



SSF Tools: Break Glass Access Request User Guide

Document Revision History

Revision Date	Written/Edited By	Comments
September 2016	Paul Wheeler	Initial release with SSD v2

© 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

Overview.....	4
Deployment	4
Notes	5

Overview

Break Glass Access Request is a simple use case solution intended to provide a way for selected users to bypass the usual approval process for access requests in emergency situations where the need for access cannot wait for the approval process to complete. After following the usual access request procedure, the user is presented with a form in which they must mark a checkbox to acknowledge use of the Break Glass procedure with no approvals; if this is not done, the request will be treated as a normal access request with approvals. The configured Security Officer will receive notification of all Break Glass requests. The ability to use this option is granted by membership of a 'Break Glass Users' workgroup.

Deployment

To deploy the Break Glass Access Request use case, follow the instructions below. If you are using the SSD Deployer tool, steps 1 and 2 will be completed for you if you selected the option to deploy Break Glass Access Request. Refer to the SSD Deployer User Guide for more information.

1. In the SSB build.properties file, set the 'deployBreakGlass' property to 'true'.
2. Copy the tokens from `config/SSF_Tools/BreakGlassAccessRequest/breakglass.target.properties` into the `target.properties` file for your environment.
3. Modify the `target.properties` for your environment:

`%%BREAKGLASS_SECURITY_OFFICER_NAME%%`

Set to the identity name of the Security Officer (or workgroup) who will receive email notification of all Break Glass requests. This must be changed from the default 'spadmin'.

`%%BREAKGLASS_PROVISIONING_WORKFLOW%%`

Defines the name of the workflow that will be called for provisioning. This should normally be the workflow that is currently used for access requests, e.g. 'LCM Provisioning'.

Note that the solution includes a merge file for the Configuration object 'System Configuration'. This will modify the IdentityIQ configuration setting that stores the name of the workflow to be used for access requests ('workflowLCMAccessRequest'). This is a requirement of this solution, but you should first note the current value of this setting in your System Configuration, and use that value for the token `%%BREAKGLASS_PROVISIONING_WORKFLOW%%`.

4. Create and deploy the build.
5. In IdentityIQ, add users to the workgroup 'Break Glass Users' to enable them to use this feature.

Notes

Passing the Request ID back to the Break Glass workflow

When the requester has successfully submitted the request, IdentityIQ normally displays a message containing the Request ID. When you use the Break Glass workflow it treats the LCM Provisioning workflow as a subprocess and does not have access to the Request ID that is generated in the LCM Provisioning workflow unless you pass this value back. You will see this message if you do not do this:

Request submitted successfully. The ID for this request is .

To pass the value of the Request ID back to the Break Glass workflow so that it displays correctly for the requester, in your LCM Provisioning workflow add a step that runs this script immediately after the Initialize step:

```
import sailpoint.workflow.WorkflowContext;

WorkflowContext parent WFC = wfcontext.getParent();
parent WFC.setVariable("identityRequestId", identityRequestId);
```

Email template

The email template provided should be considered a sample. You should modify it to fit your organization's branding or wording requirements.