

Multiple Approvers with Implementation – Customization Guide

The purpose of this guide is to inform the reader how to create a customized workflow within CA Identity Manager for use within the CA Identity Portal access request system.

The use case is requesting access to an application that is considered very sensitive and requires three approvals. Following the three approvals, the request is sent to a group of administrators to perform the manual provisioning.

For this scenario, we have three approvers:

- Manager: dynamically resolved based on the Manager ID of the requestor
- Risk Manager: hard coded to a user
- Human Resources: hard coded to a user

After approval, members of a CA Identity Manager group can implement.

The application will be called “Really Sensitive Application”.

Configure Workpoint Designer

This section assumes that Workpoint has been installed as part of the CA Identity Manager deployment, but was never configured to run (as is the case in the current Solution Pro demo image). This also assumes Workpoint is installed locally on the CA Identity Manager server. The instructions are documented on CA Support here: <http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec1917453.aspx>

Copy Workpoint JARs

1. Copy the following files into the Workpoint lib folder (e.g. CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\lib):
 - a. %JBOSS_HOME%\bin\client\jboss-client.jar
 - b. %JBOSS_HOME%\modules\system\layers\base\org\jboss\as\naming\main\jboss-as-naming-7.2.0.Final-redhat-8.jar
 - c. %JBOSS_HOME%\modules\system\layers\base\org\jboss\msc\main\jboss-msc-1.0.4.GA-redhat-1.jar
 - d. %JBOSS_HOME%\jboss-modules.jar

NOTE: version numbers may differ from the ones listed. If so, copy the file and take note of the file names (you’ll need these for the next step)

Modify init.bat file

1. Navigate to the Workpoint bin folder.
For example: CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\bin\
2. Edit the init.bat file
3. Go to the "USE WITH JBOSS EAP 6.1" section.
4. Ensure the bottom two lines are not commented out.

```
SET EJB_CLASSPATH=..\lib\jboss-client.jar;..\lib\jboss-as-naming-7.4.0.Final-redhat-19.jar;..\lib\jboss-msc-1.1.5.Final-redhat-1.jar;..\lib\jboss-modules.jar
```

```
SET JAVADPARMS=%JAVADPARMS% -  
Djboss.ejb.client.properties.file.path=../conf/workpoint-client.properties
```

5. For the first line, change the file names to the ones copied over. In some cases, the versions within the name will be different.
6. Save the file can close.

Modfiy workpoint-client.properties file

1. Navigate to the Workpoint conf folder.
For example: CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\conf
2. Edit the workpoint-client.properties file
3. Comment out the settings under: ***** PRIOR TO VERSION AS 7 *****
4. Uncomment the settings under: ***** JBOSS AS 7 SETTINGS *****
5. Verify the parameters:
 - a. java.naming.provider.url=localhost
 - b. java.naming.factory.initial=org.jboss.as.naming.InitialContextFactory
 - c. java.naming.factory.url.pkgs=org.jboss.ejb.client.naming
 - d. remote.connectionprovider.create.options.org.xnio.Options.SSL_ENABLED=false
 - e. remote.connections=default
 - f. remote.connection.default.host=localhost
 - g. remote.connection.default.port=4447
 - h. remote.connection.default.connect.options.org.xnio.Options.SASL_POLICY_NOANONYMOUS=false
 - i. client.ejbLookupPrefix=ejb:iam_im/iam_im_wpServer/
 - j. client.ejbLookupSuffix=!<CLASSNAME>

```

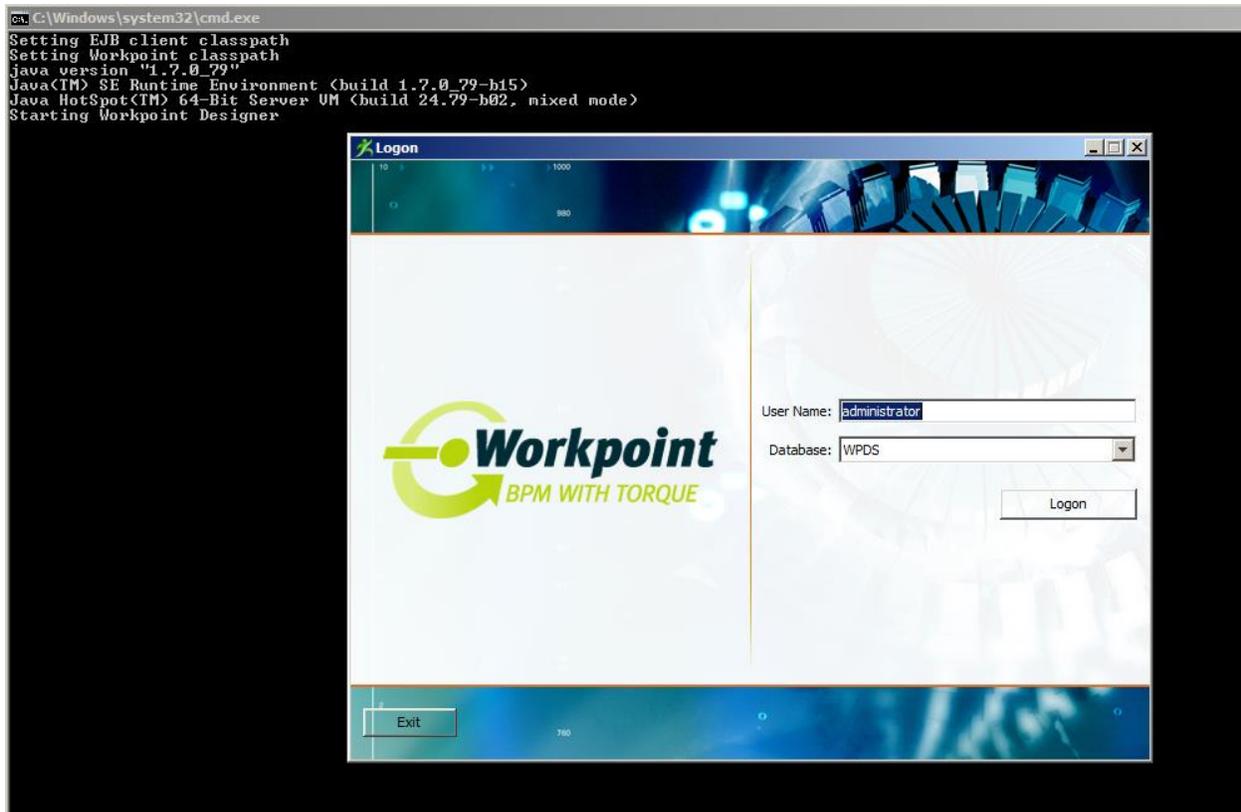
189 # *****
190 # ***** JBOSS AS 7 SETTINGS *****
191 # *****
192 # These properties should be uncommented when using JBoss AS 7
193 #
194 # *** NOTE For EXTERNAL STANDALONE CLIENTS only (does not apply to clients running in a servlet within the same app server) ***
195 # JBoss AS 7 requires a remote client to place additional properties
196 # in a separate file named jboss-ejb-client.properties. Workpoint ships
197 # with a copy of this file in the [WORKPOINT_HOME]/conf directory.
198 # That file is mandated by the JBoss remoting classes so make sure that
199 # it is included in your classpath in addition to this file.
200 #
201 java.naming.provider.url=localhost
202 java.naming.factory.initial=org.jboss.as.naming.InitialContextFactory
203 java.naming.factory.url.pkgs=org.jboss.ejb.client.naming
204 remote.connectionprovider.create.options.org.xnio.Options.SSL_ENABLED=false
205 remote.connections=default
206 remote.connection.default.host=localhost
207 remote.connection.default.port=4447
208 remote.connection.default.connect.options.org.xnio.Options.SASL_POLICY_NOANONYMOUS=false
209 client.ejbLookupPrefix=ejb:iam_im/iam_im_wpServer/
210 client.ejbLookupSuffix=!<CLASSNAME>

```

6. Save the file and close

Start Workpoint Designer

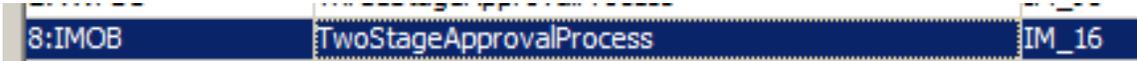
1. Navigate to the Workpoint bin folder.
For example: CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\bin
2. Run designer.bat
3. A terminal will open followed by the Workpoint login screen (note: do not close the terminal screen)
4. Click Logon



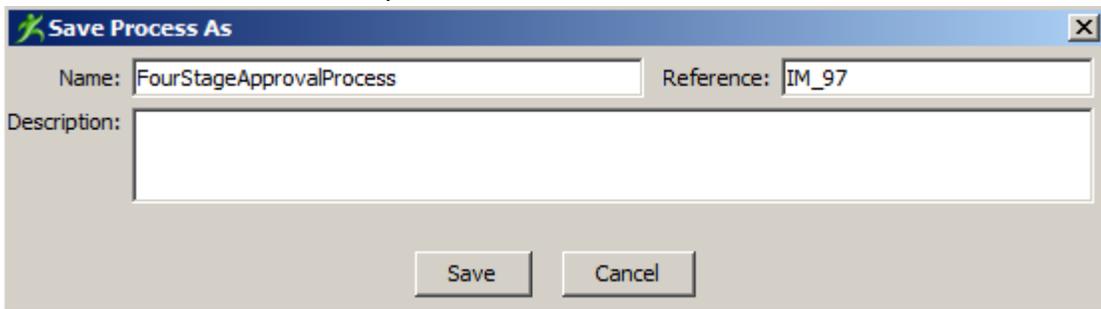
Create Custom Workflow

In this section, we'll create a new custom workflow. In this case, we'll create a copy of

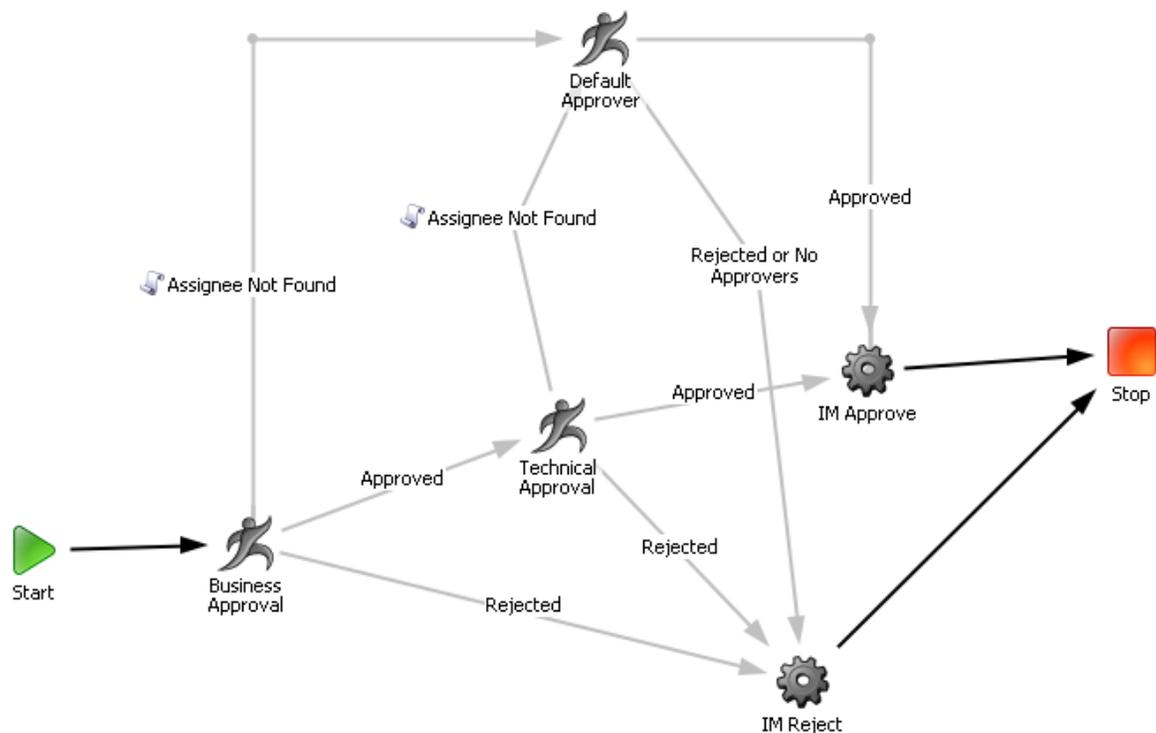
1. After logging on to Workpoint Designer, click Open Process
2. Sort the workflows by Reference
3. Note the highest reference ID. You'll need this when saving your process.
4. Double click on TwoStageApprovalProcess – 8:IMOB



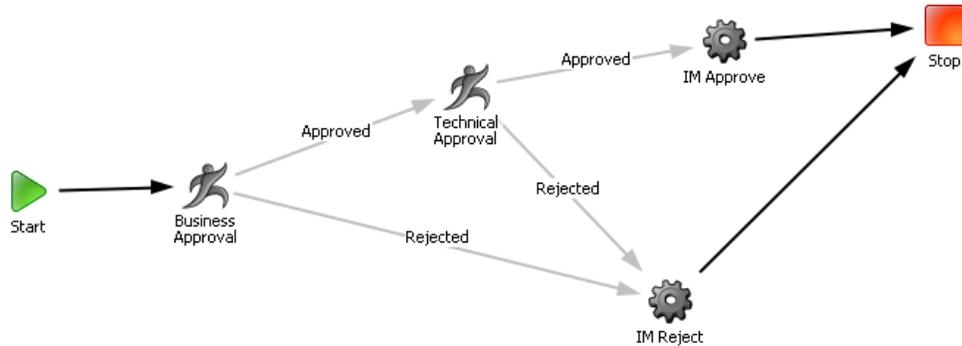
5. The process opens. Click File > Save As. Create a new name and change the Reference to IM_xx (where xx is one more than your highest workflow). Alternatively, pick a big number; this needs to be unique to the other workflows defined. Click Save.



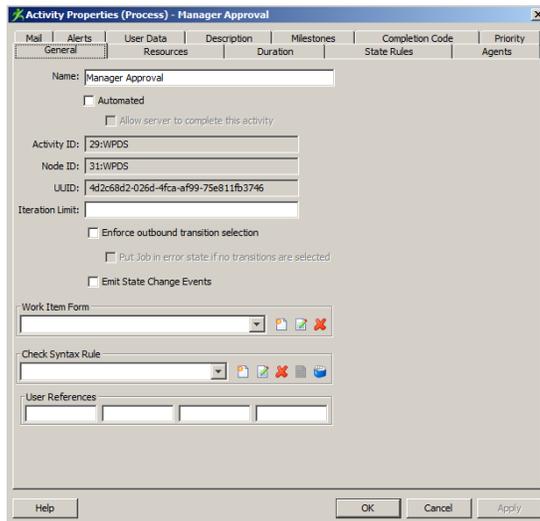
6. Now you have your very own workflow to modify.



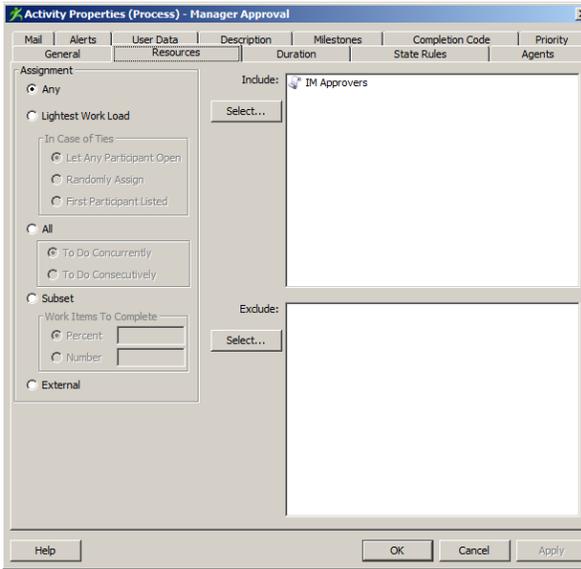
7. In this example, we're going to simplify the workflow by removing the "Assignee Not Found" flows. The easiest way to do this is to delete the Default Approver node. Alternatively, you can keep this check by adding the nodes in the following steps.



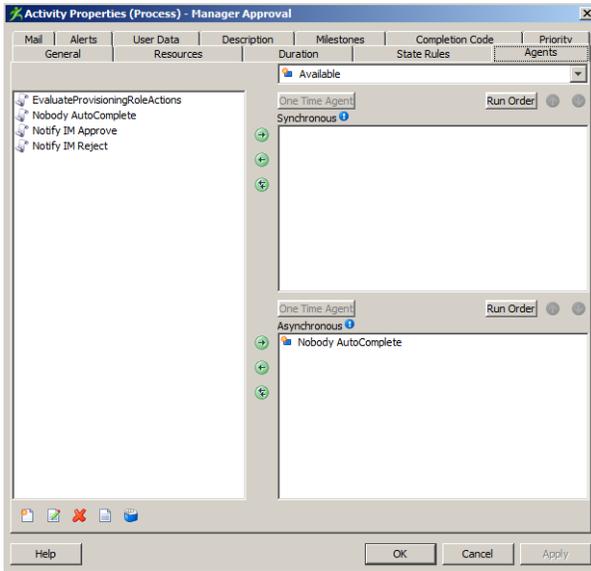
8. Double click the Business Approval node. In the General tab, rename it to "Manager Approval"



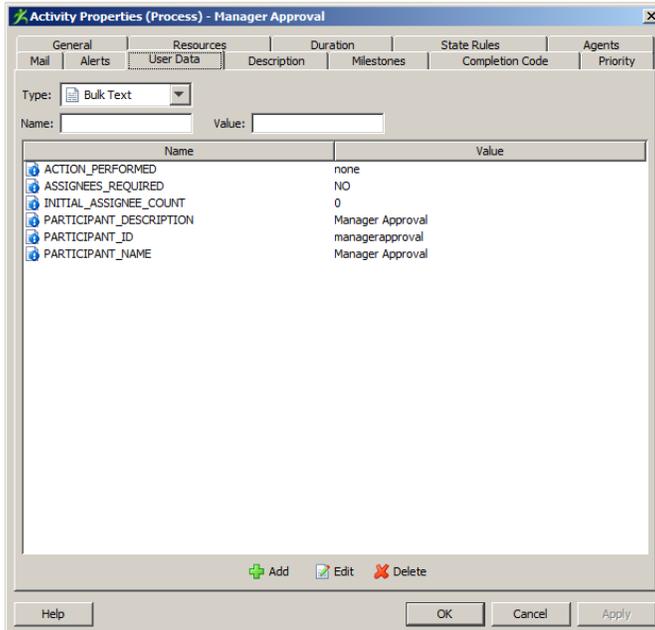
9. The Resources tab should have IM Approvers in the Include box.



10. The Agents tab should have Nobody AutoComplete in the Asynchronous Box.

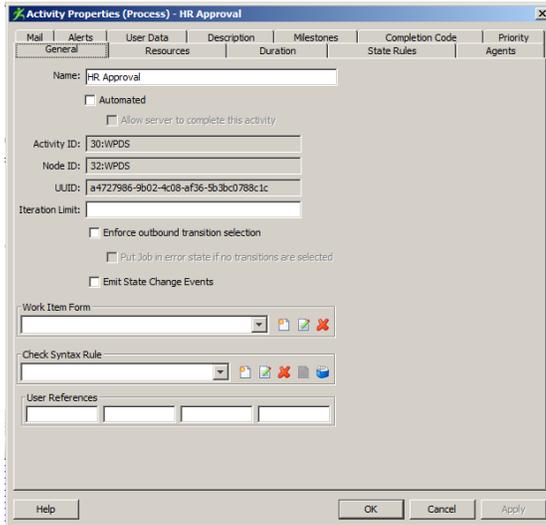


11. Under the User Data tab, change the following (note: the name is the one displayed in the Request status box. Change to meet your needs):
 - a. PARTICIPANT_DESCRIPTION = Manager Approval
 - b. PARTICIPANT_ID = managerapproval
 - c. PARTICIPANT_NAME = Manager Approval

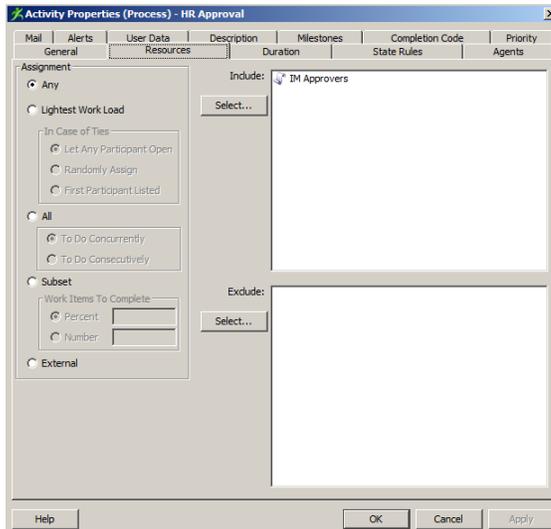


12. All other tabs should be blank. Click Apply and OK.
13. Next double click the Technical Approval node.
14. Rename the node in the General tab to: Risk Manager Approval.
15. Validate the Resources and Agents tabs are configured as above.

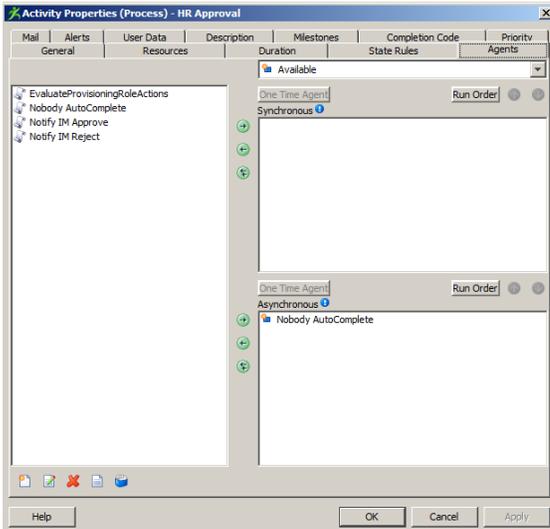
21. In the General tab, name it HR Approval.



22. In the Resources tab, add IM Approvers to the Include box.

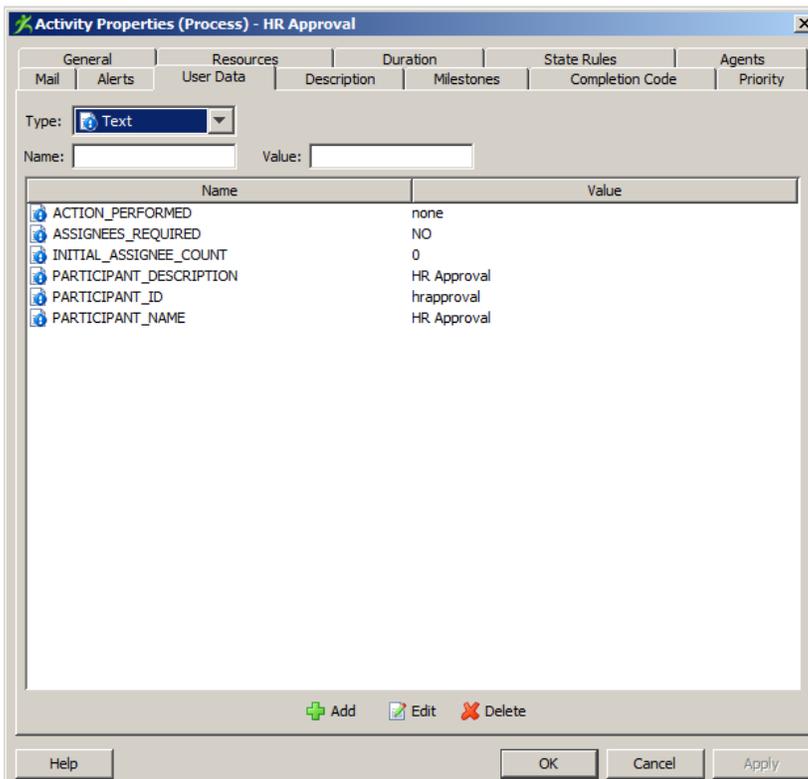


23. In the Agents tab, add Nobody AutoComplete in the Asynchronous Box

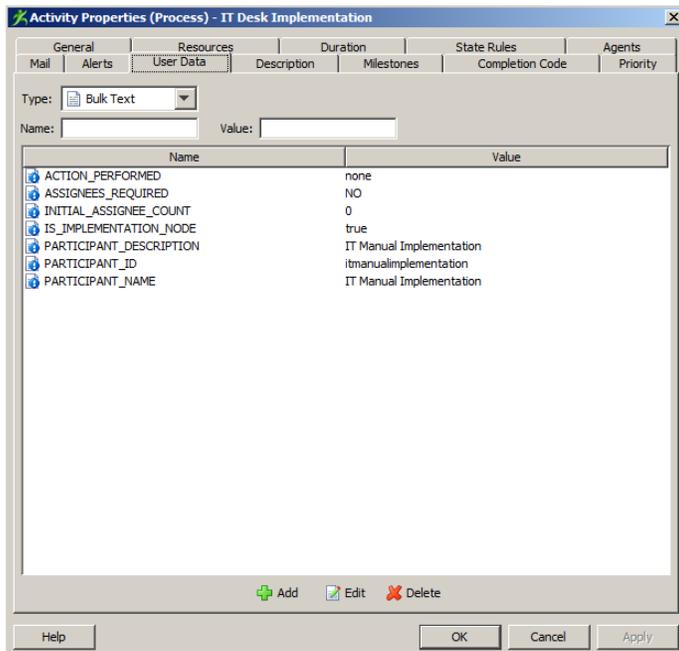


24. In the User Data tab, add the following attributes by changing Type to "Text", typing in the name and value, then click Add.

- a. ACTION_PERFORMED = none
- b. ASSIGNEES_REQUIRED = NO
- c. INITIAL_ASSIGNEE_COUNT = 0
- d. PARTICIPANT_DESCRIPTION = HR Approval
- e. PARTICIPANT_ID = hrapproval
- f. PARTICIPANT_NAME = HR Approval



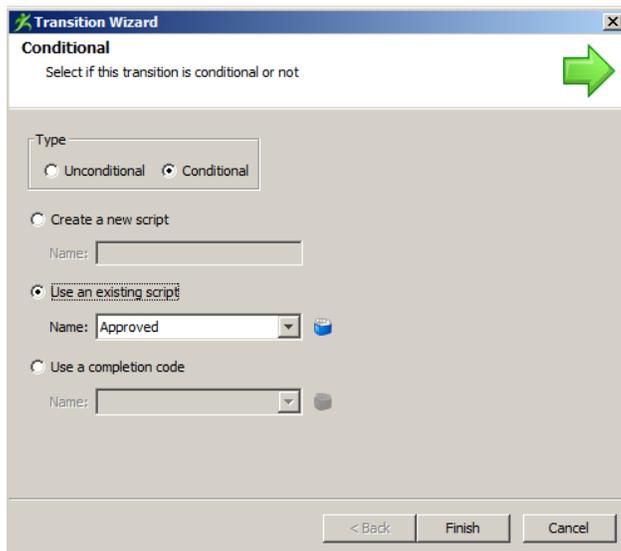
25. Leave the other tabs as is and click Apply and OK.
26. Move the existing transition between the Risk Manager Approval node and IM Approve by clicking and dragging the arrow. The flow should go from Risk Manager Approval node to the HR Approval node.
27. Repeat the same process for creating the IT Desk Implementation node (steps 18 through 25) with one added step:
 - a. In the User Data tab, add the following property of Type Text:
 - IS_IMPLEMENTATION_NODE = true
 - i. This will tell the Identity Portal to put this step under the Implementation tab versus the Approval tab in My Tasks.



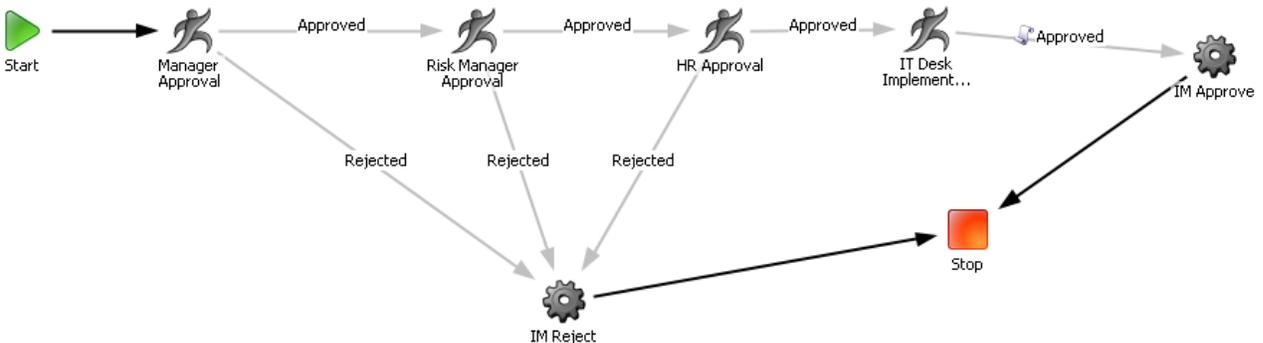
28. Go to the menu bar and click the transition button:



29. Click on the HR Approval node and drag to the IT Desk Implementation node. The transition wizard window will open. Make the following configurations:
 - a. Type = Conditional
 - b. Use an existing script = Approved
 - c. Click Finish



30. Repeat step 29 to create the exact same transition from the IT Desk Implementation node to the IM Approve node. Your workflow should look like this (without the default approver flows):



31. Click File > Save.
32. Close Workpoint Designer

CA Identity Manager Configuration

There are multiple items to configure within CA Identity Manager. In this example, we'll leverage an empty Provisioning Role that we'll be requesting. Since this is a manual implementation, no account template or automated provisioning will take place.

Create Provisioning Role

1. Navigate to: Roles and Tasks > Provisioning Roles > Create Provisioning Role > Create a new provisioning role
2. Under the Profile Tab, write in the Name: [SIGMA] Really Sensitive Application
3. Under the Owner Tab, define an owner
e.g. who are members of (admin role "System Manager")
4. Under the Administrators Tab, define an Admin Policy for all
5. Click Submit

Create Help Desk Group

1. Groups > Create Group > Create a new group
2. In the Profile Tab:
 - a. Org Name: click Browse and select northamerica
 - b. Group Name: Help Desk
3. In the Membership Tab:
 - a. Click Add a user
 - b. Select the following users: hiran01, ortra01, turta01
4. Under the Administrators Tab:
 - a. Add a user and select superuser

Create Implement "Approval" Admin Task

1. Navigate to: Roles and Tasks > Admin Tasks > Create Admin Task > Create a copy ...
2. Create Copy of Approve Request Access
3. Under the Profile Tab:
 - a. Rename the task to: Implement Request Access.
 - b. Rename the tag to: ImplementRequestAccess
4. Under the Tabs Tab:
 - a. Add a new Tab of type Profile (UserProfile)

Modify Admin Task: Implement Request Access

Profile Search **Tabs** Fields Events Role Use

Which tab controller should be used for this task?
Standard Tab Controller

Which tabs should appear in this task?

Tab	Tag	Type	
ImplementProfile	ImplementProfile	Profile	⊖ ⊕ ↕
Profile	Approve	Profile	⊖ ⊕ ↕
Approvers	Assignees	Assignees	⊖ ⊕ ↕
View Job	JobView	View Job	⊖ ⊕ ↕

Administrators (GenericAdmins)
Assignees (WorkItemAssignees)
External Tab (ExternalTab)
History Profile (HistoryProfile)
JSP (JSP)
Owners (GenericOwners)
Profile (AccountProfile)
Profile (AccountTemplateProfile)
Profile (EndpointProfile)
Profile (Generic) (ObjectProfile)
Profile (UserProfile)
Profile (UserServiceObject)
Provisioning Roles (ProvisioningRoles)
Related Object Profile (RelatedObjectProfile)
Report (ReportingTab)
Reporting Snapshots (ReportingSnapshotsTab)
Reverse Approval (ApproveReverseSyncNewAccount)
View Job (JobView)

- b. Edit the new tab by clicking the pencil next to the name
- c. Rename the Name to:
- d. Rename the Tag to:
- e. Next to Screen, click Browse
- f. At the bottom of the screen, click New
- g. Next to Create a Copy of, click Search. (you can also just create a new standard screen)
- h. Select Default User Profile
- i. Rename the Name to: Implement Profile
- j. Rename the Tag to: ImplementProfile
- k. Remove all the fields you do not want to display on the Additional Information screen within the CA Identity Portal approval screen. For this example, remove all the fields except for Full Name, User ID, and Email.
- l. Add a row and click the pencil next to the (Space) field to edit

- m. For Attribute Name, select (Screen Logical Attribute) and name it |Instructions|
- n. For Style, select Text Area
- o. For Name, type Instructions
- p. Scroll down to Initialization JavaScript, in this field create your message to the implementer. In this case, it is instructions on how to manually implement the request. For example:

```
function init(FieldContext) {  
  
    var message = "Please log into the target server and create the user in the  
    /etc/passwd file and add them to /etc/group xyz";  
  
    FieldContext.setValue(message);  
  
}
```

- q. Click Apply in the attribute box, then click OK at the bottom of the screen.
- r. On the next screen, make sure that Implement Profile is selected and click Select
- s. On the next screen, click OK
- t. On the next screen, click Submit

Create Request Admin Task

1. Navigate to: Roles and Tasks > Admin Tasks > Create Admin Task > Create a copy ...
2. Create Copy of: [SIGMA] Assign Role Manager Approval
Note: If you are not building this task in the Solutions Pro environment, you'll need to create a copy of your generic assign provisioning role task
3. In the Profile Tab:
 - a. Rename the task to: [SIGMA] Assign Really Sensitive Role
 - b. Rename the Tag to: SIGMAAssignReallySensitiveRole
4. In the Events Tab: click the pencil to edit next to Provisioning Roles – AssignProvisioningRoleEvent

Profile	Search	Tags	Fields	Events
Workflow processes associated with events in this task.				
Tab Tag	Event Name	Workflow Process		
Profile	ModifyUserEvent			
Profile	ResetPasswordEvent			
Profile	ForgottenPasswordEvent			
Profile	ViewUserEvent			
AccessRoles	AssignAccessRoleEvent			
AccessRoles	RevokeAccessRoleEvent			
AccessRoles	AddGrantorOnAccessRoleEvent			
AccessRoles	RemoveGrantorOnAccessRoleEvent			
AdminRoles	AssignAdminRoleEvent			
AdminRoles	RevokeAdminRoleEvent			
AdminRoles	AddGrantorOnAdminRoleEvent			
AdminRoles	RemoveGrantorOnAdminRoleEvent			
ProvisioningRoles	AssignProvisioningRoleEvent	SingleStepApproval		
ProvisioningRoles	RevokeProvisioningRoleEvent			
ProvisioningRoles	AccumulatedProvisioningRolesEvent			
ProvisioningRolesIndirect	AssignProvisioningRoleEvent			
ProvisioningRolesIndirect	RevokeProvisioningRoleEvent			
ProvisioningRolesIndirect	AccumulatedProvisioningRolesEvent			
Groups	AddToGroupEvent			
Groups	RemoveFromGroupEvent			
Groups	AddGroupAdminEvent			
Groups	RemoveGroupAdminEvent			
Delegation	ModifyDelegationEvent			
Delegation	DeleteDelegationEvent			

5. On the next screen, select the workflow we created in Workpoint (Step 5 of Create Custom Workflow). In our example, this is: FourStageApprovalProcess.

Workflow Mapping for AssignProvisioningRoleEvent	
<input checked="" type="radio"/> Non-Policy Based	SingleStepApproval
<input type="radio"/> Policy Based	Consultation Process
	CreateGroupApproveProcess
	CreateOrganizationApproveProcess
	CreateUserApproveProcess
	DeleteGroupApproveProcess
	DeleteOrganizationApproveProcess
	DeleteUserApproveProcess
	EscalationApproval
This process template	FourStageApprovalProcess
Default Approver	ImplementationWith1Approval
Request Description	ModifyAccessRoleMembershipApproveProcess
Approval Task	ModifyAdminRoleMembershipApproveProcess
Participant Resolver	ModifyGroupMembershipApproveProcess
Resolver Description	ModifyIdentityPolicySetApproveProcess
	ModifyObjectApproveProcess
	ModifyOrganizationApproveProcess
	ModifyUserApproveProcess
	NewOne
	SelfRegistrationApproveProcess
	SingleStepApproval

6. You should see the four stages of our custom workflow displayed:

7. For IT Manual Implementation:

a. Approval Task: Implement Request Access

Note: This is the admin task defined in the section Create Implement “Approval” Admin Task.

b. Participant Resolver: Group Members

c. Select the Help Desk Group created in the section Create Help Desk Group

8. For Manager Approval:

a. Approval Task: Approve Request Access

b. Participant Resolver: Dynamic Resolver

i. Approvers: Users

ii. User or Object: Primary object of this task

iii. Attribute: Manager ID

9. For HR Approval:

a. Approval Task: Approve Request Access

b. Participant Resolver: List of Users

i. Select jonri01 (Rita Jones) or another user of your choice

10. For Risk Manager Approval:

a. Approval Task: Approve Request Access

b. Participant Resolver: List of Users

i. Select menbr01 (Brian Mendoza) or another user of your choice

11. Click OK

12. Click Submit

Add Admin Task to Admin Group

1. Navigate to Roles and Tasks > Admin Roles > Modify Admin Role
2. Select [SIGMA] Self Manager
3. In the Tasks Tab, add the new admin task: [SIGMA] Assign Role Manager Approval
4. Click Submit

CA Identity Portal Configuration

Log into the CA Identity Portal Admin UI to perform the following configurations.

Restart IDM Connector

1. Navigate to Backend management > Connectors
2. Restart the IDM Connector

Create IDP Task

1. Navigate to Backend management > Tasks
2. Create New Task
 - a. Connector = CAIDM
 - b. Name = [SIGMA] Assign Really Sensitive Role
 - c. Tag = auto populates
 - d. additionOperation = directChange
 - e. removalOperation = directChange
 - f. IsBulkTask = False
3. Click Save

Create IDP Form

1. Navigate to Backend management > Forms
2. Create New Form
 - a. Form Name = ReallySensitiveAccess
 - b. Form Tag = auto populates
 - c. Task = SIGMAAssignReallySensitiveRole
 - d. Click Add prop
 - i. Approval Notice
 - ii. Property type = Message
 - iii. Type out a message in the body of the property
For example:

Requesting this access requires approvals from:

- Your Manager
- The Corporate Risk Manager
- Human Resources

This access will then be granted by the IT Help Desk.

3. Click Save

Create IDP Target Permission

1. Navigate to Backend management > Target Permissions
2. Click New
3. Connector = CAIDM
4. Name = [SIGMA] Really Sensitive Application
5. Tag = auto populated
6. Type (can't be changed) = Role
7. Mod Type = ADD
8. Click Add Rule
 - a. Name = default
 - b. Priority = 1
 - c. Mode = AccessRights
 - d. Expression = true
 - e. Forms:
 - i. Add = check the box and select ReallySensitiveAccess
 - ii. Remove = check the box and select AssignRole

Note: this is a blank form used to add / remove generic access in the Solution Pro Demo. If using your own, do not reuse the ReallySensitiveAccess form as this will trigger the three step approval.

Alternative: You can create a single step approval node for implementation, this will enable you to notify the Help Desk to automatically remove the access.
9. Click Save

Edit the Entitlement Tree

1. Navigate to Environment > Entitlement Tree
2. Create a new Group
3. Name the Group; in my environment, I called this Customer Assets (as this was demoed to the *customer*)
4. Under this Group create a new application; in my environment, I called this *Customer Application*. You can name this Really Sensitive Application to continue the demo flow here
5. In the middle pane, create a new permission; I called this Basic Access
6. Click on the permission and select the Target Permission in the right pane:
[SIGMA] Really Sensitive Application
7. Click Save

End Result

Here is the demo flow. This is assuming the Solution Pro demo was used.

1. Log into the CA Identity Portal as garan01 (Anne Garrett)
2. Click Access > Request for Self
3. Search for Customer Assets, click on Really Sensitive Application, add to Cart

The screenshot shows the CA Identity Portal interface. The user is logged in as Anne Garrett. The main content area is divided into three sections: a left sidebar with a search bar and a list of assets, a central pane showing details for 'Really Sensitive Application' with a 'Basic Access' request card, and a right sidebar showing a shopping cart with one item. The cart item is 'Really Sensitive Application - Basic Access'. Below the cart, there are buttons for 'Save draft' and 'Check Out'. The footer contains copyright information and the version number 1.6.1.682.

Copyright © 2015 CA. All rights reserved. 1.6.1.682

4. Click Check Out
5. Go to My Requests and click on the current request. Note the approver.

The screenshot shows the CA Identity Portal interface with the 'Request Details' and 'Timeline' sections. The 'Request Details' section shows a table of requests and a detailed view of the current request. The 'Timeline' section shows the request's history, including a 'Submitted' status and a 'Pending' status.

Requested by	Target	Submit Date	Status	ID
Anne Garrett	Anne Garrett	5/26/2016	In Progress	565
Anne Garrett	Anne Garrett	5/26/2016	Completed	564
Anne Garrett	Anne Garrett	5/24/2016	Completed	563
Anne Garrett	Anne Garrett	5/24/2016	Completed	559
Anne Garrett	Anne Garrett	5/24/2016	Completed	558
Anne Garrett	Anne Garrett	5/24/2016	Completed	557
Anne Garrett	Anne Garrett	5/24/2016	Completed	556
Anne Garrett	Anne Garrett	5/23/2016	Completed	551
Anne	Anne	5/23/2016	Completed	550

Request Details: Access Right (1) - Customer Assets - Really Sensitive Application - Basic Access (In Progress, 5/26/2016)

Timeline: Anne Garrett (Submitted, less than a minute ago) - Tony Belli, Manager Approval (Pending)

Copyright © 2015 CA. All rights reserved. 1.6.1.682

6. Logout and Login as belto01 (Tony Belli)
7. Click on Tasks
8. Type a comment and click Approve.

Copyright © 2015 CA. All rights reserved 1.6.1.682

9. Logout and Login as garan01 (Anne Garrett)
10. Click on My Requests and click on Basic Access. Note the next approver.

Copyright © 2015 CA. All rights reserved 1.6.1.682

11. Logout and Login as menbr01 (Brain Mendoza)

12. Click Tasks, leave a comment, and approve.

CA Identity Portal

Hello, Brian Mendoza

Tasks 1 Certification Campaign 59 Days left

Home My Profile Tasks Access My Requests Modify My Profile My Department User Onboarding

Apps Drafts English

Approvals Implementa... Campaigns

Requested For	Requested By	Submit Date	ID
✓ Anne Garrett	Anne Garrett	5/26/2016	565

Approval Details

For: Anne Garrett

Requester: Anne Garrett (garan01)

Assigned Date: 5/26/2016 Request Id: 565

Process step: Risk Manager Appro...

Request information Additional Information

- Customer Assets
- Really Sensitive Application
- Basic Access

Timeline

Anne Garrett 4 minutes ago

Submitted

Tony Belli, Manager Approval 2 minutes ago

Approve

"Anne needs this access for testing we are doing."

You

Waiting for you

This is an acceptable risk. I approve.

More Reject Approve

Copyright © 2015 CA. All rights reserved 1.6.1.682

13. Logout and Login as garan01 (Anne Garrett)

14. Click on My Requests and click on Basic Access. Note the next approver.

CA Identity Portal

Hello, Anne Garrett

Tasks

Home My Profile Tasks Access My Requests Modify My Profile

Apps Drafts English

Search requests for users, dates and IDs

Requested by	Target	Submit Date	Status	ID
Anne Garrett	Anne Garrett	5/26/2016	In Progress	565
Anne Garrett	Anne Garrett	5/26/2016	Completed	564
Anne Garrett	Anne Garrett	5/24/2016	Completed	563
Anne Garrett	Anne Garrett	5/24/2016	Completed	559
Anne Garrett	Anne Garrett	5/24/2016	Completed	558
Anne Garrett	Anne Garrett	5/24/2016	Completed	557
Anne Garrett	Anne Garrett	5/24/2016	Completed	556
Anne Garrett	Anne Garrett	5/23/2016	Completed	551
Anne	Anne	5/23/2016	Completed	550

Request Details

Access Right (1)

- Customer Assets
- Really Sensitive Application
- Basic Access In Progress 5/26/2016

Requesting this access requires approvals from:

- Your Manager
- The Corporate Risk Manager
- Human Resources

This access will then be granted by the IT Help Desk.

Timeline

Anne Garrett 6 minutes ago

Submitted

Tony Belli, Manager Approval 4 minutes ago

Approve

"Anne needs this access for testing we are doing."

Brian Mendoza, Risk Manager Approval less than a minute ago

Approve

"This is an acceptable risk. I approve."

Rita Jones, HR Approval

Pending

Copyright © 2015 CA. All rights reserved 1.6.1.682

15. Logout and Login as jonri01 (Rita Jones)

16. Click Tasks, leave a comment, and approve.

The screenshot shows the CA Identity Portal interface. The user is Rita Jones. The 'Tasks' section is active, showing a request for 'Basic Access' submitted by Anne Garrett on 5/26/2016. The 'Approval Details' panel shows the request information and the process step 'HR Approval'. The 'Timeline' panel shows a sequence of actions: 'Approve' (comment: 'Anne needs this access for testing we are doing.'), 'Approve' (comment: 'This is an acceptable risk. I approve.'), and 'Waiting for you'. At the bottom, there are buttons for 'More', 'Reject', and 'Approve'.

Copyright © 2015 CA. All rights reserved. 1.6.1.682

17. Logout and Login as garan01 (Anne Garrett)

18. Click on My Requests and click on Basic Access. Note the next approver.

19.

20.

21. Logout and Login as garan01 (Anne Garrett)

22. Click on My Requests and click on Basic Access. Note the next approver is a group. Hover over the Group and note the list of approvers.

The screenshot shows the CA Identity Portal interface. The user is Anne Garrett. The 'My Requests' section is active, showing a list of requests. The 'Request Details' panel shows the request for 'Basic Access' submitted by Anne Garrett on 5/26/2016. The 'Timeline' panel shows a sequence of actions: 'Approve' (comment: 'Anne needs this access for testing we are doing.'), 'Approve' (comment: 'This is an acceptable risk. I approve.'), 'Approve' (comment: 'Anne is an employee in good standing. I approve this request.'), and 'Pending'. A tooltip shows the list of approvers for the 'Group, IT Desk Implementation' role: Rafael Ortiz, Anita Hirsch, and Tania Turner.

Copyright © 2015 CA. All rights reserved. 1.6.1.682

23. Logout and Login as hiran01 (Anita Hirsch) – one of the IT Help Desk resources.
24. Click on Tasks. Note that the task is in the Implementation Tab. Click on Additional Information to see the instructions and information needed to complete the manual provisioning. Leave a comment and implement.

The screenshot shows the CA Identity Portal interface. The user is logged in as Anita Hirsch. The 'Tasks' tab is active, showing a task for Anne Garrett (garan01) with a status of 'Implementation'. The task details include the requester's name, assigned date (5/26/2016), and request ID (565). The process step is 'IT Desk Implementa..'. The request information tab is selected, showing the email (garan01@forwardinc.ca) and instructions: 'Please create the user in the [redacted] application. Assign basic level access. Inform user of password.' The full name is Anne Garrett and the user ID is garan01. The timeline shows approvals from Tony Belli (Manager Approval) and Brian Mendoza (Risk Manager Approval), both with 'Approve' buttons. A final 'Implement' button is visible at the bottom right of the timeline.

25. Logout and Login as garan01 (Anne Garrett)
26. Click on My Requests and click on Basic Access. Note that the workflow is completed.

The screenshot shows the CA Identity Portal interface with the user logged in as Anne Garrett. The 'My Requests' tab is active, displaying a list of requests. The first request is highlighted, showing it was requested by Anne Garrett for target Anne Garrett, submitted on 5/26/2016, and is in a 'Completed' status with ID 565. The 'Request Details' tab is selected for this request, showing 'Access Right (1)' and 'Basic Access' with a status of 'Completed' on 5/26/2016. A note indicates that requesting this access requires approvals from the Manager, Corporate Risk Manager, and Human Resources, and that the access will be granted by the IT Help Desk. The timeline shows approvals from Brian Mendoza (Risk Manager Approval) and Rita Jones (HR Approval), both with 'Approve' buttons. The final step is 'Implement' by Anita Hirsch (IT Desk Implementation), with a comment: 'I created your account, Anne. I'll email your password to you. Please change...'

27. Also note that the comments left by Anita exceeded the bubble size. Click on the comment bubble and show the pop-up with the complete comment.

The screenshot shows the CA Identity Portal interface. At the top, there is a navigation bar with the CA Technologies logo, a user profile for Anne Garrett, and a 'Tasks' button. Below the navigation bar, there is a search bar and a table of requests. A 'Request Details' panel is open, showing a comment from Anne Garrett: 'I created your account, Anne. I'll email your password to you. Please change once you log in.' A 'Timeline' panel on the right shows a sequence of events, including a comment that has been expanded to show its full text. The bottom of the page contains copyright information and a version number.

28. Click Ok and click Access > Request for Self. Do a search for Sensitive and click on Really Sensitive Application. Note that the Basic Access has been provisioned.

The screenshot shows the CA Identity Portal interface. At the top, there is a navigation bar with the CA Technologies logo, a user profile for Anne Garrett, and a 'Tasks' button. Below the navigation bar, there is a search bar and a table of requests. A 'Request Details' panel is open, showing a comment from Anne Garrett: 'I created your account, Anne. I'll email your password to you. Please change once you log in.' A 'Timeline' panel on the right shows a sequence of events, including a comment that has been expanded to show its full text. The bottom of the page contains copyright information and a version number.

29. End scene.