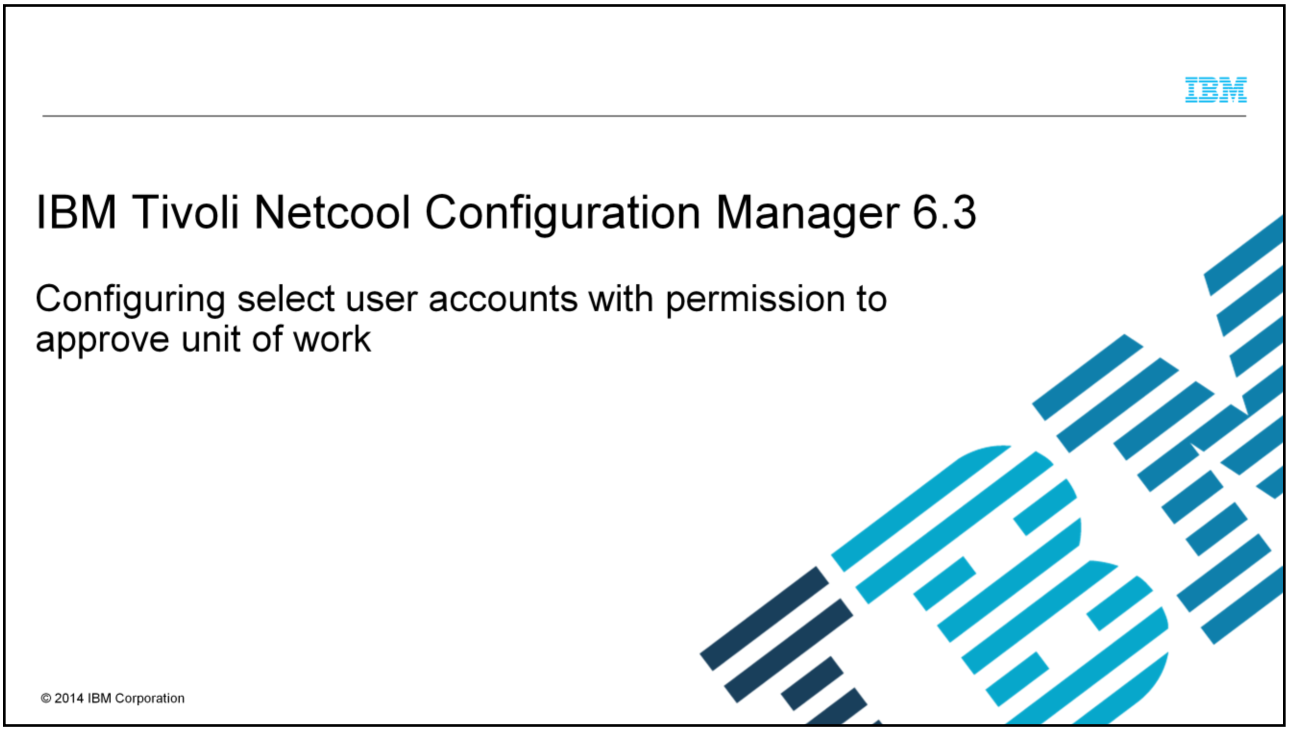
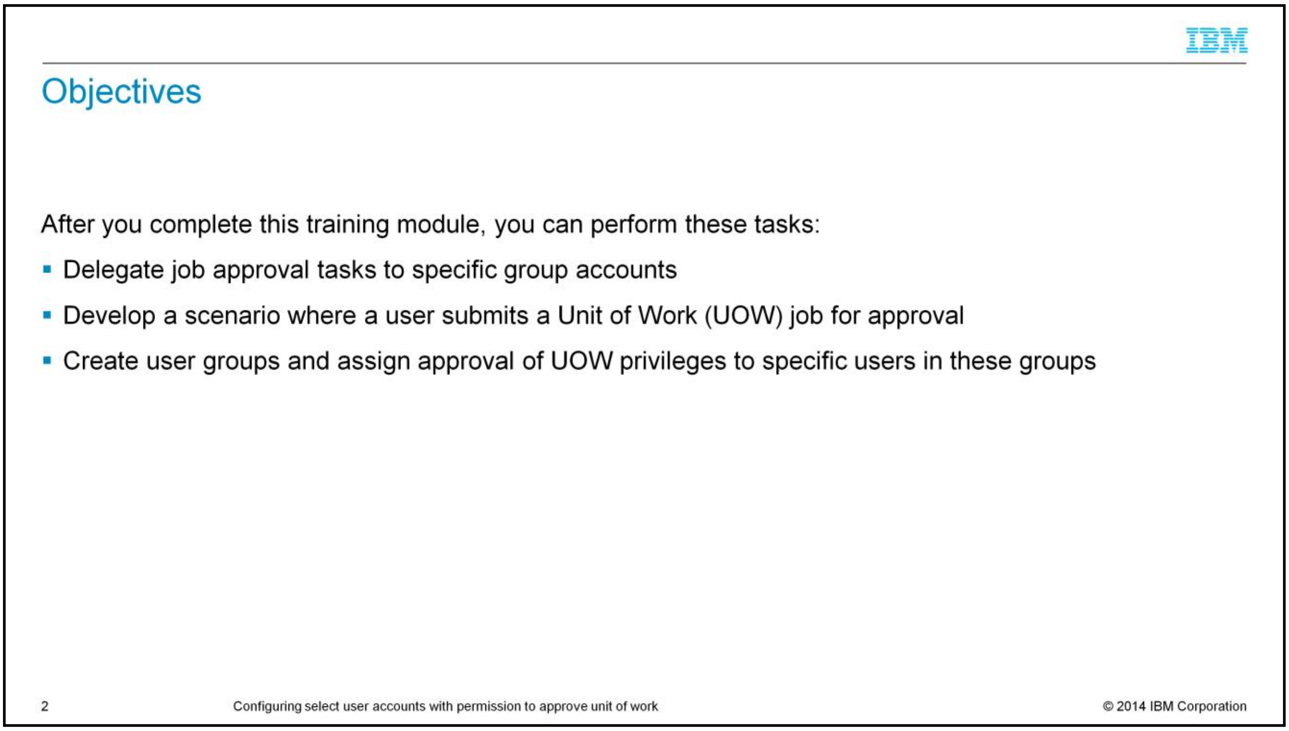


IBM Tivoli Netcool Configuration Manager 6.3

Configuring select user accounts with permission to approve unit of work

In this IBM Tivoli® Netcool® Configuration Manager version 6.3 training module, you learn how to configure user accounts with permission to approve a unit of work.



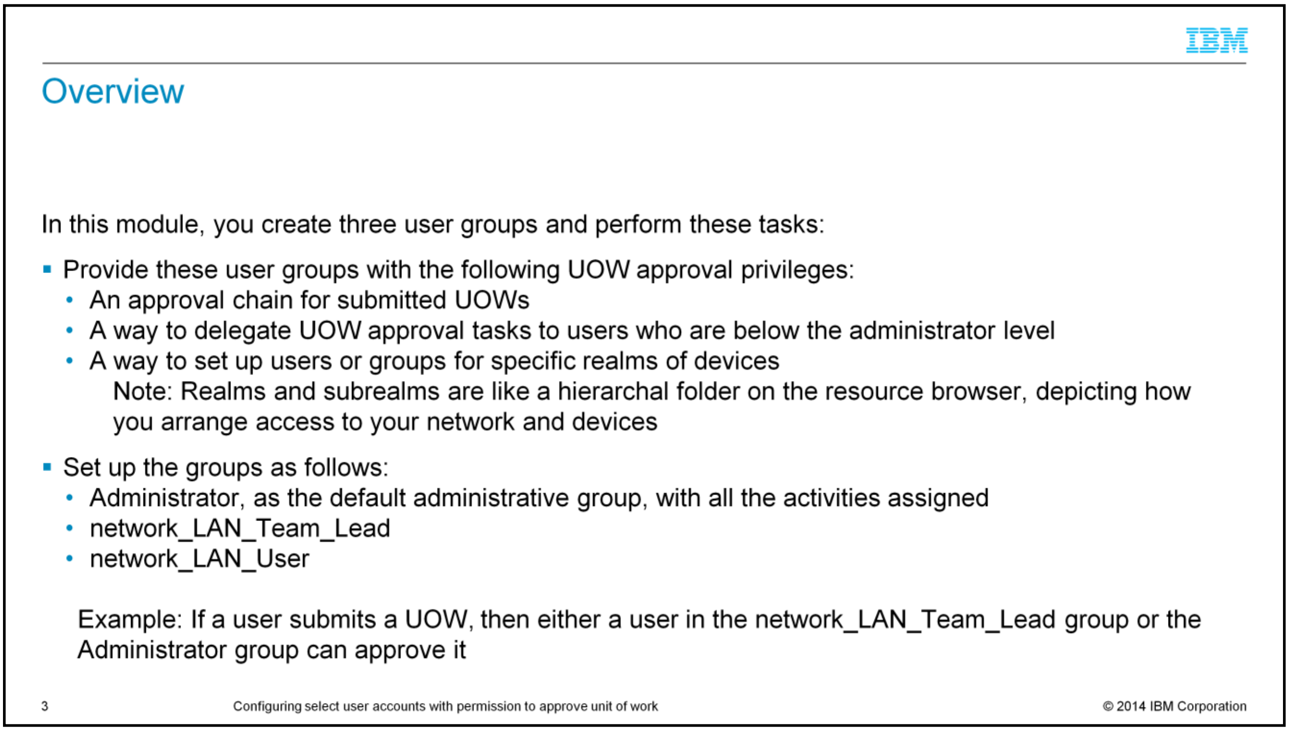
IBM

Objectives

After you complete this training module, you can perform these tasks:

- Delegate job approval tasks to specific group accounts
- Develop a scenario where a user submits a Unit of Work (UOW) job for approval
- Create user groups and assign approval of UOW privileges to specific users in these groups

After you complete this training module, you can explain how to delegate job approval tasks to specific group accounts. You also develop a scenario where a user submits a Unit of Work (UOW) job for approval, and you create user groups and assign approval of UOW privileges to specific users in these groups.



Overview

In this module, you create three user groups and perform these tasks:

- Provide these user groups with the following UOW approval privileges:
  - An approval chain for submitted UOWs
  - A way to delegate UOW approval tasks to users who are below the administrator level
  - A way to set up users or groups for specific realms of devices

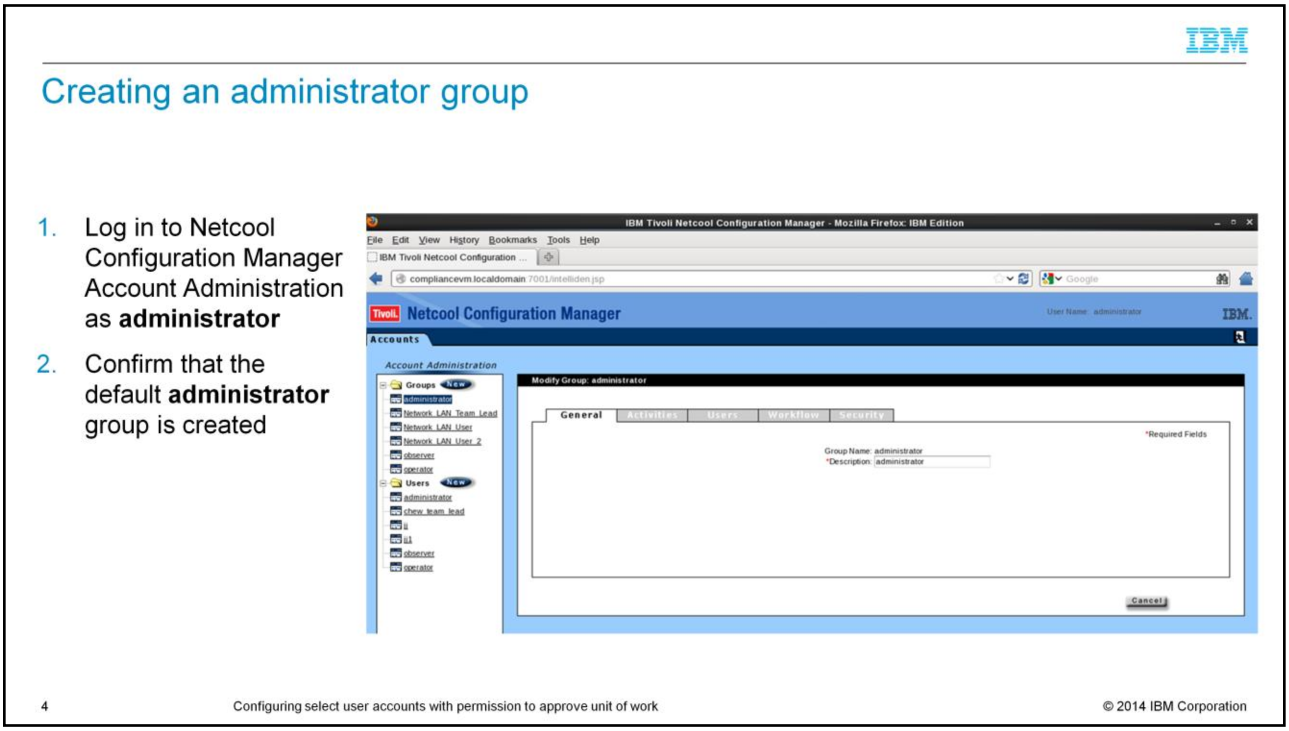
    Note: Realms and subrealms are like a hierarchal folder on the resource browser, depicting how you arrange access to your network and devices
- Set up the groups as follows:
  - Administrator, as the default administrative group, with all the activities assigned
  - network_LAN_Team_Lead
  - network_LAN_User

Example: If a user submits a UOW, then either a user in the network_LAN_Team_Lead group or the Administrator group can approve it

3 Configuring select user accounts with permission to approve unit of work

In this example scenario, an administrator of IBM Tivoli Netcool Configuration Manager has numerous users who are working with hundreds of different network devices. To ensure adequate security and control, constant updates and configuration changes must be performed. As a result, administrators have to implement an effective delegation process, which includes delegating the review and approval of updates and configuration changes.

As the administrator, you select a senior user account person in each group to handle the user group’s approval of UOW job tasks, either for all realms or specific realms. You create generic groups and select the users to assign to those groups. You also set up the workflow and security configuration for each of the three sample groups. You perform these steps as the administrator super user through the account management module that you access from the IBM Tivoli Netcool Configuration Manager GUI. The names of the three groups are displayed on this slide.



Creating an administrator group

1. Log in to Netcool Configuration Manager Account Administration as **administrator**
2. Confirm that the default **administrator** group is created

Modify Group: administrator

Group Name: administrator
*Description: administrator

*Required Fields

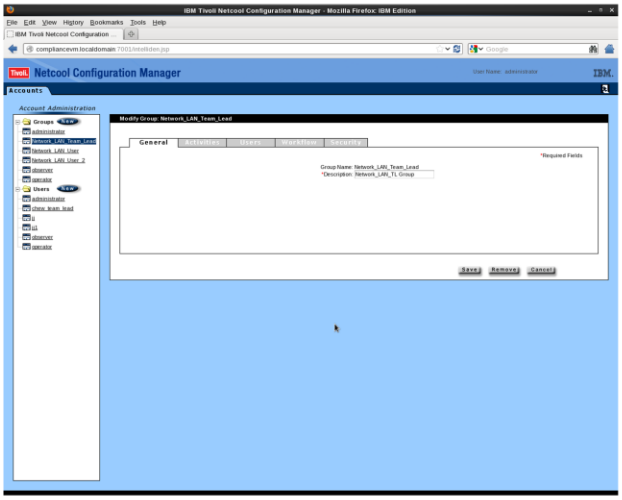
4 Configuring select user accounts with permission to approve unit of work © 2014 IBM Corporation

First, you must create all the necessary groups before creating the users and assigning activities to these groups. You begin with the administrator group. To create user groups, you must log in as user administrator, which is the default super user setup. After you log in with the administrator user and password, you select the Account Management option.

In the account management section, you click the **New** button to create new groups or users. By default, your ITNCM system should have the administrator group already created and defined, as shown on this slide (in the left pane under **Account Administration**). You do not have to re-create the administrator group.

Creating a Network_LAN_Team_Lead group

1. Click the **New** button beside the **Groups** folder icon
2. Enter **network_LAN_Team_Lead** in the **Group Name** field, and enter details in the **Description** field
3. Click **Create**



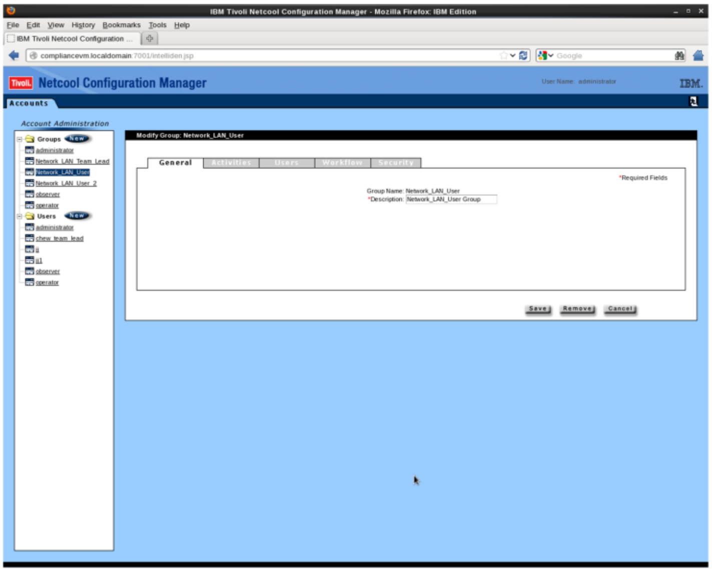
Group Name: Network_LAN_Team_Lead
*Description: Network_LAN_TL Group

Click the **New** button beside the **Groups** folder icon. Enter the relevant **Group Name** and **Description**. You can enter network_LAN_Team_Lead for both, or a relevant name that you prefer.

Click the **Create** button. The new network_LAN_Team_Lead group is created and viewable in the left pane of your account management view.

Creating a Network_LAN_User group

1. Click the **New** button beside the **Groups** folder icon
2. Enter **network_LAN_User** in the **Group Name** field and enter a description in the **Description** field
3. Click **Create**



IBM Tivoli Netcool Configuration Manager - Mozilla Firefox: IBM Edition

compliancevm.localdomain:7001/intelliden.jsp

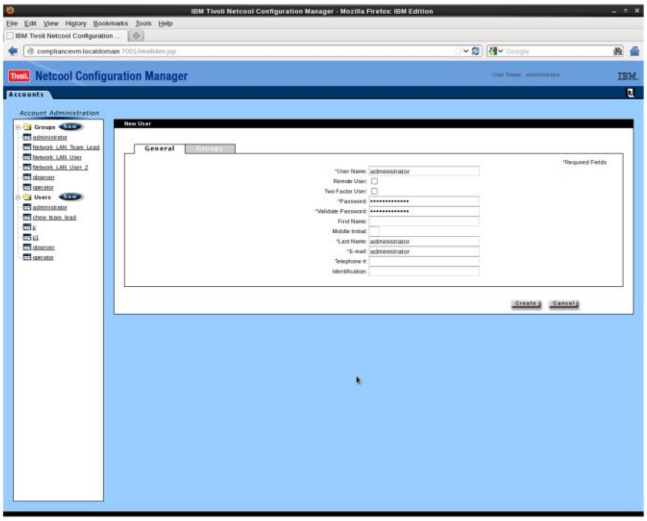
Modify Group: Network_LAN_User

Group Name: Network_LAN_User
*Description: Network_LAN_User Group

Enter the relevant **Group Name** and **Description** for the network_lan_user group, or select a relevant name that you prefer.

Click the **Create** button. The network_LAN_User group is created and viewable in the left pane of your account management view.

Confirming that the administrator user is created



*Required Fields

*User Name: administrator

Remote User: □

Two Factor User: □

*Password: ••••••••••••••

*Validate Password: ••••••••••••••

First Name:

Middle Initial:

*Last Name: administrator

*E-mail: administrator

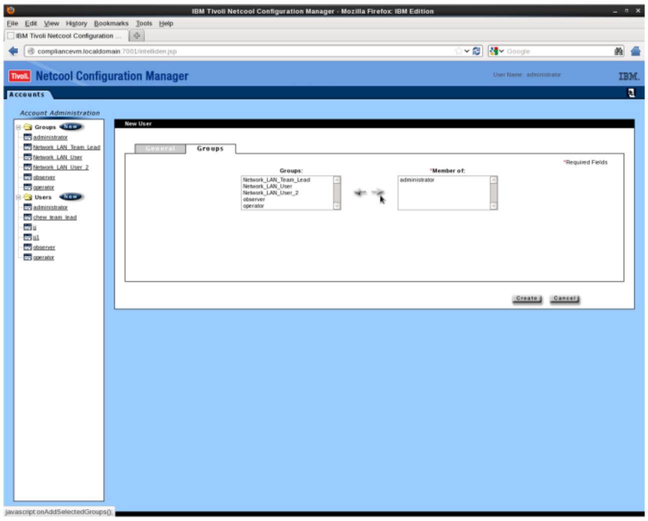
Telephone #:

Identification:

In this example scenario, you want to ensure the user administrator is created because this user is the default user to be assigned to the default administrator group. This user should already be created, as you are using it to access the account management section within ITNCM.

Under the **General** tab, you can see all the relevant information, such as user name, password, last name, and email address. There is also a **Groups** tab where you can assign groups to newly created users.

Assigning administrator user to administrator group


IBM Tivoli Netcool Configuration Manager - Mozilla Firefox: IBM Edition
File Edit View History Bookmarks Tools Help
IBM Tivoli Netcool Configuration ...
compliancevm.localdomain:7001/intelliden.jsp
Google
Tivoli. Netcool Configuration Manager
User Name: administrator
IBM.
Accounts
Account Administration
Groups New
administrator
Network_LAN_Team_Lead
Network_LAN_User
Network_LAN_User_2
observer
operator
Users New
administrator
chew_team_lead
ji
ji1
observer
operator
New User
General
Groups
*Required Fields
Create
Cancel
javascript:onAddSelectedGroups();

Groups:
Network_LAN_Team_Lead
Network_LAN_User
Network_LAN_User_2
observer
operator

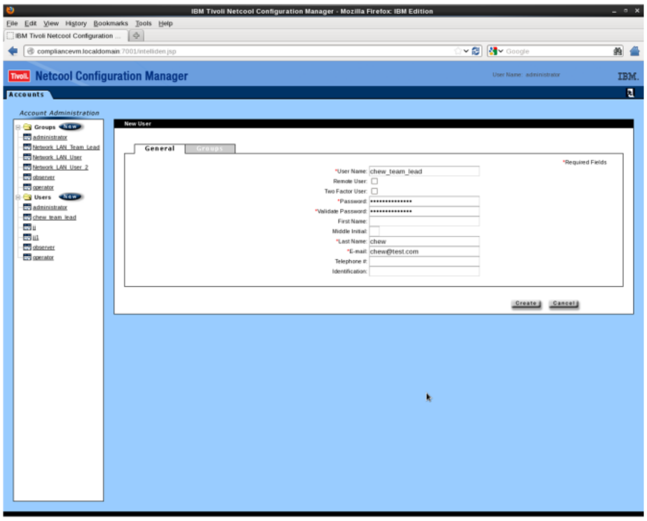
*Member of:
administrator

Configuring select user accounts with permission to approve unit of work

In the account management section, you see the groups that you created in previous steps. For the default administrator user and group, you can select the administrator group on the left pane under **Groups** and determine if the user administrator is already assigned to the group. You can select which group you want assigned to the administrator user when you create a user and assign a group to that user.

Creating a chew_team_lead user

1. Click the **New** button beside the **Users** folder icon
2. Enter a user name in the **User Name** field, for example, **chew_team_lead**
3. Enter a password and email address
4. Click the **Groups** tab



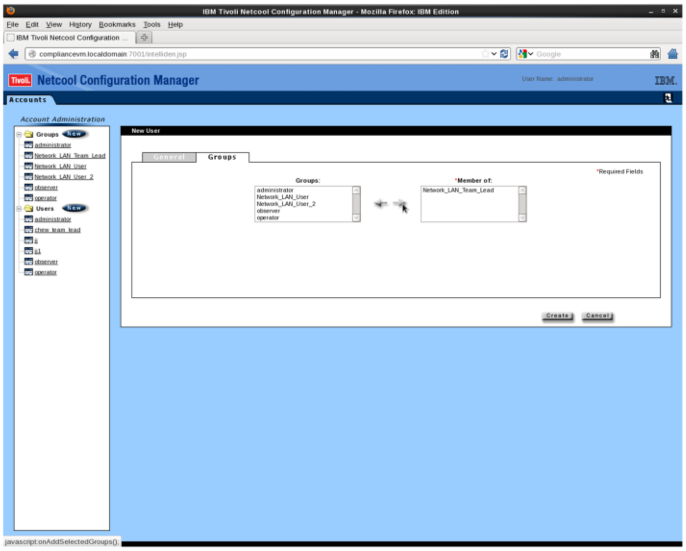
*Required Fields

*User Name: chew_team_lead
Remote User: □
Two Factor User: □
*Password: ***************
*Validate Password: ***************
First Name:
Middle Initial:
*Last Name: chew
*E-mail: chew@test.com
Telephone #:
Identification:

Select the **New** option beside the **Users** folder icon to create a user. In this example scenario, you want to ensure that the user **chew_team_lead** is created and assigned to the Network_LAN_Team_Lead group. Enter the relevant user name, password, last name, and email details, as noted in the **General** tab. You can enter whatever name or details that are relevant.

Assigning chew_team_lead user to a group

1. If not already logged in, log in to Netcool Configuration Manager Account Administration as **administrator**
2. Click the **Groups** tab
3. Click **Network_LAN_Team_Lead** in the **Groups** list**,** and click the right-facing arrow, to move the group to the **Member of** list
4. Click **Create**


IBM Tivoli Netcool Configuration Manager - Mozilla Firefox: IBM Edition
File Edit View History Bookmarks Tools Help
IBM Tivoli Netcool Configuration ...
compliancevm.localdomain:7001/intelliden.jsp
Google
Tivoli
Netcool Configuration Manager
User Name: administrator
IBM.
Accounts
Account Administration
Groups New
Users New
New User
General
Groups
Create
Cancel

Groups: administrator, Network_LAN_Team_Lead, Network_LAN_User, Network_LAN_User_2, observer, operator

Users: administrator, chew_team_lead, i, i1, observer, operator

*Required Fields

Groups:
administrator
Network_LAN_User
Network_LAN_User_2
observer
operator

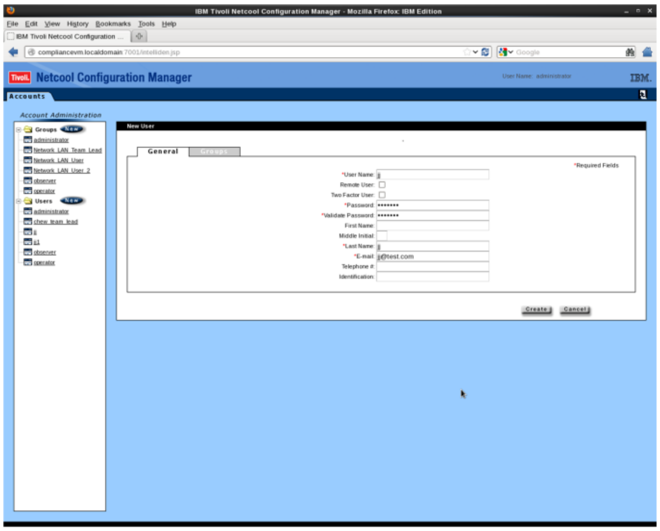
*Member of:
Network_LAN_Team_Lead

javascript:onAddSelectedGroups();

The Groups tab shown on this slide is where you can assign groups to new users. You select Network_LAN_Team_Lead as the group to be assigned to the new user of chew_team_lead. This user will be the senior user to which an administrator can assign privileges to approve or reject Unit of Work tasks. Click the Create button to create the user. You can see the user name in the left pane of your account management view.

Creating a sample user

1. If not already logged in, log in to Netcool Configuration Manager Account Administration as **administrator**
2. Click the **New** button beside the **Users** folder icon
3. Enter a user name in the **User Name** field; for example, **jj**
4. Enter a password and email address



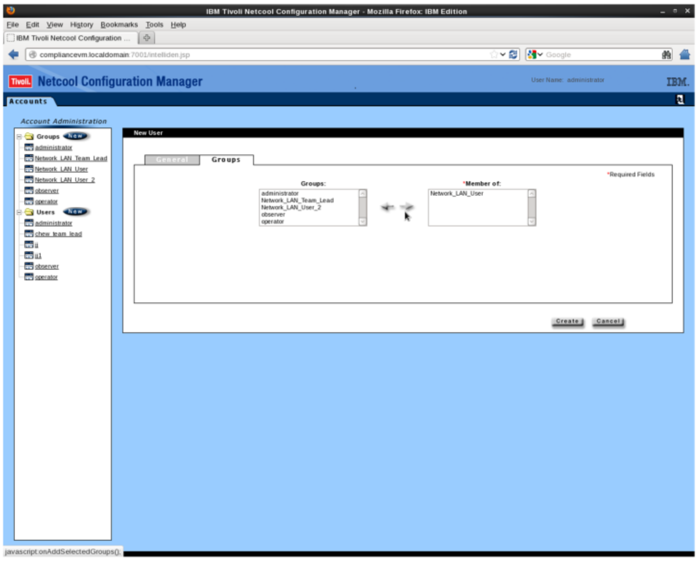
*Required Fields

*User Name:	jj
Remote User:	□
Two Factor User:	□
*Password:	********
*Validate Password:	********
First Name:	
Middle Initial:	
*Last Name:	jj
*E-mail:	jj@test.com
Telephone #:	
Identification:	

In this example scenario, you want to ensure that the user jj is created and assigned to the Network_LAN_User group. Enter the relevant user name, password, last name, and email details as noted in the General tab. You can put in any relevant name or details that you prefer.

Sample: Assigning user to a group

1. Click the **Groups** tab
2. Click **Network_LAN_Team_Lead** in the **Groups** list**,** and click the right-facing arrow, to move the group to the **Member of** list
3. Click **Create** to assign jj to this group


IBM Tivoli Netcool Configuration Manager - Mozilla Firefox: IBM Edition
File Edit View History Bookmarks Tools Help
IBM Tivoli Netcool Configuration ...
compliancevm.localdomain:7001/intelliden.jsp
Google
Tivoli. Netcool Configuration Manager
User Name: administrator
IBM.
Accounts
Account Administration
Groups New
administrator
Network_LAN_Team_Lead
Network_LAN_User
Network_LAN_User_2
observer
operator
Users New
administrator
chew_team_lead
jj
jj1
observer
operator
New User
General
Groups
*Required Fields
Create
Cancel
javascript:onAddSelectedGroups();

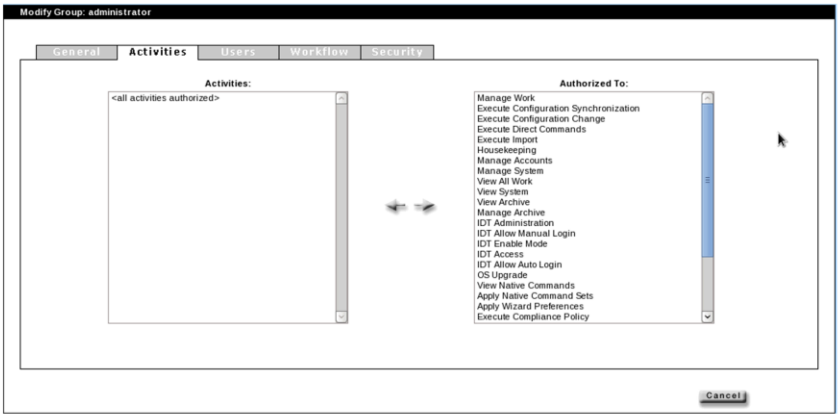
Groups: administrator, Network_LAN_Team_Lead, Network_LAN_User_2, observer, operator

*Member of: Network_LAN_User

The **Groups** tab, which you see on this slide, is where you can assign groups to a new user. In this example, you select **Network_LAN_User** as the group to be assigned to the new user jj. This sample user has rights to submit Unit of Work tasks (UOWs), but requires a senior user or administrator to approve (or reject) these tasks. They are ones that are executed against devices. Click the **Create** button to assign jj to this group.

Modifying administrator group authorizations

On the **Activities** tab, assign relevant activities to the administrator group



Activities:

<all activities authorized>

Authorized To:

Manage Work
Execute Configuration Synchronization
Execute Configuration Change
Execute Direct Commands
Execute Import
Housekeeping
Manage Accounts
Manage System
View All Work
View System
View Archive
Manage Archive
IDT Administration
IDT Allow Manual Login
IDT Enable Mode
IDT Access
IDT Allow Auto Login
OS Upgrade
View Native Commands
Apply Native Command Sets
Apply Wizard Preferences
Execute Compliance Policy

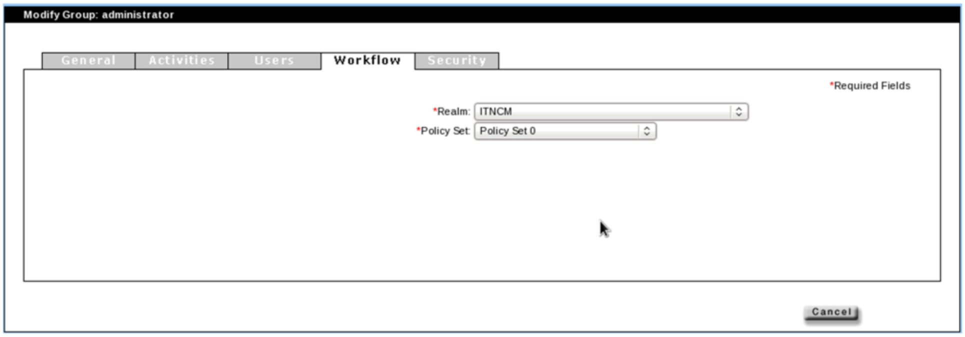
Now that you have all the necessary groups, you can assign relevant activities to each of the three groups. The administrator group is created by default. You start with the administrator group and assign activities to this group. By default, all the activities are already assigned to the administrator group because it is the default super user group.

To assign activities, you log in to the ITNCM as user administrator and select the **Account Management** option. You can select whichever group you want to display the notification tabs for.

For more information about each activity, see the "Administering users" section of the online documentation for IBM Tivoli Netcool Configuration Manager.

Configuring administrator group workflow realm and workflow policy set

1. On the **Workflow** tab, in the **Realm** field, select the realm that the group has access to
2. From the **Policy Set** list, select **Policy Set 0**



Modify Group: administrator

*Required Fields

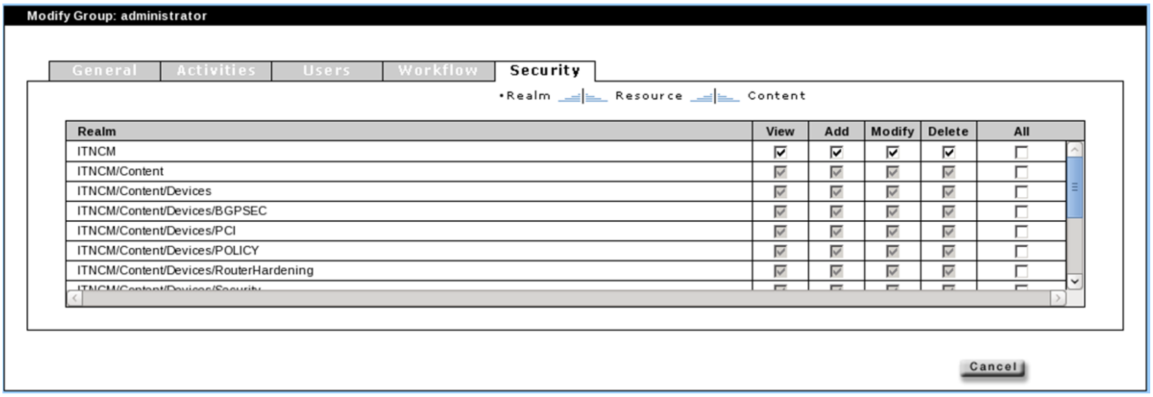
*Realm: ITNCM

*Policy Set: Policy Set 0

This slide depicts the workflow definition, which is typically for the administrator group. The realm is specific to your specific setup. In this example, ITNCM is the highest level of realm, with all other subrealms under it. Users who are assigned to this group have access to all realms that are defined in this ITNCM system. Be sure that the selection for Policy Set is zero.

Configuring administrator group security settings for individual realms

Specify **View**, **Add**, **Modify**, and **Delete** options for appropriate realms



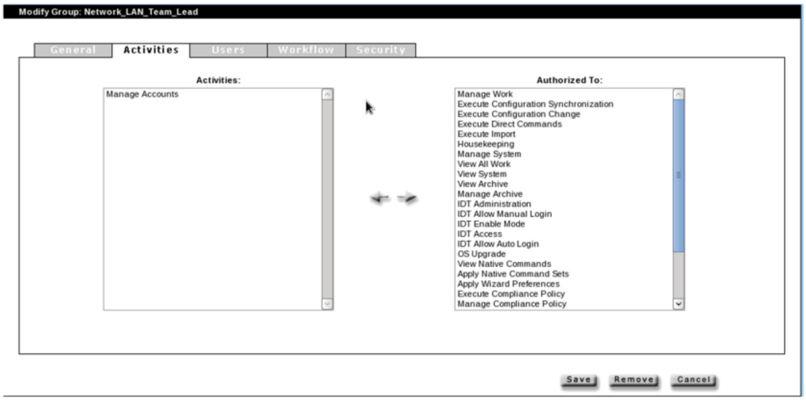
Modify Group: administrator

Realm	View	Add	Modify	Delete	All
ITNCM	☑	☑	☑	☑	☐
ITNCM/Content	☑	☑	☑	☑	☐
ITNCM/Content/Devices	☑	☑	☑	☑	☐
ITNCM/Content/Devices/BGPSEC	☑	☑	☑	☑	☐
ITNCM/Content/Devices/PCI	☑	☑	☑	☑	☐
ITNCM/Content/Devices/POLICY	☑	☑	☑	☑	☐
ITNCM/Content/Devices/RouterHardening	☑	☑	☑	☑	☐
ITNCM/Content/Devices/Security	☑	☑	☑	☑	☐

This slide depicts the security option, which shows the View, Add, Modify, Delete options for all realms that are defined in your IBM Tivoli Netcool Configuration Manager application. Because this is the administrator group, all permissions for all realms are selected.

Modifying Network_LAN_Team_Lead group activity authorizations

Select activities in the **Activities** list and move them to the **Authorized To** list



Activities:

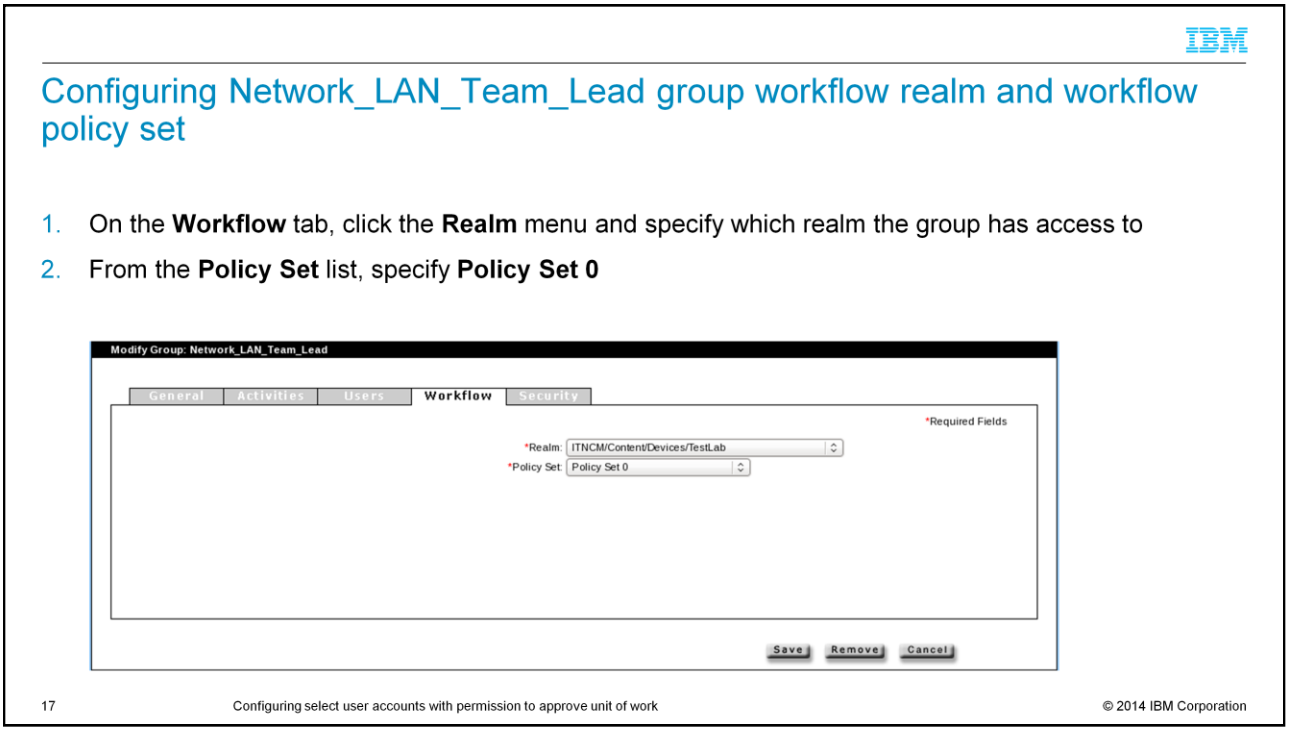
Manage Accounts

Authorized To:

Manage Work
Execute Configuration Synchronization
Execute Configuration Change
Execute Direct Commands
Execute Import
Housekeeping
Manage System
View All Work
View System
View Archive
Manage Archive
IDT Administration
IDT Allow Manual Login
IDT Enable Mode
IDT Access
IDT Allow Auto Login
OS Upgrade
View Native Commands
Apply Native Command Sets
Apply Wizard Preferences
Execute Compliance Policy
Manage Compliance Policy

Now you assign relevant activities to each of the three groups, starting with the Network_LAN_Team_Lead group. In this example, all activities except the Manage Accounts activity are assigned. The activities you want to allow this group access to is based on your own security policies. You can remove or add activities in this group as needed. However, the Manage Work option is required if the users that you assign to these groups will share the load from the administrator to approve UOWs for certain realms or devices.

For more information about each activity, see the online documentation for IBM Tivoli Netcool Configuration Manager.



Configuring Network_LAN_Team_Lead group workflow realm and workflow policy set

1. On the **Workflow** tab, click the **Realm** menu and specify which realm the group has access to
2. From the **Policy Set** list, specify **Policy Set 0**

Modify Group: Network_LAN_Team_Lead

*Required Fields

*Realm: ITNCM/Content/Devices/TestLab

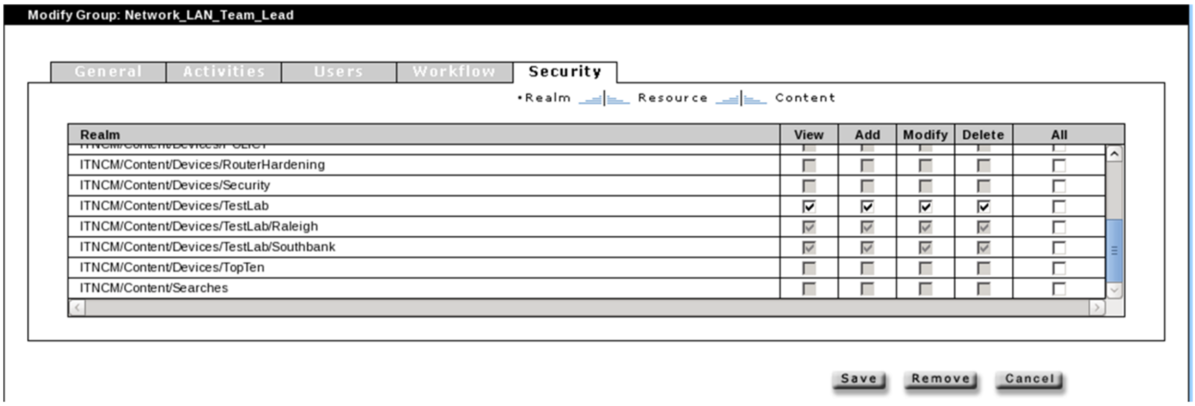
*Policy Set: Policy Set 0

On this slide, you see the workflow definition for the Network_LAN_Team_Lead group. Because this group is not the default administrator group, you must select the specific realm. This realm indicates which permissions and access you grant to the group and the users who are assigned to the group. In this example, ITNCM/Content/Devices/TestLab is the specific realm assigned to this group. All other subrealms under it get access.

You can select only the subrealms under a main subrealm, if you want. However, in the current version of IBM Tivoli Netcool Configuration Manager, under the Workflow and Security tabs, you must ensure that you select the same specific realm levels to allow access to the new group. If not, then the users assigned to this group will not have access to approve UOW tasks that are submitted for devices within the specific realm.

Configuring Network_LAN_Team_Lead group security settings for individual realms

Specify **View**, **Add**, **Modify**, and **Delete** options for appropriate realms

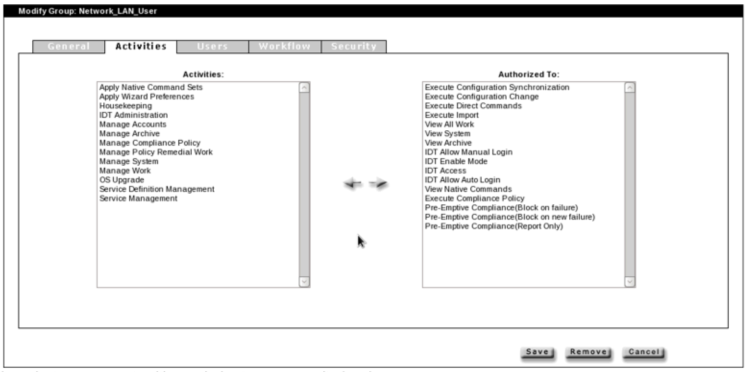


Realm	View	Add	Modify	Delete	All
ITNCM/Content/Devices/RouterHardening	□	□	□	□	□
ITNCM/Content/Devices/Security	□	□	□	□	□
ITNCM/Content/Devices/TestLab	☑	☑	☑	☑	□
ITNCM/Content/Devices/TestLab/Raleigh	☑	☑	☑	☑	□
ITNCM/Content/Devices/TestLab/Southbank	☑	☑	☑	☑	□
ITNCM/Content/Devices/TopTen	□	□	□	□	□
ITNCM/Content/Searches	□	□	□	□	□

On the **Security** tab for the network_LAN_Team_Lead group, you see that the group is assigned to the ITNCM/Content/Devices/TestLab realm. The users who are assigned to this group can approve UOW jobs that are submitted for devices that are defined within this realm.

Modifying Network_LAN_User user group activity authorizations

Select relevant activities in the **Activities** list for Network_LAN_User group and move them to the **Authorized To** list



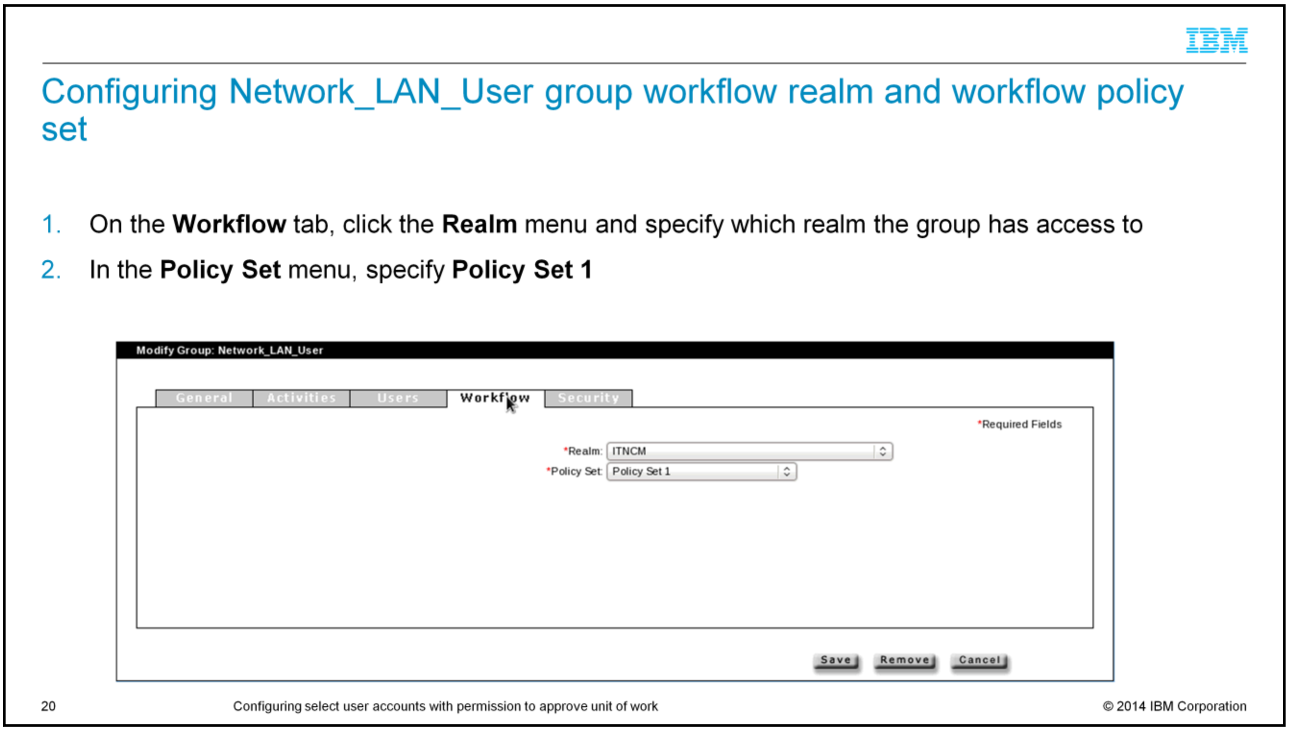
Activities:

Apply Native Command Sets
Apply Wizard Preferences
Housekeeping
IDT Administration
Manage Accounts
Manage Archive
Manage Compliance Policy
Manage Policy Remedial Work
Manage System
Manage Work
OS Upgrade
Service Definition Management
Service Management

Authorized To:

Execute Configuration Synchronization
Execute Configuration Change
Execute Direct Commands
Execute Import
View All Work
View System
View Archive
IDT Allow Manual Login
IDT Enable Mode
IDT Access
IDT Allow Auto Login
View Native Commands
Execute Compliance Policy
Pre-Emptive Compliance(Block on failure)
Pre-Emptive Compliance(Block on new failure)
Pre-Emptive Compliance(Report Only)

In this example, you assigned a reduced number of activities to the user who requires access only to run specific components or Unit of Work tasks. Again, the activities for this group access is based on your own security policies. You can remove or add activities, as needed.



IBM

Configuring Network_LAN_User group workflow realm and workflow policy set

1. On the **Workflow** tab, click the **Realm** menu and specify which realm the group has access to
2. In the **Policy Set** menu, specify **Policy Set 1**

Modify Group: Network_LAN_User

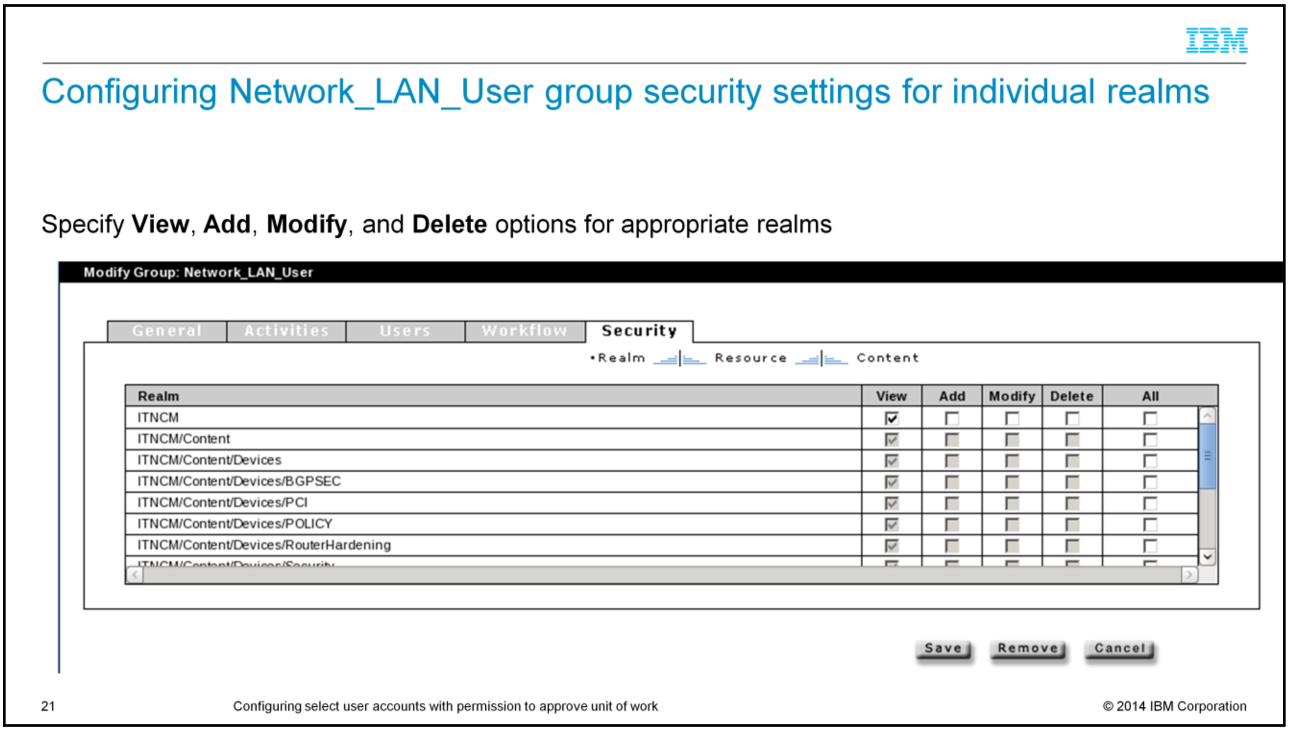
*Required Fields

*Realm: ITNCM

*Policy Set: Policy Set 1

20 Configuring select user accounts with permission to approve unit of work © 2014 IBM Corporation

For the workflow definition for the Network_LAN_User group, you must select the specific realm to grant permissions and access to the users in this group. In this example, the highest realm of ITNCM is chosen as the realm. The policy set for this group is **1** and not zero, like the two previous groups. The users in this group must have approvals for any tasks that they must complete.



Configuring Network_LAN_User group security settings for individual realms

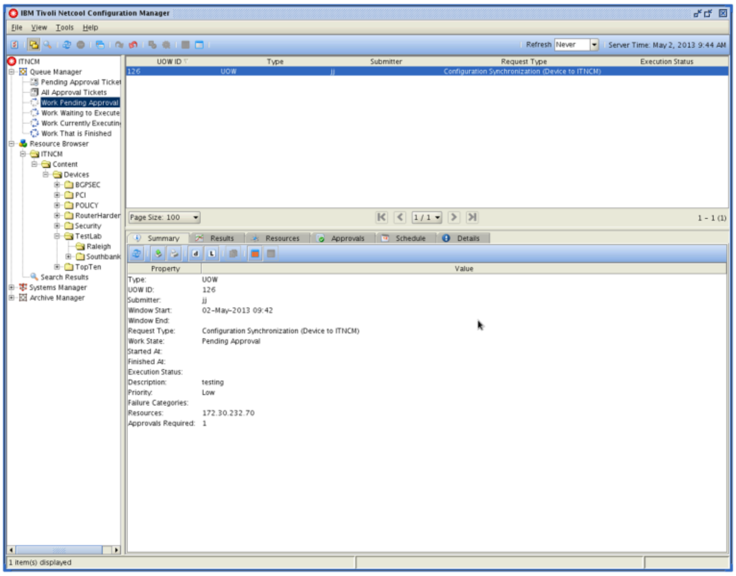
Specify **View**, **Add**, **Modify**, and **Delete** options for appropriate realms

Realm	View	Add	Modify	Delete	All
ITNCM	☑	□	□	□	□
ITNCM/Content	☑	□	□	□	□
ITNCM/Content/Devices	☑	□	□	□	□
ITNCM/Content/Devices/BGPSEC	☑	□	□	□	□
ITNCM/Content/Devices/PCI	☑	□	□	□	□
ITNCM/Content/Devices/POLICY	☑	□	□	□	□
ITNCM/Content/Devices/RouterHardening	☑	□	□	□	□
ITNCM/Content/Devices/Security					

21 Configuring select user accounts with permission to approve unit of work © 2014 IBM Corporation

For the Network_LAN_User group, the users have view-only access in all realms and subrealms. These users cannot modify anything.

UOW in pending approval status

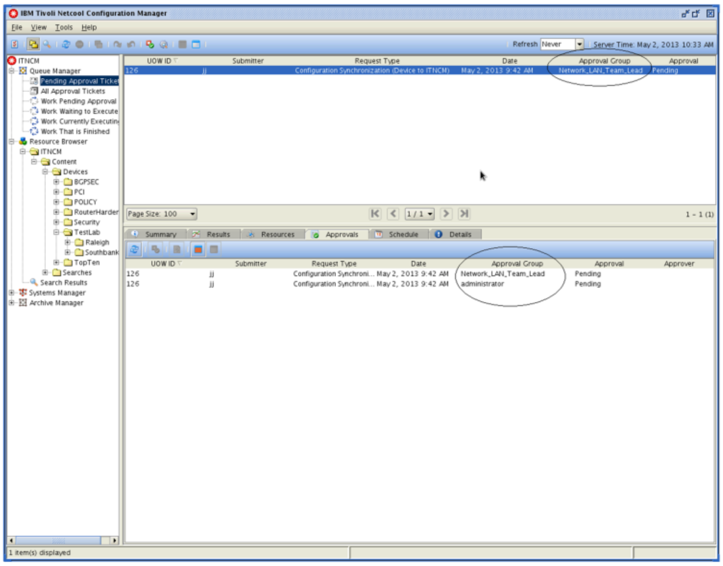


UOW ID	Type	Submitter	Request Type	Execution Status
126	UOW	jj	Configuration Synchronization (Device to ITNCM)	

Property	Value
Type:	UOW
UOW ID:	126
Submitter:	jj
Window Start:	02-May-2013 09:42
Window End:	
Request Type:	Configuration Synchronization (Device to ITNCM)
Work State:	Pending Approval
Started At:	
Finished At:	
Execution Status:	
Description:	testing
Priority:	Low
Failure Categories:	
Resources:	172.30.232.70
Approvals Required:	1

In an IBM Tivoli Netcool Configuration Manager production environment, you have multiple users. As an administrator of an IBM Tivoli Netcool Configuration Manager system, managing the numerous user requests for hundreds of different devices can be a tedious task. Administrators must ensure that up-to-date security and control exist for all network devices. The administrator can create and delegate multiple senior users to manage different subrealms or different devices for more effective review and approval of submitted UOW jobs or tasks. On this slide, a Configuration Synchronization Unit of Work (UOW) is performed as the user jj. The work state depicts **Pending Approval**. This work state relates to the policy set of **1** that was set for the Network_LAN_Users group, to which the user jj belongs. This user must not run any tasks without the appropriate approvals. Remember, the user permissions are based on the activities assigned earlier, and are based on your own security policies.

Viewing the approval groups



Refresh: Never | Server Time: May 2, 2013 10:33 AM

UOW ID	Submitter	Request Type	Date	Approval Group	Approval
126	jj	Configuration Synchronization (Device to ITNCM)	May 2, 2013 9:42 AM	Network_LAN_Team_Lead	Pending

Page Size: 100

1 - 1 (1)

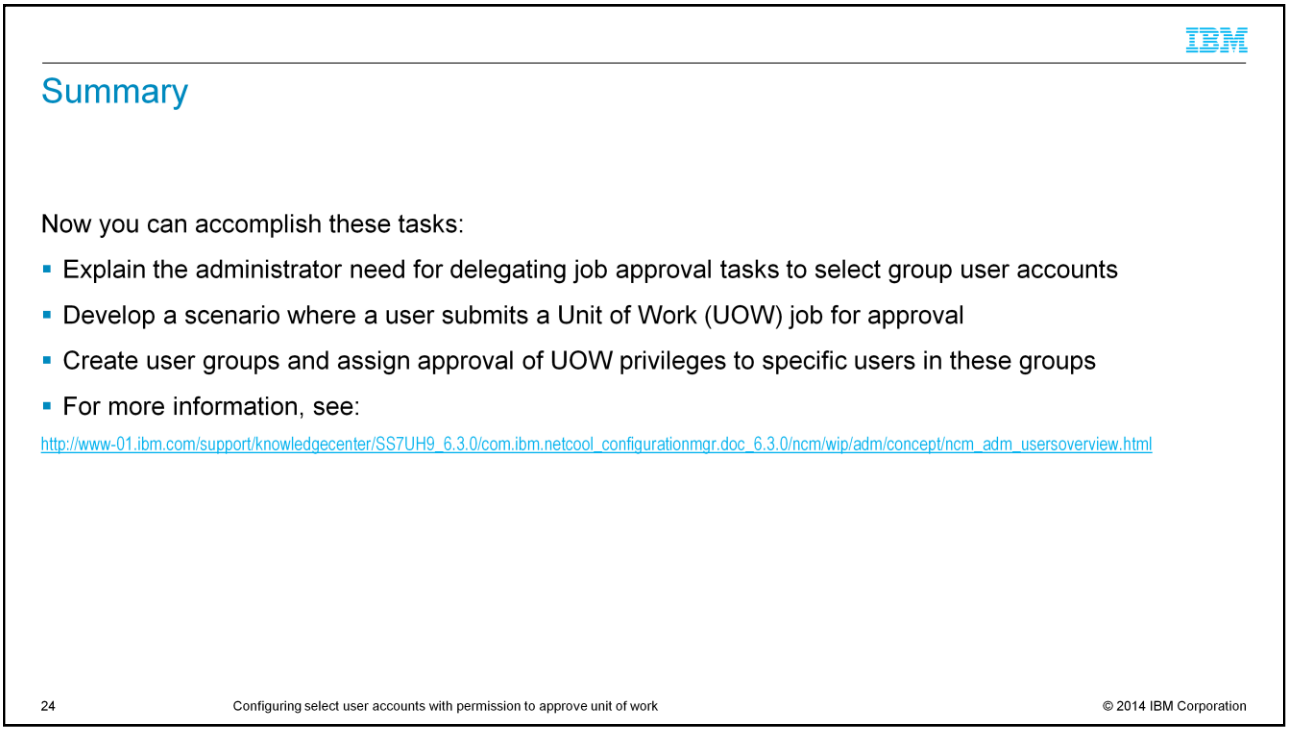
UOW ID	Submitter	Request Type	Date	Approval Group	Approval	Approver
126	jj	Configuration Synchroni...	May 2, 2013 9:42 AM	Network_LAN_Team_Lead	Pending	
126	jj	Configuration Synchroni...	May 2, 2013 9:42 AM	administrator	Pending	

1 item(s) displayed

After the user jj submits a UOW, and it enters a state of pending approval, both the administrator and Chew_Team_Lead users can see jj's submitted UOW when they log in to the IBM Tivoli Netcool Configuration Manager GUI. In this example, both of these users can approve or reject because they were assigned all the necessary activities that control approvals.

The users who are assigned to either the network_LAN_Team_Lead group or administrator group, have the two Approval_Groups present on the **Approvals** tab of the **Work Pending Approval** section. Either senior user can right-click the UOW and approve or reject the job.

If you want to assign the approvals of UOW tasks to senior users other than the administrator, then you can remove the manage work activity from the administrator group under the Account Management section. To do that, you select the administrator group, and on the **Activities** tab, you remove the relevant activity. Then, only those specific senior users, who are assigned to the specific group for that particular realm or subrealm, can approve or reject a job that a user submits.



IBM

Summary

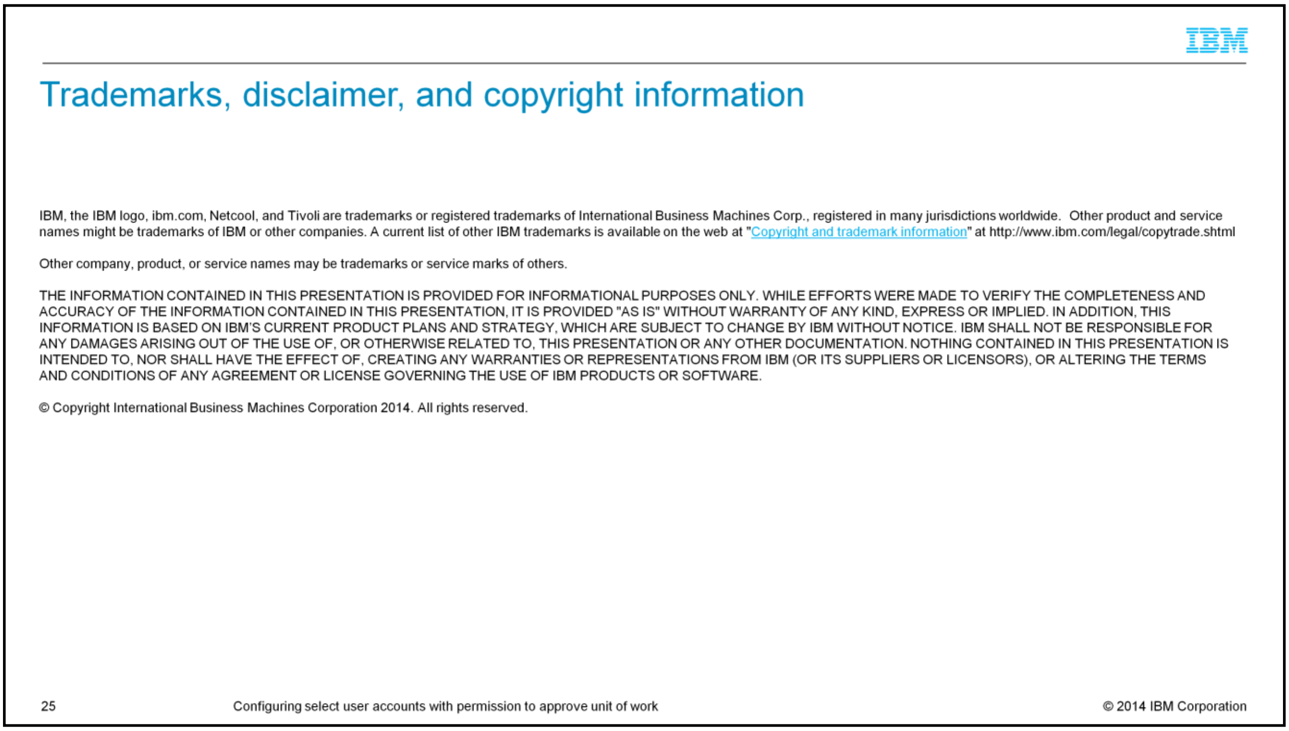
Now you can accomplish these tasks:

- Explain the administrator need for delegating job approval tasks to select group user accounts
- Develop a scenario where a user submits a Unit of Work (UOW) job for approval
- Create user groups and assign approval of UOW privileges to specific users in these groups
- For more information, see:

http://www-01.ibm.com/support/knowledgecenter/SS7UH9_6.3.0/com.ibm.netcool_configurationmgr.doc_6.3.0/ncm/wip/adm/concept/ncm_adm_usersoverview.html

24 Configuring select user accounts with permission to approve unit of work

Now you can set up specific user account privileges, set up different groups to approve Unit of Work (UOW) job tasks for users, and configure these accounts so that the approvers have the necessary privileges to approve UOW jobs.



Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.