first full sync cycle after the policy is disabled, Riva stops syncing the target users.

1. Start the **Riva Manager** application. On the menu bar, select **Policies**.
2. Right-click the sync policy for the desired target users, and select **Disable**.

On the next sync cycle, the Riva CRM Agent service stops syncing data to the disabled users.

3. In the **Riva CRM Monitor** application, confirm that data sync to the target users has ceased.



## Enable data sync for a sync policy:

Enable a sync policy to start data sync to all target users of that policy. On the first full sync cycle after the policy is enabled, Riva starts syncing the target user.

1. Start the **Riva Manager** application. On the menu bar, select **Policies**.
2. Right-click the policy for the desired disabled sync policy, and select **Enable**.

On the next sync cycle, the Riva CRM Agent service resumes syncing data to the re-enabled users.

3. In the **Riva CRM Monitor** application, confirm that data sync to the target users has restarted.

## Remove User from a Riva Sync Policy and Reset License Count

The challenge with removing a user from a Riva sync policy is two fold:

- Does the user have a mobile device that is syncing to the mailbox using Active Sync. There may be a requirement to clear the Riva-synced data from the user's mobile device.
- The Riva license for that use needs to be released so it can be re-used by a different user.

The following steps are required to permanently remove a user. They are described in detail below:

1. Change the user's password in the CRM. That should prevent the user from accessing important data.

**IMPORTANT** for appointments & tasks. Removing Riva synchronized appointments, events or tasks from the mailbox will also remove them from the CRM. As a best practice, re-assign all tasks and appointments to another CRM user before performing a re-init on the user being removed. To preserve those items in the CRM, perform a Re-init "Clear" which will remove all Riva-synchronized calendar and task items from the user's mailbox but preserve those items in the CRM.

2. Select the user and select the Clear All option. **(optional)** This will remove all Riva synced data from the user's mailbox. This is especially important if mobile devices were enabled for synchronization. Clearing Riva synchronized data will remove the contacts, leads, calendar items, tasks, and module email drop-folders from the user's mailbox.
3. Remove the target user(s) from the sync policy.
4. Release the license count for the removed user so that the license can be re-used when adding a new target user.
5. Remove the target user's transaction data (optional).
6. Remove the target user's sync log files (optional).

## Remove the user(s) to disable data sync to a user

To remove a user from a sync policy.

1. Open the **Riva Manager** application.
2. Under "**Policies**", right-click the policy for the desired target user(s) and select "**Edit**".
3. Under "**General**", in the mailbox user list, select the user(s) to remove and click remove >>.
4. Save the sync policy. On the next sync cycle, the Riva CRM Agent service will stop syncing data to the removed user.
5. In the **Riva CRM Service Monitor** application, confirm that data sync to the target user has ceased.

*Note: The removed user will remain visible in the user queue in the CRM Monitor application until the service is stopped/started or restarted.*

## Release the License

Riva will only recalculate license counts when the CRM Agent sync service is started or restarted.

1. In the **Riva CRM Service Monitor** application, STOP the service.
2. In the **Riva Manager** application, double-click the Riva logo (top left).
3. In the "**About Riva**" window, double-click the Riva version information (top right).
4. Close the **Riva Manager** application.
5. In Windows Explorer, navigate into the **\Riva\Licenses** folder.
6. Remove the **{guid\_crmex}.licensees** file or the **{guid\_crm}.licensees** file.
7. In the **Riva CRM Service Monitor** application, START the service.
8. In the **Riva CRM Service Monitor** application, confirm that the deleted target user has been removed from the user queue.
9. In Windows Explorer, confirm that a new **{guid\_crmex}.licensees** file or the **{guid\_crm}.licensees** file appears in the **\Licenses** folder.
10. Open the **Riva Manager** application. Under "**Policies**", right-click one of the sync policies and select "**License Details**". Confirm that one additional user count has been returned to the license pool and is available for a new target user. Close the "**License Details**" window.

In the event that user(s) were removed and new user(s) have been already added to the Riva sync policy, follow steps 5 to 9 above

## Remove the user(s) transaction data (OPTIONAL)

Riva maintains a set of transaction records for each sync policy a user is assigned to. This allows a Riva administrator to temporarily remove a user from a sync policy and re-add them back into a sync policy. Once added, Riva will start to sync the user from the last time Riva completed a sync cycle for that user. If a user is permanently removed, there is no reason to retain those transaction files.

Use this procedure to permanently remove the transaction data files for the recently removed target user.

1. Open the **Riva Manager** application.
2. Under "**Policies**", edit the policy from which the removed user was assigned;
3. On the "**General**" page, hold down the **CTRL** key and double-click the "**Name:**" label.
4. Windows explorer will open to the root of the transaction folder for that policy.
5. Navigate into the "**Lookup**" folder and remove the folder for the removed target user, e.g. IMSAMPLE@MYCOMPANY\$COM.
6. Close Windows explorer and the sync policy edit window.

### Remove the user(s) sync log files (OPTIONAL)

Riva maintains a set of CRM integration logs for each user. Those log files contain the stream of data that would be visible in the Monitor Activity window in the **CRM Service Monitor** application. If a user is permanently removed, and those log files are not required, they can be permanently removed.

To remove user sync log files:

1. Open the **Riva Manager** application.
2. Double-click the "**Riva**" logo (top left corner).
3. In the "**About Riva**" window, double-click the Riva release version number (top right corner).
4. Windows explorer will open to the root of the Riva installation folder.
5. Navigate into "**CRM Integration Logs**" folder and remove the removed user's logs folder, e.g. "**imsample@mycompany.com**"
6. Close Windows explorer and the sync policy edit window.

## [Add Users to an Existing Riva Sync Policy](#)

One of the most common activities involved in managing a Riva On-Premises server deployment is to add target users to an existing Riva server deployment. The primary concerns include:

1. Prepare the target email and CRM environments.
2. Adjust the Riva license to account for additional users.
3. Add the new target users.

### [Step 1: Prepare the Target Email and CRM Environments](#)

Before adding a new target user to a CRM sync policy, ensure that

- The Riva email system connection account can access the target user mailbox.
- The Riva CRM connection account can access the target user CRM account.

#### [Prepare the Target Email User](#)

[Accounts](#) Perform the following

tasks:

- Create and configure the target user account in the corresponding email system:
  - For Exchange: Create an Active Directory user and enable the Exchange mailbox. Ensure that the Riva Exchange connection account is granted full access permissions to the mailbox (On-Premises Exchange) or is granted Delegate access to the target mailbox (hosted Exchange), **or**
  - For GroupWise: Create an eDirectory user and enable the GroupWise account.
  - Ensure that the user has logged into the email account at least once to create the default directory structure in the mailbox.
- Ensure that the Riva email system connection account can access the new target user.
  - In the **Riva Manager** application, on the menu bar, select **Setup**.
  - In the right pane, double-click the corresponding email system connection.
  - In the window that appears, select the **Test Connection** tab.
  - On the **Test Connection** page, provide the email address of the new target user, and test the connection. If the connection test passes, the target user account is correctly configured.

#### [Prepare the Target CRM User Accounts](#)

Perform the following tasks:

- Create the target user account in the corresponding CRM system:

- Create the new target user in the CRM system.
  - Ensure that the CRM account meets any special system requirements.
  - Ensure that the primary email account value for the CRM account is identical to the primary email account value in the corresponding target user email account.
  - Confirm the Riva CRM connection account administrator or master account privileges for the new target CRM user account.
  - Depending on the CRM, you may need to ensure that the user has logged into the CRM account at least once.
- Ensure that the Riva CRM connection account can access the new target user.
- In the **Riva Manager** application, on the menu bar, select **Setup**.
  - In the right pane, double-click the corresponding CRM connection.
  - In the window that appears, select the **Test Connection** tab.

- On the **Test Connection** page, provide the user name of the new target user, and test the connection. If the connection test passes, the target user account is correctly configured.

## Step 2: Adjust the Riva License

Before adding target users, confirm if additional license counts need to be purchased.

1. In the **Riva Manager** application, on the menu bar, select **Policies**.
2. In the right pane, right-click the corresponding CRM sync policy, and select **License Details**.
3. Confirm if there are any unused user license counts.  
You need one email system license count and one CRM system license count per user.
4. Close the **License Details** window.
5. If you need additional license counts, [contact the Riva Success Team](#). You will receive the replacement license file by email.
6. Follow the instructions provided in the email.

## Step 3: Add New Target User(s)

1. In the **Riva Manager** application, on the menu bar, select **Policies**.
2. In the right pane, double-click the corresponding CRM sync policy to edit it.
3. In the window that appears, select the **General** tab. On the **General** page, select **add >>** for the target email user.
  - For each new Exchange user: In the **Exchange Browser** window, provide the mailbox user name, and select **check name >>**. If the email address resolves, select **add >>**. After adding all new target users to the list, select **Ok >>**.
  - For each new GroupWise user: In the **Choose Connection** window, select the target eDirectory tree (preferred) or the applicable GroupWise post office. In the applicable **Browser** window, navigate to and select the new target user. After selecting all target users, select **Ok >>**.
4. Save the CRM sync policy.
5. When prompted to restart the Riva CRM Agent service, select **Yes**.
6. In the **Riva CRM Monitor** application, verify that the new target users have been added to the target user sync queue.
7. For each new target user, view the **Monitor Activity** window, and confirm that there are no license errors and no connection errors, and that a full initial sync is completed.

## [Bulk Manage User Mailboxes Assigned to a Riva Sync Policy](#)

The default procedure is to add target mailboxes, one at a time, to a Riva CRM sync policy. For organizations that want to add multiple target mailboxes to the policy, Riva supports three options:

- Use distribution groups.

- Import the mailboxes from a .csv file. (Release 2.4.40 or higher.)
- Manually edit the policy XMLfile.

**Caution:** Errors occur when users are renamed in the email-enabled group and CRM but not in the Riva sync policy. For more information, see the following:

- [Error: Synchronization failed due to Crm ID conflict.](#)
- [Procedure to correct improperly renamed users.](#)
- [How to rename target users in a Riva sync policy](#) right the first time.

## Warning

Be absolutely sure that a user is not assigned to multiple CRM policies for the same environment. This would result in duplicate records in both the mailbox and the target CRM.

If multiple sync policies will be created and users will be added by using different distribution groups, we recommend implementing a **common transaction folder** structure. [Contact the Riva Success Team](#) to ask to configure that structure for you.

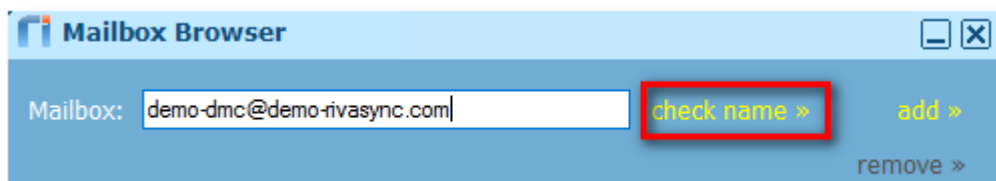
For more information, see [Do not run Riva twice against the same user](#): That article includes information on how to recover from running Riva twice against the same user.

## Use Exchange Distribution Groups

Riva supports using Exchange-enabled AD groups (distribution groups). Both the distribution group and members of the group must be mail-enabled and visible in the global access list.

### To add a distribution group

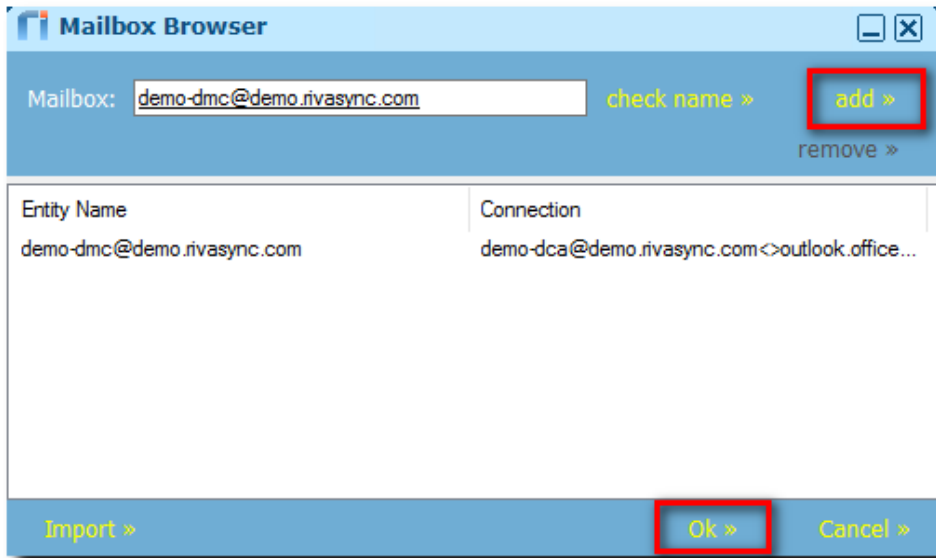
1. In the **Riva Manager** application, on the menu bar, select **Policies**. Right-click the CRM policy, and select **Edit**.
2. In the window that appears, for the **Mailboxes**, select **add >>**.
3. In the **Mailbox Browser** window, enter the common name for the desired distribution group, and select **check name >>**.





The full email address assigned to the distribution group mailbox should resolve and be displayed.

4. Select **add >>** to add the group to the list.

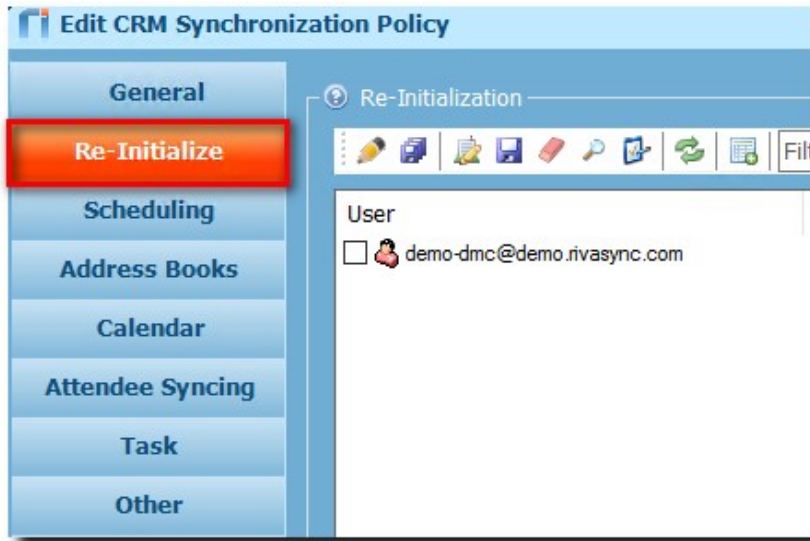


5. Select **OK** to close the **Mailbox Browser** window.

The distribution group now appears in the list of MailboxAccounts in the **General** tab of the CRM policy.



After the CRM policy is saved and the initial synchronization cycle is complete for the users that are members of the selected distribution groups, the list of group members is displayed in the **Re- Initialization** list on the **Sync Start Time** page of the CRM policy.



## Detecting changes to the members of distribution groups

By default, Riva dynamically refreshes changes made to the membership of distribution groups every 24 hours.

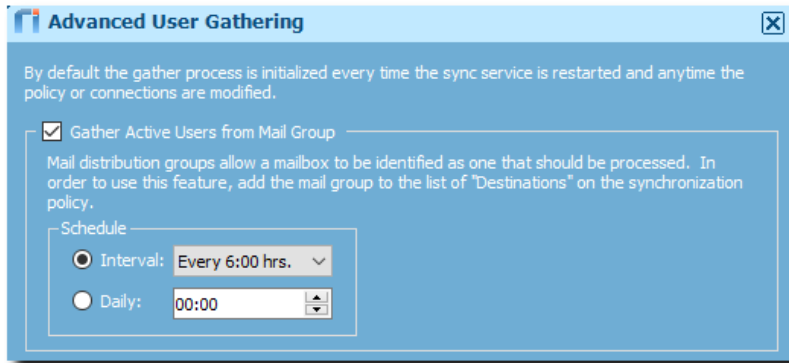
The list of users in assigned distribution groups is also gathered when the synchronization service starts.

- **To Force Riva to Refresh:** In the **CRM Service Monitor** application, select **Restart** or manually stop and start the service.
- **To Enable Automatic Refresh:** Starting with Riva 2.4.21, a Riva CRM policy advanced option can be applied to enable an automatic refresh of assigned distribution groups.

### To enable automatic refresh interval

1. In the **Riva Manager** application, under Policies, select the policy you want to edit.
2. Edit the CRM policy.
3. Select **Advanced Options**.
4. Select **Advanced User Gathering**.
5. Select **Gather Active Users from Mail Group**.
6. Here you can select an interval or daily refresh of the mail group.
7. Select **OK>>**.

**Note:** The change is applied when the CRM policy is saved and the CRM synchronization service is restarted.



## Troubleshooting Changes to the members of distribution groups

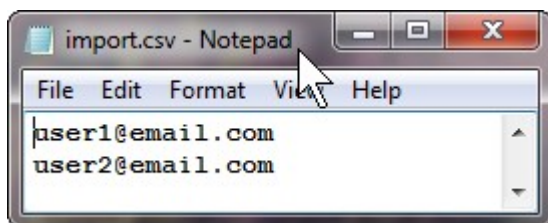
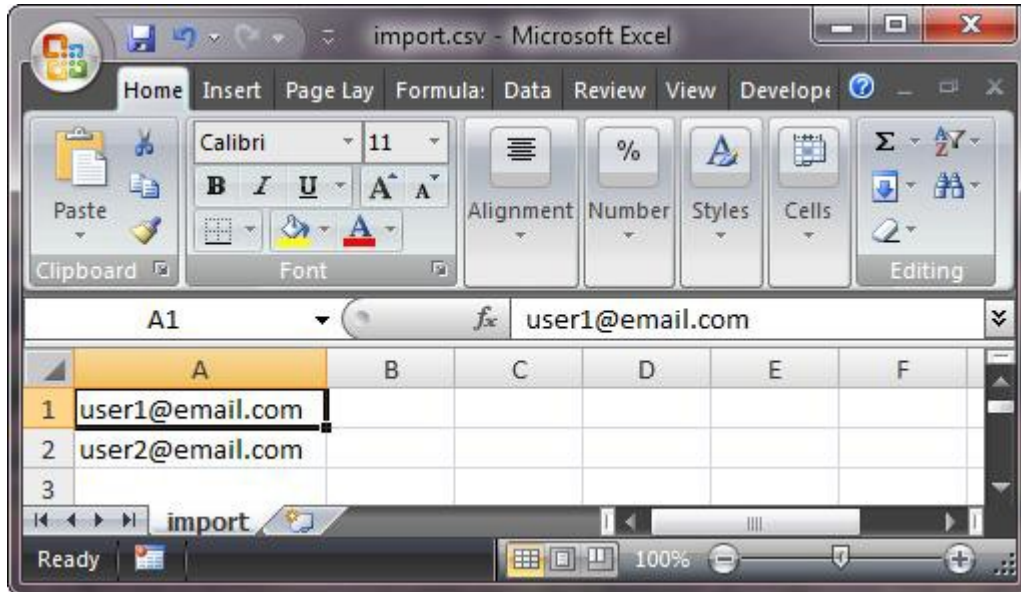
If changes made to the distribution group have not been detected by Riva, proceed as follows.

### To troubleshoot changes to the members of distribution groups

1. Confirm if the changes to users in the distribution group were made in Outlook. If so, confirm that the changes appear in the member list of the group. To do so, use Exchange Management Console, Exchange Manage Shell, or Exchange Admin Portal (Exchange 2013+).
2. Confirm that users that have been added are visible in the Global Access List (GAL). If the user is not visible in the GAL, Riva cannot detect the user when resolving the membership list of the group.
3. If the user is **not visible in the GAL**, manually add the user to the sync policy file by using the steps described in [Manually edit the policy XML file](#).
4. If the user is **visible in the GAL**, perform the following steps.
5. Stop the Riva sync service in the **CRM Service Monitor** application.
6. In the **Riva Manager** application, remove the distribution group from the sync policy.
7. Start the Riva syncservice.  
This forces Riva to remove the group members from the active user sync queue.
8. Let Riva perform two or three complete sync polls of all of the active users.
9. Stop the Riva syncservice.
10. In the **Riva Manager** application, add the distribution group back to the sync policy.
11. Start the Riva syncservice.  
This forces Riva to resolve the member list of the distribution group members.
12. In the **CRM Service Monitor** application, confirm the users in the active user list.

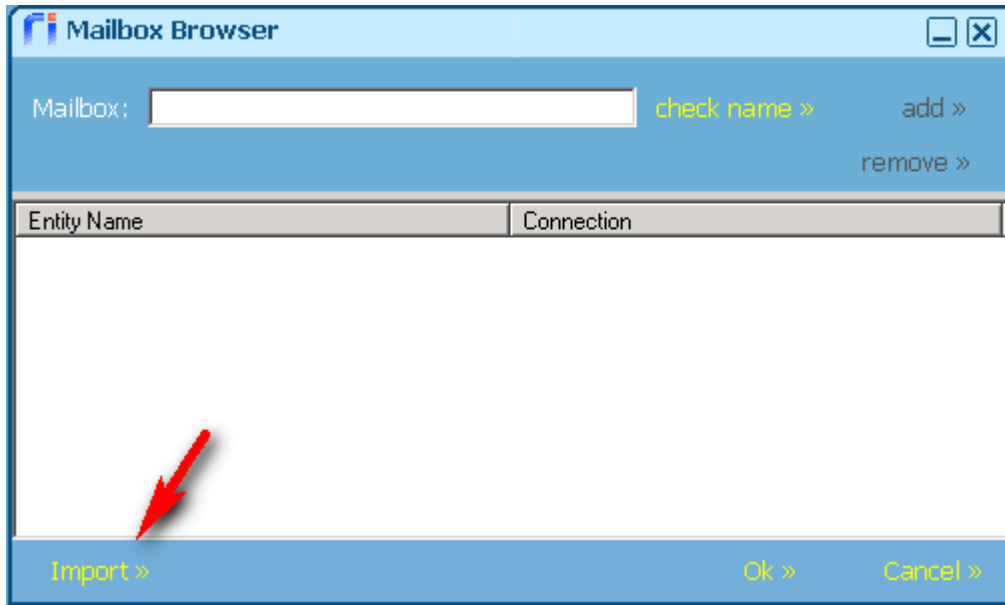
## Import Mailboxes from a .csv file

One email address per line:



### To import mailboxes from a .csv file

1. In the **Riva Manager** application, on the menu bar, select **Policies**.
2. In the right pane, right-click the CRM policy, and select **Edit**.
3. In the window that appears, to the right of the **Mailboxes** list box, select **add >>**.
4. At the bottom of the **Mailbox Browser** window, select **Import >>**.

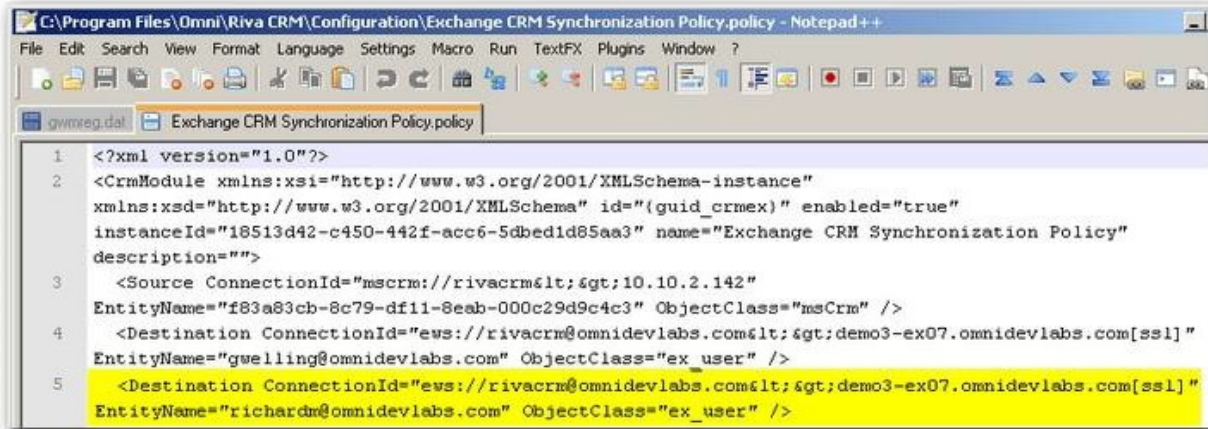


5. In the window that appears, navigate to the desired .csv file, and select **Open**.

### Manually Edit the Policy XML File

The second method is to manually edit the .policy XML file for the Riva CRM synchronization policy. Policy files are located in the **\Riva\Configuration** folder and should be modified only if the Riva CRM synchronization service is stopped.

1. In the **Riva Manager** application, edit the CRM policy, and ensure that one target mailbox user has been added to the policy.  
This ensures that one example of the correct formatted EntityName entry is available to copy.
2. Do one of the following:
  - In the **Riva CRM Monitor** application, stop the service; or
  - Use **Windows services** to stop the **OmniRiva(CRM Agent for ....)** service.
3. Make a backup copy of the applicable CRM policy file, and move it out of the \Riva\Configuration folder.
4. Use a standard ASCII text editor to open the applicable CRM policy file. Copy the existing target exchange user immediately below the first entry. Modify the **EntityName** value entry to use the primary exchange mailbox email address of another user for CRM synchronization.



**Note:** Remember that the primary email address value of the CRM account must be identical to the email address value of the target Exchange mailbox account.

5. Save the .policy file.
6. In the **Riva Manager** application, edit the CRM policy. On the **General** tab, ensure that the new users appear on the target **Mailbox Accounts** list.
7. Do one of the following:
  - In the **Riva CRM Monitor** application, start the service; or
  - In **Windows services**, start the **Omni Riva (CRM Agent for ...)** service.
8. In the **Riva CRM Monitor** application, monitor the additional user accounts for possible email mismatch or license errors.

## [Move Target Exchange or Notes Users to another Sync Policy Using Identical Category Names](#)

Riva can support running multiple CRM sync policies at the same time. It is common for organizations' Riva administrators to create and manage CRM sync policies to meet the unique data sync needs for specific groups of target users, for example a sync policy for internal users and a different sync policy for mobile users.

For this article:

- the "**source**" CRM sync policy is the policy that the users to be moved is currently assigned to.
- the "**target**" CRM sync policy is the policy that the users will be moved to.

These procedures will only work if the category names in the source and target CRM sync policies are identical. If the category names are different, refer to the steps in [How to migrate target Exchange or Notes users to a different CRM sync policy](#). If you need to move target users to a new

CRM sync policy, refer to the steps in [How to transfer target email users to a new email CRM sync policy](#).

For this scenario, a user is being provided with a smart phone and tablet device and needs Riva to accommodate those sync requirements. The Riva administrator needs to move the user from the "Internal Users" policy to the "Mobile Users" policy.

**To satisfy the user request, the admin needs to:**

1. Disable the source and target CRM sync policies.
2. Move the user to the target sync policy.
3. Enable the "source" sync policy and confirm that target users syncing.
4. Enable the "target" sync policy and confirm moved target users are syncing.
5. Inform the users of changes with how Riva will sync data between their CRM and email accounts.

**Warning:** These procedures involve working with two policies with target users. Ensure that **both policies are DISABLED** until all steps are completed. If both policies are enabled too soon, Riva may create duplicate items in the target CRM and/or email systems. In addition, **do not re-initialize** any of the target users.

## Step 1: Disable the “Source” and “Target: CRM Sync Policies

These steps are used to disable the "source" and "target" CRM sync policies that will be modified:

1. Ensure that the Riva CRM Monitor application is open.
2. In the Riva Manager application, under "Policies", right-click the "source" policy and choose to "Disable" it. *Riva will stop syncing for the users in this CRM sync policy. The state for those target users will show as "PolicyStopped" in the Riva CRM Monitor application.*
3. Right-click the "target" policy and choose to "Disable" it. *Riva will stop syncing for the users in this CRM sync policy. The state for those target users will show as "PolicyStopped" in the Riva CRM Monitor application.*
4. Close the Riva CRM Monitor application.

## Step 2: Move the User to the “Target” Policy

These steps are used to move the users from the "source" policy to the "target" policy. This involves moving the transaction files for the desired users.

**Note:** *There is no need to re-initialize the users being moved. This process will move the user to the "new" policy and once the policy is enabled, syncing will resume but use the sync options of the "new" policy.*

1. In the Riva Manager application, under "Policies", open the "target" CRM sync policy.
2. Under the "General" tab, press the CTRL key and double click the "Name:" label on the "General" page. *This opens Windows Explorer to the transaction folder structure for the "target" policy.*
3. Close the policy edit window for the "target" sync policy.
4. In Windows Explorer, navigate to the "Lookup" folder.

You should see folders that match the primary email address of each target user assigned to the policy, for example for the user **rhicks@dev03-ex07.com** there would be a folder named **RHICKS\$DEV03-EX07\$COM**.

Leave Windows Explorer open.

5. In the Riva Manager application, under "Policies", open the "source" CRM sync policy.
6. Under the "General" tab, press the CTRL key, and double-click the "Name:" label on the "General" page. *This will open Windows Explorer to the transaction folder structure for the "source" policy.*
7. Close the policy edit window for the "source" sync policy.
8. In Windows Explorer, navigate to the "Lookup" folder. You should see folders that match the primary email address of each target user assigned to the policy.
9. Move the folder(s) for the desired target users from the "source" policy "Lookup" folder to the "target" policy "Lookup" folder.

**NOTE:** *Ensure that the target user folders are moved and not copied. If the folders are copied, there will be two policies with the same target user and it will create duplicate items in the CRM and email systems once data sync is enabled.*

10. Close both Windows Explorer windows.
11. In the Riva Manager application, under "Policies", open the "source" CRM sync policy.
12. Under the "General" tab, remove the target users that will be moved to the "target" CRM sync policy. Ensure that the **Enabled** check box **is not checked**. Save the "source" CRM sync policy.
13. Under "Policies", open the "target" CRM sync policy.
14. Under the "General" tab, add the target users that will be moved from the "source" sync policy to the "target" sync policy. Ensure that the **Enabled** check box **is not checked**. Save the "target" CRM sync policy.



### Step 3: Enable to “Source” CRM Sync Policy

These steps are used to enable the "source" CRM sync policy and confirm that the correct users are synchronizing.

1. Open the Riva CRM Monitor application. *If the Riva CRM Monitor application is already open, close and reopen it.*
2. In the Riva Manager application, under "Policies", right-click the "source" CRM sync policy, and select "Enable".
3. In the Riva CRM Monitor application, confirm that the target users from the modified "source" sync policy are synchronizing. *The user accounts' "state" should change back to "Synchronizing" and sync activities should be visible in the user activity monitor windows. The users that were removed from this policy should not resume syncing.*

### Step 4: Enable the “Target” CRM Sync Policy

These steps are used to enable the "target" CRM sync policy and confirm that the correct users are synchronizing.

1. In the Riva Manager application, under "Policies", right-click the "target" CRM sync policy and select "Enable".
2. In the Riva CRM Monitor application, confirm that the target users from the "target" sync policy are synchronizing. *The user accounts' "state" should change back to "Synchronizing" and sync activities should be visible in the user activity monitor windows. The users that were added to this policy should also resume syncing.*

### Step 5: Inform Moved User(s) of Sync Changes

Once the "moved" users are syncing, their CRM sync policy will sync only items according the "target" sync policy settings. Items that were previously synced when the user was assigned to the "source" sync policy will no longer be synced by Riva. In addition, sync pattern (way of handling synced email items) may change, especially if [advanced policies for mobile devices](#) are configured in the "target" sync policy.

Riva admins need to provide clear instructions to users about the corresponding changes with syncing data, and how Riva works on mobile devices (if applicable), and which items can be safely removed from their email client application.

## [Move Target Exchange or Notes Users to another Sync Policy Using Different Category Names](#)

Riva supports running multiple CRM sync policies at the same time. It is common for enterprise Riva administrators to create and manage CRM sync policies to meet the unique data sync needs for specific groups of target users, for example a sync policy for internal users and a different sync policy for mobile users.

In this article:

- the source CRM sync policy is the policy that the users to be moved are currently assigned to.
- the target CRM sync policy is the policy that the users will be moved to.

These procedures should be used to move users between source and target CRM sync policies when the category names in both sync policies are different. If the category names in both sync policies are identical, refer to the steps in [Move target Exchange or Notes users to another sync policy using identical category names](#). If you need to move users to a new CRM sync policy, refer to the steps in [Move target email users to a duplicate sync policy](#).

For this scenario, a user is being provided with a smart phone and tablet device and needs Riva to accommodate those sync requirements. The Riva administrator needs to move the user from the Internal Users policy to the Mobile Users policy.

To satisfy the user request, the admin needs to:

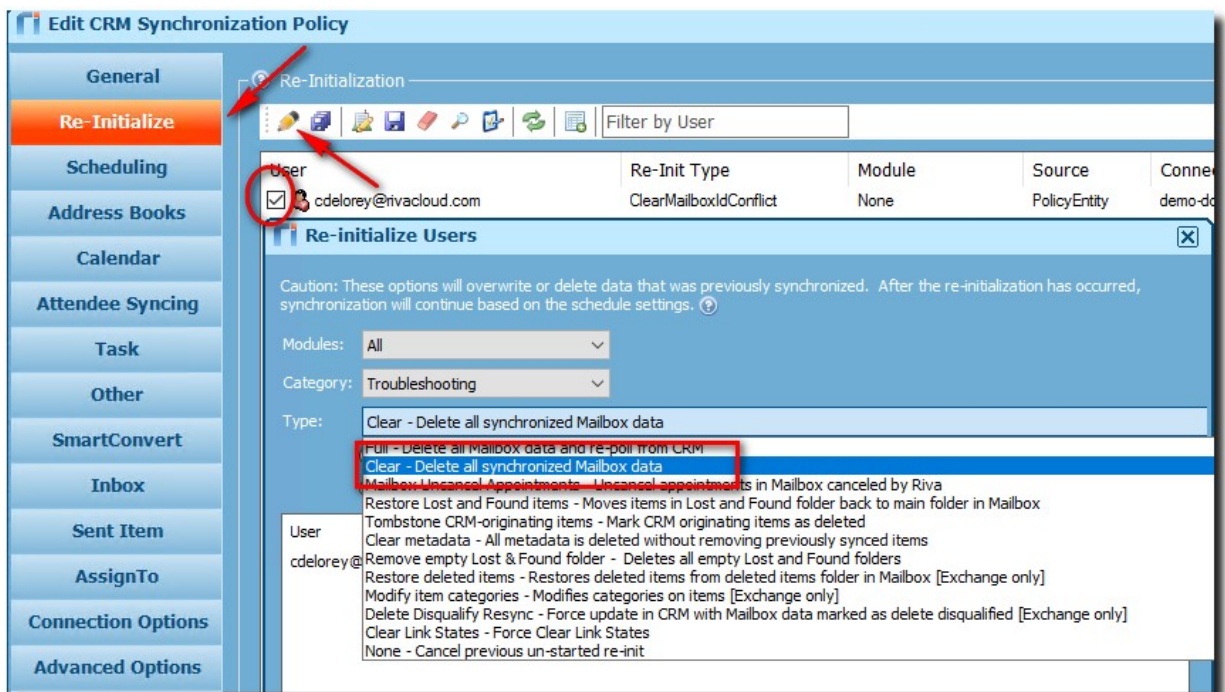
1. Clear the synchronized data for the target user accounts.
2. Move the users to the target sync policy.
3. Inform the users of changes with how Riva will sync data between their CRM and email accounts.

**Warning:** These procedures involve re-initializing the target users and can be data-transfer intensive. If at all possible, this activity should be scheduled to occur during periods of minimal data synchronization. These procedures will wipe Riva synced data from target email accounts, so Riva administrators will need to coordinate this activity with the target users to warn them of the results.

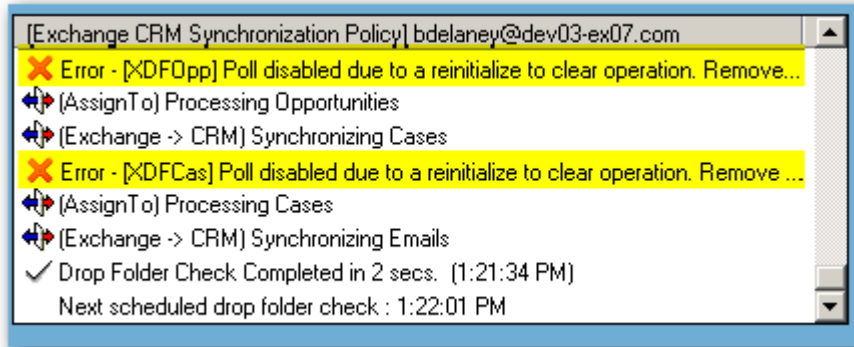
## Step 1: Clear the Synchronization Data for the Target User Accounts

These steps are used to clear the Riva-synced data from the target users that will be moved:

1. Ensure that the **Riva CRM Monitor** application is open.
2. In the **Riva Manager** application, open the source sync policy that the users being moved are currently assigned to.
3. Select the **General** tab. On the **General** page, confirm that the target users being moved are assigned to this policy.
4. Select the **Re-Initialize (Sync Start Time)** tab. Select the users to be moved. Select the pencil to re-initialize the user. On module select **All**. On Category select **Troubleshooting**. On Type select **Clear – Delete all synchronized mailbox data**.



5. Save the CRM sync policy.  
Riva clears the synced data from the target users on the next full sync cycle.
6. In the **Riva CRM Monitor** application, look for clear operation errors in the target user Monitor windows.  
This is expected and normal for a Clear re-initialize sync.



## Step 2: Move the Users from the Source Policy to the Target Policy

**Warning:** These steps remove Riva-synced data from target user email accounts and from mobile devices.

This process **does not remove** category names, address books, or the existing SmartConvert drop folder structure from email accounts. The empty address books and SmartConvert drop folder structure remain, so that target users will need instructions on how to manually remove those items.

New category names, address books, and a SmartConvert drop folder structure will be synchronized to the target accounts.

### To move the users from the source policy to the target policy:

1. In the **Riva Manager** application, on the menu bar, select **Policies**. In the right pane, open the source CRM syncpolicy.
2. Select the **General** tab. On the **General** page, remove the target users that are to be moved to the target CRM sync policy. Ensure that the **Enabled** check box is **selected**. Save the source CRM syncpolicy.
3. On the menu bar, select **Policies**. In the right pane, open the target CRM sync policy.
4. Select the **General** tab. On the **General** page, add the target users that are to be moved from the source sync policy to the target sync policy. Ensure that the **Enabled** check box is **selected**. Save the target CRM sync policy.

### Step 3: Inform Moved User(s) of Sync Changes

When the moved users are syncing, their CRM sync policy will sync only the items determined by the target sync policy. The sync pattern (way of handling synced email items) may change, especially if [advanced settings for BlackBerry, iPad, iPhone, Android, and ActiveSync mobile devices](#) are configured in the target sync policy; and the category and address book names, and SmartConvert drop folder names will be different.

Riva admins need to provide clear instructions to users about the corresponding changes with syncing data, and how Riva works on mobile devices (if applicable), and which items can be safely removed from their email client application.

### Move Target Email User(s) to a Duplicate Sync Policy

When organizations first set up Riva On-Premises, there can be a tendency to add all the users to a single CRM synchronization policy. At some point in the future, Riva administrators may want to create additional CRM sync policies for special groups of target users, for example "BES Mobile Users". These procedures will allow the Riva administrator to create and configure new policies to best suit the sync needs for specific target users.

Procedures for moving users between existing CRM sync policies:

- [Move target Exchange or Notes users to another sync policy using identical category names - if the category names are the same for the source and target CRM sync policies,](#)  
or
- [Move target Exchange or Notes users to another sync policy using different category names - if the category names are different between the source and target CRM sync policies.](#)

For this scenario, a user wants to prevent phone calls from syncing between their CRM account and their Exchange mailbox. Their target user is currently assigned to a CRM policy that syncs phone calls. To satisfy the user's request, the admin needs to:

1. Duplicate an existing CRM sync policy to create a new policy.
2. Configure the new policy to not sync phone calls.
3. Move the user to the new sync policy.
4. Enable the "source" sync policy and confirm that target users syncing.
5. Enable the "new" sync policy and confirm moved target users are syncing.
6. Instruct the moved users to delete unwanted items from their email and/or CRM accounts.

**Warning:** These procedures involve working with two policies with the same target users. One policy is the "source" policy that is currently in use, and the other is a duplicate "new" policy. Ensure that **both policies are DISABLED** until all steps are completed. If both policies are enabled too soon, Riva may create duplicate items in the target CRM and/or email systems. In addition, **do not re-initialize** any of the target users.

## Step 1: Duplicate a CRM Sync Policy

These steps are used to create a new CRM sync policy based on a "source" policy. *Riva administrators can create a new CRM sync policy if they do not want to create a duplicate of an existing policy.*

1. In the **Riva Manager** application, on the menu bar, select **Policies**. In the right pane, locate the CRM sync policy that will act as the "source" policy to be used to duplicate a new policy.
2. Right-click the "source" policy, and select **Duplicate**.

*This creates a disabled copy of the source policy with the same policy settings and target users. This policy will be referred to as the "new" policy. Although the target users are included in the duplicate policy, the transaction records are not duplicated. (It helps to [understand how Riva maintains transaction records](#).) It is important NOT TO ENABLE this policy, until specified in the procedures in this article.*

## Step 2: Configure the New Policy

This procedure can be used to modify the "duplicate" CRM sync policy. The duplicate policy should be modified to sync in the desired manner before moving users into it.

1. In the **Riva Manager** application, on the menu bar, select **Policies**. In the right pane, right-click the "duplicate" CRM sync policy, and choose **Edit**.
2. On the **General** page, change the name of the duplicate policy, and add a suitable description. From the **Exchange Accounts** list, remove the target users that will not be assigned to this policy. *Only the target users that are being moved from the "source" policy should remain on this list.* Ensure that the **Enabled** check box is **cleared (not selected)**.
3. On the **Sync Start Date** page, ensure that the **Re-Initialize All** option is **cleared**.
4. Work through all pages in the sync policy, and make any desired changes. Do not change category or folder names.

5. After making all your changes, select the **General** tab. Ensure that the **Enabled** check box is **cleared**.
6. Save the "new" policy. If prompted, do NOT restart the sync service.

### Step 3: Move the Users to the New Policy

These steps are used to move the users from the "source" policy to the "duplicate" policy. This involves moving the transaction files for the desired users. (It helps to [understand how Riva maintains transaction records](#).)

**Note:** *There is no need to re-initialize the users being moved. The following process moves the user to the "duplicate" policy, and after the policy is enabled, syncing resumes and uses the sync options of the "duplicate" policy.*

1. In the **Riva Manager** application, on the menu bar, select **Policies**. In the right pane, edit the "duplicate" sync policy.
2. On the **General** page, press the CTRL key and double-click the **Name** label. Windows Explorer displays the transaction folder structure for the "duplicate" policy.
3. Close the policy edit window for the "duplicate" sync policy.
4. In Windows Explorer, navigate to the **Lookup** folder.

You should see folders that match the primary email address of each target user that was originally listed in the policy. For example, for the user **rhicks@example.com**, there would be a folder named **RHICKS\$EXAMPLE\$COM**. *If you were to open one of those folders, you would see that it contains a single **Entity.settings** file.*

5. In the **Lookup** folder, remove all of the user folders. Leave Windows Explorer open.
6. In the **Riva Manager** application, on the menu bar, select **Policies**. In the right-pane, edit the "source" sync policy.
7. On the **General** page, press the CTRL key and double-click the **Name** label. Windows Explorer displays the transaction folder structure for the "source" policy.
8. Close the policy edit window for the "source" sync policy.
9. In Windows Explorer, navigate to the **Lookup** folder.

You should see folders that match the primary email address of each target user that was originally listed in the policy. *If you were to open one of those folders, you would see that it contains many metadata and metadata-journal files.*

10. Navigate back to the **Lookup** folder for the "source" sync policy. Move the folders for the desired target users to the empty **Lookup** folder of the "new" sync policy.

**NOTE:** Ensure that the target user folders are moved — not copied. If the folders are unfortunately copied, there would be two policies with the same target user, which would create duplicate items in the CRM and email systems when data sync is enabled.

11. Close both Windows Explorer windows.
12. In the **Riva Manager** application, on the menu bar, select **Policies**. In the right pane, edit the "source" sync policy.
13. On the **General** page, remove the target users that have been moved to the "duplicate" sync policy.
14. Save the "source" sync policy.

#### Step 4: Enable the “Source” CRM Sync Policy

These steps are used to enable the "source" sync policy and confirm that the correct users are synchronizing.

1. If the **Riva CRM Monitor** application is open, close it, and reopen it.
2. In the **Riva Manager** application, on the **Policies** page, right-click the "source" CRM sync policy, and select **Enable**.
3. In the **Riva CRM Monitor** application, confirm that only the target users from the modified "source" sync policy are synchronizing; confirm that the user accounts' "state" changes to **Synchronizing** and that the sync activities are visible in the user activity monitor windows.

#### Step 5: Enable the Duplicate CRM Sync Policy

These steps are used to enable the "duplicate" sync policy and confirm that the correct users are synchronizing.

1. In the **Riva Manager** application, on the menu bar, select **Policies**. In the right pane, right-click the "duplicate" sync policy, and select **Enable**.
2. In the **Riva CRM Monitor** application, confirm that only the target users from the "duplicate" sync policy are synchronizing; confirm that the user accounts' "state" changes to **Synchronizing** and that the sync activities are visible in the user activity monitor windows.

#### Step 6: Instruct the Moved User(s) to Delete Unwanted Items

When the "moved" users are syncing, their CRM sync policy will sync items only according to the

[www.rivacrmintegration.com](http://www.rivacrmintegration.com)



new policy settings. Items that were previously synced when the user was assigned to the "source" policy will no longer be synced by Riva, unless they are also specified in the new policy. For example, in the case scenario, the RHICKS user will have phone calls in his email client calendar which can be safely removed without affecting the phone call items in the CRM. As the user schedules phone calls in the CRM, they will no longer sync to the user's email account and will not be visible in their email client.

Riva admins need to provide clear instructions to users about which items can be safely removed from their email client application.

## Managing Riva Sync Policies

Before creating a Riva CRM sync policy, ensure that the following tasks have been completed:

- A Riva connection to the target CRM has been created and tested.
- A Riva connection to the target email system has been created and tested.
- A trial or purchase license has been requested and activated.

With respect to this article, Riva performs four types of data synchronization:

- **Initial Sync:** After a target user has been added to a CRM sync policy, Riva reads all of the policy filter settings and syncs data from the CRM to the target user's mailbox. The initial sync normally makes the following changes to the mailbox (which are reflected in the email client):
  - Contacts and leads are copied from the CRM to the user's Address Book and assigned a Riva sync category.
  - Appointments and phone calls are copied to the user's calendar and assigned a Riva sync category.
  - Tasks are copied to the user's task list and assigned a Riva sync category.
  - If SmartConvert is enabled, a set of **Create New** email sync drop folders are created.
  - If AssignTo is enabled, a set of **AssignTo** folders are created with corresponding unique email sync drop folders by module type.
- **Full Sync:** Normal scheduled sync of all new and modified data for enabled modules.
- **Drop Folder Sync:** Scheduled check for and sync of email from drop folders to the CRM.
- **Re-initialize Sync:** If data sync has stopped or become unlinked or corrupted, the administration can re-initialize all or selected target user accounts. For more information, see [Manage syncing users and re-init options for sync policies](#).

The goal is to create a CRM sync policy that can be configured and tested against the target systems with minimal disruption to the target systems or users. These best practices should be followed for evaluation and production deployments:

- Ensure that you **DO NOT** select the **SAVE** button on a sync policy until all of the policy options have been configured.
- When creating a CRM sync policy, [always ensure that the policy is disabled](#). This will permit installing and configuring the Riva sync service without having to attempt to sync individual users.
- To limit testing and mitigate the impact against the target systems, select only one or two target users. Actively involve those users in the testing of Riva syncing of CRM and email data.

- Configure the CRM sync policy to meet the expected requirements of the target users.
- Enable the CRM sync policy, and confirm that the initial synchronization is successful and at least two complete data sync cycles are completed.
- Tweak the CRM sync policy settings to better meet the needs and expectations of the target users, and confirm the results of all changes.
- After the CRM sync policy settings are finalized and tested, add the remaining target users. Confirm that the initial synchronization is successful and at least two complete data sync cycles are completed for every new target user added to the policy.

To get more specific information regarding configuring a sync policy please reference the below Knowledge Base Articles on our website, dependent on your mail client:

[Configure a sync policy for Exchange and IBM Notes](#)

[Configure a sync policy for Google's G Suite](#)

[Configure a sync policy for GroupWise](#)

[Set Advanced or Custom Options for Connection\(s\) or Sync Policy](#)

In the Riva Manager application and Riva On-Premises documentation, both terms are used interchangeably.

These advanced options are made available for several reasons:

- New features that do not yet have a user interface;
- A way of changing default values used in advanced deployments or configurations;
- When advanced configurations are specifically designed for a customer to meet a non-standard, customer-specific sync requirement. Typically, such options are provided through a billable professional service.

## The Way to Set an Option

There are multiple ways to set an option:

- **By interacting with the Riva Manager application user interface when selecting an option.** (For example, by selecting a check box.)
  - Riva has many advanced features — only the most commonly used options are available in the user interface. These options are often initially available as advanced options, and then due to customer request, they are made [www.rivacrmintegration.com](http://www.rivacrmintegration.com)

available to the user interface.

- **Entering keys and values in the Riva Manager application:** Many advanced options available to all users and many customer-specific options are applied by entering keys and values into fields, as [described in this article](#).
  - This method provides support for
    - advanced options that are not used very often; and
    - non-standard, customer-specific advanced business requirements.
- **Editing a file in a text editor:**
  - Some options are entered by [creating or editing an App.Setting file](#).
  - There are many tiers of options that are applied. "Application Executable" > "Riva Instance" > "Per-Connection" > "Per-Policy" > "Per-User" > "Sync Now API". As a rule of thumb, these are applied from least specific (left) to most specific (right). For more information, see [Settings hierarchy and overrides](#).

## Apply Advanced or Custom Options to a Sync Policy or Connection Object

**Note:** Because there is a distinct sync policy wizard and edit window for every [supported email system](#), options specific to an email system are configured in the sync policy.

### Key and value:

An advanced or custom option has two components:

- a **key**: the name of the advanced or custom option; also known as the **key name**; and
- a **value**: the part of the advanced or custom option that determines the option's behaviour; also known as the **key value**.

Example:

**Sync.Crm.EmailFields.Contact = "Email,Email2,Email3"** is the complete option.

Key (Key Name)	Value (Key Value)
Sync.Crm.EmailFields.Contact	Email,Email2,Email3

### Notes:

- The value is not case sensitive.
- The equal sign (=) is not part of the option. It is used only in the documentation.

## To configure advanced or custom options for a sync policy or connection object in Riva 2.4.43 or higher:

This procedure applies to Riva On-Premises 2.4.43 or higher.

For Riva 2.4.42 or earlier, see [Configure options in Riva 2.4.42 or earlier](#).

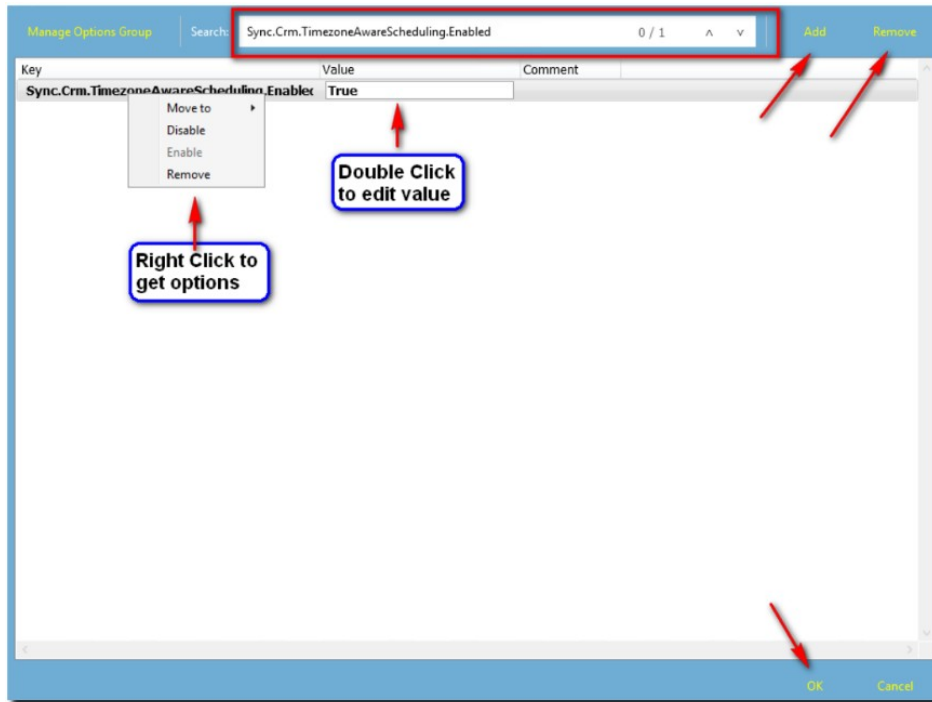
1. Edit the relevant Riva sync policy or connection.
2. Select **Advanced Options** and select **Custom Options**.

The screenshot shows the 'Edit CRM Synchronization Policy' window. The left sidebar has 'Advanced Options' selected. The main area shows several configuration sections. The 'Custom Options' button is highlighted with a red rectangle. Other visible options include 'Attachment Options' (with checkboxes for disabling synchronization and appending details), 'Attachments Filtering' (with filters for file size and extension), 'Privilege Exception Handling Options' (with dropdowns for Create, Modify, and Delete), 'Contact Deletion Options' (with checkboxes for synchronizing deletions and moving deleted items), and 'Sync Protections' (with buttons for Delete Safety and First Sync Protections).

3. Best practice: In the **Advanced Options** window that appears, search for the [key](#) to confirm whether it already exists.
4. If the key exists, the key appears in bold within the list. To change the value, select the key from the list, and in the right pane, within the **Key Value** area, change the value.

If the key name does not exist, select **Add New**. In the **Option Properties** panel, note that the **Key Name** has already been entered, and then enter the desired value in the **Key Value**.

Select **Update** and verify that the key and value appear as desired in the list.

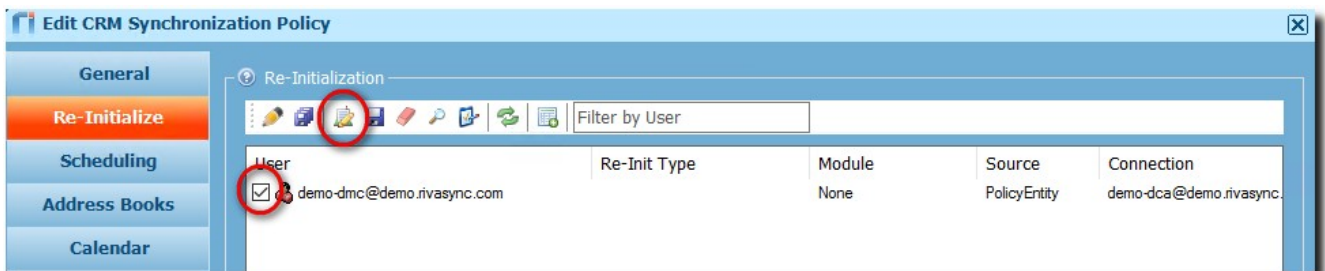


5. In order to add multiple keys and their values: For each key and value, repeat steps 3 and 4.
6. When done editing, select **OK**.
7. Save the sync policy or connection.

## Apply Advanced or Custom Options to Individual Target User(s) in the Riva Sync Policy

**To set advanced or custom options for specific target users in Riva 2.4.43 or higher:**

1. In the Riva sync policy, select the **Sync Start Time** tab.
2. Select a user and select the third icon from the left (**User Advanced Options**).

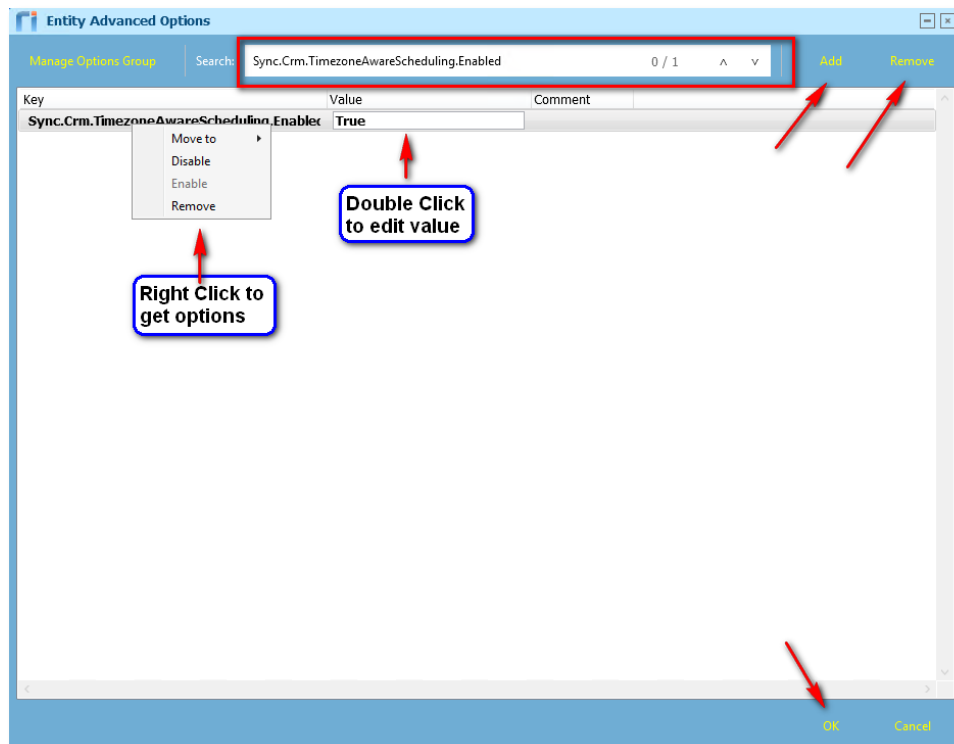


3. Best practice: In the **Entity Advanced Options** window that appears, search for the [key](#) to confirm whether it already exists.

4. If the key exists, the key will appear in bold within the list. To change the value, select the key from the list, and in the right pane, within the **Key Value** area, change the value.

If the key name does not exist, select **Add New**. In the **Option Properties** panel, note that the **Key Name** has already been entered, and then enter the desired value in the **Key Value**.

Select **Update**, and verify that the key and value appear as desired in the list.



5. Select **OK** to close the **Entity Advanced Options** window.
6. To save the changes,
  - Right-click the selected user, and then select **Save Changes**; or
  - Save the syncpolicy.

## How the Changes to the Advanced or Custom Options Are Applied

The changes made to the advanced or custom options take effect as follows:

- **Connection and Sync Policy changes:** If the synchronization service is already running, the service detects changes to the synchronization policy and will automatically restart the synchronization with the new configuration.
- **Per-User change:** During the user's next synchronization cycle, the new options are automatically used. If changed keys were applied only to users, there is no need to modify the synchronization policy.
- **Best practice:** If multiple changes to connections or sync policies are anticipated, we recommend first stopping the Riva synchronization services, applying the changes, and then starting the service.

## What Data is Affected

Applying an advanced or custom option to a sync policy affects all the data that Riva syncs afterwards.

To apply the advanced or custom option to previously synced data, the target users need be re- initialized. For instructions on selecting the correct re-initialization option, see [Re-Initialization Options for Riva Sync Policies](#).

## How to Rename a Riva Sync Policy

It may be desirable to add multiple sync policies and apply a custom naming strategy. Multiple policies will appear in the policy list in Ascending alphabetical order.

There are two procedures to rename a policy:

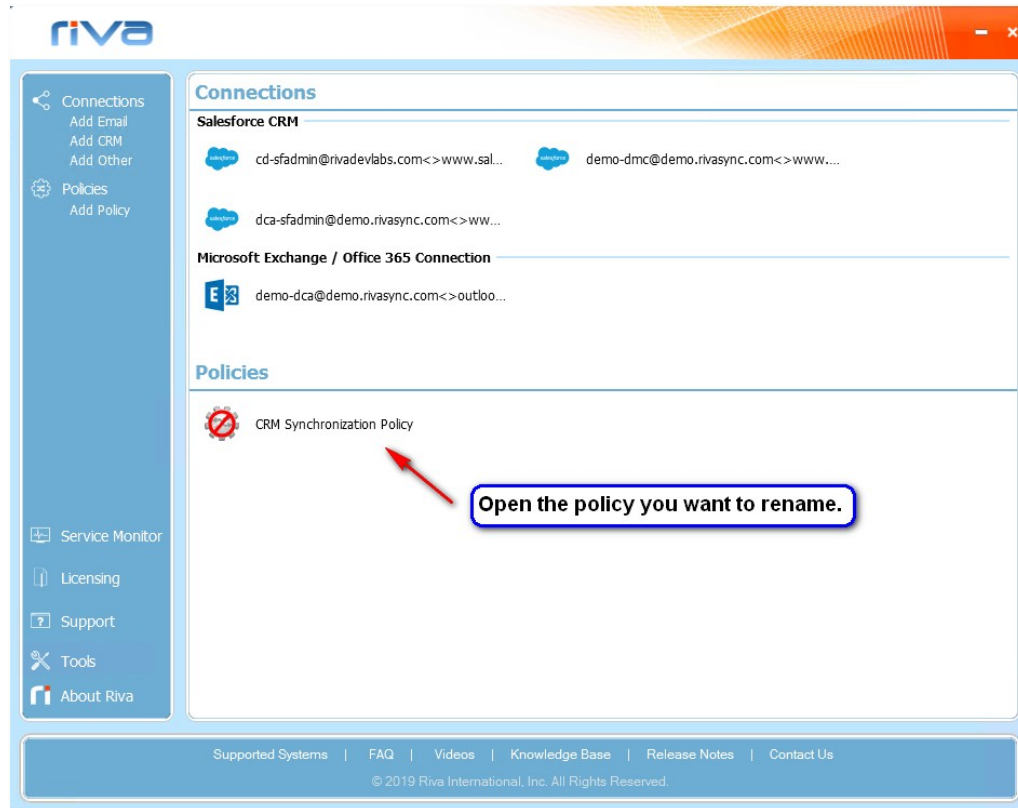
- Rename a synchronization policy
- Rename the sync policy file



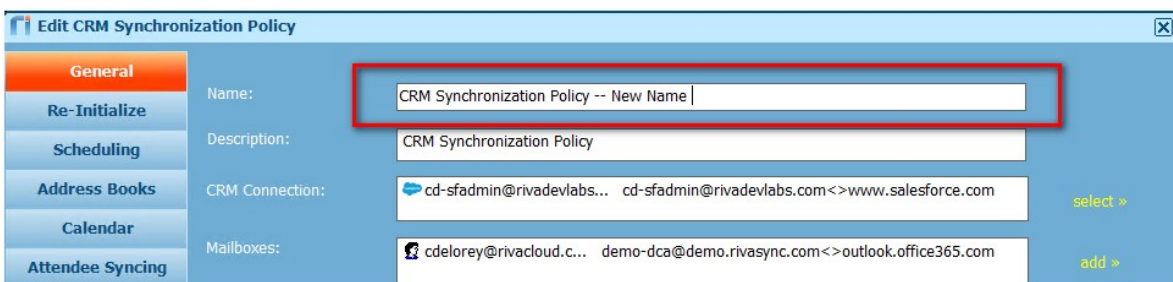
## Rename a Synchronization Policy

### To rename a sync policy:

1. Launch the **Riva Manager** application.
2. Select the **Policies** tab.



3. In the right pane, double-select the policy.
4. In the **Name** field, rename the policy.



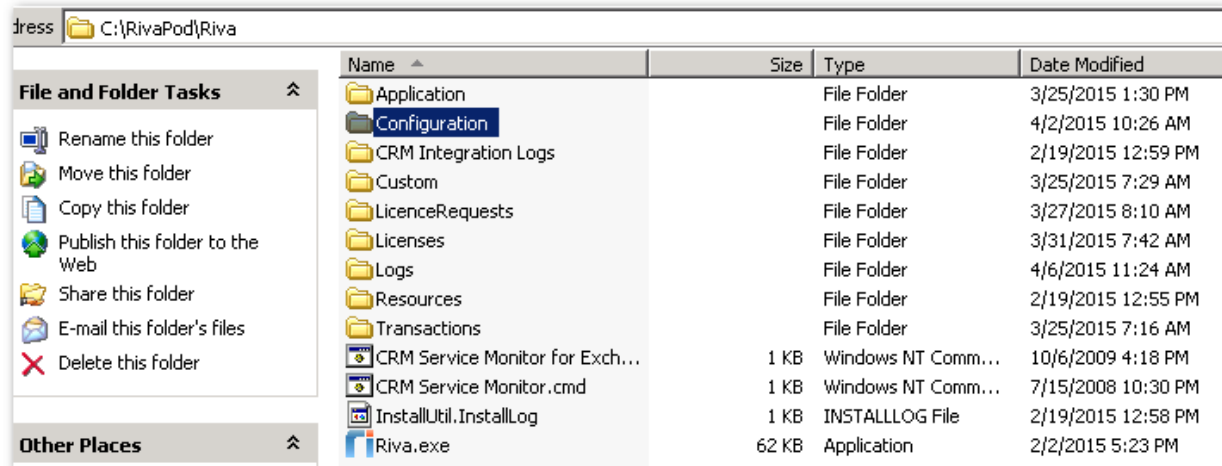
5. Save the policy.

## Rename the Policy File

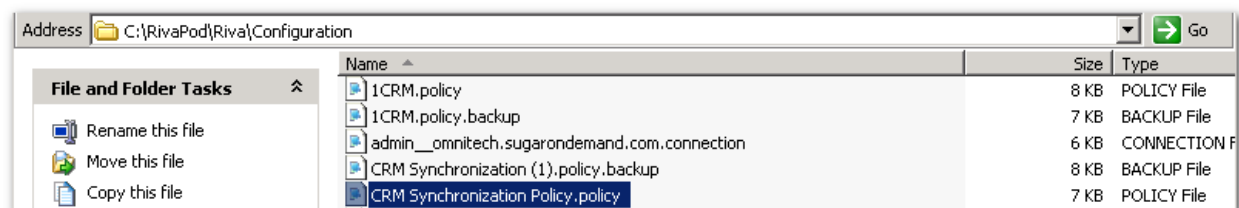
Renaming the synchronization policy for Riva On-Premises does not change the name of the policy file located in the \Riva\Configuration folder. You must manually rename this file:

### To rename the policy file:

1. In **Windows Explorer**, navigate to the Riva configuration folder: \Riva\Configuration



2. Select the **Type** column header to sort the files by file type. The old file is still named "CRM Synchronization Policy.policy".



3. Rename the file while keeping the **.policy** extension.

Name	Size	Type	Date Modified
admin__omnitech.sugaronde...	6 KB	CONNECTION File	3/27/2015 8:10 AM
customer.config	1 KB	CONFIG File	3/31/2015 7:39 AM
Dynamics 2015.policy	8 KB	POLICY File	3/31/2015 1:07 PM
Dynamics 2015.policy.backup	8 KB	BACKUP File	3/31/2015 1:07 PM
Salesforce.policy	7 KB	POLICY File	4/2/2015 10:26 AM
Salesforce.policy.backup	7 KB	BACKUP File	4/2/2015 10:26 AM
success1@rivademo.onmicros...	17 KB	CONNECTION File	3/26/2015 8:32 AM
success1@rivademo.onmicros...	17 KB	BACKUP File	3/26/2015 8:03 AM
success-admin@rivacloud.co...	28 KB	CONNECTION File	3/25/2015 7:29 AM
success-admin@rivacloud.co...	28 KB	BACKUP File	3/25/2015 7:03 AM
SugarNew.policy	7 KB	POLICY File	4/2/2015 10:21 AM
Sugar.policy.backup	7 KB	BACKUP File	4/2/2015 10:20 AM
taustin@rivacloud.com__ex2...	1 KB	CONNECTION File	9/24/2014 3:20 PM

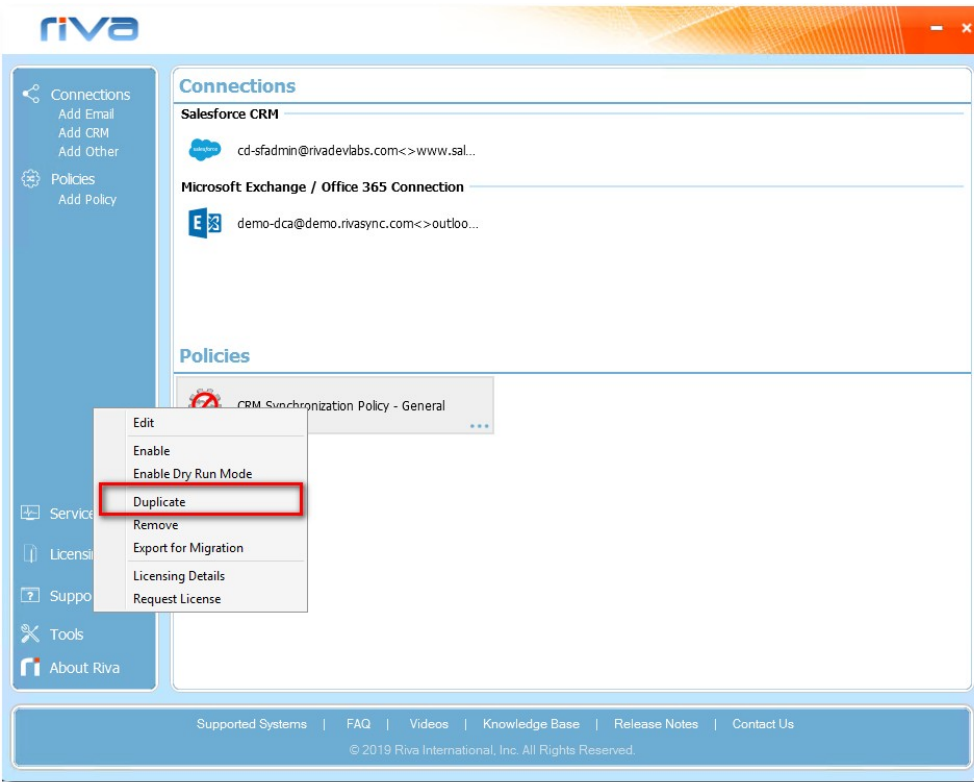
## How to Duplicate a Riva Policy

Many organizations start with a single sync policy and then want to create similar sync policies that will have slightly different options. Riva provides a **Duplicate** option that creates a disabled duplicate of the original sync policy. Riva administrators can then modify option settings and add new users or even move users from the original sync policy to the new duplicate sync policy.

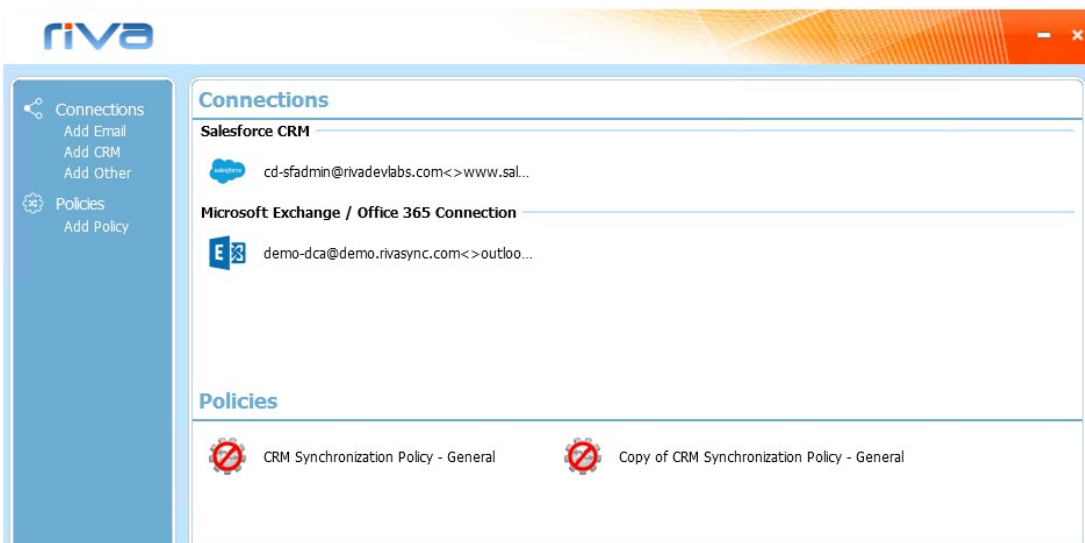
**Note:** Understanding Riva transaction records and how Riva handles those records when a sync policy is duplicated is very useful. We recommend that Riva administrators review the information in [Understand how Riva maintains transaction records](#).

### To duplicate a policy:

1. Start the **Riva Manager** application.
2. Under policies, right-click the policy, and select **Duplicate**.

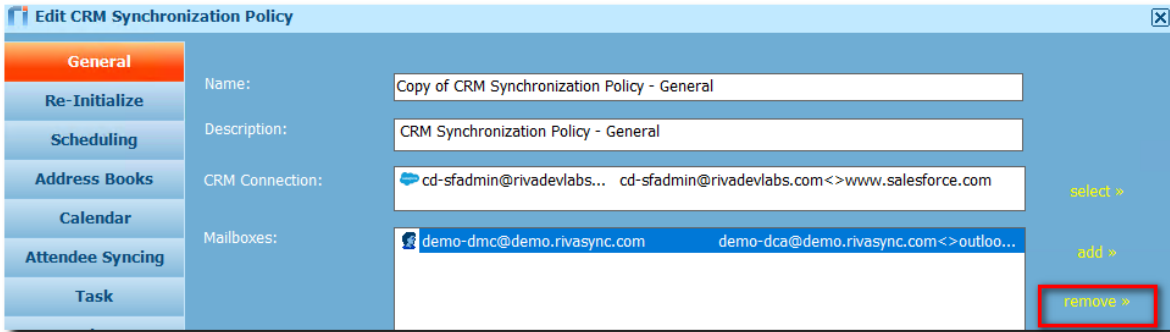


The duplicate policy appears. Its name is a combination of the words "Copy of " and the name of the original policy that was duplicated. For example, the illustration shows that the duplicate of the file "**Off 365 <> Sugar OD 6.7 Sync Policy**" was named "**Copy of Off 365 <> Sugar OD 6.7 Sync Policy**".



**WARNING:** Do not enable the duplicate sync policy until it has been modified.

- Double-click the **Copy of ...** sync policy. On the **General** page, remove all of the users. [Learn why removing users is important.](#)



- Save** the sync policy.

## What Happens When a Sync Policy is Duplicated

When a sync policy is duplicated, the following actions occur:

- The Riva Manager application creates a **disabled** sync policy object. The duplicate contains the same user list and same policy option settings as the original source sync policy. Example: **Copy of Off 365 <> Sugar OD 6.7 Sync Policy**.
- In the **\Riva\Configuration** folder, a sync policy file is created. If the sync policy name contains characters that are not permitted in a file name, Riva substitutes an underscore character (\_). Example: **Copy of Off 365 <> Sugar OD 6.7 Sync Policy** is changed to **Copy of Off 365 \_\_ Sugar OD 6.7 Sync Policy.policy**.

Name	Date modified	Type	Size
Off 365 __ Sugar OD 6.7 Sync Policy.policy	6/1/2016 2:48 PM	POLICY File	9 KB
Copy of Off 365 __ Sugar OD 6.7 Sync Policy.policy	6/1/2016 2:56 PM	POLICY File	8 KB
	10/23/2015 10:23 AM	CONNECTION File	25 KB

- A corresponding [sync policy transaction folder is created](#).

**Tip:** Most Riva administrators rename the duplicate policy. See [How to rename a Riva sync policy](#).

## Remove a Riva On-Premises Sync Policy or Connection

**WARNING:** Removing a sync policy while the sync service is running can have unpredictable results. We highly recommend disabling and backing up a sync policy before removing it.

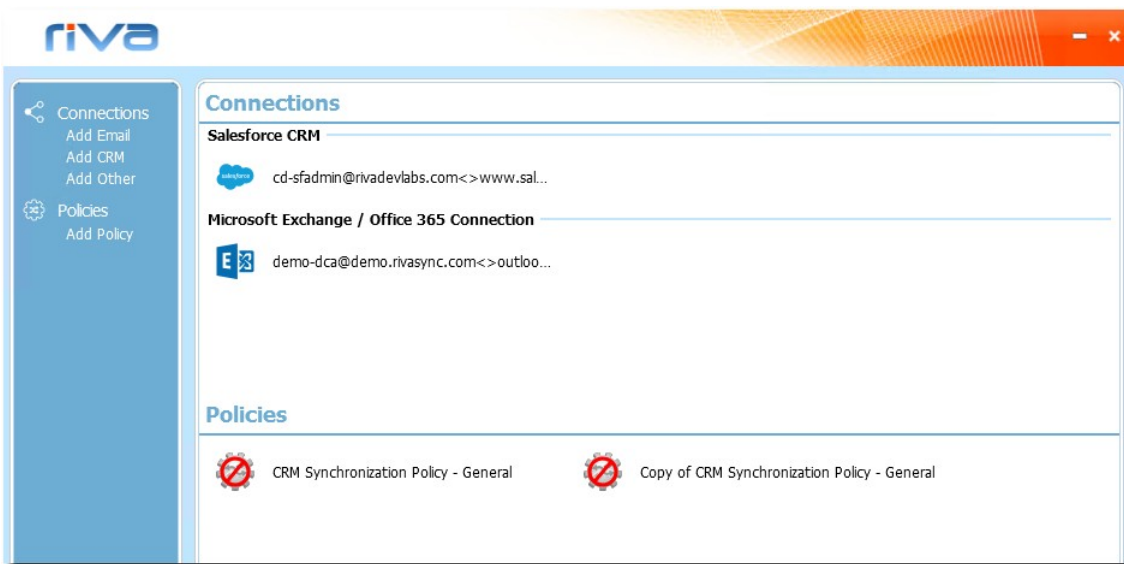
[www.rivacrmintegration.com](http://www.rivacrmintegration.com)

## Ensure That You Are Working with the Correct Riva Files

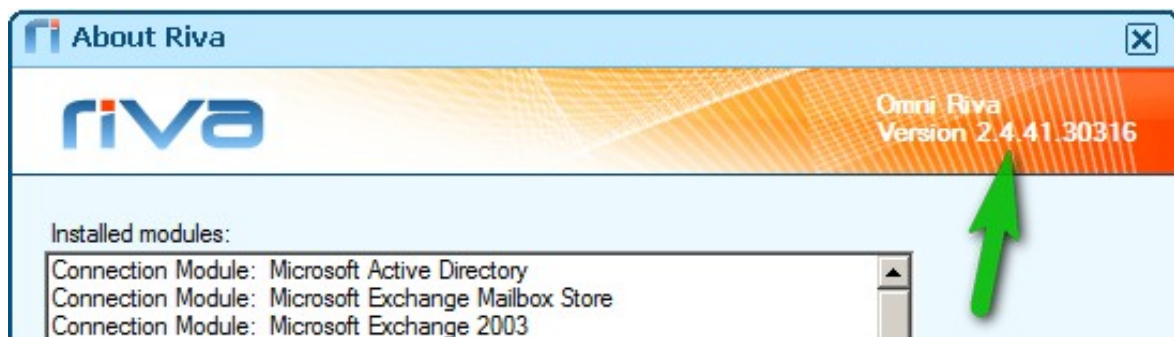
It is important to access the correct set of Riva files and folders throughout these procedures.

**To access the correct \Riva folder structure:**

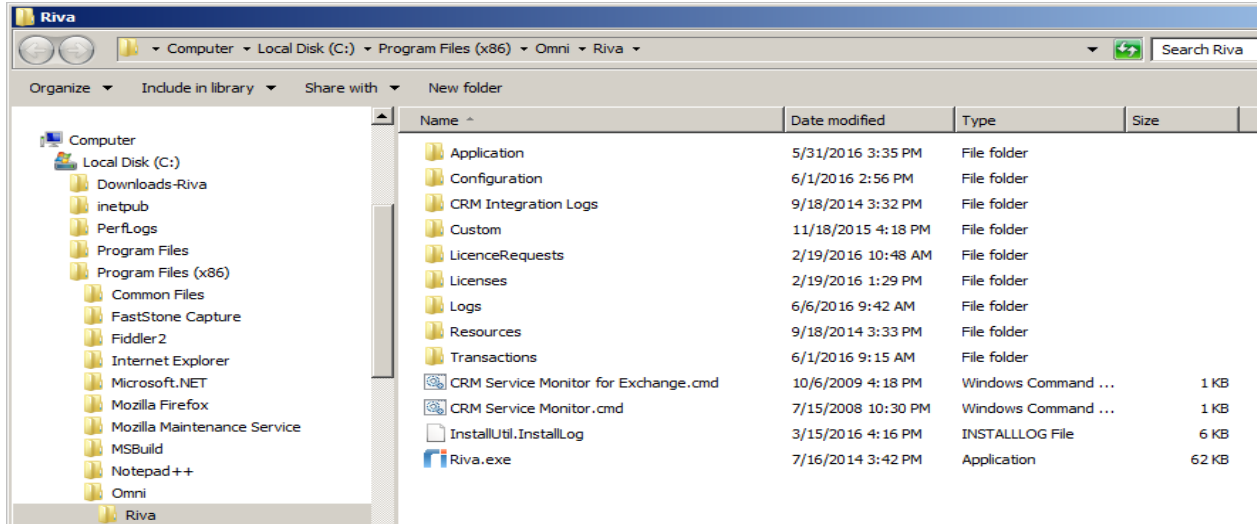
1. Start the **Riva Manager** application.
2. On the menu bar, select **Policies** to see the sync policies on the policies list.



3. In the top left corner, select the **Riva** logo.
4. In the **About Riva** window, in the top right corner, double-click the Riva version number



Windows Explorer displays the **\Riva** parent folder for the set of Riva files that the Riva Manager application and the Riva sync service are reading.

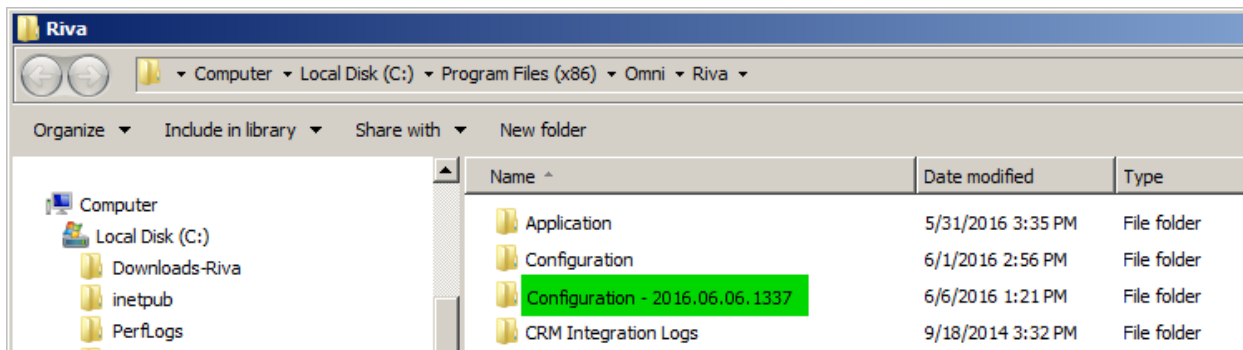


## Recommended: Make a Backup of the Riva Configuration Files

Before making any changes to sync policy names or files, Riva administrators should make a backup copy of those files.

### To make a backup of the Riva configuration files:

1. In **Windows Explorer**, make a copy of the **\Riva\Configuration** folder.
2. Rename the copy **\Riva\Configuration - YYYY.MM.DD.HHMM**. (Insert the local Windows date and time.)

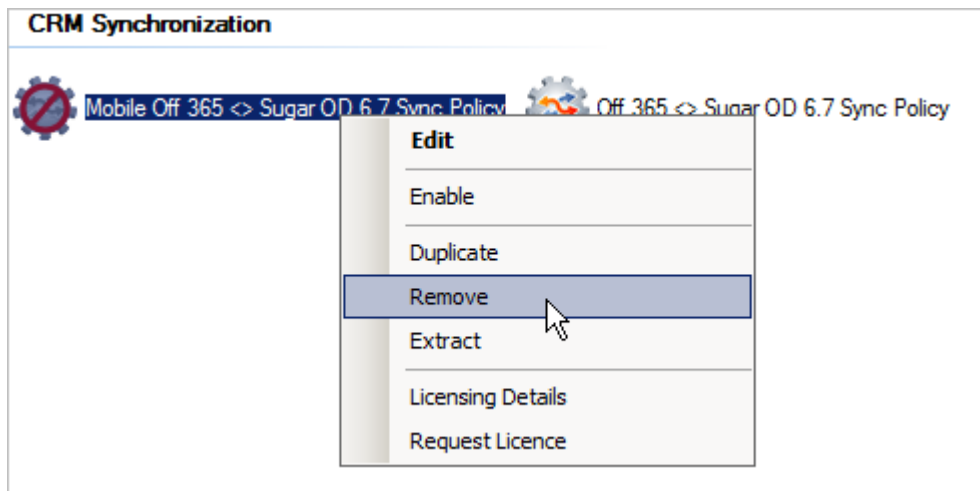


## Remove a Synchronization Policy

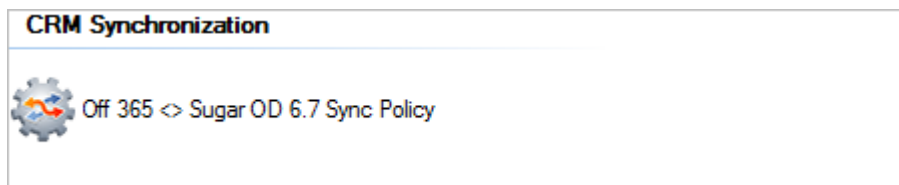
Sometimes a sync policy needs to be removed because it is no longer in use. This can cause Riva to stop syncing, because the transaction records will no longer be pointing to the correct users. (It helps to [understand how Riva maintains transaction records](#).)

### To remove a sync policy:

1. Start the **Riva Manager** application. On the menu bar, select **Policies**.
2. In the right pane, edit the sync policy to be removed. Disable the policy, and save it. These actions create a new backup policy file.
3. Right-click the policy to be removed, and select **Remove**.



4. In the **Remove Policies** window, select **Yes**. The policy is no longer visible in the Riva Manager application.



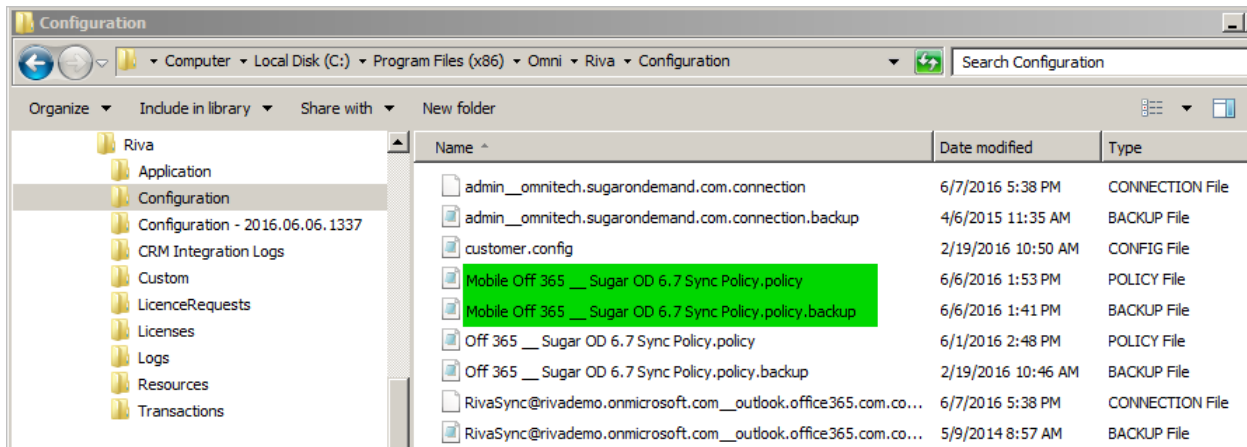
5. If the Riva sync service was syncing users assigned to the deleted sync policy, we recommend restarting the service, to reduce the number of errors that may be written to log files.



## What Happens When a Policy is Removed

A Riva sync policy consists of three components:

- a sync policy object that is visible in the Riva Manager application,
- a .policy file and a .policy.backup file in the \Riva\Configuration folder,



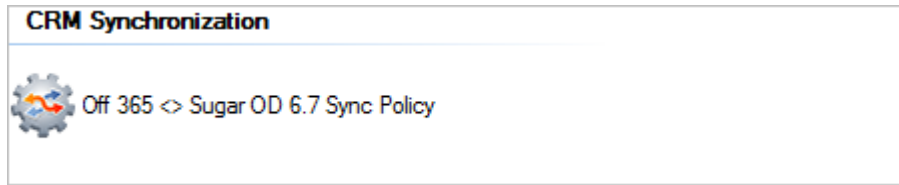
and a sync policy transaction folder. (It helps to [understand how Riva maintains transaction records](#).)

When a sync policy object is removed in the Riva Manager application:

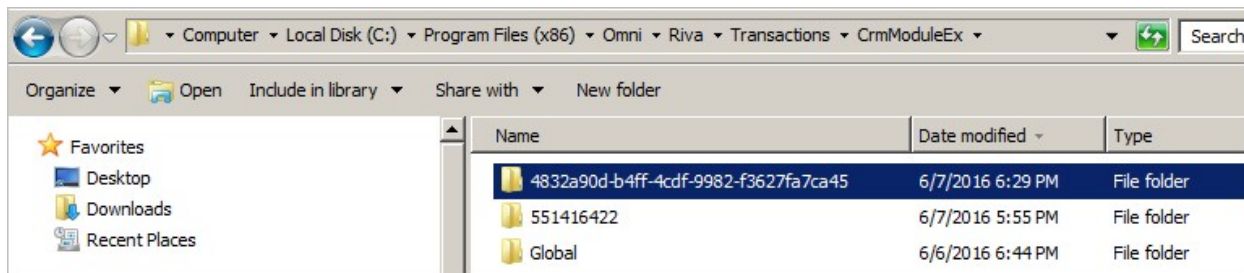
- the **.policy** file is removed from the \Riva\Configuration folder

admin__omnitech.sugarondemand.com.connection	6/7/2016 5:38 PM	CONNECTION File
admin__omnitech.sugarondemand.com.connection.backup	4/6/2015 11:35 AM	BACKUP File
customer.config	2/19/2016 10:50 AM	CONFIG File
Mobile Off 365 __ Sugar OD 6.7 Sync Policy.policy.backup	6/6/2016 1:41 PM	BACKUP File
Off 365 __ Sugar OD 6.7 Sync Policy.policy	6/1/2016 2:48 PM	POLICY File
Off 365 __ Sugar OD 6.7 Sync Policy.policy.backup	2/19/2016 10:46 AM	BACKUP File
RivaSync@rivademo.onmicrosoft.com__outlook.office365.com.co...	6/7/2016 5:38 PM	CONNECTION File
RivaSync@rivademo.onmicrosoft.com__outlook.office365.com.co...	5/9/2014 8:57 AM	BACKUP File

- and the object is removed from view in the Riva Manager application



- and the sync policy transaction folder remains undisturbed, which allows the [sync policy to be restored from a backup](#) without worrying about missing transaction records.

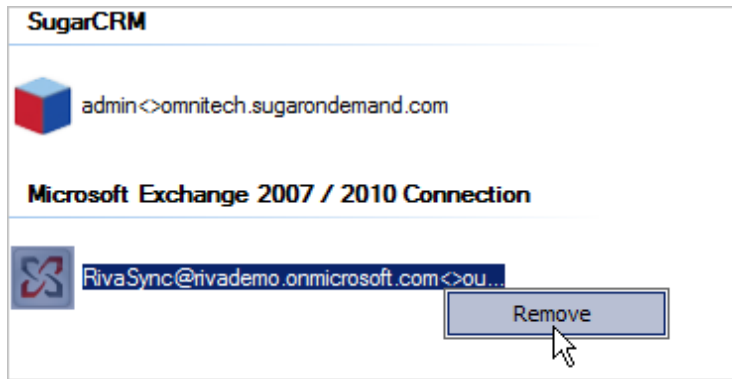


## Remove a Connection

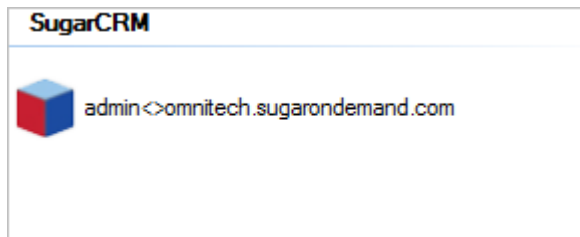
**WARNING:** Removing a connection affects all sync policies that use that connection. Before removing a connection, ensure that it is not being used by any active or disabled sync policy. Usually, connections are removed only if user mailboxes have been migrated to a different host or service or if the CRM user accounts have been migrated to a different vendor CRM. If backups of the .connection files are created, it is possible to restore connections that are removed by accident.

### To remove a connection:

1. Start the **Riva Manager** application. On the menu bar, select **Setup**.
2. Edit the connection to be removed, do not make any changes, and save it. These actions create a backup connection file.
3. Right-click the connection to be removed, and select **Remove**.



4. In the **Remove Connection** window, select **Yes**. The connection is no longer visible in the Riva Manager application.



If the Riva sync service was syncing users assigned to a sync policy that was using the connection that was just removed, those sync polls for those users would fail.

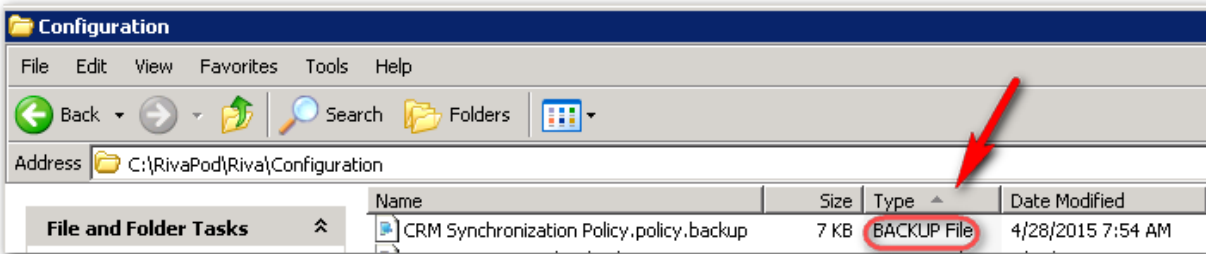
## What Happens When a Connection is Removed

When a connection is removed:

- the **connection object** is no longer visible in the **Riva Manager** application, and
- the **.connection file** is removed from the **\Riva\Configuration** folder.

## [How to Restore an Accidentally Removed Riva Sync Policy or Connection](#)

If a Riva sync policy or a connection is accidentally removed or no longer appears in the Riva manager application, it can be recovered through the backup file that Riva creates automatically once a change is made to that policy or connection.



**To restore a sync policy or connection:**

1. Close the **Riva Manager** application.
2. In **Windows Explorer**, navigate to the Riva installation folder, for example C:\Program Files\Riva\Configuration.
3. Select the **Type** column header to sort the files by file type.
4. Find the policy or connection **BACKUP File** that has the same name as the policy or connection that has been accidentally removed.
5. Right-click the file, select **Rename**, remove the **.backup** extension, and accept the new name.
6. Launch the **Riva Manager** application to restore the policy or the connection.

## Appendix – Corresponding Knowledge Base Articles:

[Upgrade to the latest public release](#) from the Riva Manager application.

[Manually upgrade a Riva server](#) from a downloaded ZIP file.

[Roll back from an upgrade.](#)

[Uninstall a Riva server](#)

[Add App.Setting advanced custom options.](#)

[Move a Riva server to a different Windows system.](#)

[Relocate the Riva files on the existing Windows system](#)

[Disable or enable syncing for a single user.](#)

[Disable or enable syncing for a sync policy.](#)

[Permanently remove a user from a sync policy.](#)

[Add a new user to a sync policy.](#)

[Add multiple Exchange users to a sync policy.](#)

[Move users to another sync policy using the same category names.](#)

[Move users to another sync policy using different category names.](#)

[Move target users to a duplicated sync policy.](#)

[Configure a sync policy for Exchange and IBM Notes.](#)

[Create and configure a sync policy for Google's G Suite.](#)

[Configure a sync policy for GroupWise.](#)

[Set advanced custom options.](#)

[Rename a sync policy.](#)

[Duplicate a sync policy.](#)

[Remove a sync policy.](#)

[Restore an accidentally removed sync policy or connection.](#)