IBM Software Group

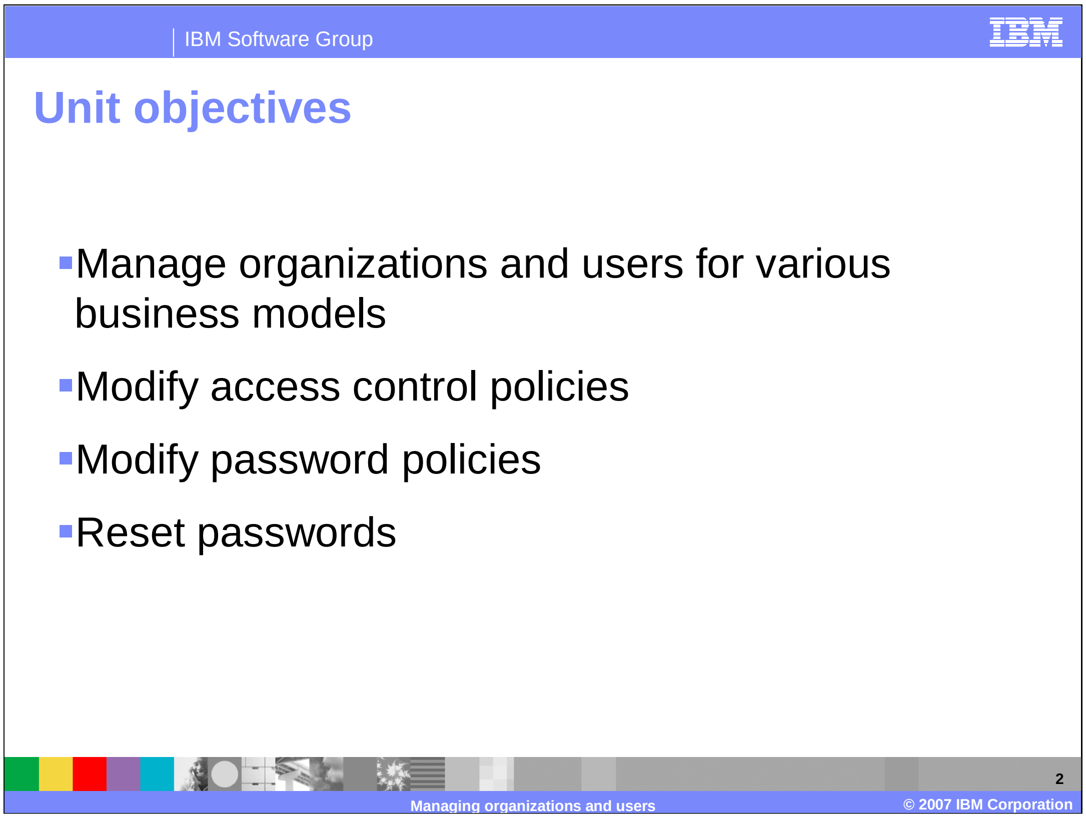
# WebSphere® Commerce V6

## *Managing organizations and users*

business on demand.

Updated September 24, 2007

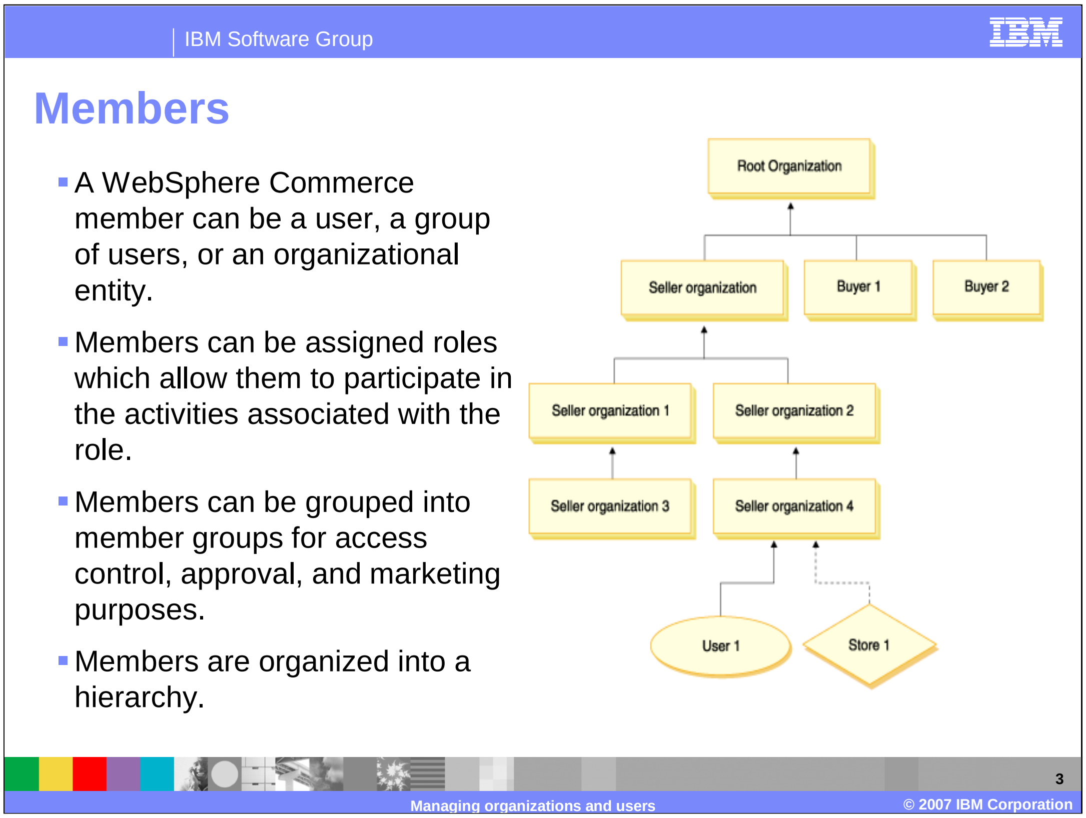
Welcome to the WebSphere® Commerce V6 Managing organizations and users presentation.



## Unit objectives

- Manage organizations and users for various business models
- Modify access control policies
- Modify password policies
- Reset passwords

This presentation discusses how to manage organizations and users for various business models, modify access control and password policies, and lastly reset passwords.



IBM Software Group

## Members

- A WebSphere Commerce member can be a user, a group of users, or an organizational entity.
- Members can be assigned roles which allow them to participate in the activities associated with the role.
- Members can be grouped into member groups for access control, approval, and marketing purposes.
- Members are organized into a hierarchy.

3

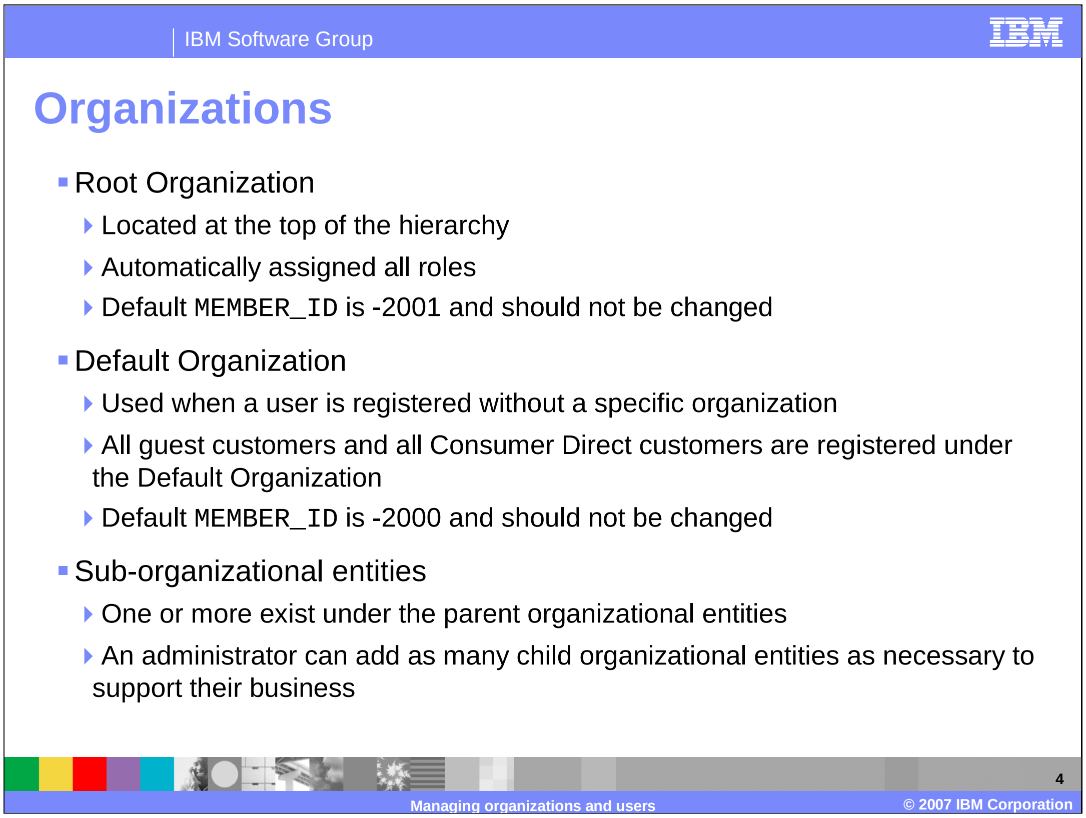
Managing organizations and users

© 2007 IBM Corporation

The member subsystem is a component of the WebSphere Commerce server that includes data for participants of the WebSphere Commerce system.

A WebSphere Commerce member can be a user, a group of users, or an organizational entity. Members can be assigned roles which allow them to participate in the activities associated with the role.

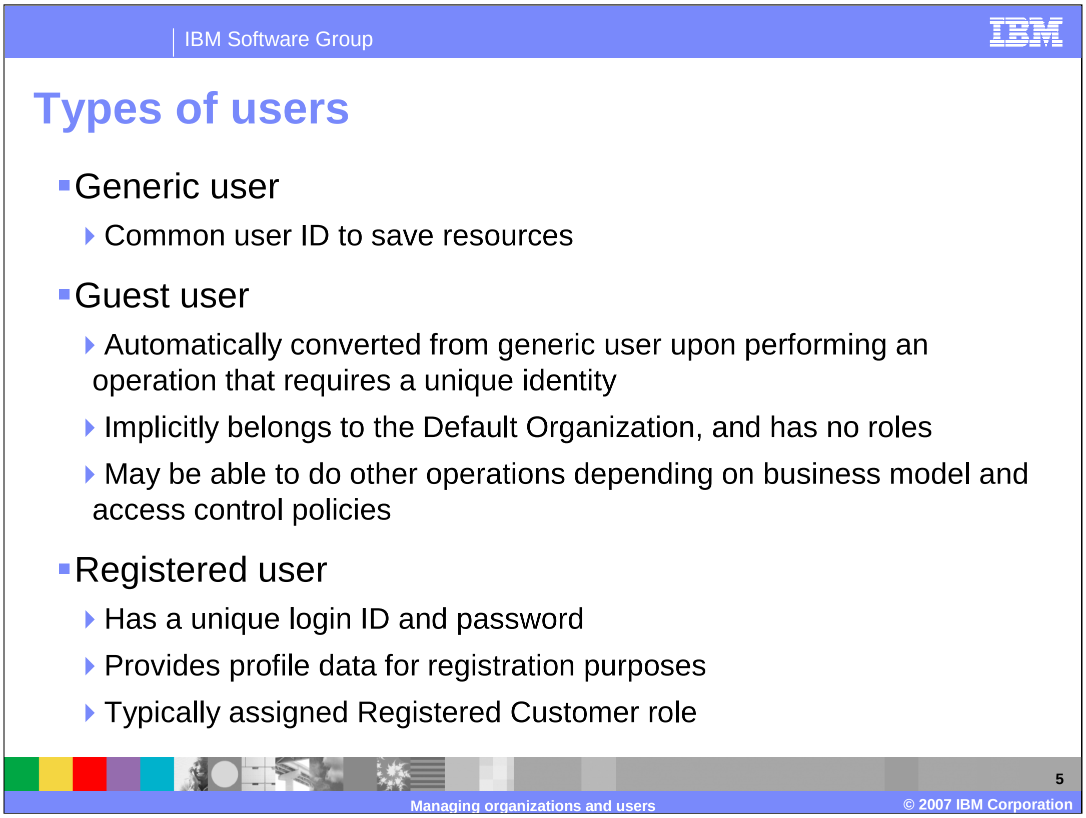
Members can be grouped into member groups for access control, approval, and marketing purposes. Members are organized into a hierarchy, which mimics a typical organizational structure.



# Organizations

- Root Organization
  - Located at the top of the hierarchy
  - Automatically assigned all roles
  - Default `MEMBER_ID` is -2001 and should not be changed
- Default Organization
  - Used when a user is registered without a specific organization
  - All guest customers and all Consumer Direct customers are registered under the Default Organization
  - Default `MEMBER_ID` is -2000 and should not be changed
- Sub-organizational entities
  - One or more exist under the parent organizational entities
  - An administrator can add as many child organizational entities as necessary to support their business

The Root Organization is located at the top of the hierarchy and is its own parent.  The Default Organization is used for all guest customers and Consumer Direct customers. In addition, a business user who registers without specifying a registered organization will be assigned to the Default Organization.



IBM Software Group

# Types of users

- Generic user
  - Common user ID to save resources
- Guest user
  - Automatically converted from generic user upon performing an operation that requires a unique identity
  - Implicitly belongs to the Default Organization, and has no roles
  - May be able to do other operations depending on business model and access control policies
- Registered user
  - Has a unique login ID and password
  - Provides profile data for registration purposes
  - Typically assigned Registered Customer role

5

Managing organizations and users

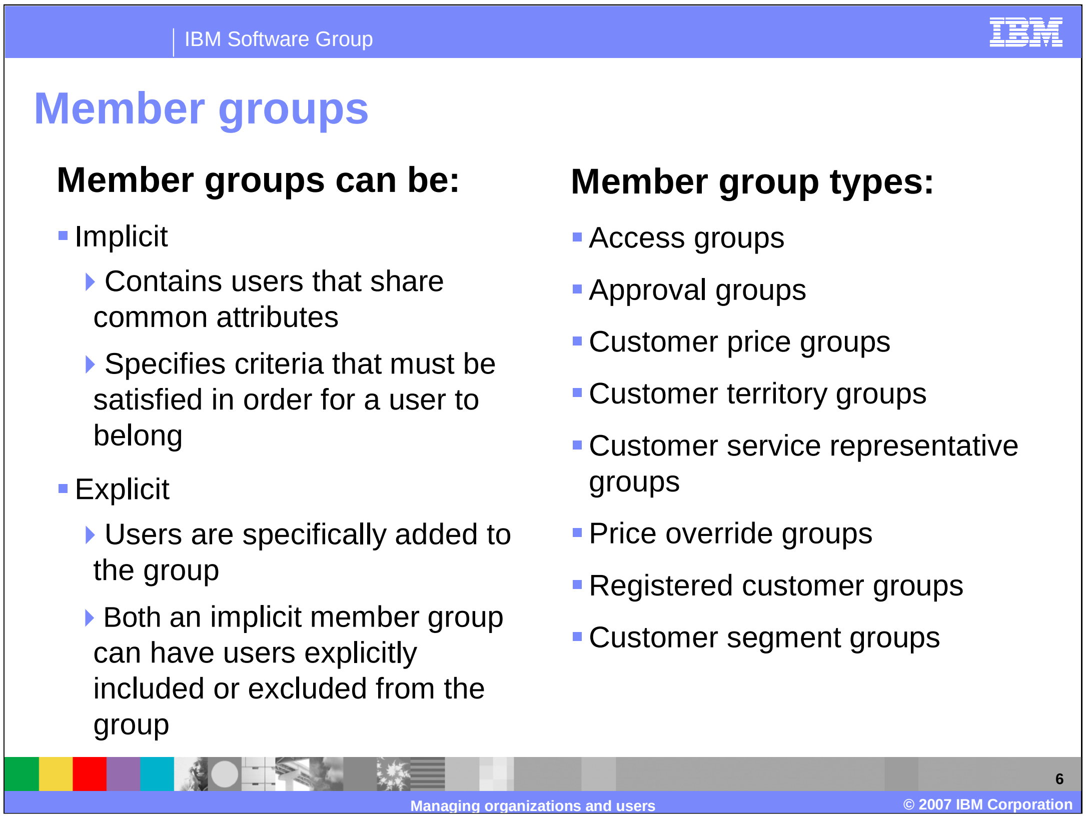
© 2007 IBM Corporation

There are four registration types.  G for guest or generic user, R for registered user, S for site administrator and A for administrator.  A guest user is automatically converted from the generic user upon performing an operation that requires a unique identity. If a guest user later registers, all assets that user owns will become owned by the registered user.

Approval may be required for user registration, depending on the configuration of the parent organization. If approval is needed, it will initially be in pending approval state. Only approved users can log into the site. If a user's registration is rejected, the user could try to register again. When a business user registers, the organizational entity that the user belongs to should be specified, otherwise WebSphere Commerce will default to using the Default Organization.

Registered users can be classified according to their user profile type. Profile type B denotes a business user while profile type C denotes a retail user.

A basic user profile incorporates registration information, demographics, address information, purchase history, and other miscellaneous attributes. A business user profile contains the same information as a basic user profile and employment information, such as an employee number or a job title, or a job description. The business profile may also contain a link to the business organization to which the user belongs.



IBM Software Group

# Member groups

## Member groups can be:

- Implicit
  - Contains users that share common attributes
  - Specifies criteria that must be satisfied in order for a user to belong
- Explicit
  - Users are specifically added to the group
  - Both an implicit member group can have users explicitly included or excluded from the group

## Member group types:

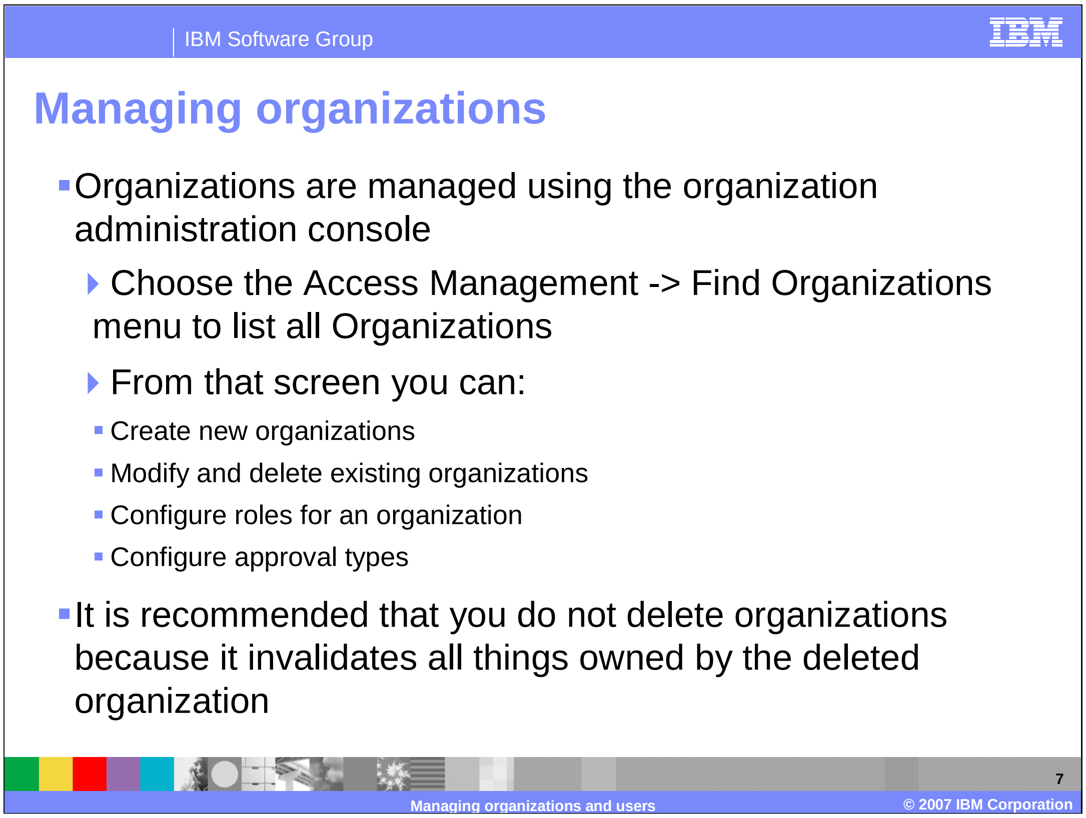
- Access groups
- Approval groups
- Customer price groups
- Customer territory groups
- Customer service representative groups
- Price override groups
- Registered customer groups
- Customer segment groups

6

Managing organizations and users

A member group is a grouping of members - users, organizations, or other member groups - used for various business purposes.

Exact definitions of the member group types can be found in the WebSphere Commerce Information Center under the topic “Member Groups”



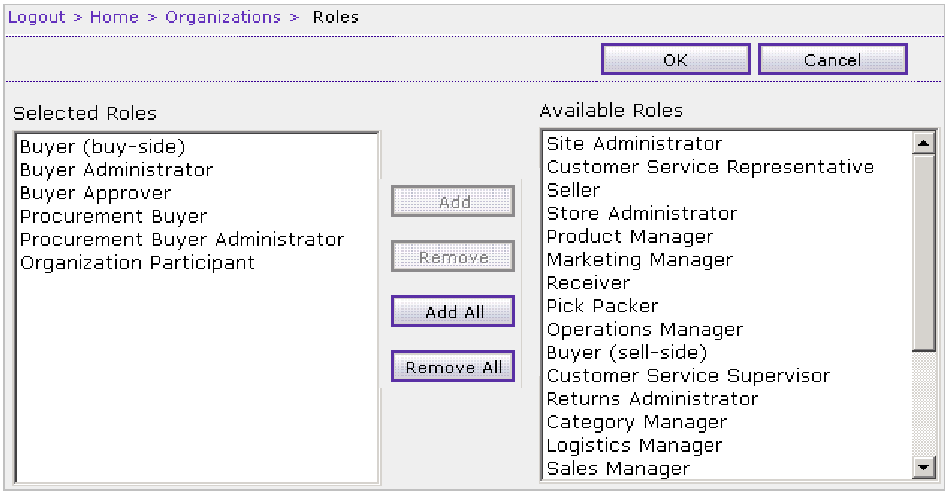
# Managing organizations

- Organizations are managed using the organization administration console
  - Choose the Access Management -> Find Organizations menu to list all Organizations
  - From that screen you can:
    - Create new organizations
    - Modify and delete existing organizations
    - Configure roles for an organization
    - Configure approval types
- It is recommended that you do not delete organizations because it invalidates all things owned by the deleted organization

Organizations are managed using the Organization Administration Console. To create an organization, click N**ew** on the organization list page. On the **Create Organization** details page, provide the necessary information, name, type, parent organization, and address. After an organization is created, configure roles and approval types for that organization.

# Assigning roles to an organization

- Members of an organization may only be assigned roles which belong to that organization



Logout > Home > Organizations > Roles

Selected Roles

Buyer (buy-side)
Buyer Administrator
Buyer Approver
Procurement Buyer
Procurement Buyer Administrator
Organization Participant

Available Roles

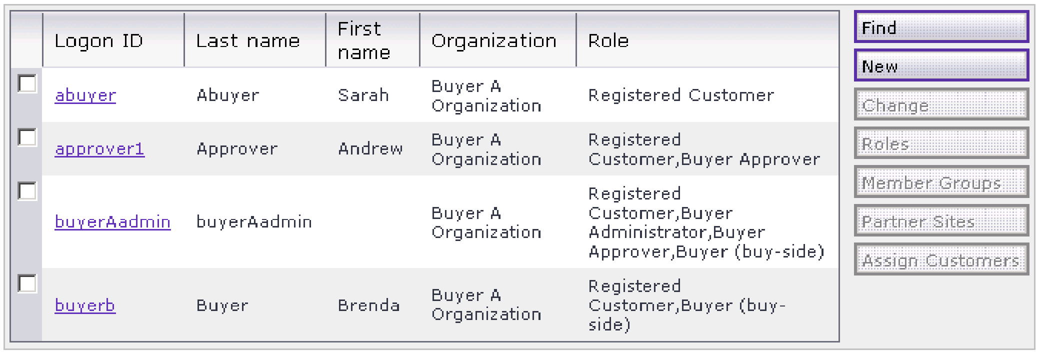
Site Administrator
Customer Service Representative
Seller
Store Administrator
Product Manager
Marketing Manager
Receiver
Pick Packer
Operations Manager
Buyer (sell-side)
Customer Service Supervisor
Returns Administrator
Category Manager
Logistics Manager
Sales Manager

This is a typical role assignment for a buyer organization. You should see roles like Buyer (buy-side), Buyer Administrator, Buyer Approver, and several others. Users that are created under this parent organization can now be assigned any of the selected roles.

Seller organizations would typically be assigned roles like Marketing Manager, Seller, Customer Service Representative, and others depending on the needs of the organization. A site administrator can select roles for any organization. A seller administrator can select roles for the sub-organizations of the organizations where you directly play your administrator role. A buyer administrator or channel manager can only select roles for the sub-organizations of the organizations where you directly play your administrator role.

## Creating business users and administrators

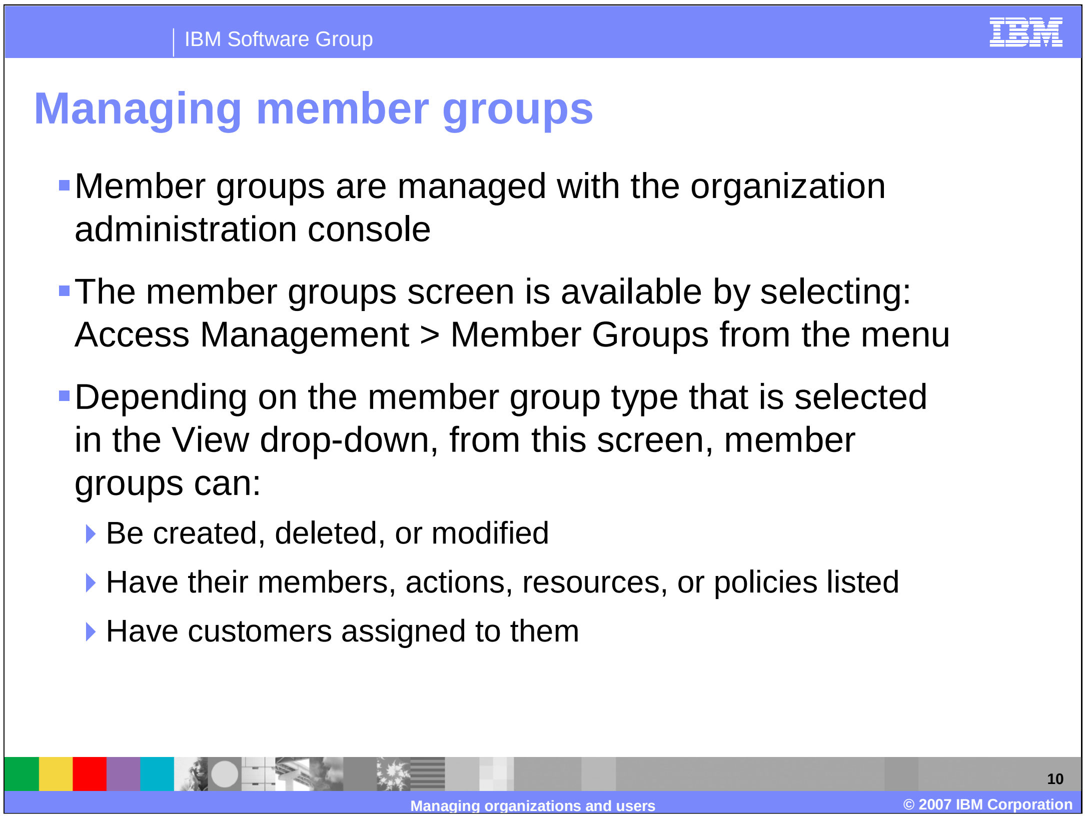
- Once you have created a business user for an organization, that user needs to be assigned one or more roles in the organization



|  | Logon ID | Last name | First name | Organization | Role |
|---|---|---|---|---|---|
| □ | abuyer | Abuyer | Sarah | Buyer A Organization | Registered Customer |
| □ | approver1 | Approver | Andrew | Buyer A Organization | Registered Customer,Buyer Approver |
| □ | buyerAadmin | buyerAadmin |  | Buyer A Organization | Registered Customer,Buyer Administrator,Buyer Approver,Buyer (buy-side) |
| □ | buyerb | Buyer | Brenda | Buyer A Organization | Registered Customer,Buyer (buy-side) |

Use the **Create User** menu on the Access Management page to create a business user or administrator. The **New User** details page includes a large number of fields. Required information includes a logon id, last name, password, parent organization, and address. This page also contains the account policy for the user and the account status for the user.

Users must be assigned to a parent organization and will then need to be assigned a role in that organization.



IBM Software Group

## Managing member groups

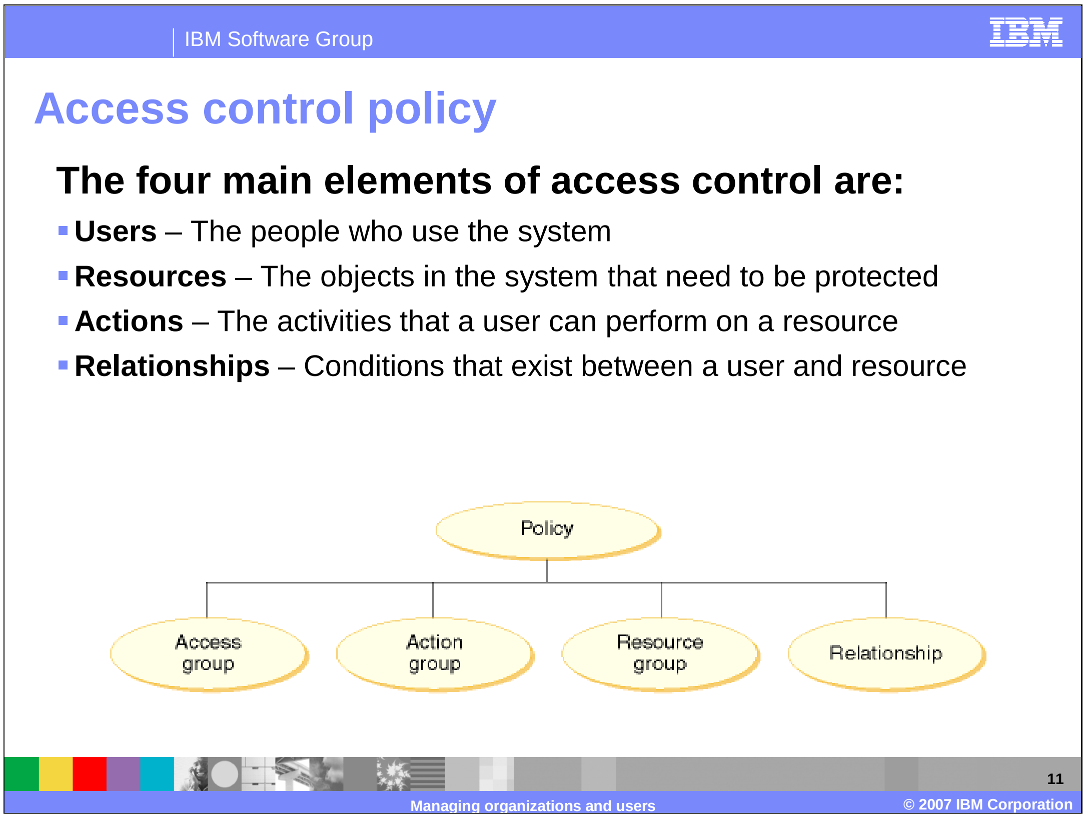
- Member groups are managed with the organization administration console
- The member groups screen is available by selecting: Access Management > Member Groups from the menu
- Depending on the member group type that is selected in the View drop-down, from this screen, member groups can:
  - Be created, deleted, or modified
  - Have their members, actions, resources, or policies listed
  - Have customers assigned to them

10

Managing organizations and users

You can manage member groups with the Organization Administration Console. To explicitly add or remove users from a group, select the groups from the list, press the **Change** button, and choose the **Select Members** section of the notebook. From this screen, members can be searched for and then added to the include or exclude lists.

Not all of the member group types can be managed and created from this console. Customer segments are defined in the WebSphere Commerce Accelerator. It is also possible to create custom groups by manually adding data to the database.



IBM Software Group

IBM

## Access control policy

### The four main elements of access control are:

- **Users** – The people who use the system
- **Resources** – The objects in the system that need to be protected
- **Actions** – The activities that a user can perform on a resource
- **Relationships** – Conditions that exist between a user and resource

Policy

Access group

Action group

Resource group

Relationship

11

Managing organizations and users

© 2007 IBM Corporation

An access control policy consists of four elements. These four parts define a policy in WebSphere Commerce. They do this by specifying the users, the actions they can take, the business object or set of commands on which their actions are taken, and the relationship that the users have to the resource group.

An **access group** is a group of users to which the policy applies.

An **action group** is a group of actions performed by the user on system resources.

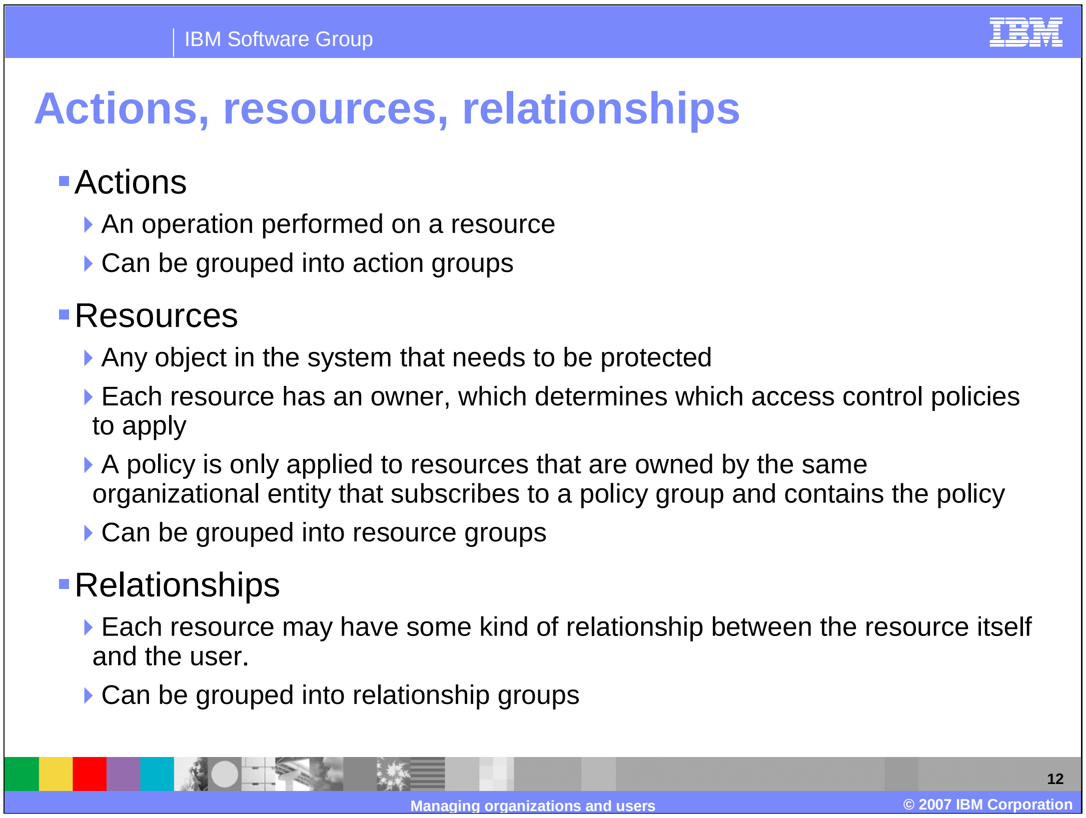
A **resource group** may include business objects like contract or order, or a set of related commands such as all the commands that users of a particular role can perform.

Each resource group can have a set of relationships associated with it. Each resource can have a set of users that fulfill each relationship.

There are two types of access control policies.

Groupable standard policies (or policy type -2) are applied once, to organizations that subscribe to a policy group that contains the policy.

Groupable template policies (or policy type -3) dynamically scope the role in the access group to the context of the current resource's owner.



IBM Software Group

## Actions, resources, relationships

- Actions
  - An operation performed on a resource
  - Can be grouped into action groups
- Resources
  - Any object in the system that needs to be protected
  - Each resource has an owner, which determines which access control policies to apply
  - A policy is only applied to resources that are owned by the same organizational entity that subscribes to a policy group and contains the policy
  - Can be grouped into resource groups
- Relationships
  - Each resource may have some kind of relationship between the resource itself and the user.
  - Can be grouped into relationship groups

12

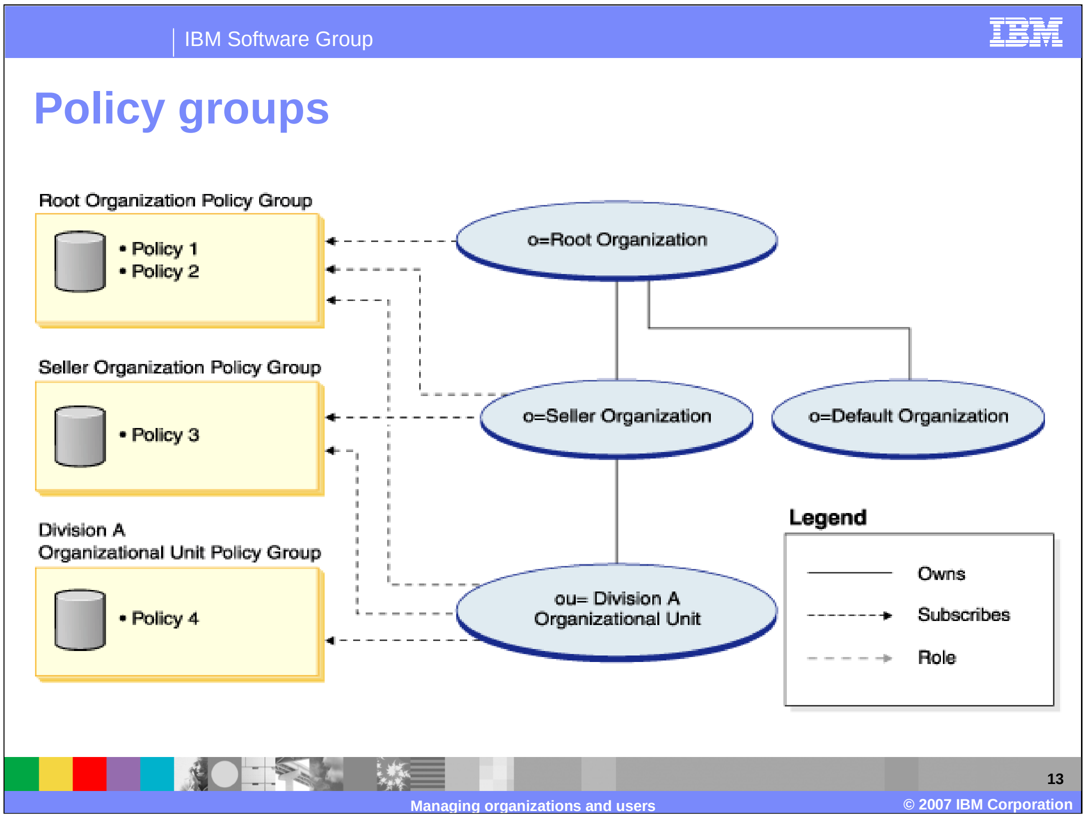
Managing organizations and users

© 2007 IBM Corporation

Actions are operations that are performed on resources. They can be grouped together into action groups.

Resources are objects in the system that need to be protected. Each resource has an owner, which determines which access control policies apply to the resource. A policy is only applied to resources that are owned by the same organizational entity that subscribes to a policy group and contains the policy. Resources can also be grouped together.

Each resource may have some kind of relationship between the resource and the user. The relationships can be grouped together. A relationship group that consists of a single relationship chain with a single parameter element, is functionally equivalent to a simple relationship. In this case, it is easier to use relationship instead of relationship group in the policy.



## Policy groups

Root Organization Policy Group

- Policy 1
- Policy 2

Seller Organization Policy Group

- Policy 3

Division A
Organizational Unit Policy Group

- Policy 4

o=Root Organization

o=Seller Organization

o=Default Organization

ou= Division A
Organizational Unit

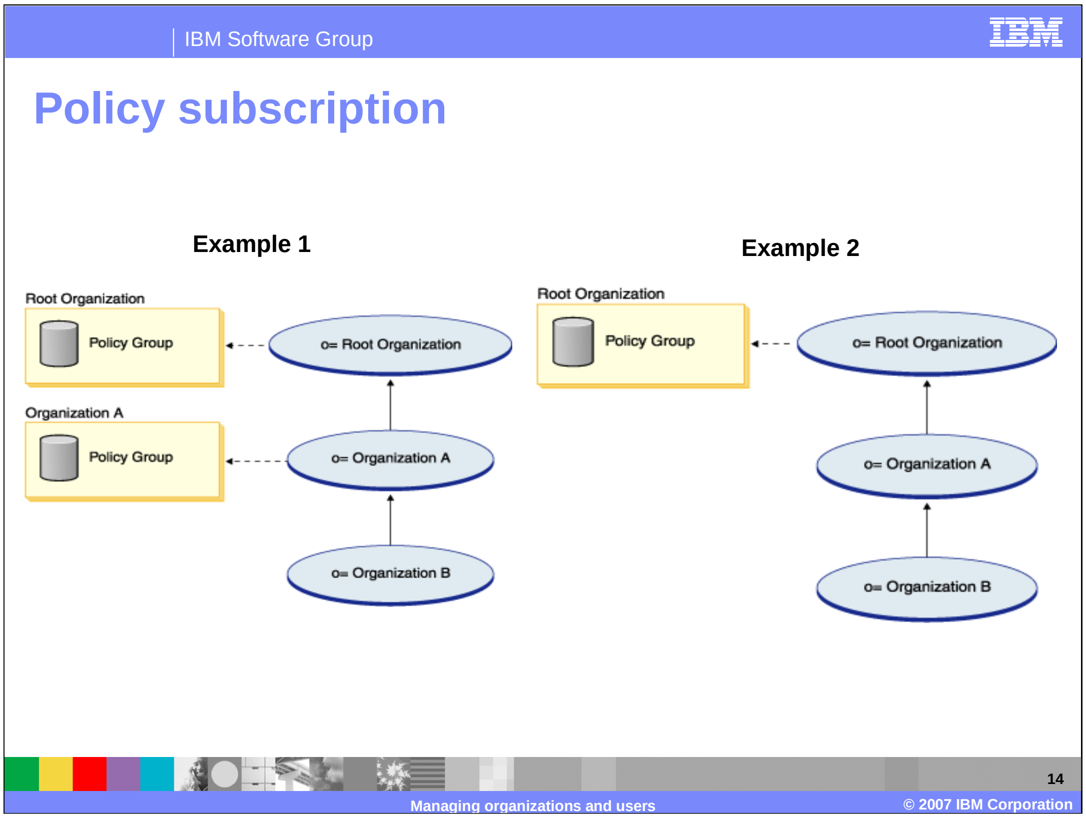
Legend

Owns

Subscribes

Role

Each business model has its own set of access control policies. Policy groups are used to group the sets of policies within the models. To group these policies, each policy is explicitly assigned to one or more appropriate policy groups and then organizations can subscribe to one or more of those policy groups.



IBM Software Group

# Policy subscription

**Example 1**

Root Organization

Policy Group

o= Root Organization

Organization A

Policy Group

o= Organization A

o= Organization B

**Example 2**

Root Organization

Policy Group

o= Root Organization

o= Organization A

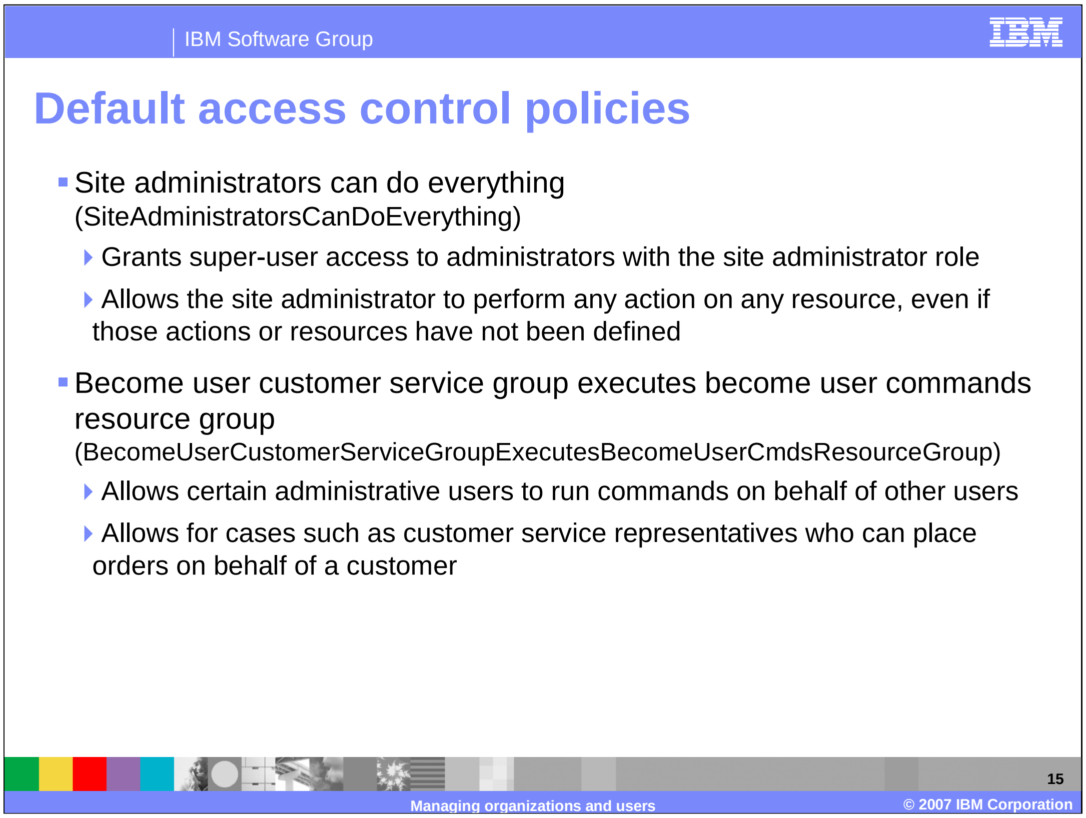
o= Organization B

14

Managing organizations and users

© 2007 IBM Corporation

Policy subscription means that organizations can subscribe to policy groups.  If an organization does not subscribe to any policy groups, the access control framework will begin searching up the organization hierarchy until it encounters an organization that subscribes to at least one policy group. This means, as shown in example 1, if Organization B's immediate parent organization, Organization A, subscribes to a policy group, the search will stop.  Organization B will subscribe to Organization A's policy groups.  If Organization A did not subscribe to a policy group, the search would continue to the Root Organization and both Organization A and Organization B would subscribe to the Root Organization's policy groups.



IBM Software Group

## Default access control policies

- Site administrators can do everything (SiteAdministratorsCanDoEverything)
  - Grants super-user access to administrators with the site administrator role
  - Allows the site administrator to perform any action on any resource, even if those actions or resources have not been defined
- Become user customer service group executes become user commands resource group (BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup)
  - Allows certain administrative users to run commands on behalf of other users
  - Allows for cases such as customer service representatives who can place orders on behalf of a customer

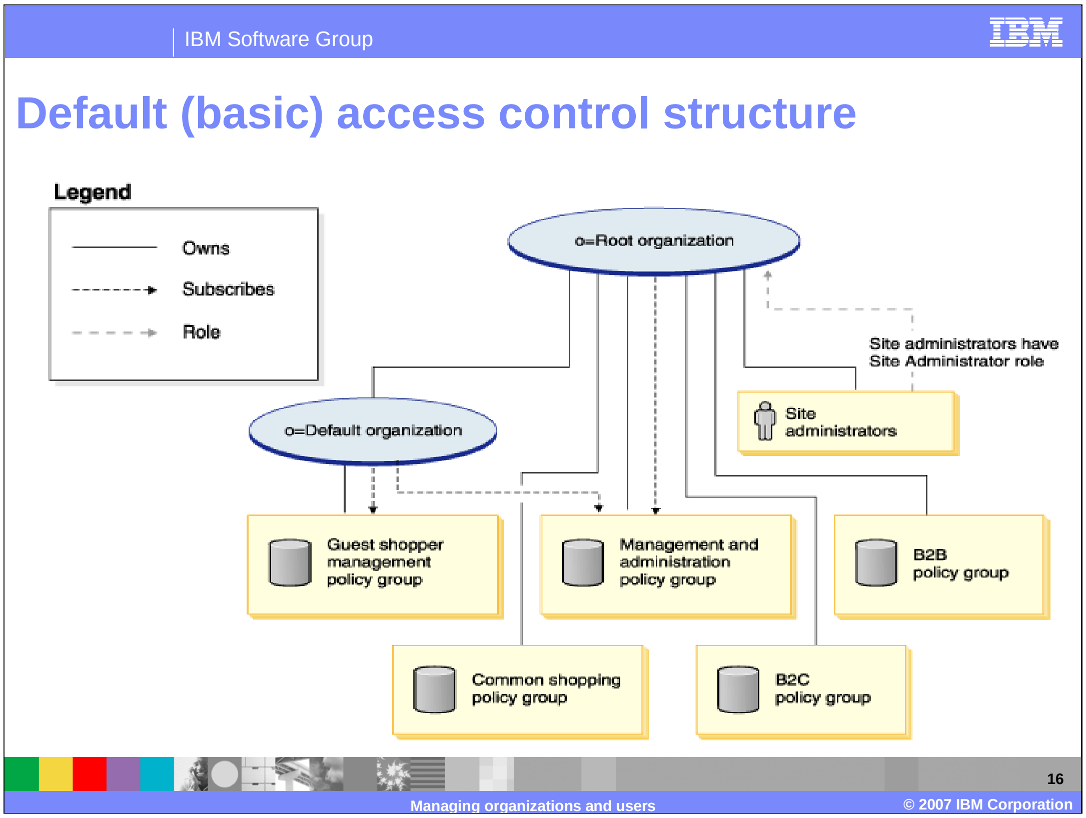
15

Managing organizations and users

There are two special access control policies for administrative users.

The ‘site administrators can do everything’ policy grants super-user access to administrators with the site administrator role.  It allows the site administrator to perform any action on any resource, even if those actions or resources have not been defined.

The ‘become user customer service group executes become user commands resource group’ policy allows certain administrative users to run specific commands on behalf of other users.  This allows customer service representatives to place orders on behalf of customers.



IBM Software Group

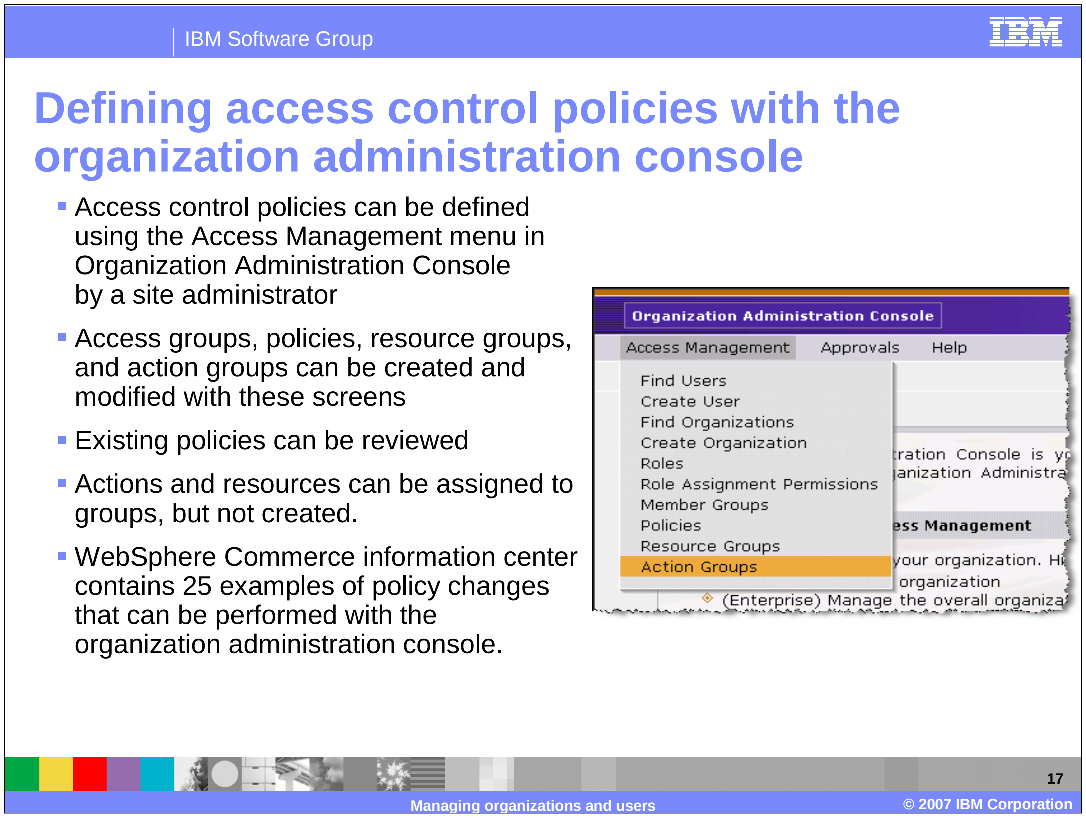
## Default (basic) access control structure

16

Managing organizations and users

© 2007 IBM Corporation

Every business structure starts with the same basic access control structure. According to this structure, the root organization only subscribes to the management and administration policy group. As a result, these policies apply to the site administrators, who are directly under the root. The policies in the management and administration policy group do not apply to the default organization through inheritance, because the default organization subscribes to the guest shopper management policy group. Because of this, the default organization also needs to subscribe to the management and administration policy group.

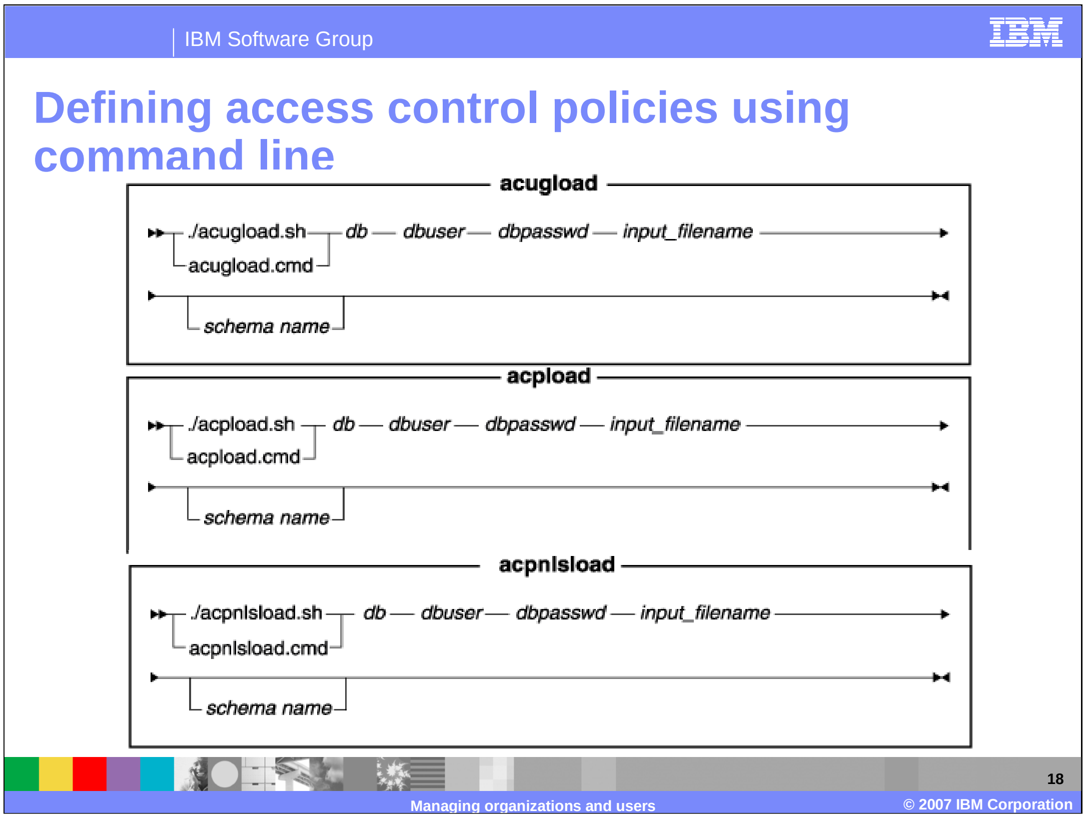


## Defining access control policies with the organization administration console

- Access control policies can be defined using the Access Management menu in Organization Administration Console by a site administrator
- Access groups, policies, resource groups, and action groups can be created and modified with these screens
- Existing policies can be reviewed
- Actions and resources can be assigned to groups, but not created.
- WebSphere Commerce information center contains 25 examples of policy changes that can be performed with the organization administration console.

The WebSphere Commerce Organization Administration Console can be used to make simple changes to access control policies.  Some changes must be loaded directly into the database using XML-based utilities. These include creating or modifying an action, creating a role-based policy for views, changing the action group in a role-based policy for views, creating or modifying a policy group and associating policies with policy groups.

Before you change a policy to use a different access group, review the definition of that access group to ensure it meets your requirements. To do so, select Access Management -> Member Group, then select Access Groups from the drop down list in the Organization Administration Console.  Depending on the value you select for View, the Policies page lists the policies that are owned by the selected organization.  It does not distinguish between site-level policies and policies specific to a particular organization.  Rename any default policies you change so that the policy name reflects what the policy does and so that you can identify the default policies you have changed.  Consider implementing a naming convention for your customized policies. If appropriate, you should also modify the description of the policy and its display name.



IBM Software Group

## Defining access control policies using command line

**acugload**

```
./acugload.sh   db  dbuser  dbpasswd  input_filename
acugload.cmd
[schema name]
```

**acpload**

```
./acpload.sh   db  dbuser  dbpasswd  input_filename
acpload.cmd
[schema name]
```

**acpnlsload**

```
./acpnlsload.sh   db  dbuser  dbpasswd  input_filename
acpnlsload.cmd
[schema name]
```

18

Managing organizations and users

© 2007 IBM Corporation

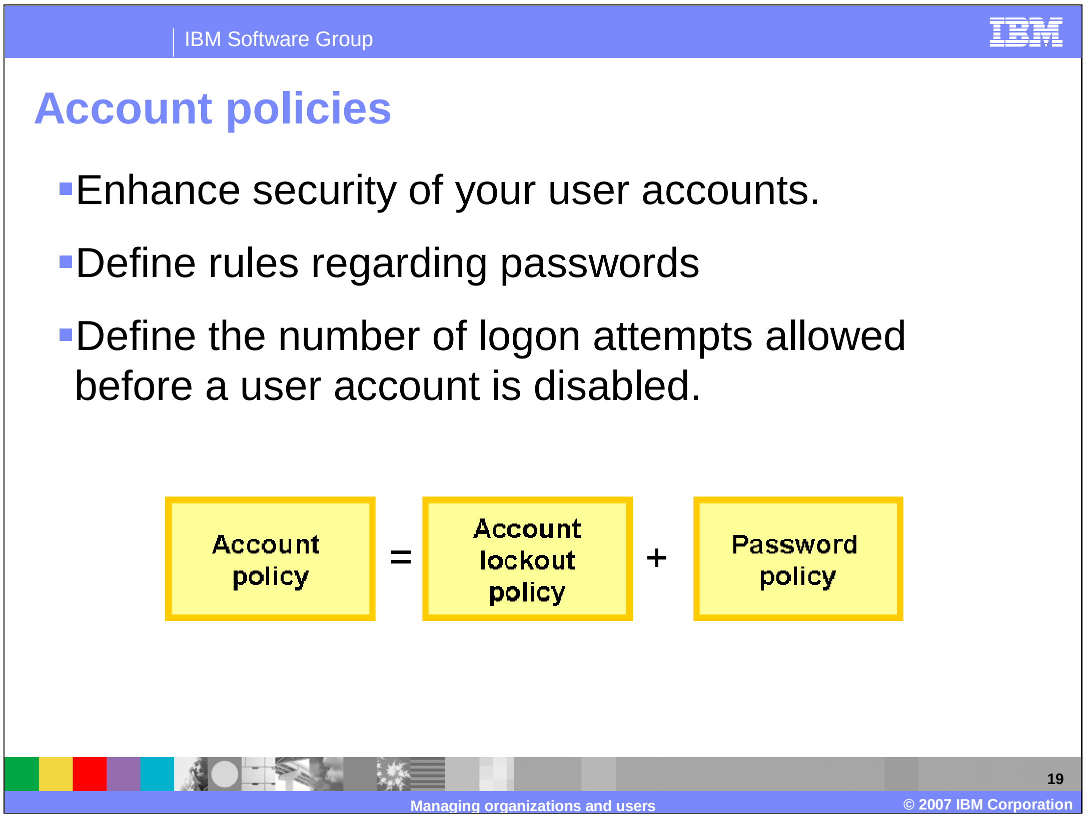
Policies should be loaded in the sequence specified here.  Custom xml files should be placed in the <WC_installdir>/xml/policies/xml directory.

There are three command line utilities for loading xml policies into WebSphere Commerce.

The acugload utility loads the user access group definitions.

The acpload utility loads the access control policy definitions and other policy-related elements.

The acpnlsload utility loads the policy display names and descriptions.



## Account policies

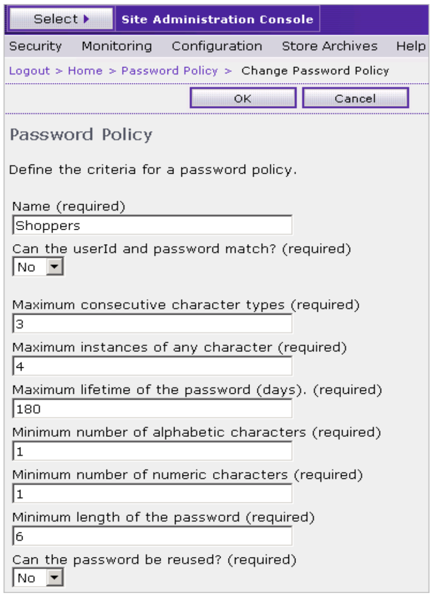
- Enhance security of your user accounts.
- Define rules regarding passwords
- Define the number of logon attempts allowed before a user account is disabled.

Account policy = Account lockout policy + Password policy

There are two default account policies that are included with WebSphere Commerce.  One policy is for shoppers and defines that an account should be locked out after 6 failed logon attempts. The other account is for administrators. It defines an account lockout policy of three attempts and much stricter rules on the password strength.

# Configuring password policies

- Password policies can be administered from the **Security → Password Policy** screen of the site administration console
- From this screen existing policies can be modified or new policies can be created
- Password policies can be used to enforce password strength
- Once a password policy is defined, it can be added to an account policy, which can be assigned to a user


Select
Site Administration Console
Security Monitoring Configuration Store Archives Help
Logout > Home > Password Policy > Change Password Policy
OK
Cancel

Password Policy

Define the criteria for a password policy.

Name (required)
Shoppers

Can the userId and password match? (required)
No

Maximum consecutive character types (required)
3

Maximum instances of any character (required)
4

Maximum lifetime of the password (days). (required)
180

Minimum number of alphabetic characters (required)
1

Minimum number of numeric characters (required)
1

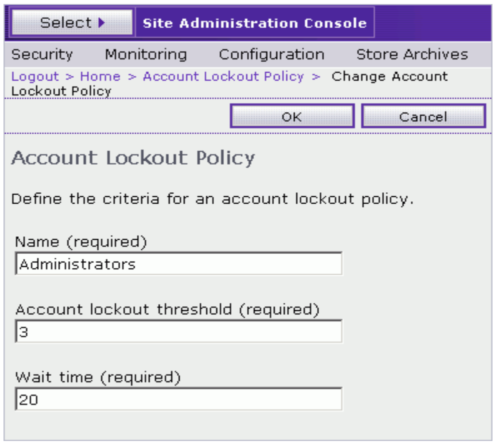
Minimum length of the password (required)
6

Can the password be reused? (required)
No

Password policies can be administered from the Security Password Policy screen of the site administration console. From this screen, you can modify existing policies or create new policies. You can use password policies to enforce password strength. Once you define a password policy, you can add it to an account policy, which can then be assigned to a user.

# Configuring account lockout policies

- Account lockout policies can be administered from the **Security → Account Lockout Policy** screen of the site administration console
- From this screen existing policies can be modified or new policies can be created
- Account lockout policies are used to disable an account when potential misuse of the account is detected.
- Once an account lockout policy is defined, it can be added to an account policy, which can be assigned to a user


Select ▸
Site Administration Console
Security
Monitoring
Configuration
Store Archives
Logout > Home > Account Lockout Policy > Change Account Lockout Policy
OK
Cancel

Account Lockout Policy

Define the criteria for an account lockout policy.

Name (required)
Administrators

Account lockout threshold (required)
3

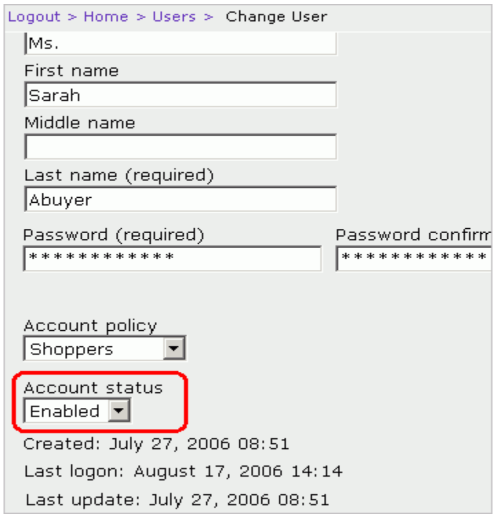
Wait time (required)
20

Account lockout policies are used to disable an account when potential misuse of the account is detected through too many failed logon attempts. The default administrator policy allows only three logon attempts before disabling the account. Each time the login fails, the user must wait a defined amount of time before being allowed to try again.

The wait time is incremented each time the login fails. In this example, after one attempt, the user will have to wait 20 seconds. After attempt two, the user will have to wait 40 seconds, then 60 seconds, and so on until the lockout threshold is reached.

# Resetting an account

- An account can be reset by modifying the **Account status** on the user **Details** page.



Logout > Home > Users > Change User

Ms.

First name
Sarah

Middle name

Last name (required)
Abuyer

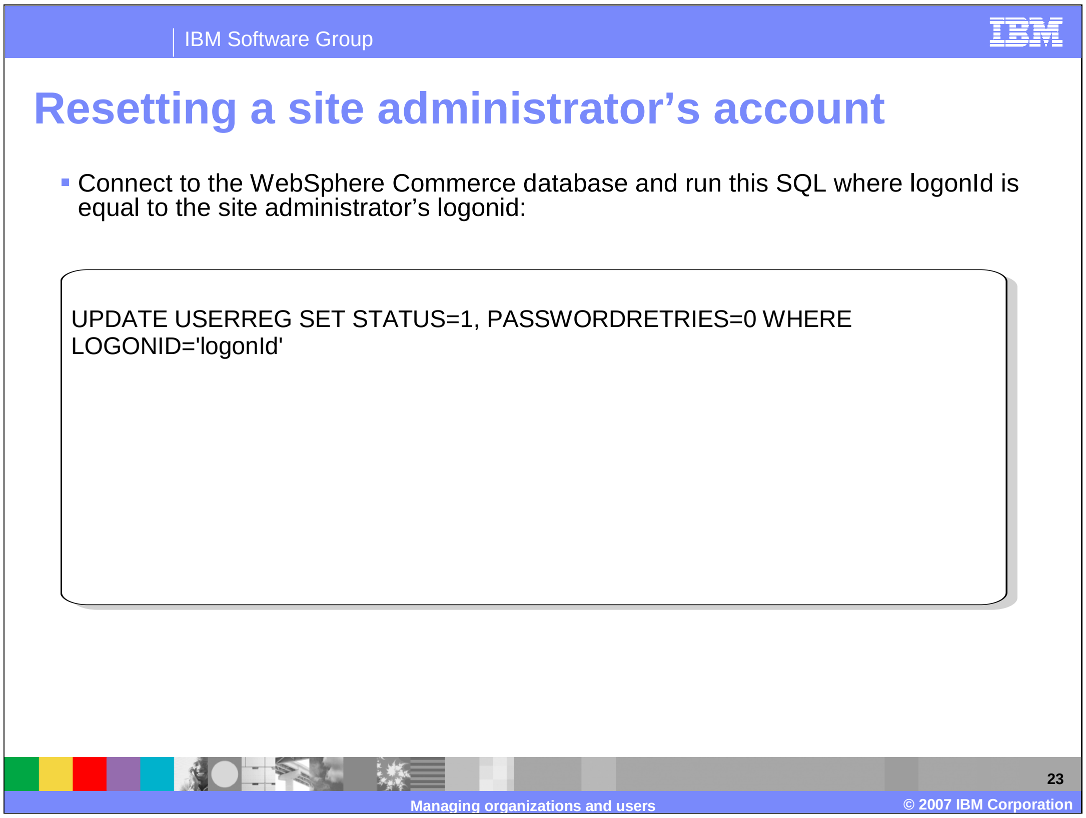
Password (required) ************
Password confirm ************

Account policy
Shoppers

Account status
Enabled

Created: July 27, 2006 08:51
Last logon: August 17, 2006 14:14
Last update: July 27, 2006 08:51

If a user reaches the account timeout threshold defined in their account policy, the account will be disabled. An account for a business user or administrator can be reset by changing the Account status back to Enabled on the user Details page.

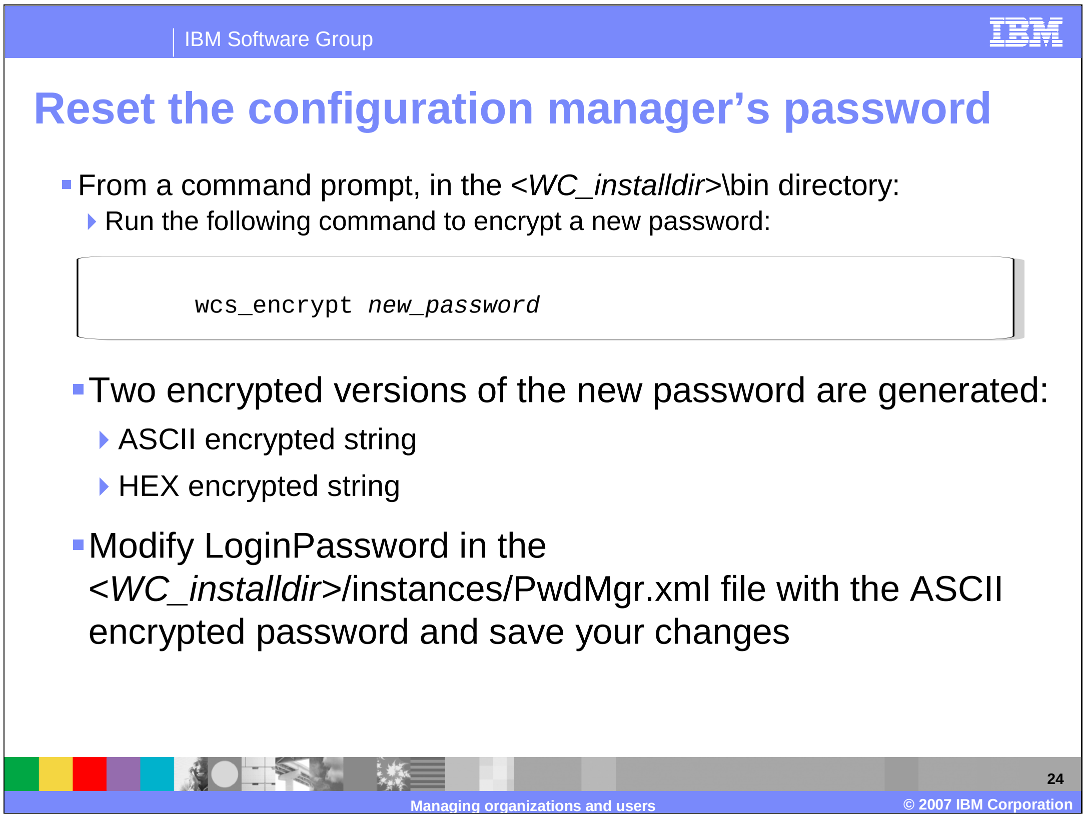


## Resetting a site administrator’s account

- Connect to the WebSphere Commerce database and run this SQL where logonId is equal to the site administrator’s logonid:

```
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE
LOGONID='logonId'
```

A site level administrator can always log into the WebSphere Commerce Organization administration console to reset the account of another administrator. To reset a user account, select the user from the User list, click **Change**, and change the value of Account Status to **Enabled**.  However, if the site level administrator becomes locked out, there is not a higher-level administrator to make that change.



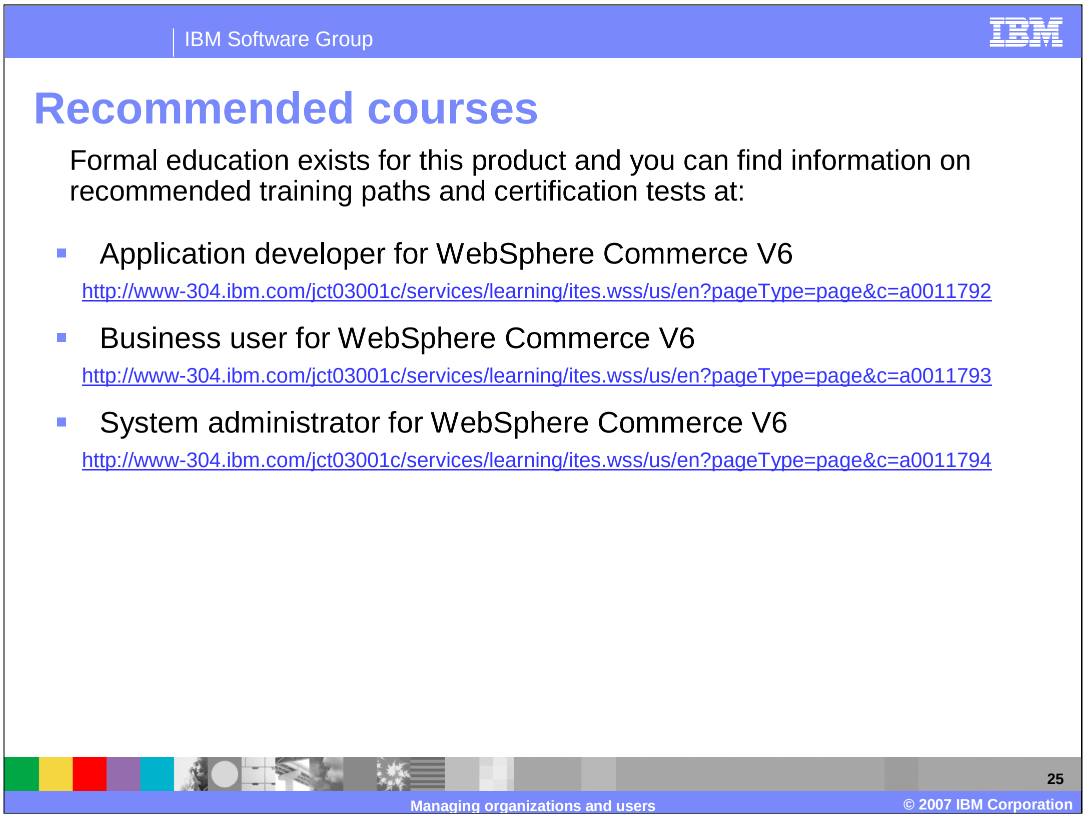
## Reset the configuration manager’s password

- From a command prompt, in the <*WC_installdir*>\bin directory:
  - Run the following command to encrypt a new password:

```
wcs_encrypt new_password
```

- Two encrypted versions of the new password are generated:
  - ASCII encrypted string
  - HEX encrypted string
- Modify LoginPassword in the <*WC_installdir*>/instances/PwdMgr.xml file with the ASCII encrypted password and save your changes

You can reset the configuration manager’s password from a command prompt in the <WC_installdir>\bin directory by running the command shown here. Two encrypted versions of the new password will be generated, one encrypted in ASCII and another in HEX. You can modify the LoginPassword in the <WC_installdir>/instances/PwdMgr.xml file with the ASCII encrypted password and save your changes.

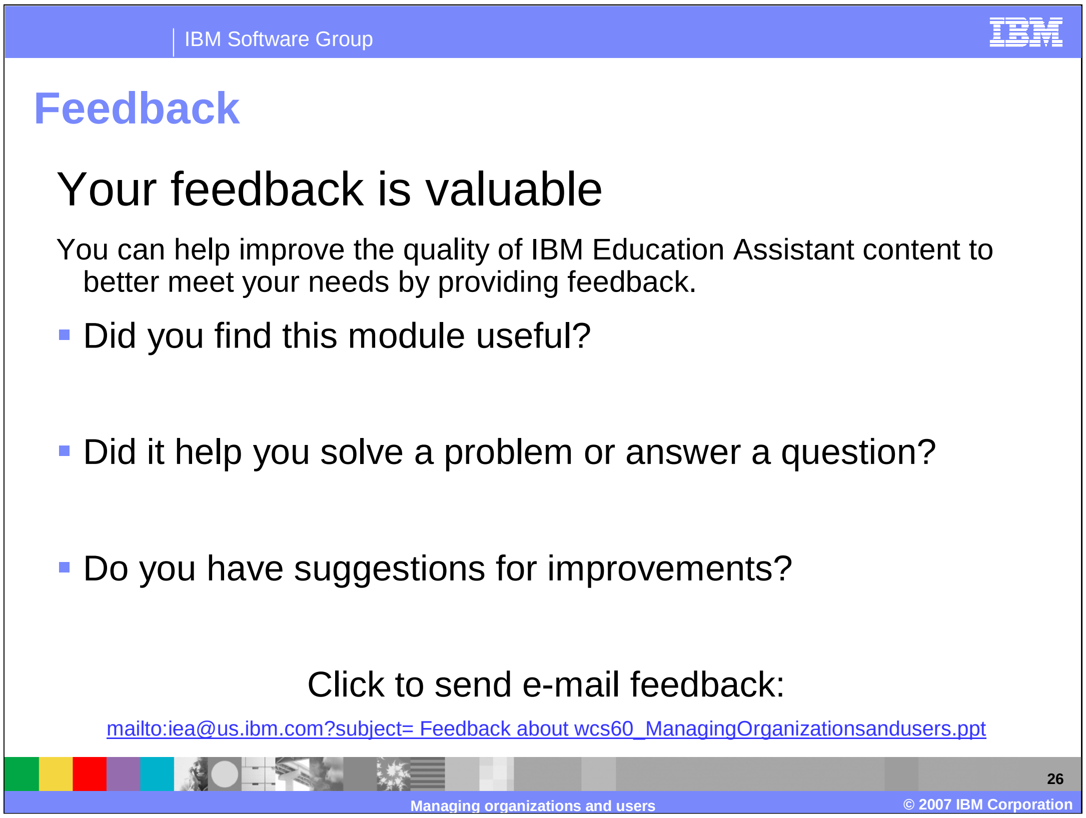


## Recommended courses

Formal education exists for this product and you can find information on recommended training paths and certification tests at:

- Application developer for WebSphere Commerce V6
  http://www-304.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=page&c=a0011792
- Business user for WebSphere Commerce V6
  http://www-304.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=page&c=a0011793
- System administrator for WebSphere Commerce V6
  http://www-304.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=page&c=a0011794

IBM provides the following training paths for the skill or certification you want to explore.



IBM Software Group

## Feedback

### Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

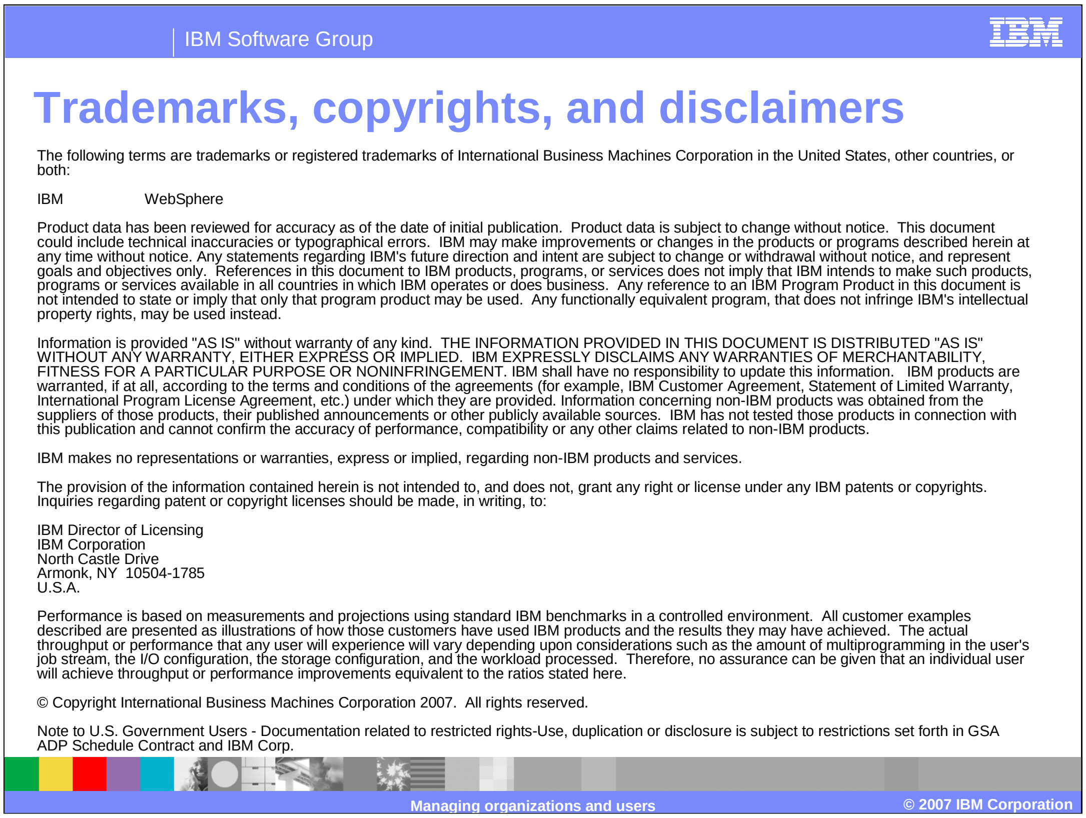
mailto:iea@us.ibm.com?subject= Feedback about wcs60_ManagingOrganizationsandusers.ppt

26

Managing organizations and users

© 2007 IBM Corporation

You can help improve the quality of IBM Education Assistant content by providing feedback.



# Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM WebSphere

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.