



CHAPTER 8

Managing Activities

When using Workflow mode, all policy definition and assignment tasks must be done within the context of an activity. If you are using non-Workflow mode (the default mode of operation in Security Manager), you do not need to explicitly create and manage activities, because activity creation and management happens automatically and transparently. For more information, see [Working in Non-Workflow Mode, page 1-13](#).

The following topics provide information about activities:

- [Understanding Activities, page 8-1](#)
- [Working with Activities, page 8-6](#)

Understanding Activities

An activity is a temporary context within which you define policies and assign them to devices. You do not need to create an activity to import, create, or delete devices (unless you perform policy discovery as part of the action), or to perform various system management tasks.

The requirements for creating or opening activities differ depending on your Workflow mode:

- **Non-Workflow mode**—An activity is created automatically and transparently for you whenever you define, modify, or assign policies to devices. You cannot actively open or manage activities in non-Workflow mode. These types of activities are also called configuration sessions.
- **Workflow mode**—If you do not explicitly open an activity, you are prompted to create a new activity or open an existing one whenever you perform an action that requires an activity. You must actively open and manage activities in Workflow mode.

When you create an activity, or one is created for you, you open a virtual copy of the Security Manager policy database. You define and assign policies within this copy. Changes that you made within this copy are only available within the copy. Other users in different activities cannot see these changes. After the activity is submitted and, in Workflow mode, approved, the changes within this copy are committed to the database so that all other users can view the changes. Then, you can create a deployment job to generate the relevant CLI commands and deploy them to the devices.

How you submit your activity changes differs depending on Workflow mode:

- **Non-Workflow mode**—Select **File > Submit** to submit your changes to the policy database.
- **Workflow mode**—Select **Activities > Submit Activity** if you are working with an activity approver, or **Activities > Approve Activity** if you do not have a separate activity approver.

The following topics describe why activities are important and how they operate in Workflow mode:

- [Benefits of Activities, page 8-2](#)
- [Activity Approval, page 8-2](#)
- [Activities and Locking, page 8-2](#)
- [Activities and Multiple Users, page 8-3](#)
- [Understanding Activity States, page 8-4](#)

Benefits of Activities

You use activities to control changes made to policies and policy assignments. Although how activities are implemented depends on the workflow settings you choose, all activities provide the following benefits:

- **Audit trail**—Activities track changes that are made in Security Manager. You can use this information to determine what changes were made and who made the changes. For more information, see [Viewing Activity Status and History, page 8-15](#).
- **Safety mechanism**—Activities provide a means for experimenting with changes. You can make changes using an activity, then view the configuration that results from those changes. If you do not want to implement the changes, you can discard the activity. For more information, see [Discarding an Activity, page 8-15](#).
- **Task isolation**—When you create an activity, the policies that are modified within that activity are locked from being modified within other activities. This prevents conflicting changes that could make a policy unstable. For more information, see [Activities and Locking, page 8-2](#).

In addition, the changes you make within an activity are visible *only* within the activity. Other users will see only the last approved committed configurations, unless they view your activity before you close it.

Activity Approval

When you enable Workflow mode, you can choose to operate with or without an activity approver.

If your organization requires a different person with higher permissions to approve activities, you can enable workflow with an approver. When using Workflow mode with an approver, the activity must be approved by a person with the appropriate permissions so the policies can be committed to the database. This approval process at the policy definition level helps to ensure that no inappropriate configurations reach the network devices.

If you choose to operate without an approver, the person defining the policies has the permissions to approve them.

For information about enabling or disabling activity approval and changing the default activity approver, see [Workflow Page, page A-44](#).

Activities and Locking

Activities introduce a locking model. This is useful in large networks where several people have the authority to make configuration changes. It prevents two or more people from making changes to the same feature policy, policy assignment, or object at the same time.

In addition, Security Manager uses locking to ensure that operations related to the committed configuration always run exclusive of one another. These operations can be divided into two categories:

Operations that change the committed configuration:

- Activity approval
- Device deletion
- Editing device properties

Operations that read the committed configuration:

- Configuration preview
- Deployment (in non-Workflow mode)
- Creation of deployment job (in Workflow mode)
- Activity validation

If you are performing an operation that changes the committed configuration, you cannot perform any of the operations in either list until this operation is complete. An error message is displayed if you try. For example, if you are approving an activity (which occurs automatically when an activity is submitted in non-Workflow mode), you cannot delete a device or validate a different activity until the approval is complete. This type of locking is particularly important in multi-user settings as it prevents multiple users from simultaneously making changes to the committed configuration.

If you are performing an operation that reads the committed configuration, you cannot perform an operation that changes the committed configuration. For example, if you are validating an activity, another user cannot approve an activity. However, you may perform another operation that reads the configuration. For example, if you are validating an activity, another user can create a deployment job. Similarly, if you are previewing the configuration before deployment, another user is permitted to do the same. This is because these two operations are limited to reading the committed configuration; they do not make any changes to it.

Related Topics

- [Understanding Locking, page 7-7](#)
- [Approving or Rejecting an Activity, page 8-14](#)
- [Deleting Devices from the Security Manager Inventory, page 6-24](#)
- [Viewing or Changing Device Properties, page 6-17](#)
- [Working with Deployment and the Configuration Archive, page 18-16](#)
- [Validating an Activity, page 8-11](#)

Activities and Multiple Users

Only one user can define or change policies within an individual activity at one time. However, when Workflow mode is enabled, multiple users can work in the activity in sequence. That is, if an activity is closed (but not yet approved or submitted for approval), another user can open it and make changes to it. Multiple users can work in parallel in different activities.

Understanding Activity States

In Workflow mode, an activity has four primary states:

- **Edit Open**—Policy changes can be made within the selected activity. The activity remains in this state until it is submitted for approval, approved, or deleted. The activity can be opened, closed, and edited any number of times while it is in this state. The policies, policy assignments (devices being assigned policies), and objects being configured or modified in the activity are locked. That is, they cannot be configured or modified within the context of another activity. The configuration changes can be seen only in the context of the current activity.
- **Submitted**—The activity was submitted for approval. (This state is available only if you have Workflow mode enabled with activity approval required. For more information, see [Workflow Page, page A-44](#).) No further changes can be made within the activity. The policies, devices (through policy assignment), or objects affected by the policy changes remain locked to other activities.

When an activity is submitted, an e-mail is sent to the approver. The approver can open the activity (in read-only mode) to review the changes within the activity, then approve or reject it. An approved activity moves to the approved state. A rejected activity returns to the Edit state.

- **Approved**—The activity was approved by a person with activity approval permissions. The policies defined within the activity are committed and ready to be deployed to devices or to a file. The devices affected by the policy changes are no longer locked to other activities.
- **Rejected**—The activity was reviewed and rejected by a person with activity approval permissions. This state is available only if you have Workflow mode enabled with activity approval required. The policies defined within the activity are not committed. The activity returns to the Edit state and the devices affected by the policy changes remain locked to other activities.

[Figure 8-1](#) shows the stages in the activity workflow without an approver. [Figure 8-2](#) shows the stages in the activity workflow with an approver.

For a complete list and descriptions of activity states, see [Activity States, page E-3](#).

Figure 8-1 Activity Workflow without an Approver

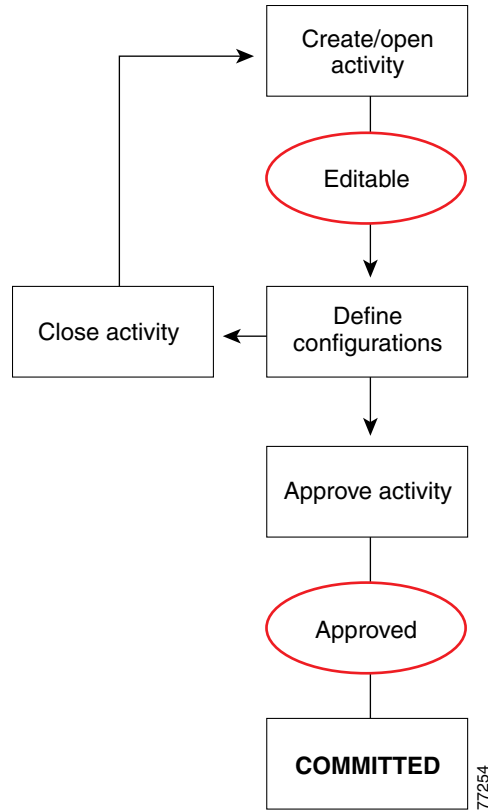
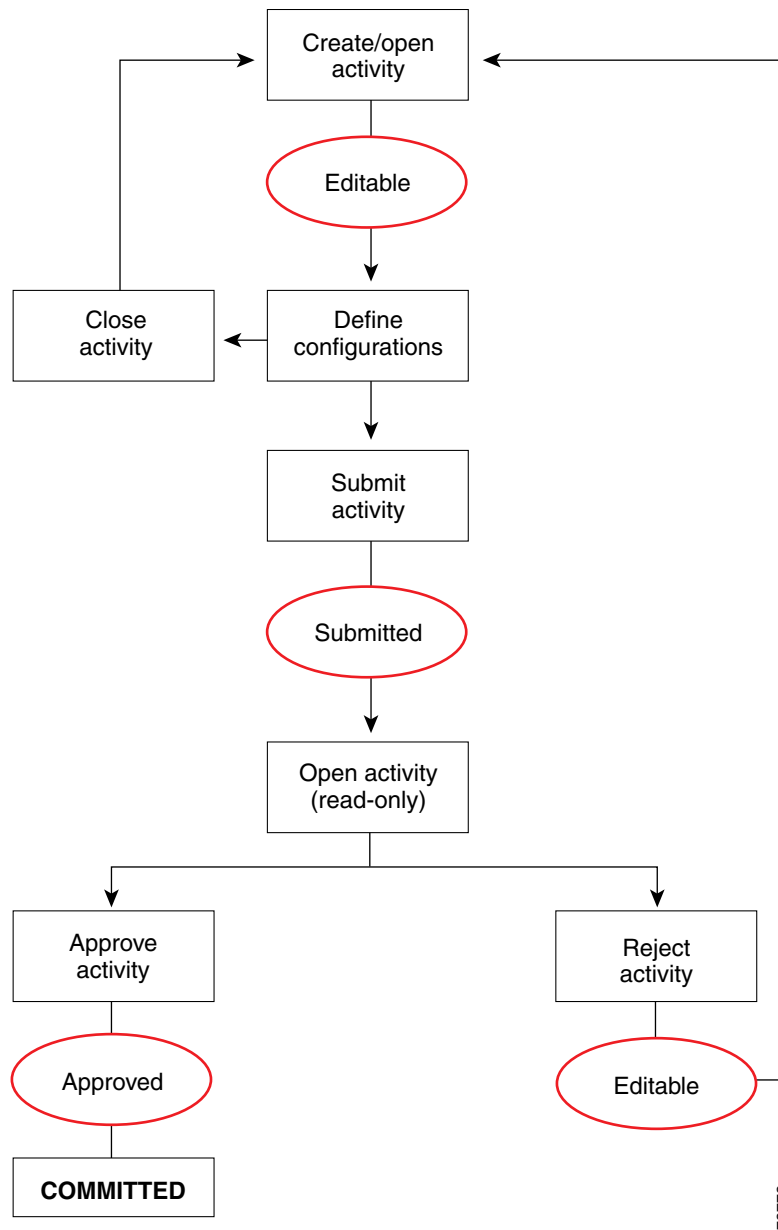


Figure 8-2 Activity Workflow with an Approver



Working with Activities

The following topics provide information to help you use activities:

- [Accessing Activity Functions, page 8-7](#)
- [Creating an Activity, page 8-9](#)
- [Opening an Activity, page 8-9](#)
- [Closing an Activity, page 8-10](#)

- [Viewing Activity Change Reports, page 8-10](#)
- [Validating an Activity, page 8-11](#)
- [Submitting an Activity for Approval, page 8-13](#)
- [Approving or Rejecting an Activity, page 8-14](#)
- [Discarding an Activity, page 8-15](#)
- [Viewing Activity Status and History, page 8-15](#)

Accessing Activity Functions

In Workflow mode, you can access activity management functions in the following ways:

- Select **Tools > Activity Manager**. The Activity Manager window contains a list of existing activities and their states. From this window, you can create new activities, and open, close, submit, approve, reject, or discard existing activities. For more information, see [Activity Manager Window, page E-1](#).
- Click a button in the Activities portion of the main toolbar or select the equivalent command in the Activities menu. Whether a button or command is active depends on your user permissions, the state of the activity, and whether you are using workflow with or without an approver. [Table 8-1](#) explains the buttons and commands and the conditions under which you can them.

Table 8-1 Activities Tool Bar Buttons and Commands When Workflow Mode Is Enabled










Button	Activities Menu Command	Description
	New Activity	Creates an activity.
	Open Activity	Opens an activity. You can open an activity when it is in the Edit or the Submitted state. To open a submitted activity, you must have user privileges to approve or reject changes made in that activity. For more information, see Setting Up User Permissions, page 2-1 .
	Close Activity	Saves all changes made while the activity was open and closes it. You can close an activity when it is in the Edit Open or the Submit Open state.
	View Changes	Evaluates all changes made in the activity and produces an Activity Change Report in PDF format in a separate window. For more information, see Viewing Activity Change Reports, page 8-10

Table 8-1 Activities Tool Bar Buttons and Commands When Workflow Mode Is Enabled

Button	Activities Menu Command	Description
	Validate Activity	Validates the integrity of changed policies within the current activity. By validating an activity, you can check for configuration errors that you might have introduced by your policy changes.
	Submit Activity	In Workflow mode with an activity approver, submits the activity for approval. You can submit an activity when it is in the Edit or the Edit Open state.
	Approve Activity	Approves the changes proposed in an activity. You can approve an activity when it is in the Submitted state when using an activity approver, or the Edit or Edit Open state when not using an approver. You must have user privileges to accept the changes proposed in an activity. For more information, see Setting Up User Permissions, page 2-1 .
	Reject Activity	In Workflow mode with an activity approver, rejects the changes proposed in an activity. You can reject an activity when it is in the Submitted or Submitted Open state. You must have user privileges to deny changes proposed in an activity. For more information, see Setting Up User Permissions, page 2-1 .
	Discard Activity	Discards the selected activity. The activity is discarded and later purged from the system after it exceeds the age for keeping activities as set under Tools > Security Manager Administration > Workflow. The activity state is shown as discarded until the activity is actually purged from the system.

Creating an Activity

In Workflow mode, before you create or change policies or assign policies to devices, you must create an activity.

Related Topics

- [Understanding Activities, page 8-1](#)

Procedure

- Step 1** Do one of the following:
- Click the **Create Activity** button in the activity toolbar.
 - Select **Activities > New Activity**.
 - Click **Create** in the Activity Manager window.

The Create Activity dialog box appears (see [Create Activity Dialog Box, page E-4](#)).

- Step 2** In the Create Activity dialog box, enter a name for the activity or keep the system-generated name. You can also enter a comment to describe the activity.

- Step 3** Click **OK**.

The activity is listed in the Activity Manager window. For more information, see [Activity Manager Window, page E-1](#).

Opening an Activity

In Workflow mode, you can open an existing activity if no one else has it opened. You might open an existing activity in the Edit state to make further policy changes, or you might open an existing activity in the Submitted state to review proposed policy changes before approving or rejecting it (if you have the appropriate permissions and you are working in Workflow mode with an approver).



Note

An activity in the Submitted state opens in read-only mode.

To open an activity, do one of the following:

- Click the **Open** button in the activity toolbar or select **Activities > Open Activity**. From the Openable activities dialog box, select the activity you want to open, then click **OK**.
- Select **Tools > Activity Manager**. From the Activity Manager window, select the activity you want to open and click **Open**.

Related Topics

- [Understanding Activities, page 8-1](#)

Closing an Activity

You can close an activity without approving it (or submitting it for approval) if you or others want to continue configuring policies at a later time.

A person with administrator privileges can close an activity opened by another user.

To close an open activity, do one of the following:

- Click the **Close** button in the activity toolbar.
- Select **Activities > Close Activity**.
- Select **Tools > Activity Manager**. From the Activity Manager window, click **Close**.

Related Topics

- [Understanding Activities, page 8-1](#)

Viewing Activity Change Reports

There are many places in the interface where you can open activity change reports. Typically, the button or command to generate the report is **View Changes**. These change reports provide detailed information about the policy and policy object changes, and the devices that were acted on, that have been made in an activity, whether you are operating in Workflow or non-Workflow mode.

The activity change report is in Adobe Acrobat (PDF) format. You can use all of the Acrobat features, including the bookmarks tab, to view the report.

If you discover a device or rediscover policies on a device, then subsequent policy changes in the same activity performed on that device are not listed in the activity change report. This is also true on a device that you clone from another device.

Following are some of the ways you can view activity reports:

- Non-Workflow mode:
 - Select **File > View Changes** to view the changes made during the current configuration session.
 - Select **Tools > Change Reports** to view the changes made during previous sessions (which are closed when you submit or discard your changes). Select a configuration session from the Change Report window and click **View Changes**.
- Workflow mode:
 - Select **Activities > View Changes**, or click the **View Changes** button in the toolbar, to view the changes made during the currently open activity.
 - Highlight an activity in the Activity Manager window and click **View Changes** to view the changes made in that activity.
- In both modes, you can view changes from various dialog boxes when creating deployment jobs.




Note

You must disable any popup-blocker applications you have running to ensure the activity report will open.

Figure 8-3 shows a sample activity report.

Figure 8-3 Activity Report



Activity Change Report

User: celia
 Session started on: 26-Oct-2006 00:49:16
 Current state: Edit Open
 Report created on: 26-Oct-2006 18:14:22

Devices

- router2600
 - Policy Objects Override
 - InterfaceRole

Operation	Category ID	Name Patterns	Comment	Patterns	Name
Add	None	Ethernet1 , Dialer0 , Serial0 , Async1 , Serial0/0 , Outside	External interfaces	Ethernet1 , Dialer0 , Serial0 , Async1 , Serial0/0 , Outside , Ethernet1 , Dialer0 , Serial0 , Async1 , Serial0/0 , Outside	External

Shared Policies

No changes

Policy Objects

- Ike

Operation	Category ID	Dh Group	Lifetime	Priority	Hash	Encryption	Authentication	Name
Add	None	1	86400	-1	SHA	aes-128	Preshared Key	New IKE Proposal

The activity report includes these elements:

- Activity name—The name of the activity (or the user and session start date and time if it is unnamed).
 - Created by—The username of the person who created the activity, with the date and time.
 - Current state—The current state of the activity.
 - Report created on—The date and time the report was created.
 - Devices section—A summary of the devices that were acted on in the activity (that is, they were added, modified, or deleted). Changes to local policies are displayed here.
- Changes in this section and the other sections of the report are color-coded to help you identify changes:
- Green—Indicates a newly inserted item.
 - Red—Indicates a deleted item or the old value of a changed item.
 - Blue—Indicates the new value of a changed item.
- Shared Policies section—Changes to all shared policies are displayed here.
 - Policy Objects—Changes to all policy objects are displayed here.

Validating an Activity

In Workflow mode, Security Manager validates activities when you submit them for approval, or you can validate an activity at any time while you are creating and changing policies in an activity. After an activity is submitted, the validation report remains static.

In non-Workflow mode, Security Manager validates policies when you submit them to the database, when you try to deploy them, or when you validate them. The validation process reports on policy changes that were made up until the changes are saved or deployed.

The validation process checks the following areas. If there are errors, you can display a detailed summary of the validation results.

- Policy integrity—There are no unresolvable references (for example, missing objects, unresolved interface roles, overrides of mandatory settings, and so on).
- Policy deployability—The platform, operating system, and configured features are supported by the target devices so that policies can be correctly translated into CLI commands.
- FlexConfig integrity—There are no corrupted FlexConfig objects. If corrupted objects are found, a warning with a list of the corrupted FlexConfig objects results.
- FlexConfig syntax—If syntax errors are found, a warning with a list of affected FlexConfigs and their syntax errors results.
- FlexConfig object references—All object references are resolvable. If FlexConfig objects reference non-existent objects, a warning with a list of the missing objects results.

Related Topics

- [Submitting an Activity for Approval, page 8-13](#)
- [Deploying Configurations in Non-Workflow Mode, page 18-17](#)

Procedure

-
- Step 1** Do one of the following:
- In Workflow mode:
 - Open an activity, and then click the **Validate** button on the activity toolbar or select **Activities > Validate Activity**.
 - Select **Tools > Activity Manager**. From the Activity Manager window, select an activity, and then click **Validate**.
 - In non-Workflow mode, select **File > Validate**, or try to deploy policies.

Security Manager performs the validation and opens an informational message dialog box that summarizes the validation results. If there are no errors, validation passes. If there are errors or warnings, click **Details** to open the Validation dialog box, where you can view detailed information about the errors.

- Step 2** Evaluate the errors to determine how to fix them.

The Validation dialog box organizes the errors and warnings in two ways, which are displayed on separate tabs:

- Errors tab—The Errors tab organizes validation problems based on the type of error. Each error indicates the number of devices that are affected and the severity of the error.

Select an error in the upper pane, and a list of devices (with the type of device) that have the error appears in the lower left pane. The lower right pane describes the error, its cause, and what you might do to fix it.

- **Devices tab**—The Devices tab organizes validation problems based on the device. Each device indicates the number and types of errors and warnings for the device, and the device type. The device status indicates the worst problem in the device configuration (error or warning).

Select a device in the upper pane, and a list of the errors for that device appears in the lower left pane. Select an error and the lower right pane describes the error, its cause, and what you might do to fix it.

You must correct errors before submitting the activity. Security Manager does not allow an activity to be submitted with validation errors.



Note A validation warning (as opposed to an error) will not prevent activity approval or deployment.

Submitting an Activity for Approval

In Workflow mode with an activity approver, you must submit activities for approval. When you submit it, the integrity and deployability of the activity is validated. For details about the validation process and report, see [Validating an Activity, page 8-11](#).

The activity is also closed so that it can be opened by the user who has the permissions to approve it. When the activity is approved, its configurations are committed to the Security Manager database, and they can be deployed to the devices.

When you submit an activity, Security Manager sends an e-mail to the relevant approvers to notify them that an activity requires approval.

If you are working in Workflow mode without an activity approver, you do not need to submit activities (in fact, you cannot submit them). You can approve the activity yourself. For more information about changing activity approval settings, and configuring the e-mail addresses for notifications, see [Workflow Page, page A-44](#).

Related Topics

- [Understanding Activities, page 8-1](#)
- [Opening an Activity, page 8-9](#)

Procedure

Step 1 Do one of the following:

- Open an activity and click the **Submit** button on the activity toolbar or select **Activities > Submit Activity**.
- Select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Submit**.

The Submit Activity dialog box opens (see [Submit Activity Dialog Box, page E-5](#)).

Step 2 In the Submit Activity dialog box, enter the e-mail address of the person who should approve the activity (if the default address is not the right one) and enter comments that will help the approver evaluate the activity.

You can also change the submitter e-mail address, which normally is the address associated with the user account you used to log into Security Manager. Notifications of activity state changes are sent to this address.

Step 3 Click **OK**. The activity status changes to Submitted in the Activity Manager window.



Note Security Manager warns you if the e-mail cannot be sent and you must contact the approver directly.

Approving or Rejecting an Activity

Before the changes in an activity are committed to the database, you must approve the activity. If you have activity approval permissions, you can open an activity, review the policies and policy assignments, and then either approve or reject the activity.

If you are operating in Workflow mode without an approver, you can approve your own activities. When working without an approver, you cannot reject an activity, but you can discard it if you do not want to save your changes.

In Workflow mode with an activity approver, the activity must be submitted before you can open it and approve it. In this mode, you can also reject the activity.

If you approve an activity, policies and policy assignments are committed to the database and are ready to be deployed to devices or files. Devices associated with the activity are unlocked, meaning they can be included in policy definitions and changes in other activities.

If you reject the activity, the submitter can reopen the activity to make the necessary changes and resubmit it for approval. Devices associated with the activity are not unlocked, meaning that they cannot be included in policy definitions or changes in another activity.



Note After an activity is approved, changes cannot be undone. You must create a new activity and manually change policies and policy assignments to the desired state.

Related Topics

- [Understanding Activities, page 8-1](#)
- [Opening an Activity, page 8-9](#)

Procedure

Step 1 Do one of the following:

- Open an activity and click the **Approve** or **Reject** button, as appropriate, on the activity toolbar.
- Open an activity and select **Activities > Approve Activity** or **Activities > Reject Activity**, as appropriate.

- Select **Tools > Activity Manager**. From the Activity Manager window, select an activity and click **Approve** or **Reject**.

The Approve Activity or Reject Activity dialog box appears.

- Step 2** In the Comment field, enter a brief explanation of why you are approving or rejecting the activity. If you are rejecting the activity, you might want to include suggested revisions.
- Step 3** Click **OK**. The activity status changes to Approved or Edit (if rejected) in the Activity Manager window. For a description of the elements in the window, see [Activity Manager Window, page E-1](#).
-

Discarding an Activity

You can discard an activity if it is no longer required. When you discard an activity, you delete all the policies and policy assignments that were defined within the activity. Those policies and policy assignments are not in the database; therefore, they cannot be deployed.

Discarded activities are removed from the system according to the settings defined in the Security Manager settings for Workflow and devices associated with the activity are unlocked, meaning they can be used by other activities. For more information, see [Workflow Page, page A-44](#).

To discard an activity, do one of the following:

- Open an activity, then click the **Discard** button on the activity toolbar or select **Activities > Discard Activity**.
- Select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Discard**. Only an activity in the Edit or Edit Open state can be discarded.

Related Topics

- [Understanding Activities, page 8-1](#)
- [Opening an Activity, page 8-9](#)

Viewing Activity Status and History

In Workflow mode, you can view the status and history of changes for activities in the Activity Manager window.

To open the window, click the Activity Manager button in the toolbar or select **Tools > Activity Manager**.

The upper pane lists all available activities, including the current state of the activity. Select an activity to see additional information in the tabs in the lower pane:

- Details tab—Shows the date and time the activity was created, and its description.
- History tab—Shows the transaction history for the activity. Each time the activity state is changed, a record of the change is kept, including the user who made the change and any comments about the change.

Related Topics

- [Understanding Activities, page 8-1](#)
- [Activity Manager Window, page E-1](#)

