IBM Workload Deployer

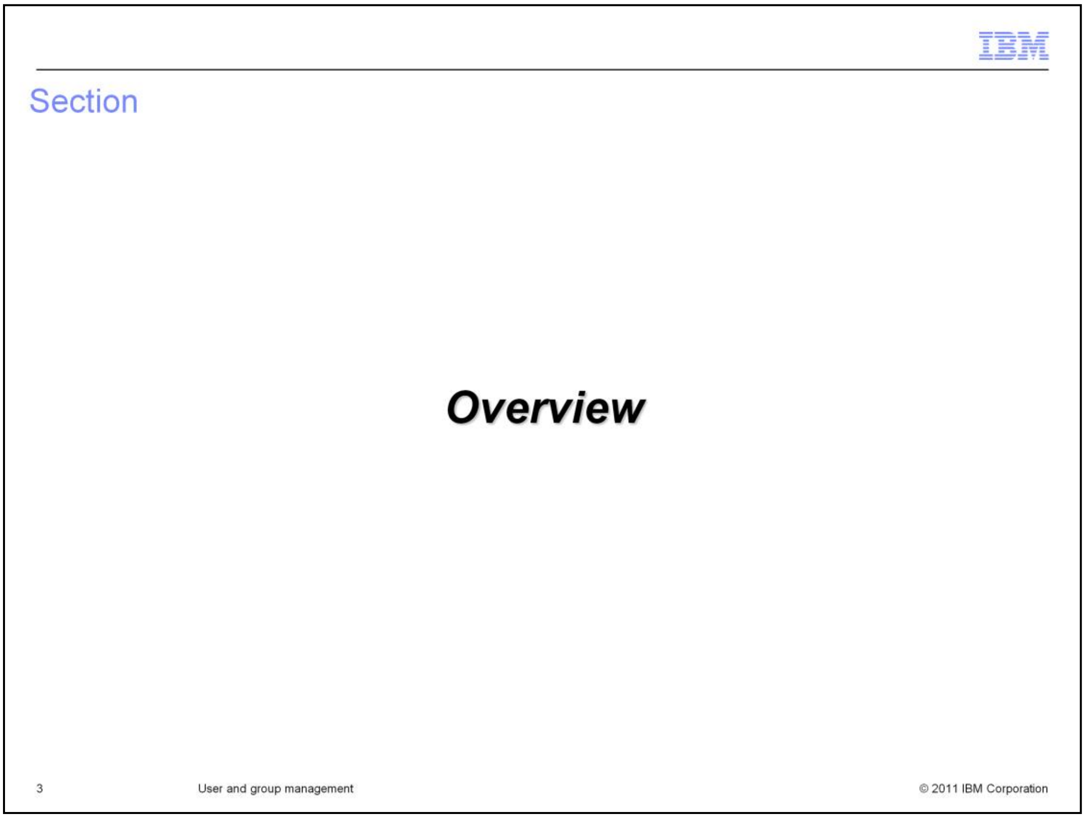
User and group management

This presentation provides an overview of the user and group management security features of the IBM Workload Deployer.

Table of contents

- Overview
- User management
- Group management

This presentation will cover the management of users and groups in order to effectively secure your Workload Deployer Appliance.



Section

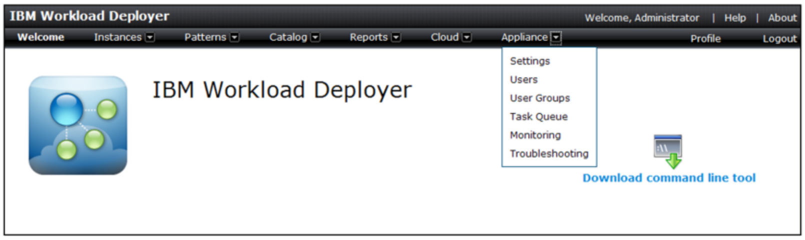
Overview

3 User and group management © 2011 IBM Corporation

This section of the presentation provides an overview of the users and user groups features of the Workload Deployer Appliance.

Overview

- A user account allows an individual to access the IBM Workload Deployer
- The users feature of Workload Deployer allows you to define individual users in order to create new accounts
- The user groups feature of Workload Deployer allows you to group user accounts into logical sets
- Users and user groups are provided so that you can manage the permissions set for each individual for the IBM Workload Deployer



A user account is required to access the Workload Deployer Appliance. The users and user groups feature of WebSphere Deployer allows you to create individual user accounts and put them together into logical groups. These features allow you to manage the level of access for each individual as a security mechanism. Also, Workload Deployer user activity can be tracked for audit purposes.

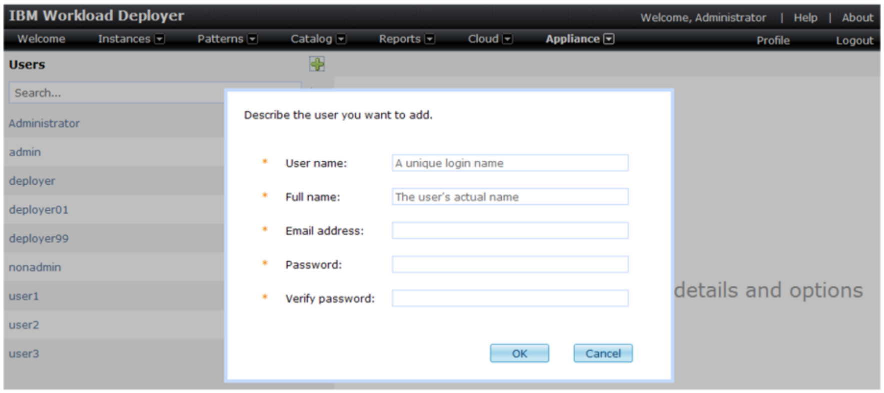
Section

User management

This section will cover setting up and managing Workload Deployer users.

Administrator creates new user account

- Administrator creates a user account and an initial password for a new user
- New user will receive user ID and password by way of email
- New user can then change his password



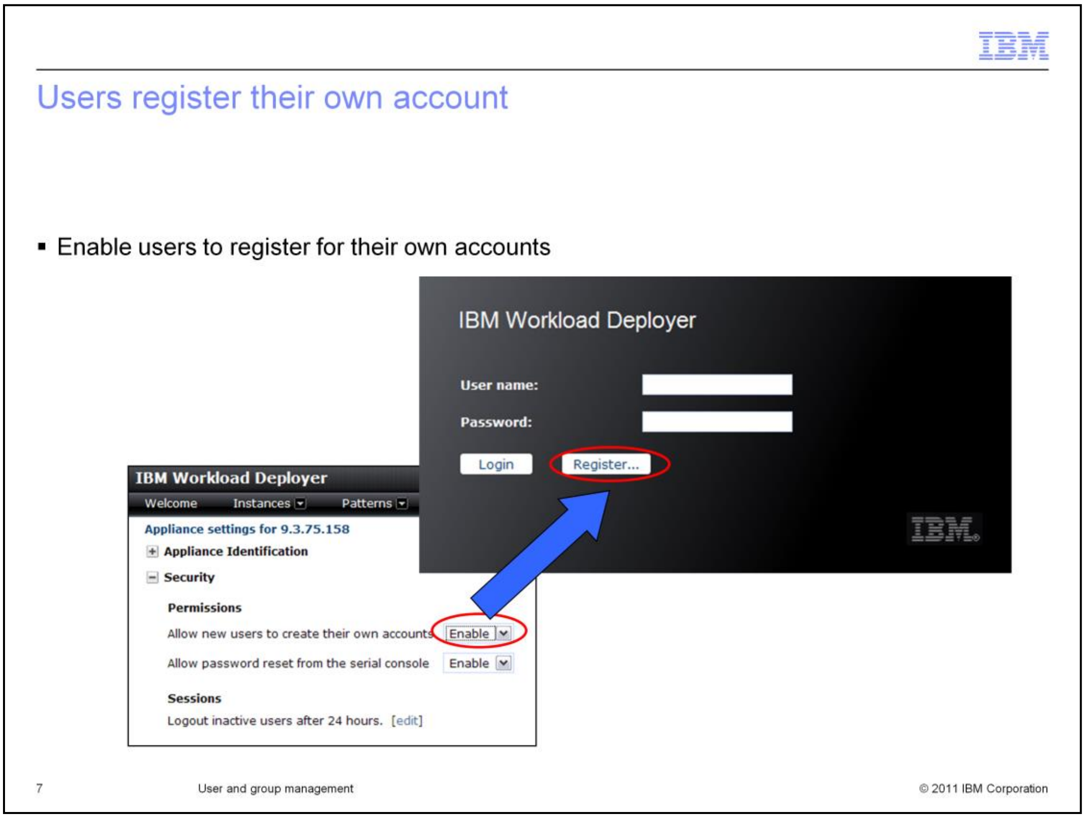
Describe the user you want to add.

- * User name: A unique login name
- * Full name: The user's actual name
- * Email address:
- * Password:
- * Verify password:

OK Cancel

A user account can be created by an administrator by navigating to the **Users** panel from the **Appliance** menu at the top of the Workload Deployer web console. Then click the add icon to begin adding a new user.

Creating the user account is a two step process. You first need to supply basic information such as user name, full name, password, and an email address. The e-mail address is used to send the user his or her initial password and other Workload Deployer notifications, such as notification of a deployment. The second part of user creation is to assign the user permissions which are discussed in detail in the “**Permissions**” presentation.



Users register their own account

- Enable users to register for their own accounts

Appliance settings for 9.3.75.158

⊞ Appliance Identification

⊟ Security

Permissions

Allow new users to create their own accounts: Enable

Allow password reset from the serial console: Enable

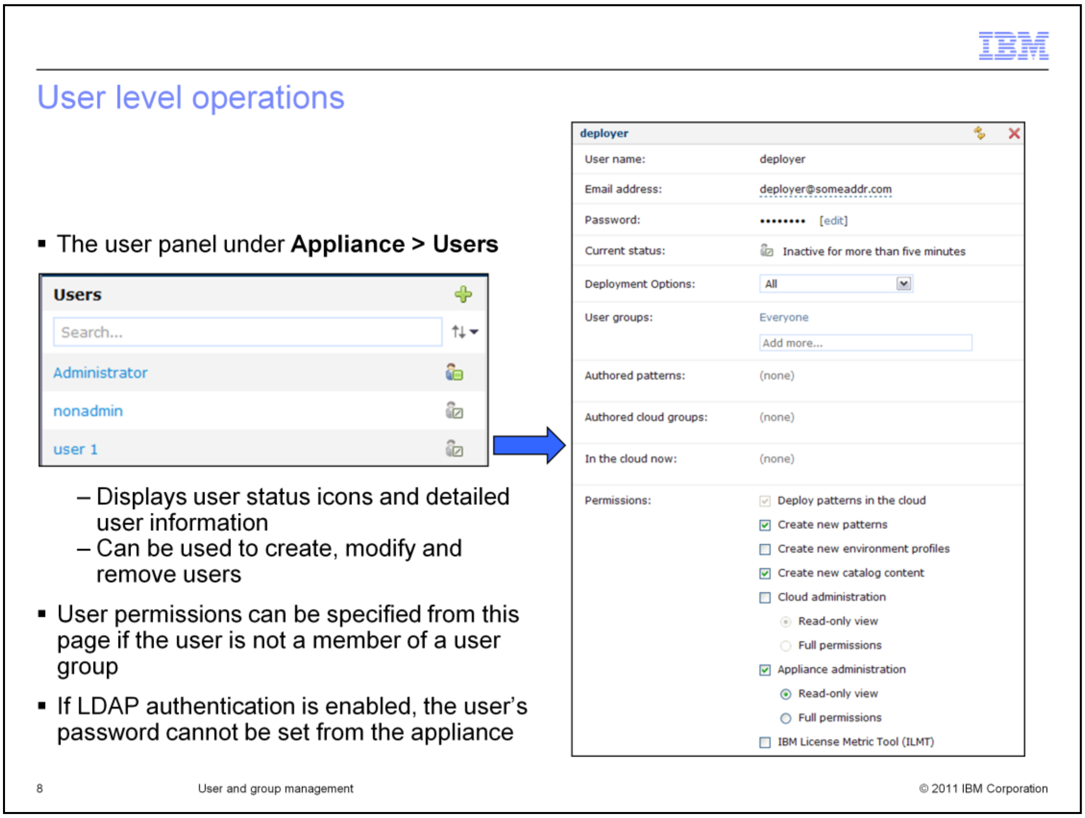
Sessions

Logout inactive users after 24 hours. [edit]

7 User and group management © 2011 IBM Corporation

There are two ways to create a user account. Either an administrator can create the account, as you have seen in the prior slide, or users can create their own accounts. In order to allow the users to create their own account, you must activate this feature. To activate this feature, navigate to the "**Settings**" panel from the menu bar at the top of the Workload Deployer web console. Then expand the "**Security**" section and select "**Enable**" next to "**Allow new users to create their own accounts**".

This will add a "**Register**" button to the initial log in screen. Any user is then able to create an account and is assigned the default deploy patterns permission. If the user requires additional permissions, an administrator will have to assign those permissions.



User level operations

- The user panel under **Appliance > Users**
  - Displays user status icons and detailed user information
  - Can be used to create, modify and remove users
- User permissions can be specified from this page if the user is not a member of a user group
- If LDAP authentication is enabled, the user's password cannot be set from the appliance

Users

Search...

Administrator

nonadmin

user 1

deployer

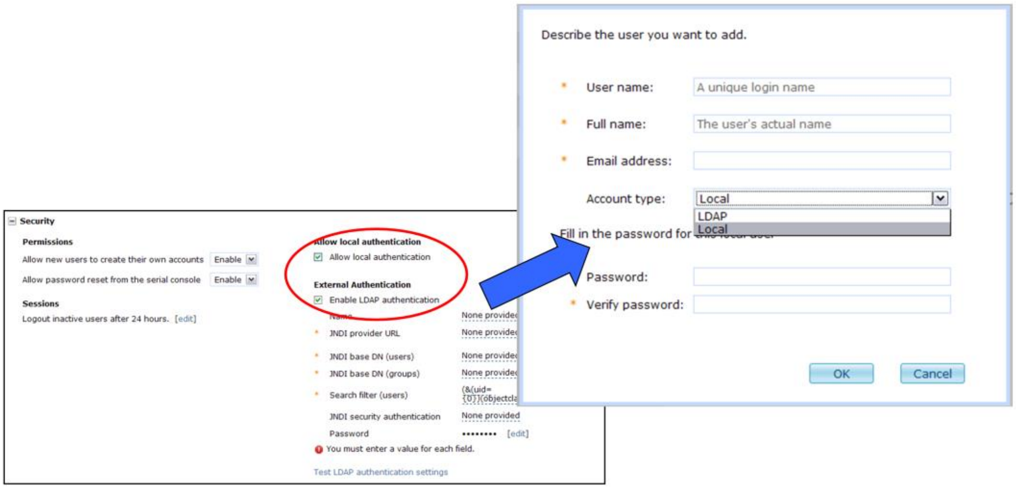
User name:	deployer
Email address:	deployer@someaddr.com
Password:	•••••••• [edit]
Current status:	Inactive for more than five minutes
Deployment Options:	All
User groups:	Everyone Add more...
Authored patterns:	(none)
Authored cloud groups:	(none)
In the cloud now:	(none)
Permissions:	☑ Deploy patterns in the cloud ☑ Create new patterns ☐ Create new environment profiles ☑ Create new catalog content ☐ Cloud administration ● Read-only view ○ Full permissions ☑ Appliance administration ● Read-only view ○ Full permissions ☐ IBM License Metric Tool (ILMT)

To manage users, navigate to the **User** panel by selecting "**Appliance**" then "**Users**" from the menu bar at the top of the Workload Deployer web console. From here you can create users. If you then click a username, the user's attributes are displayed like the screen capture shown here on the right. From this panel, you can view the user activity to determine whether the user was active in the last five minutes, inactive for more than five minutes, or not currently logged in. You can also modify and remove users as needed from here.

If a user is not a member of a user group, you can modify the permissions for this user to control the level of access that is assigned. If LDAP is enabled, the password field is not displayed during user creation and you will not be able to set or modify the user's password from the "**User**" panel.

Integrated local and LDAP user management support

- Define users in belonging to local or LDAP



⊟ Security

Permissions

Allow new users to create their own accounts: Enable

Allow password reset from the serial console: Enable

Sessions

Logout inactive users after 24 hours. [edit]

Allow local authentication

☑ Allow local authentication

External Authentication

☑ Enable LDAP authentication

Name	None providec
* JNDI provider URL	None providec
* JNDI base DN (users)	None providec
* JNDI base DN (groups)	None providec
* Search filter (users)	(&(uid={0})(objectcla
JNDI security authentication	None provided
Password	•••••••• [edit]

You must enter a value for each field.

Test LDAP authentication settings

Describe the user you want to add.

* User name:	A unique login name
* Full name:	The user's actual name
* Email address:	
Account type:	Local

Fill in the password for this local user

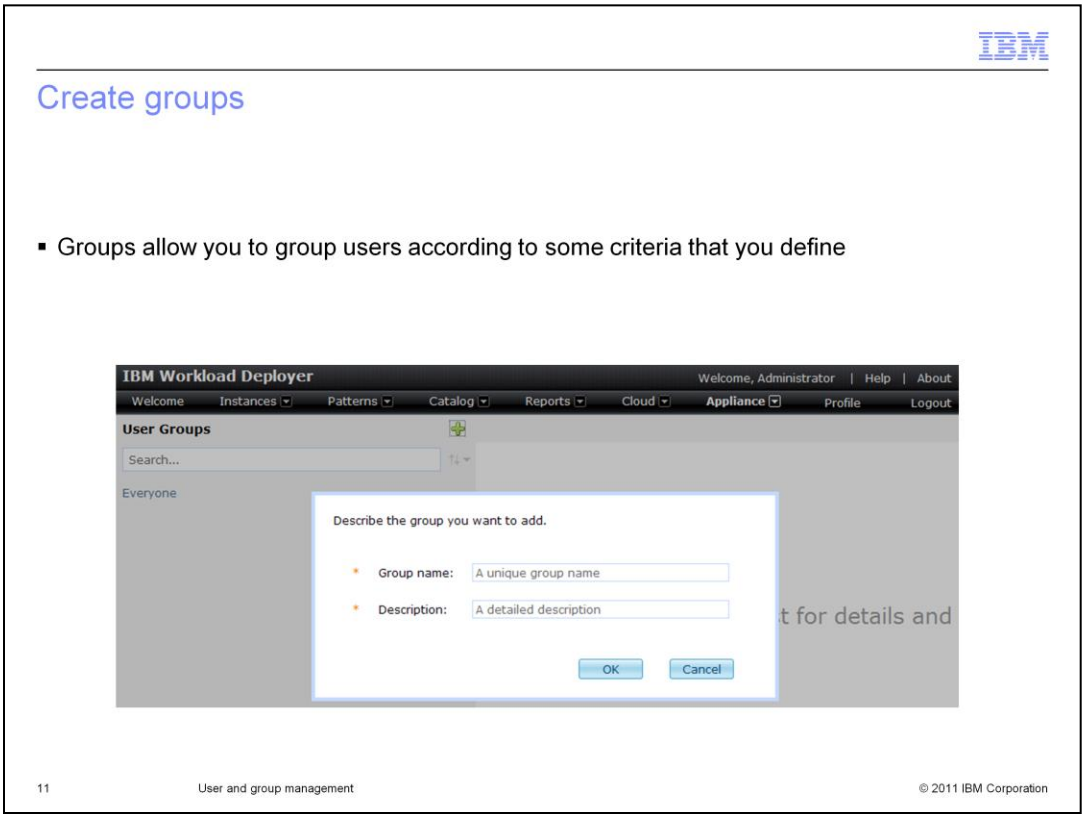
* Password:	
* Verify password:	

Workload Deployer supports local and LDAP user management integration. If both local and LDAP authentication are enabled, then you can define users that belong in either the LDAP server or local to the appliance. LDAP type users do not require a password because the password is stored in the LDAP server.

Section

Group management

This section will cover setting up and managing Workload Deployer user groups.



Create groups

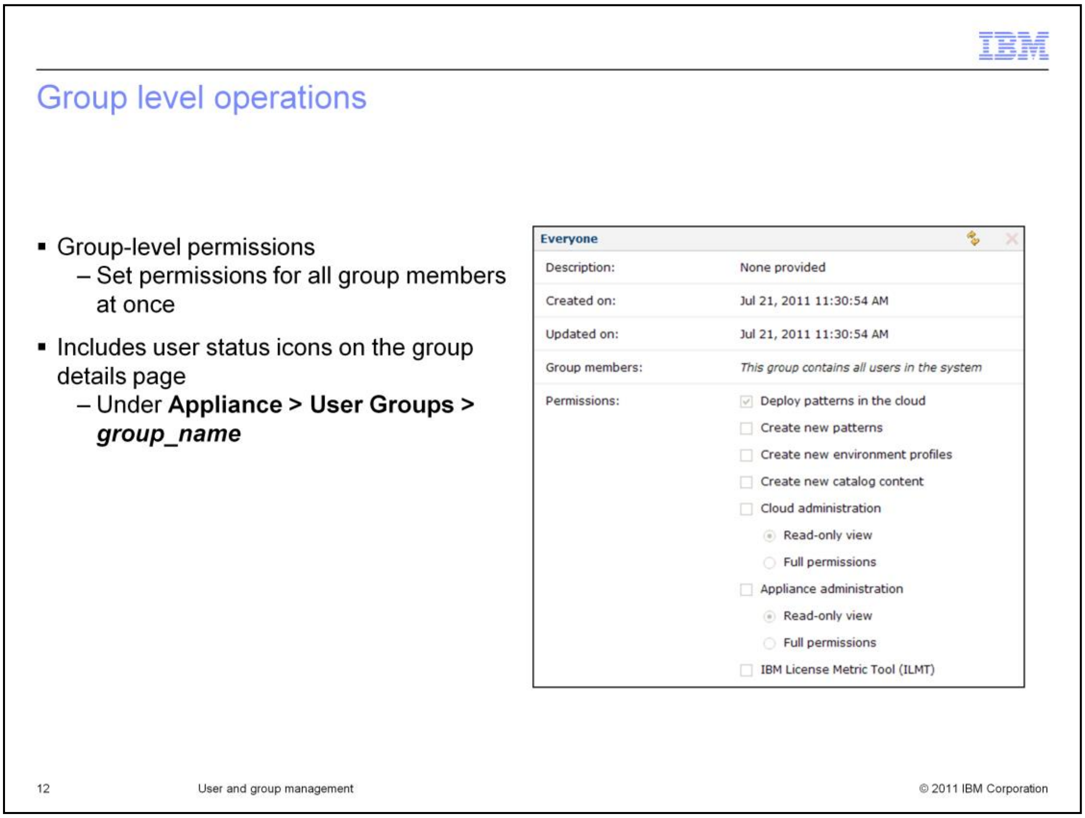
- Groups allow you to group users according to some criteria that you define

Describe the group you want to add.

* Group name: A unique group name

* Description: A detailed description

Groups allow you to group users by some criteria that you define. For example, you can group administrators together or group users by department. A group can be created by an administrator by navigating to the “**User groups**” panel from the **Appliance** menu at the top of the Workload Deployer web console. Then click the add icon to begin adding a new group.



Group level operations

- Group-level permissions
  - Set permissions for all group members at once
- Includes user status icons on the group details page
  - Under **Appliance > User Groups > *group_name***

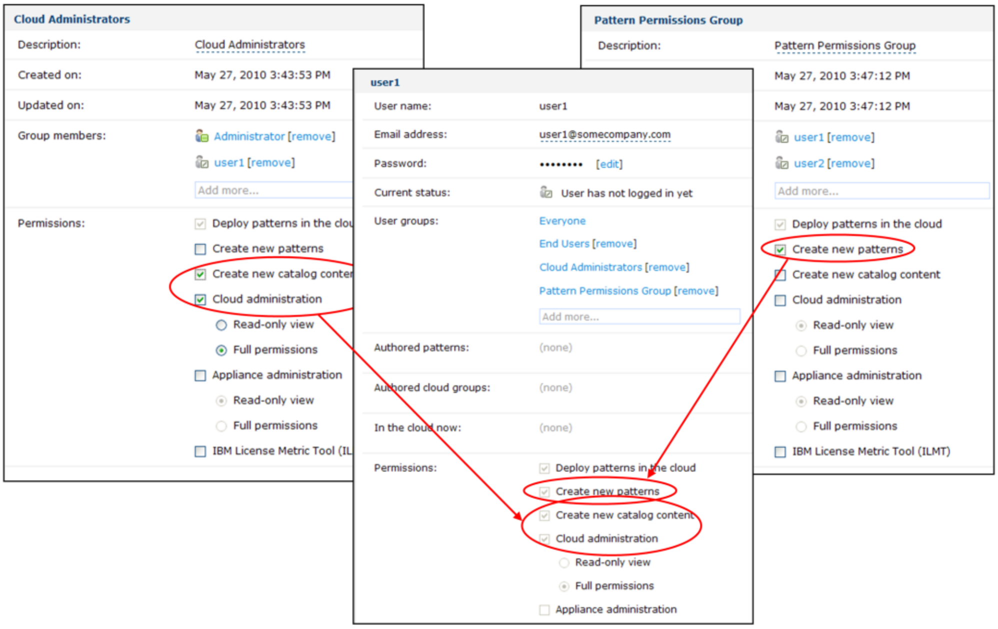
Everyone

Description:	None provided
Created on:	Jul 21, 2011 11:30:54 AM
Updated on:	Jul 21, 2011 11:30:54 AM
Group members:	*This group contains all users in the system*
Permissions:	☑ Deploy patterns in the cloud □ Create new patterns □ Create new environment profiles □ Create new catalog content □ Cloud administration ● Read-only view ○ Full permissions □ Appliance administration ● Read-only view ○ Full permissions □ IBM License Metric Tool (ILMT)

12 User and group management

After creating or modifying a user account, you can add the user to a user group by navigating to “**Appliance**” then “**User Groups**” from the web console. To use a user group, you must manually add users to the group in the “**Group members**” section. User status icons for group members are also available on the group page. When you set permissions for a group from the “**Permissions**” section of this panel, you will grant permissions for all members of the group at the same time. Once a user is a member of a group, you will no longer be able to set permissions from the “**Users**” panel. Also, if any permissions were set before adding a user to a group, they will be reset to the group permissions set.

User in multiple user groups



Cloud Administrators

Description: Cloud Administrators

Created on: May 27, 2010 3:43:53 PM

Updated on: May 27, 2010 3:43:53 PM

Group members: Administrator [remove]
user1 [remove]
Add more...

Permissions:
- ☑ Deploy patterns in the clou
- ☐ Create new patterns
- ☑ Create new catalog conte
- ☑ Cloud administration
  - ○ Read-only view
  - ● Full permissions
- ☐ Appliance administration
  - ● Read-only view
  - ○ Full permissions
- ☐ IBM License Metric Tool (IL

user1

User name: user1

Email address: user1@somecompany.com

Password: •••••••• [edit]

Current status: User has not logged in yet

User groups: Everyone
End Users [remove]
Cloud Administrators [remove]
Pattern Permissions Group [remove]
Add more...

Authored patterns: (none)

Authored cloud groups: (none)

In the cloud now: (none)

Permissions:
- ☑ Deploy patterns in the cloud
- ☑ Create new patterns
- ☑ Create new catalog content
- ☑ Cloud administration
  - ○ Read-only view
  - ● Full permissions
- ☐ Appliance administration

Pattern Permissions Group

Description: Pattern Permissions Group

May 27, 2010 3:47:12 PM

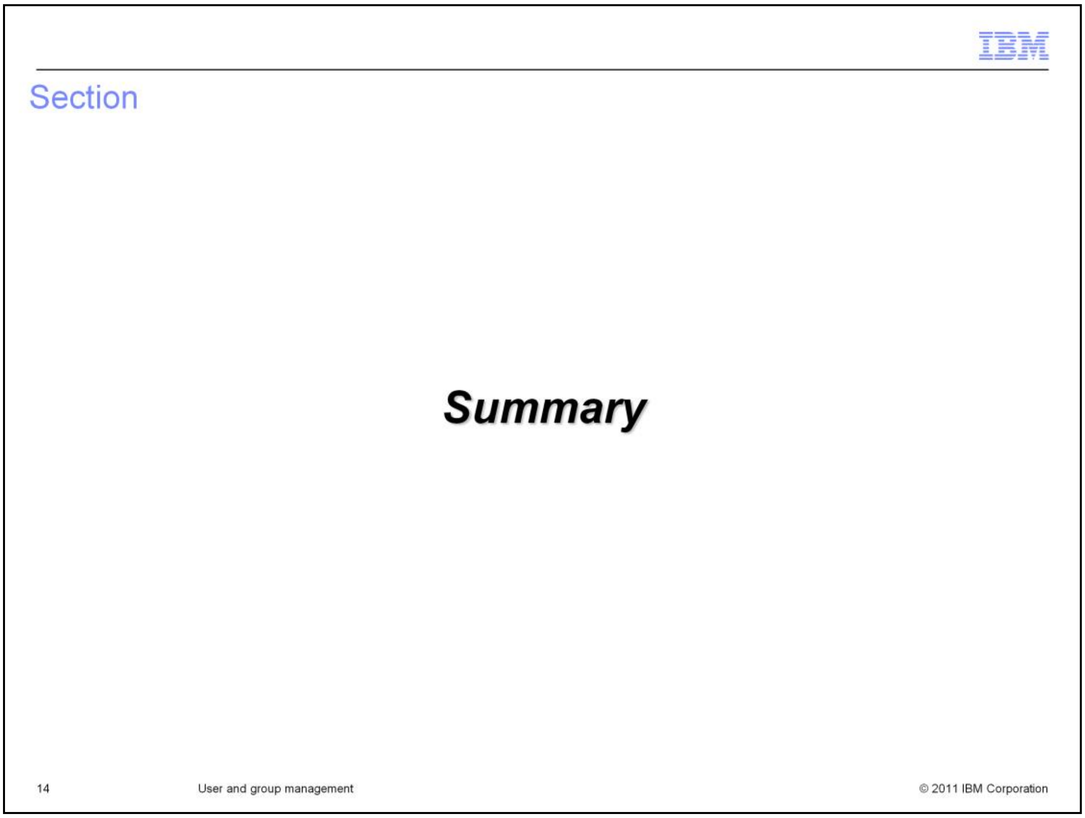
May 27, 2010 3:47:12 PM

user1 [remove]
user2 [remove]
Add more...

- ☑ Deploy patterns in the cloud
- ☑ Create new patterns
- ☐ Create new catalog content
- ☐ Cloud administration
  - ● Read-only view
  - ○ Full permissions
- ☐ Appliance administration
  - ● Read-only view
  - ○ Full permissions
- ☐ IBM License Metric Tool (ILMT)

13 User and group management © 2011 IBM Corporation

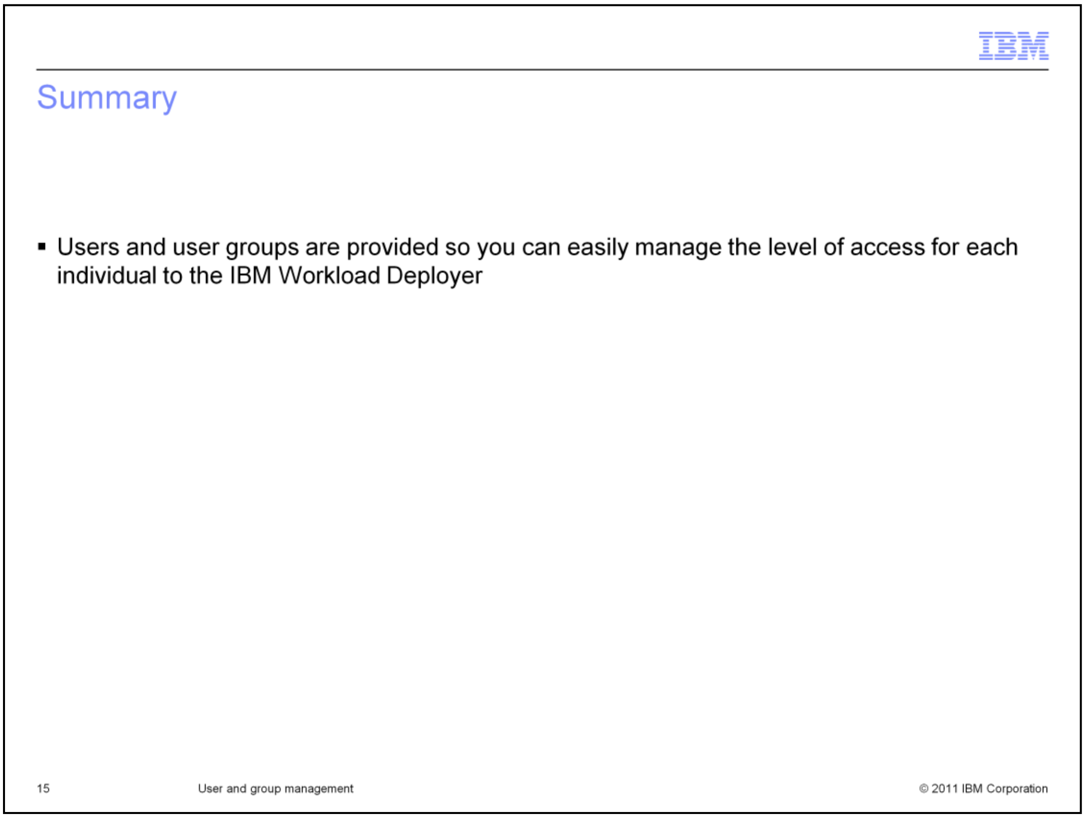
When a user is included in multiple groups, his or her permissions set will reflect the combined permissions for all assigned groups. For example, if user1 is assigned to a group that set “**Cloud administration**” permissions and to another group that set the “**Create new patterns**” permission, then user1 is a cloud administrator and will be able to create new patterns.



Section

Summary

This section is the summary.

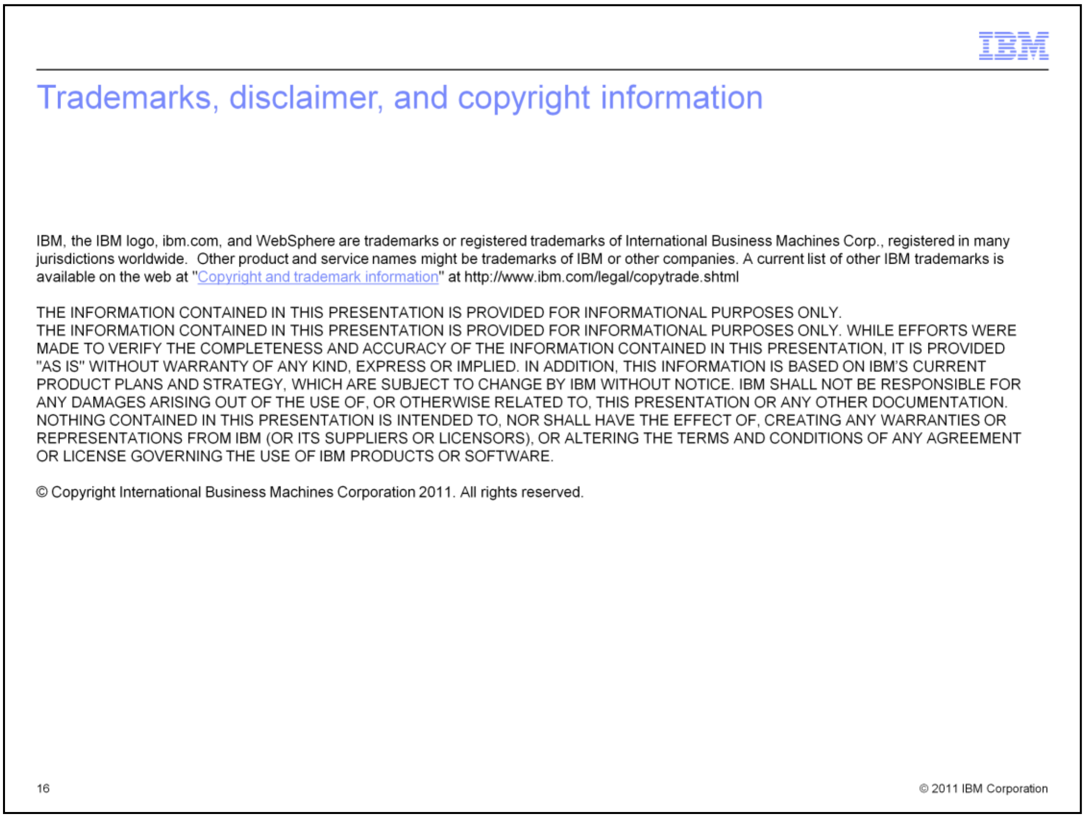


Summary

- Users and user groups are provided so you can easily manage the level of access for each individual to the IBM Workload Deployer

15 User and group management © 2011 IBM Corporation

The users and user groups features allow you to manage which individuals have access to the Workload Deployer and to control their permissions set as a security mechanism.



Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
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.