© 2009-2015 NextLabs, Inc. All rights reserved.
The information in this document is subject to change without notice.

To provide feedback on this document, email NextLabs, Inc. at info@nextlabs.com.

TRADEMARKS

GRC Adapter™, ACPL™ and the GRC Adapter logo are registered trademarks of NextLabs, Inc. All other brands or product names used herein are trademarks or registered trademarks of their respective owners.

LICENSE AGREEMENT

This documentation and the software described in this document are furnished under a license agreement or nondisclosure agreement. The documentation and software may be used or copied only in accordance with the terms of those agreements. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, either electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's use, without the prior written permission of NextLabs, Inc.

The content of this document is provided for informational and instructional use only. It is subject to change without notice, and should not be construed as a commitment by NextLabs, Inc.

NextLabs, Inc. assumes no responsibility or liability for any inaccuracies or technical errors that may appear in the content of this document.
Contents

1 Introducing the NextLabs GRC Adapter ......................................................... 5
   Introducing the GRC Adapter ................................................................. 5
   Key Benefits ................................................................................................ 5
   System Architecture .................................................................................. 6

2 Setting Up the NextLabs GRC Adapter .......................................................... 9
   Software Requirements ............................................................................. 9
   Supported Versions .................................................................................... 9
   Overview of Process .................................................................................. 10
   Install the NextLabs SAP GRC Plug-in ..................................................... 10
   Configure the NextLabs SAP GRC Plug-in .............................................. 11
      Configuring SoD Object and Creator Information .................................. 11
      Defining the Enhancement Implementation ......................................... 12
      Defining the Enhancement Implementation for Vendors and Payments ... 13
      Specifying the Transactions to Intercept .............................................. 14
   Registering the SAP GRC Obligation ....................................................... 15
   Configure the SAP GRC User Attribute Plugin ....................................... 16
   Installing Support Pack SP01 .................................................................... 18
   Enrolling SAP GRC user data into the NextLabs Policy Server ............... 19
      Downloading User Data from GRC ...................................................... 19
      Uploading User Information into the NextLabs Policy Server .............. 21
      Configuring Function Group GRAC_NL .............................................. 22
   Implement the GRC Solex solution ............................................................ 23

3 Designing Policies ......................................................................................... 25
   Example Policy .......................................................................................... 25
Introducing the NextLabs GRC Adapter

This guide provides information on installing and configuring the GRC Adapter, and creating policies that use GRC risk and mitigation information to allow or block user transactions.

Topics include:

- **Introducing the GRC Adapter** describes the benefits of the GRC Adapter, as well as a logical architecture that details how data flows between components and describes which components must be configured.
- **Setting Up the NextLabs GRC Adapter** explains how to install and configure the GRC Adapter.
- **Designing Policies** describes how to write a policy that checks for GRC risk and mitigation information and applies the appropriate enforcement action.

Introducing the GRC Adapter

The GRC Adapter is a NextLabs solution that integrates with SAP GRC, enabling NextLabs policies to access risk and mitigation controls in GRC to determine the action to take when a user performs a transaction that falls under a segregation of duties (SoD) violation. SoD compliance is a control that ensures that no individual has the authority to execute multiple conflicting sensitive transactions that can result in financial fraud, for example, creating a new vendor and posting a payment for that vendor. Depending on the risk and mitigation controls defined, the resulting policy action can be to permit or block the user transaction, or to inform the user of the SoD risk and prompt the user to continue or cancel the transaction. These events are then logged for audit purposes.

Key Benefits

Businesses use SAP GRC to manage risk, enforce compliance with regulations or company policies, and audit the effectiveness of risk and mitigation controls. If
Introducing the NextLabs GRC Adapter

your organization already uses SAP GRC to enforce and monitor SoD compliance, integrating the NextLabs GRC Adapter enables you to:

- Augment SAP GRC’s role-based access control with NextLabs attribute-based access control (ABAC). Providing access based on the evaluation of user attributes, such as citizenship or department, or resource attributes, such as data location or classification, enables you to express access control policies more simply; for example,Allow only US persons in US locations to access data classified as ITAR. In addition, the proper enforcement of ABAC policies is not dependent on roles to be immediately reassigned to users as their responsibilities change.
- Leverage current risk and mitigation controls to enforce policies consistently across SAP systems.
- Prevent SoD violations in real time, and log all policy enforcement events.
- Monitor and audit SoD compliance using NextLabs Reporter, the Control Center web application that provides dashboard views and detailed reports of policy enforcement activities.

System Architecture

The NextLabs and SAP GRC solution consists of the following software components:

- NextLabs Control Center—the enterprise platform that provides centralized management of policies deployed in the system.
- NextLabs Entitlement Manager for SAP and Entitlement Pack for SAP ECC—standard policy enforcement software (PEP) that run on an SAP ECC system.
- NextLabs GRC Plug-in—the add-on software component on SAP ECC that integrates the risk and mitigation controls with the enforcement action.
- NextLabs Policy Controller—the Policy Decision Point (PDP) component that receives policy requests from the Entitlement Manager, evaluates the requests, and returns an enforcement decision.
- NextLabs Attribute Plug-in—the add-on software to the Policy Controller that retrieves risk and mitigation information from SAP GRC to use for policy evaluations.
- NextLabs Policy Studio—the application for creating and deploying policies.
Figure 1-1: System view of the GRC solution
Introducing the NextLabs GRC Adapter
2 Setting Up the NextLabs GRC Adapter

This section describes how to install and configure the NextLabs GRC Adapter.

Topics include:

- Software Requirements 9
- Overview of Process 10
- Install the NextLabs SAP GRC Plug-in 10
- Configure the NextLabs SAP GRC Plug-in 11
- Registering the SAP GRC Obligation 15
- Configure the SAP GRC User Attribute Plugin 16
- Installing Support Pack SP01 18
- Enrolling SAP GRC user data into the NextLabs Policy Server 19

Software Requirements

Before you begin verify that your environment meets the requirements described in this section.

Supported Versions

The GRC Adapter is certified to work with the following software versions:

- SAP GRC, version 10.0 with Support Pack 14, and higher
- NextLabs SAP GRC User Attribute Plugin
- NextLabs Entitlement Manager for SAP, version 7.6 with Support Pack SP01
- NextLabs Entitlement Pack for SAP ECC, version 7.6
- NextLabs Entitlement Pack for DAC, version 7.5
- NextLabs Java Connector 7.6
- NextLabs Control Center, version 7.6
- NextLabs Policy Controller, version 7.6
- NextLabs Policy Studio, version 7.6

This user guide assumes you have already installed and configured all the software listed above. For information on the platform requirements for each component, refer to the relevant user guide.
Setting Up the NextLabs GRC Adapter

Overview of Process

Setting up and configuring the NextLabs GRC Adapter entails procedures that must be performed in both NextLabs and SAP systems. These procedures are typically performed on different hosts in your environment.

To set up the NextLabs GRC Adapter, perform the following procedures:

1. Install the NextLabs SAP GRC Plug-in
2. Configure the NextLabs SAP GRC Plug-in
3. Registering the SAP GRC Obligation
4. Configure the SAP GRC User Attribute Plugin

Install the NextLabs SAP GRC Plug-in

The NextLabs GRC Plug-in is installed on SAP ECC using a standard .car file procedure.

Before you begin

Obtain the necessary installation files and passwords from NextLabs Support.

1. In the SAP interface, log in to client 000.
2. Enter transaction SAINT. The Add-on Installation Tool window displays a list of all preconfigured add-ons and systems. Click Start to begin a new Add-on Installation.
3. Locate an Installation Package from Installation Package > Load Package > From Front End.
4. Navigate to the NXLDAC_750.car file, then click Open.
5. When prompted, click Decompress to extract the installer files. The installation screen appears.
6. Click Start.
7. Select the installation package from the installation queue and click Continue to launch the installation.
8. On the screen that appears, click Continue. You do not need to enter any information.
Setting Up the NextLabs GRC Adapter

9 When prompted to add Modification Adjustment Transports to the queue, click **No**.

10 When prompted, enter the appropriate password for the OCS package, then click **OK**. The installation begins.

   *Note:* Contact NextLabs Support to obtain the necessary installation passwords.

11 When the installation is complete, do either of the following:

   - Click **Logs** to view the installation logs and confirm the installation was successful.
   - Click **Finish** to exit the installer. When you click **Finish**, the final screen displays informing you that the installation was successfully completed.

   *Note:* You can verify in the Status/Remarks that the installation was successful. You can also scroll through the components to locate the newly installed NextLabs Add-on.

12 Log off client 000 and log in to client 100.

**Next steps**

Configure the NextLabs SAP GRC Plug-in.

---

**Configure the NextLabs SAP GRC Plug-in**

The NextLabs GRC Plug-in supports the interception of transactions as specified in the segregation of duties (SoD) policies. Configuration of this component consists of the following procedures:

- Configuring SoD Object and Creator Information
- Defining the Enhancement Implementation
- Defining the Enhancement Implementation for Vendors and Payments
- Specifying the Transactions to Intercept

**Configuring SoD Object and Creator Information**

In this procedure, you configure a table, `/NXLDAC/REF_CONF`, to maintain source information about objects and their creators in transactions governed by SoD compliance.

**Procedure**

1. In the SAP interface, enter transaction **SM30**. The **Table Maintenance View** appears.

2. In **Table/View**, enter `/NXLDAC/REF_CONF`. Select **Maintain**.
3 Click New Entries to create an entry for each object to track for an SoD transaction.

- In Object Type, enter the type of object.
- In Table Name, enter the table in which the object’s data is stored.
- In Field Name, enter the field that stores the Created by information.

Figure 2-1 shows an example of entries created in the table.

![Figure 2-1: Configuring object and creator information](image)

4 Click Save.

**Defining the Enhancement Implementation**

In this procedure, you define the enhancement implementation to intercept and process transactions with SoD impact. The enhancement point that you select for your implementation depends on your SoD compliance requirements. Use the function module /NXLDAC/GRC_SOD_PROCESS in your implementation. Figure 2-2 and Table 2-1 show the import parameters of the function module.
Defining the Enhancement Implementation for Vendors and Payments

This release of the NextLabs GRC Adapter provides access control over vendor payments. You can define an enhancement implementation that checks if there is an SoD risk when a user posts a payment using transaction FBZ2 or F-53. Checks are triggered when users enter vendor names in the payments screen. Using this implementation in conjunction with a policy (described in Chapter 3, "Designing Policies"), you can prevent a single user from both creating a vendor and posting a payment for that vendor.

Procedure

1. In the SAP interface, enter transaction SE18.

Table 2-1: Import parameters of function module /NXLDAC/GRC_SOD_PROCESS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_SECIDTCMK</td>
<td>NextLabs multiple classification evaluation that passes the identifier</td>
</tr>
<tr>
<td>S_GENERIC_ATTR</td>
<td>Generic attributes for transaction interception</td>
</tr>
<tr>
<td>S_TCODE</td>
<td>Transaction code to pass</td>
</tr>
<tr>
<td>OBJECT_TYPE</td>
<td>Key type maintained in the /NXLDAC/REF_CONF table</td>
</tr>
<tr>
<td>OBJECT_KEY_VALUE</td>
<td>Generic import data for the key master/reference data.</td>
</tr>
</tbody>
</table>
2 Create a BADI implementation for FAGL_SEGMENT_BS_ACC.

3 Insert the following code in the GET_SUBST method:

   Include /NXLDAC/NRC_PRSRV_FI_VEND_CHK

4 Save and activate the method and the BADI implementation.

Specifying the Transactions to Intercept

You must specify the transactions to intercept for SoD policy checks. For example, to check for SoD risks when users post payments using transaction FBZ2 or F-53, you must configure transactions FBZ2 and F-53 in the /NEXTLABS/TXFLTR table.

Procedure

1 In the SAP interface, enter transaction /NEXTLABS/TXFLTR. The Maintain Executable Objects for Common Interception screen appears, as shown in Figure 2-3.

2 Do any of the following:

   • To specify new transactions to intercept, click Create.
   • To view or modify transactions that are already in the table, click Modify/Display.
   • To specify criteria for filtering the list of transactions, click Existing Objects Selection.

3 If you are adding transactions, do the following for each transaction:

   a Click Insert Row.

   b In Executable Object, enter a transaction code.
c In Active, enter X to enable interception of the transaction. Use the Active setting to disable or enable interception for each transaction as your authorization requirements change.

Figure 2-4 shows an example of one transaction, FBZ2, and its status set to Active.

As an alternative to entering each transaction code here, you can type the values in an Excel file, then click Import as shown in Figure 2-4 to import the values from the file.

![Figure 2-4: Adding a transaction to the /NEXTLABS/TXFLTR table](image)

### Registering the SAP GRC Obligation

Obligations are events that occur when policies are enforced. For example, the GRC Mitigation PopUp (GRCPOP) obligation displays messages informing users of SoD risks that are identified during policy enforcement. Before they can be used in policies, however, obligations must be added to the configuration.xml file used by the NextLabs Control Center. This is referred to as registering obligations.

**Before you begin**

Obtain the obligation file, product.xml, from NextLabs Support.

**Procedure**

1. If it is running, stop the Control Center Policy Server using the Windows Services utility:
Setting Up the NextLabs GRC Adapter

In Windows 7, select Start > Control Panel > System and Security > Administrative Tools > Services.

Select Control Center Policy Server, then select Stop.

Place the GRCPOP obligation file, `product.xml`, on the host where the NextLabs Control Center Policy Server is installed, and open the file with a text editor.

In a separate text editor window, open `configuration.xml`, the main configuration file for the NextLabs Control Center. The file is located in the following directory on the NextLabs Control Center Policy Server host: `<ControlCenterInstallDirectory>\server\configuration`.

Copy and paste the GRCPOP obligation from `product.xml` into `configuration.xml`. The obligation must be placed inside the `<Obligations>` section, as follows:

```xml
<Obligation>
  <DisplayName>GRC Mitigation PopUp</DisplayName>
  <RunAt>PEP</RunAt>
  <Name>GRCPOP</Name>
  <Arguments>
    <Argument usereditable="false" hidden="false">
      <Name>logid</Name>
      <Value default="true">$CELogUid</Value>
    </Argument>
    <Argument>
      <Name>requestid</Name>
      <Value>$environment.request_id</Value>
    </Argument>
  </Arguments>
</Obligation>
```

Save the `configuration.xml` file and restart the NextLabs Control Center Policy Server:

In Windows 7, select Start > Control Panel > System and Security > Administrative Tools > Services.

Right-click Control Center Policy Server, then select Start.

Test the configuration by opening NextLabs Policy Studio and creating a new policy. The GRC Mitigation PopUp appears in the drop-down list of custom obligations.

Configure the SAP GRC User Attribute Plugin

The configuration procedure in this section assumes you have already installed and configured the NextLabs Java Connector, which is the communication inter-
face between the Policy Controller and the SAP Agent. The steps here are additional configuration steps that are specific to the NextLabs GRC Adapter.

Before you begin

- Obtain the GRC Plug-in zip file from NextLabs Technical Support.
- Know the administrative password required to stop the Policy Controller. This password is associated with the profile used on the host where the Policy Controller is running.

Procedure

1. If it is running, stop the Policy Controller:
   a. In Windows 7, select Start > Stop Policy Controller.
   b. When prompted, enter the Policy Controller password.

2. Extract the GRC Plug-in zip file obtained from NextLabs Support.

3. From the extracted zip file, copy the following JAR file:
   SAPGRCUserAttributePlugin.jar

4. Paste the JAR file into the following folder:
   <Policy Controller install dir>/Policy Controller/jservice/jar/sap

5. From the extracted zip file, copy the following properties file:
   SAPGRCUserAttributePlugin.properties

6. Paste the properties file into the following folder:
   <Policy Controller install dir>/Policy Controller/jservice/config

7. Edit the SDK Service properties file:
   a. Using a text editor, open the following file:
      SAPJavaSDKService.properties
   b. Locate the following line: server_prefix=SERV1_; and add SERVGRC_; at the end of the line as follows:
      server_prefix=SERV1_;SERVGRC_;  
   c. Add the following code below that line:
      # START of SERVGRC Settings
      #destination data provider Connection details
      SERVGRC_jco.client.ashost=[!CLIENT_HOST!]
      SERVGRC_jco.client.sysnr=[!CLIENT_SYSNR!]
      SERVGRC_jco.client.client=[!CLIENT_ID!]
Setting Up the NextLabs GRC Adapter

SERVGRC_jco.client.user=[!CLIENT_USER!]
SERVGRC_jco.client.passwd=[!CLIENT_PASSWD!]
SERVGRC_jco.client.lang=en
#please note jco.destination.pool_capacity <=jco.destination.peak_limit
#comment below two lines if connection pool is not required
SERVGRC_jco.destination.peak_limit=3
SERVGRC_jco.destination.pool_capacity=1
#server data provider Connection details
SERVGRC_jco.server.gwhost=[!GATEWAY_HOST!]
SERVGRC_jco.server.gwserv=[!GATEWAY_SERV!]
SERVGRC_jco.server.progid=[!GATEWAY_PRGID!]
SERVGRC_jco.server.connection_count=02

# END of SERVGRC Settings
d Replace the following variables, including the brackets and exclamation points, with the appropriate values for your system:

- [!CLIENT_HOST!]: The hostname of your server. For example: lab.nextlabs.com
- [!CLIENT_SYSNR!]: The system to use. For example: 00
- [!CLIENT_ID!]: The client ID to use. For example: 100
- [!CLIENT_USER!]: The user name of the account. For example: developer
- [!CLIENT_PASSWD!]: The password of the account. For example: password
- [!GATEWAY_HOST!]: The hostname of the gateway server. For example: qalab01.nextlabs.com
- [!GATEWAY_SERV!]: The gateway server name. For example: sapgw00
- [!GATEWAY_PRGID!]: The ID of the gateway. For example: NXL_CONNECT_TO_PC

5 Save the file and restart the Control Center Policy Server:

- In Windows 7, select Start > Control Panel > System and Security > Administrative Tools > Services.
- Right-click Control Center Policy Server, then select Start.

Installing Support Pack SP01

You must install Support Pack SP01 for NextLabs Entitlement Manager for SAP version 7.6. To install Support Pack SP01, follow the standard Support Pack
Enrolling SAP GRC user data into the NextLabs Policy Server

You can enroll user data from the SAP GRC system into NextLabs Control Center Policy Server. This enables you to use that data when creating enforcement policies in Policy Studio. Enrolling user data is a two-stage process. First, you need to download user data from GRC. You then upload user data into NextLabs Control Center Policy Server.

Downloading User Data from GRC

The first step in enrolling user data from GRC into NextLabs Control Center Policy Server is downloading the user data from GRC.

Procedure

1 Configure the file path in the GRC Settings:
   a In the SAP GRC interface, enter transaction SPRO.
   b Navigate to the node, Maintain Configuration Settings, as shown in Figure 2-5.
c. Click the **Execute** button next to **Maintain Configuration Settings**.

d. In the **Maintenance Table**, enter the appropriate file path in the **Parameter Value** column as shown in **Figure 2-6**.
e Click Save.

2 In the SAP GRC interface, enter transaction SE38.

3 Run the program GRAC_NL_USER_ATTRIBUTES. GRC user data are downloaded into the file sap_nextlabs_com.ldif.

Next steps
The next step is to enroll the downloaded GRC user data into the NextLabs Control Center Policy Server.

Uploading User Information into the NextLabs Policy Server
After you have downloaded user data from GRC, you need to upload it to the NextLabs Control Center Policy Server. This enables you to add the data to User components in Policy Studio.

Before you begin
• Download user data as described in Downloading User Data from GRC.
• Obtain the Enrollment Adapter zip file from NextLabs Technical Support.

Procedure
1 Copy the GRC user data file, sap_nextlabs_com.ldif, which was downloaded in step 3 of Downloading User Data from GRC, and paste it into the following folder on the Control Center Policy Server:

    C:\Program Files\Next-Labs\Policy Server\tools\enrollment

2 Locate and extract the Enrollment Adapter zip file.

3 In the extracted Enrollment Adapter file, copy the file sap_nextlabs_com.def and paste it into the following folder on the Control Center Policy Server:

    C:\Program Files\Next-Labs\Policy Server\tools\enrollment

    Note: The .def file maps the .ldif file to the dictionary.

4 Open sap_nextlabs_com.def in a text editor and verify the location of ldif.filename:

    ldif.filename c:/program files/nextlabs/policy server/tools/enrollment/sap/sap_nextlabs_com.ldif

5 Open a command prompt and set up enrollment for the .ldif file using the enroll and sync commands in enrollmgr:
enrollmgr -u Administrator -enroll -t LDIF -n sap.domain_name.com
-d "C:\Program Files\NextLabs\Policy Server\tools\enrollment\sap_nextlabs_com.def"

enrollmgr -u Administrator -sync -t LDIF -n sap.domain_name.com
-d "C:\Program Files\NextLabs\Policy Server\tools\enrollment\sap_nextlabs_com.def"

Configuring Function Group GRAC_NL

Create a Function Group named GRAC_NL in function module GRAC_NL_AD.

Procedure

1. In the SAP GRC interface, enter transaction SE80.
2. Choose Function Group from the drop-down list as shown in Figure 2-7.
3. In the group name field, enter GRAC_NL, then click Enter as shown in Figure 2-7.

Figure 2-7: Creating the Function Group GRAC_NL
4 In the Create Function Group confirmation popup, click Yes to create the Function Group as shown in Figure 2-8.

![Create Function Group Confirmation popup](image)

*Figure 2-8: Create Function Group Confirmation popup*

5 When prompted, enter the Access Key provided by the SAP Basis Administrator.

6 Click Activate.

**Implement the GRC Solex solution**

Implement the GRC Solex solution provided by SAP.

**Procedure**

1 Find note number 0002243718 in the SAP Service Marketplace.

2 In the SAP GRC interface, enter transaction SNOTE.

3 Click the Execute button shown in Figure 2-9.
Figure 2-9: SAP Note Assistant
3 Designing Policies

This section describes policies you create in NextLabs Policy Studio for the GRC Adapter. The procedure to create these policies is no different than for other NextLabs policies.

Example Policy

This policy applies to transactions FBZ2 and F-53 executed on the NQ7 server and the NQ7 system. These transactions are used to post a payment to a specified vendor. The definition of the policy, shown in Figure 3-1, specifies the following:

- The enforcement type is set to Allow.
- The Run action component is specified.
- Two resource components are specified, designating the resources to which to target access control.
  - The first resource component, SAP - NQ7, specifies that access control applies to all clients, applications, functions and business objects in the NQ7 server and NQ7 system:
    ```
sap://NQ7/NQ7/*//*//*
    ```
  - The second resource, Vendor Payment Tx, specifies that access control applies to transactions FBZ2 and F-53:
    ```
sap://*/*/*/FBZ2/*
sap://*/*/*/F-53/*
    ```
- In Condition Expression, the user.riskflag = "X" condition verifies that SAP GRC has returned a risk event.
- In Obligations, the GRC Mitigation Popup is selected. This obligation runs when a risk event is identified.
Figure 3-1: Policy to block transactions used to post payments

At run time, this policy is triggered when a user runs either of these transactions. The Entitlement Manager checks if the same user created the vendor whose payment is being posted to, and based on the risk and mitigation infor-
mation retrieved from SAP GRC, allows or blocks the action, or prompts the user to continue or cancel the transaction. **Table 3-1** summarizes the resulting actions:

**Table 3-1: Resulting action based on the risk and mitigation information**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigation</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>User is denied. A message is displayed and the event is logged.</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>A popup message prompts the user to continue or cancel the action. The event is logged.</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No action is triggered.</td>
</tr>
</tbody>
</table>

**Figure 3-2** shows the Post Outgoing Payments screen, which appears when a user enters transaction FBZ2 or F-53. The Entitlement Manager checks the vendor name entered in the Account field.

**Post Outgoing Payments: Header Data**

<table>
<thead>
<tr>
<th>Process open items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Date</td>
</tr>
<tr>
<td>Posting Date</td>
</tr>
<tr>
<td>Document Number</td>
</tr>
<tr>
<td>Reference</td>
</tr>
<tr>
<td>Doc/Header Text</td>
</tr>
<tr>
<td>Clearing text</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bank data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
</tr>
<tr>
<td>Amount</td>
</tr>
<tr>
<td>Bank charges</td>
</tr>
<tr>
<td>Value Date</td>
</tr>
<tr>
<td>Text</td>
</tr>
</tbody>
</table>

**Open item selection**

| Account | NEXTLABS | |

**Additional selections**

- None
- Amount
- Document Number
- Posting Date
- Running Area
- Others

**Figure 3-2: Post Outgoing Payment screen**
If the user posting the payment is the same user who created the vendor, NEXTLABS, and there is risk and mitigation defined for that scenario, the user is prompted to cancel or continue the action, as shown in Figure 3-3. This policy enforcement event is then logged in the Activity Journal. You can run and view a report of these enforcement events using NextLabs Reporter, the Control Center web application.

![Figure 3-3: SoD risk identified](image-url)