SSF Tools: Email Approvals User Guide

Document Revision History

Revision Date	Written/Edited By	Comments
September 2016	Clement Liu / Jennifer Mitchell	Initial creation for SSD v2
February 2017	Paul Wheeler	Updated for SSD v3 including details for imap configuration

© Copyright 2017 SailPoint Technologies, Inc., All Rights Reserved.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Restricted Rights Legend. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and reexport of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or reexport outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Entities List; a party prohibited from participation in export or reexport transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Trademark Notices. Copyright © 2017 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo, SailPoint IdentityIQ, and SailPoint Identity Analyzer are trademarks of SailPoint Technologies, Inc. and may not be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

Table of Contents

Introduction

IdentityIQ Access Requests can be approved or rejected through the IdentityIQ UI. Some customers have a requirement to allow approvers to make these decisions using email rather than requiring approvers to access the UI. This tool has been developed to meet this requirement.

When an Access Request is submitted:

1. An email will be sent to the Approver containing two hyperlinks: Approve and Reject. The Hyperlinks have the Work Item ID embedded in them.
2. When the approver clicks either Approve or Reject, a reply email is automatically drafted by the Email client. This email contains the decision and the Work Item ID. The email is sent to a service account mailbox which is read by a custom task in IdentityIQ.
3. The custom task processes the email and verifies that it came from the Work Item owner's email address. It then processes the decision and advances the Access Request workflow forward.

The Email Approvals tool will work with email servers using the IMAP or POP3 protocols.

Limitations

The tool has the following limitations:

- Approvals by email are limited to “approval all” or “reject all”. It is not possible to approve some line items and reject others; in this case the approver would need follow the link to the IdentityIQ UI.

Components

This tool is composed of four XML artifacts and three java classes.

The XML artifacts are found in the /config/SSF_Tools/EmailApprovals/Source folder of the SSF.

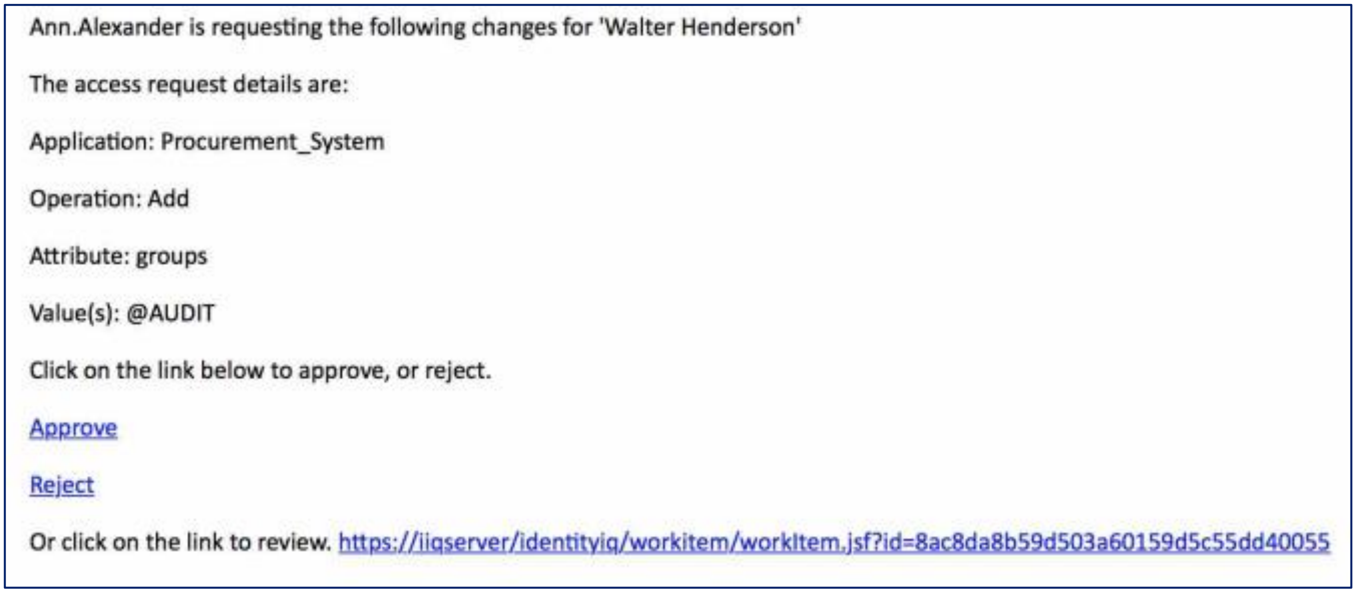
- **Email Approvals -** Custom object that defines the variables needed by the solution; all values are tokenized and will be set to per-installation values automatically by the build process, so this object does not need to be edited per installation; provided in Email_Approvals_Custom.xml
- **Email Approvals** – emailTemplate for the email sent to the approver to list the items requiring their approval; includes the Approve and Reject links that submits the email approval
- **Email Approvals Confirmation** – emailTemplate for email sent back to the approver (if the tool is configured to do so) to notify them whether or not the email approval was processed successfully.
- **Email Approvals Task** - template TaskDefinition for processing the approvals

The Java artifacts are provided in the /src/sailpoint/services/standard/task folder.

- **CustomJavaMailServerTask.java**: the main class that will be invoked when the Email Approvals task is executed. This invokes the CheckEmail.java and ApproveDenyWorkItem.java to do the processing.
- **CheckEmail.java**: checks for any incoming approval emails and parses and sends the information to ApproveDenyWorkItem.java
- **ApproveDenyWorkItem.java**: Processes the approval or rejection of the work item.

How It Works

1. A user completes an Access Request in IdentityIQ.
2. The required approver, according to the provisioning workflow approval scheme, gets an approval workItem and receives an email with links to approve or reject the request. For example, if the approval scheme of your LCM Provisioning workflow is 'manager', the user's manager will receive an email with links to approve or reject.



Ann.Alexander is requesting the following changes for 'Walter Henderson'

The access request details are:

Application: Procurement_System

Operation: Add

Attribute: groups

Value(s): @AUDIT

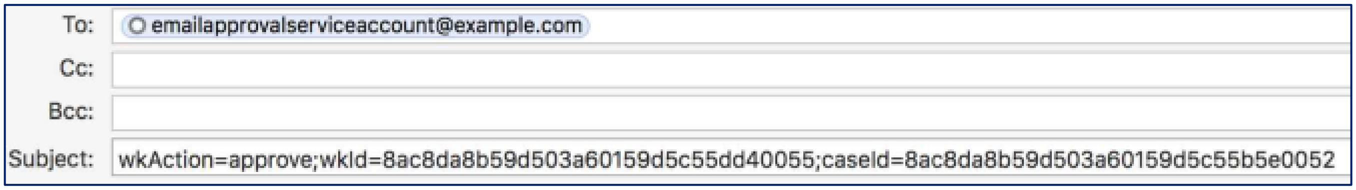
Click on the link below to approve, or reject.

Approve

Reject

Or click on the link to review. https://iiqserver/identityiq/workitem/workItem.jsf?id=8ac8da8b59d503a60159d5c55dd40055

3. The manager clicks one of the links to approve or reject the request. This automatically composes a formatted email to the service email account that is defined in the **Email Approvals** Custom object. The subject line contains the information the tool requires to process the approval or rejection. The manager must send this email to complete the approval or rejection.



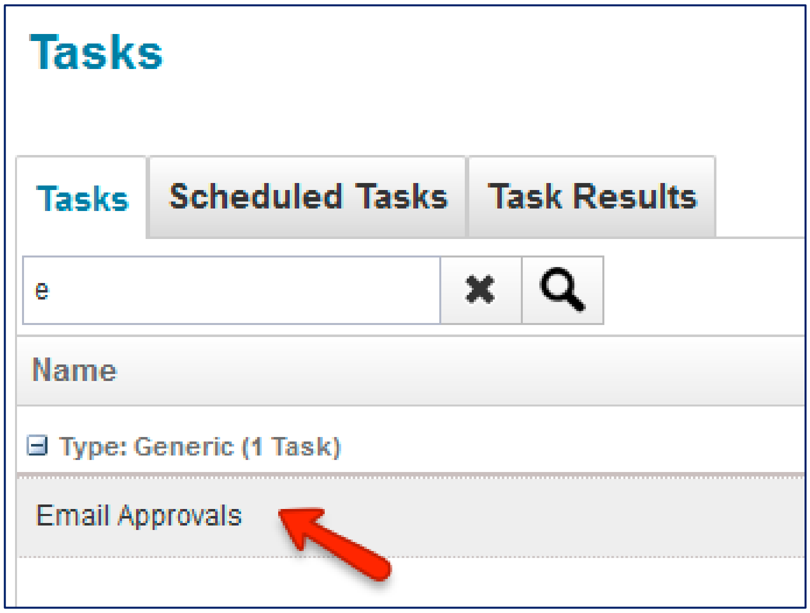
To: emailapprovalserviceaccount@example.com

Cc:

Bcc:

Subject: wkAction=approve;wkId=8ac8da8b59d503a60159d5c55dd40055;caseId=8ac8da8b59d503a60159d5c55b5e0052

4. The **Email Approval** task runs and processes the incoming email. It validates that the sending email address matches the work item owner's email address on record in IdentityIQ, and that the WorkflowCase ID supplied in the email is a valid match to the one referenced by the Work Item in IdentityIQ indicated by the supplied Work Item ID. If there is a match, it approves or rejects the request as specified in the email reply. This task should be scheduled to run regularly in the customer environment to pick up new approvals/rejections submitted by email (e.g. hourly or at the frequency determined by customer requirements).



Tasks

Email Approvals

5. If **notifyApprover** is set to "true" in the **Email Approvals** Custom object, a confirmation email will be sent back to the approver to tell them whether the approval went through in IdentityIQ.
   - In the case of a failure in processing the email approval, if **notifyadmin** is set to "true" in the Email Approvals Custom object, a notification will also be sent to the admin email address specified in **notifyadminemail** in the Email Approvals Custom object.

How to Install

Note that you can choose to use the SSD Deployer tool to set up Email Approvals (refer to the SSD Deployer User Guide). If you do this, steps 1 and 2 below will be done for you.

- To enable the solution, in the build.properties file in the SSD, set the **deployEmailApprovals** property to "true".
- Copy the contents of the file config/SSF_Tools/EmailApprovals/emailapprovals.target.properties to the target.properties file for your environment
- Modify the token values in the target.properties file as appropriate for your environment

Token	**Value Definition**
%%SP_EA_SVC_ACCOUNT%%	The service account that will be monitored for incoming approval or rejection emails.
%%SP_EA_SVC_ACCOUNT_PASSWORD%%	The password for the service account.
%%SP_EA_MAIL_PROTOCOL%%	The protocol used by the mail server. Set to 'imap', 'imaps', 'pop3' or 'pop3s', depending on the protocol supported and enabled on your mail server.
%%SP_EA_HOST%%	The name of the mail host where the service account mailbox is located.
%%SP_EA_PORT%%	The mail server port.
%%SP_EA_NOTIFY_ADMIN%%	Set to true or false to define whether

	notification will be sent to the administrator if errors are encountered. This will only be used if the token %%SP_EA_NOTIFY_STATUS%% is set to true.
%%SP_EA_ADMIN_EMAILADDRESS%%	The administrator email address that will be notified if errors are encountered. This will only be used if the token %%SP_EA_NOTIFY_STATUS%% is set to true.
%%SP_EA_NOTIFY_STATUS%%	Set to true or false to define whether the approver receives a confirmation email after making the approval or rejection decision; also determines whether the admin will be notified of errors
%%SP_EA_IIQ_BASE_URL%%	Base IdentityIQ URL used in the email template to the approver in order to provide a link to the work item.

- To integrate Email Approvals with the out-of-the-box **LCM Provisioning** workflow, direct the workflow to use the **Email Approvals** email template for approval email notifications by setting the “approvalEmailTemplate” process variable to “Email Approvals”, and ensure this variable is being passed through to the approval sub-workflow. If you are using a different provisioning workflow or approval process, ensure that the workItemNotificationTemplate specified on your approval points to the **Email Approvals** emailTemplate.
- Make any desired changes to the email templates.
  - The wording and formatting in either template can be customized as needed.
  - The Email Approvals template includes a link which allows the user to log in to the IdentityIQ installation, if they prefer to forego the email approval option or make line-item approval decisions.
- Follow the SSB process to build and deploy the code.
- In IdentityIQ, create a new task of type **Email Approvals Task** and schedule it to run regularly to process the approval emails as approval decisions are returned to the system.

Troubleshooting

To turn on debug level logging while testing or troubleshooting the solution, add the following entries to your log4j.properties file and reload the logging configuration in the Debug pages.

- log4j.logger.sailpoint.services.standard.task.CheckEmail=debug
- log4j.logger.sailpoint.services.standard.task.ApproveDenyWorkItem=debug
- log4j.logger.sailpoint.services.standard.task.CustomJavaMailServerTask=debug