SpiraTeam® | Email Integration Guide

Inflectra Corporation

Date: February 5th, 2017

Contents

1. Introduction

SpiraTeam® is an integrated Application Lifecycle Management (ALM) system that manages your project's requirements, releases, test cases, issues and tasks in one unified environment:

SpiraTeam® contains all of the features provided by SpiraTest® - our highly acclaimed quality assurance system and SpiraPlan® - our agile-enabled project management solution. With integrated customizable dashboards of key project information, SpiraTeam® allows you to take control of your entire project lifecycle and synchronize the hitherto separate worlds of development and testing.

This guide describes how to setup the integration between SpiraTeam and your company's email system so that inbound emails can be processed by SpiraTeam and automatically converted into either new incidents or as comments on existing artifacts.

For information regarding how to use SpiraTeam, please refer to the *SpiraTeam User Manual* instead.

2. Installing the Email Integration Service

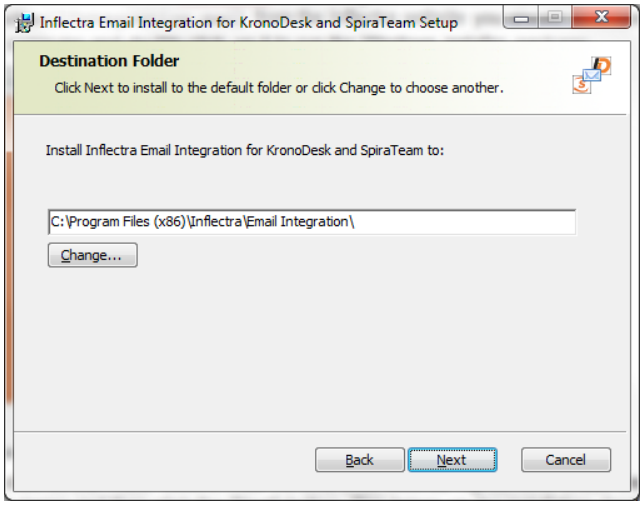
This section outlines how to install the SpiraTeam email integration service onto your environment. Depending on your environment you can install the email integration service on:

1. Your SpiraTeam application server
2. Your corporate mail server
3. A separate workstation that can connect to both SpiraTeam and your mail server

If your SpiraTeam installation is installed on-premise, then you can use options (1), (2) or (3), if your SpiraTeam installation is hosted by Inflectra as a Software as a Service (SaaS) subscription then you'd need to use either option (2) or (3).

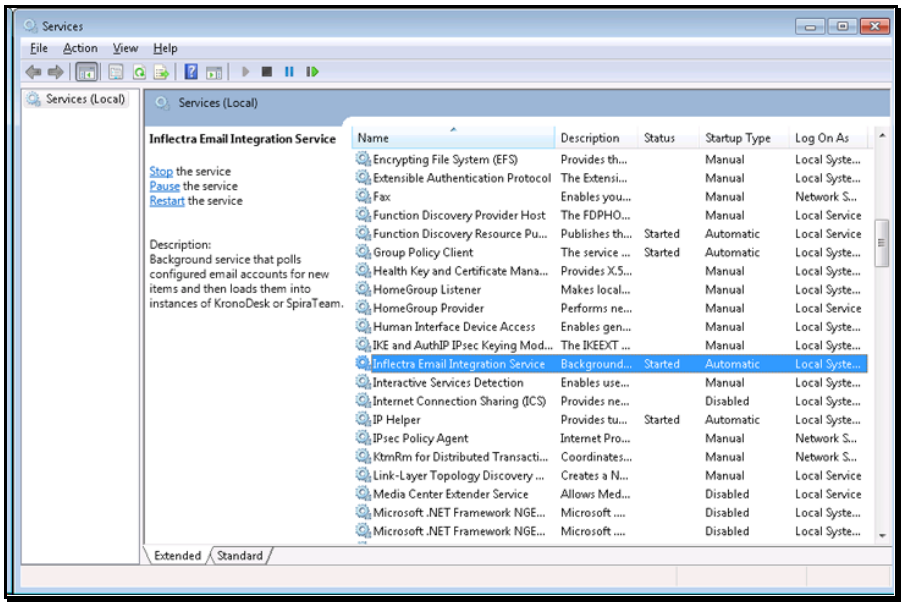
Once you have downloaded the SpiraTeam email integration installation package (`InflectraEmailIntegration.msi`) from the Inflectra website you should download it onto the appropriate computer and double-click on it to run the Windows installer package:

You should click on the "Next" button, read the End User License Agreement, check the box that you agree with its terms and then click the "Next" button. This brings up the installation location page:



You should choose the appropriate place to install the email integration service and then click “Next”. On the next screen click the “Install” button and it will complete the software installation.

Once the installation has completed, you will see the following new service listed in the Control Panel > Administrative Tools > Windows Services section:

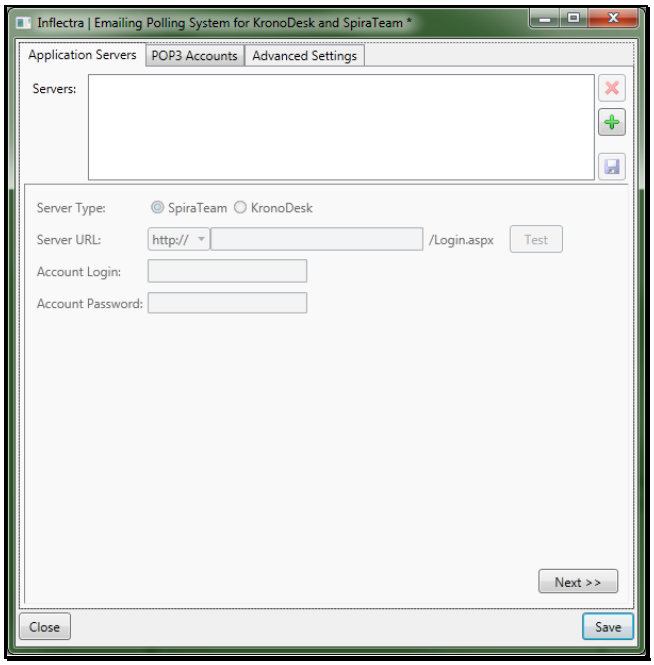


The service should be listed to run in Automatic mode and should already be started.

Note: This email integration service is able to integrate with both KronoDesk and SpiraTeam from Inflectra, however the focus of this guide is the integration with SpiraTest, SpiraPlan and SpiraTeam (hereafter SpiraTeam) only.

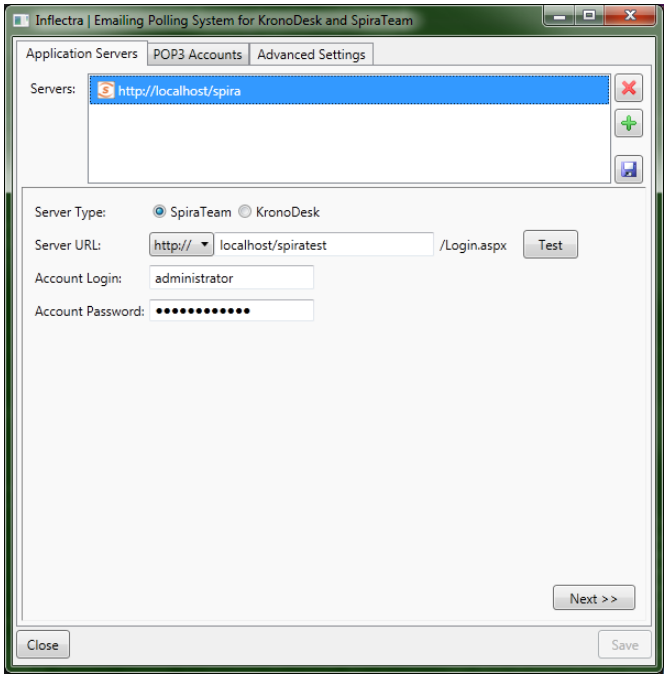
3. Configuring the Email Integration Service

Once you have completed the installation, you can configure the email integration service by going to Start > Program Files > Inflectra SpiraTeam > Tools > Email Integration which will bring up the management interface.



3.1. Connecting to the SpiraTeam Server

The first tab lets you specify the SpiraTeam instances that the email integration service will connect to. To add a new SpiraTeam server, click on the green Add (+) icon to switch the screen to allow you to enter a new server:



You need to enter the following information:

- **Server URL -** The URL to SpiraTeam server
- **Account Login -** The account login that will be used to connect to SpiraTeam. It needs to be a user with the “administrator” role.
- **Account Password -** This is the password for the account

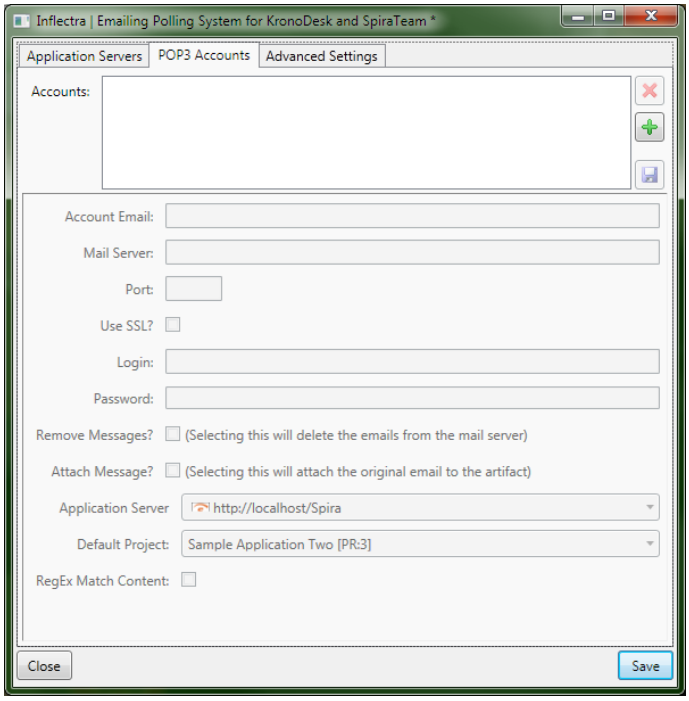
Click the “Test” button to verify the connection. Once it has passed, click the Save icon to save the new SpiraTeam server information.

To modify an existing SpiraTeam server instance, just click on its name in the server list. To delete a server, select its name in the server list and click the Delete icon (X).

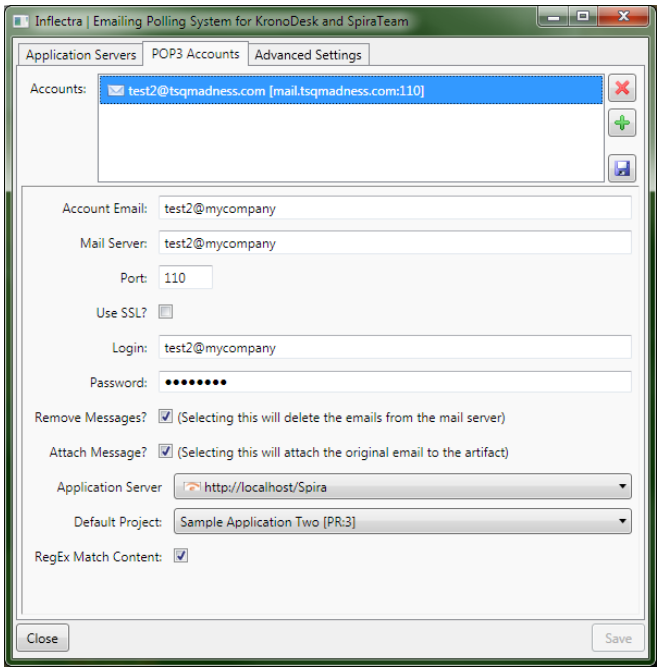
Once you have entered all the SpiraTeam instances that you will be connecting to, click the “Next” button to move to the next tab and configure the mail server integration.

3.2. Connecting to the POP3 Mail Server

The “POP3 Accounts” tab displays a list of all the configured mail servers:



Initially it will be empty, so just click the Add (+) icon to add a new mail server:



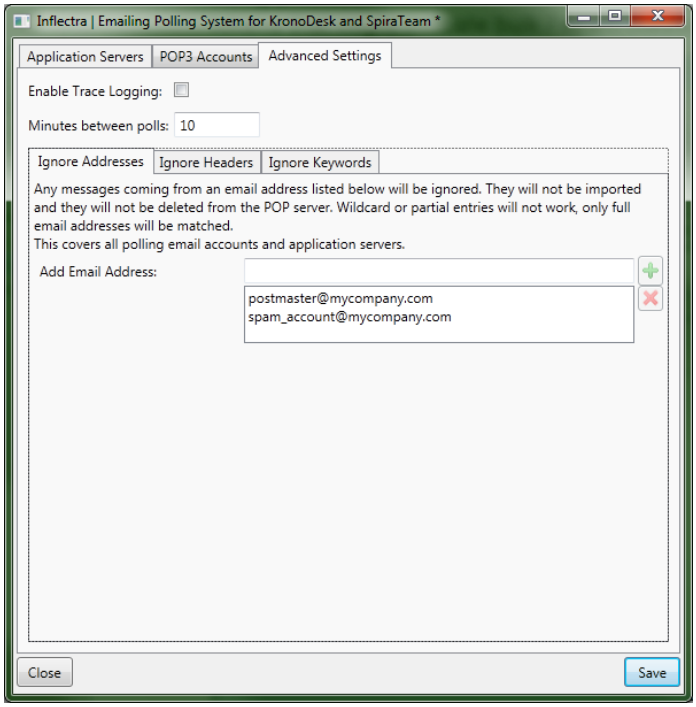
You need to enter the following information:

- **Account Email –** This should be the email address that will be polled for new support emails.
- **Mail Server –** This should be the fully-qualified name or IP address of your POP3 mail server.
- **Port –** This is the port that your mail server expects incoming POP3 requests to use. The default for unencrypted POP3 requests is 110 and the default for SSL encrypted POP3 requests is 995.
- **Use SSL –** You should check this option if your mail server requires a secure SSL connection.

- **Login/Password –** You should enter the login/password for the mail server that allows reading of inbound messages for the email address specified above.
- **Remove Messages –** Checking this option will make the email integration service remove the email messages from in the Inbox of the user's email account. We recommend leaving this unchecked when first using the service. Once you are happy that the integration is correctly handling spam and not ignoring correct messages, you can check this option to prevent the email inbox getting too large.
- **Attach Message –** Checking this option will attach the original email message to the new help desk ticket created in SpiraTeam as well as populating the ticket with the contents of the message. This is useful when debugging a new installation but typically would be unchecked during normal operation.
- **Application Server –** You should specify the instance of SpiraTeam that this email account will be linked to.
- **Default Project** – When creating new incidents, this will be the default project that the new incident will be created in, unless the Match Content option is selected below. For any incoming email that has an artifact token (For example: `[IN:45]` for Incident #45, or `[RQ:912]` for Requirement #912), and the user's email is registered to a user in that project, then the email will be imported as a comment to that artifact.
- **RegEx Match Content** – Checking this option will allow the email integration service to do a name match in the body of the email for possible project names instead of just relying on the "default project". For example if your email contains "Project1" in the message text it will be routed to Product1 in SpiraTeam. Items looked for are Project tokens (`[PR:##]`), and then the Project name in the subject line of the email and the text of the email.

3.3. Configuring the Advanced Settings

Once you have finished configuring the SpiraTeam server instances and POP3 mail accounts, you can click on the "Advanced Settings" tab to setup special rules that prevent emails from specific accounts being processed as well as allow the email integration service to look for special mail headers and subject tokens that might indicate bulk / spam messages that should be ignored.



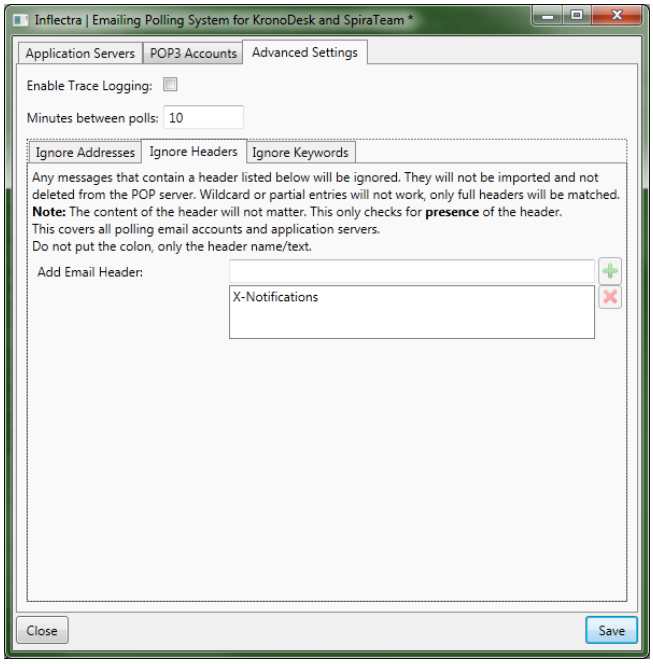
You can configure the following settings:

- **Enable Trace Logging –** When this option is checked, the email integration service will log information messages to the Windows Application Event Log on the machine running the integration service. This is useful when first deploying the system or when you are encountering issues and Inflectra support personnel have asked you switch on trace logging to aid in support. For normal use we recommend turning this setting off to avoid too many messages being logged in the Event Log.

- **Minutes Between Polls –** This setting specifies the interval (in minutes) between each time the email integration service attempts to retrieve new email messages from the email server.

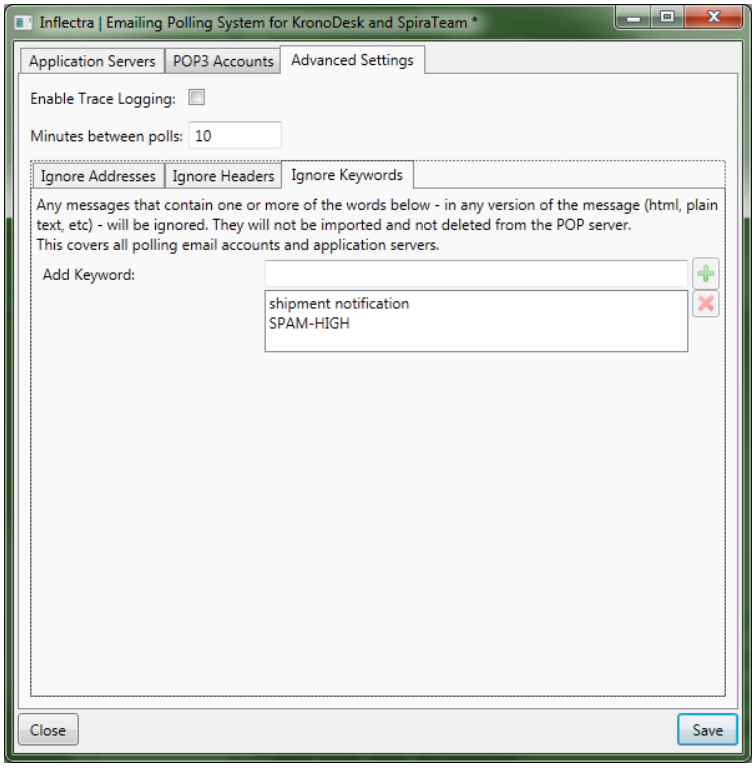
- **Ignore Addresses –** In this section you can add a list of any email addresses that you want to ignore and not use for creating new SpiraTeam help desk tickets. If there are any known senders or internal email accounts, you should add them in this section.

In addition, there are two other sub-tabs to the Advanced Settings tab that provide configuration options:



The “Ignore Headers” section allows you to specify any email message headers that if present in an email message will be ignored by the email integration service.

Note: Right now, the importer will only check the *presence* of a header, not its *contents*. As long as the header exists, even if it’s value is null, the message will not be imported.



The “Ignore Keywords” section allows you to specify any keywords/phrases that if present in the subject-line or body of an email message will be ignored by the email integration service. Some mail servers that have built-in SPAM detection systems will automatically add SPAM-HIGH, SPAM-MEDIUM, SPAM-LOW to the subject line (for example).

4. Using the Email Integration Service with SpiraTeam

Once you have the email integration service configured, we recommend that you initially clear the Windows Application Log on the machine. This will allow you to quickly see any errors that occur due to misconfiguration. The event viewer can be found in Control Panel > Administrative Tools > Event Viewer.

Once you have the email integration enabled and running, any users that email in a support ticket to one of the "watched" email addresses will experience the following process:

1. The user emails incident.logger@mycompany.com with an incident to create.
2. The contents (including attachments) of the email will be parsed by the email integration service.
    - The application will look for tokens to decide if it should be inserted in the default project or another user-specified project.
    - The sender's email address will be queried to make sure that the user has access to create incident in the selected project. (If not, the system will then check the user's permissions for the default project.)
    - If the user has permission, the new incident is created.
3. The user will receive an automated email from the system letting them know that the incident was created:

> SpiraTeam
> Incident "Need New Security Settings updated in Documentation" in project "Project1" has been changed.
> Please log into SpiraTeam to view this Incident's details.
>
> https://localhost/spirateam/6/Incident/2196.aspx

4. The user will not be subscribed to the ticket unless the user falls under normal Workflow Notification or Event Notification settings.
5. Any time the user gets a notification email from the server, they can reply to the email – leaving the token in the subject line unaltered – and their reply will be put into the ticket as a new comment. It's important that – if enabled in the SpiraTeam application – the separator line is not altered, and the reply is kept above the line. Any test under that line will not be imported. (If the separator line is altered, or the option is disabled in the SpiraTeam administration, then the entire email, including quotes and reply text, will be inserted.)

Legal Notices

This publication is provided as is without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information contained herein; these changes will be incorporated in new editions of the publication. Inflectra® Corporation may make improvements and/or changes in the product(s) and/or program(s) and/or service(s) described in this publication at any time.

The sections in this guide that discuss internet web security are provided as suggestions and guidelines. Internet security is constantly evolving field, and our suggestions are no substitute for an up-to-date understanding of the vulnerabilities inherent in deploying internet or web applications, and Inflectra® cannot be held liable for any losses due to breaches of security, compromise of data or other cyber-attacks that may result from following our recommendations.

The section of the manual that describes modifying the Windows System Registry ("Registry") should only be attempted by experienced Windows administrators who are familiar with its organization and contents. Inflectra® cannot be held liable for any losses due to damage to the system registry made by inexperienced personnel.

SpiraTest®, SpiraPlan®, SpiraTeam® and Inflectra® are registered trademarks of Inflectra Corporation in the United States of America and other countries. Microsoft®, Windows®, Explorer® and Microsoft Project® are registered trademarks of Microsoft Corporation. All other trademarks and product names are property of their respective holders.

Please send comments and questions to:

Technical Publications

Inflectra Corporation

8121 Georgia Ave

Suite 504

Silver Spring, MD 20910

U.S.A.

support@inflectra.com