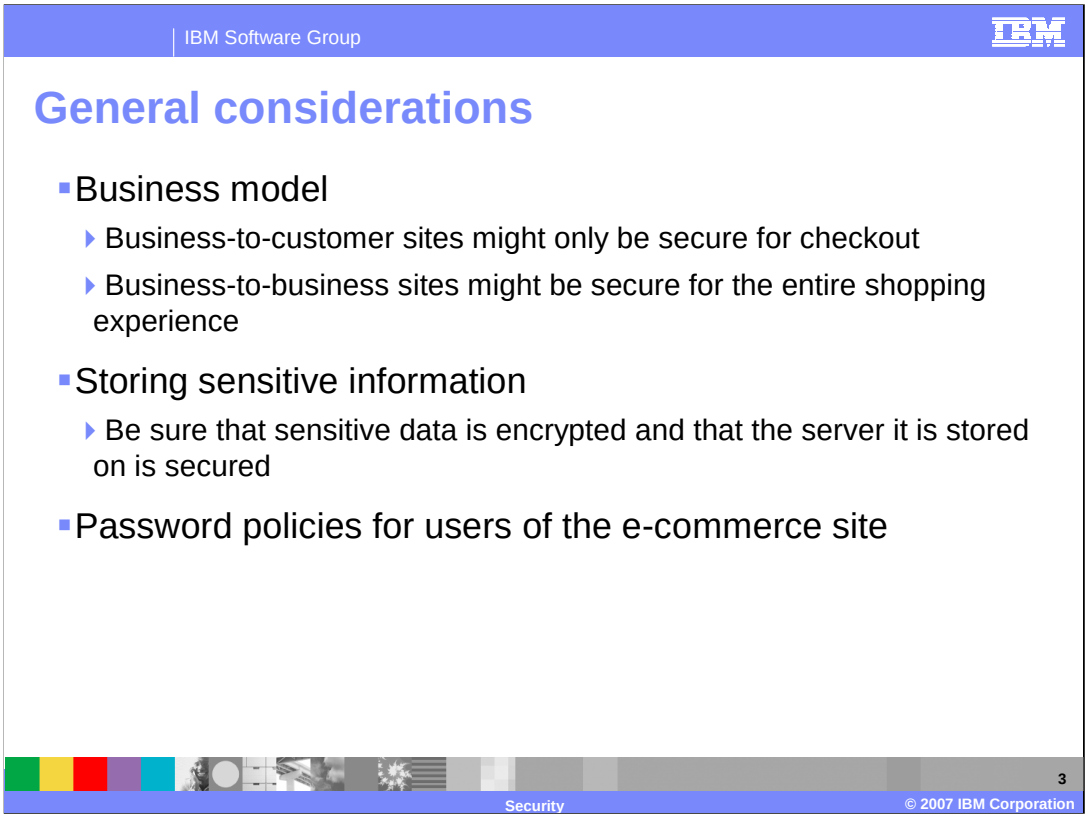
Welcome to the WebSphere Commerce V6 presentation on security.

Unit objectives

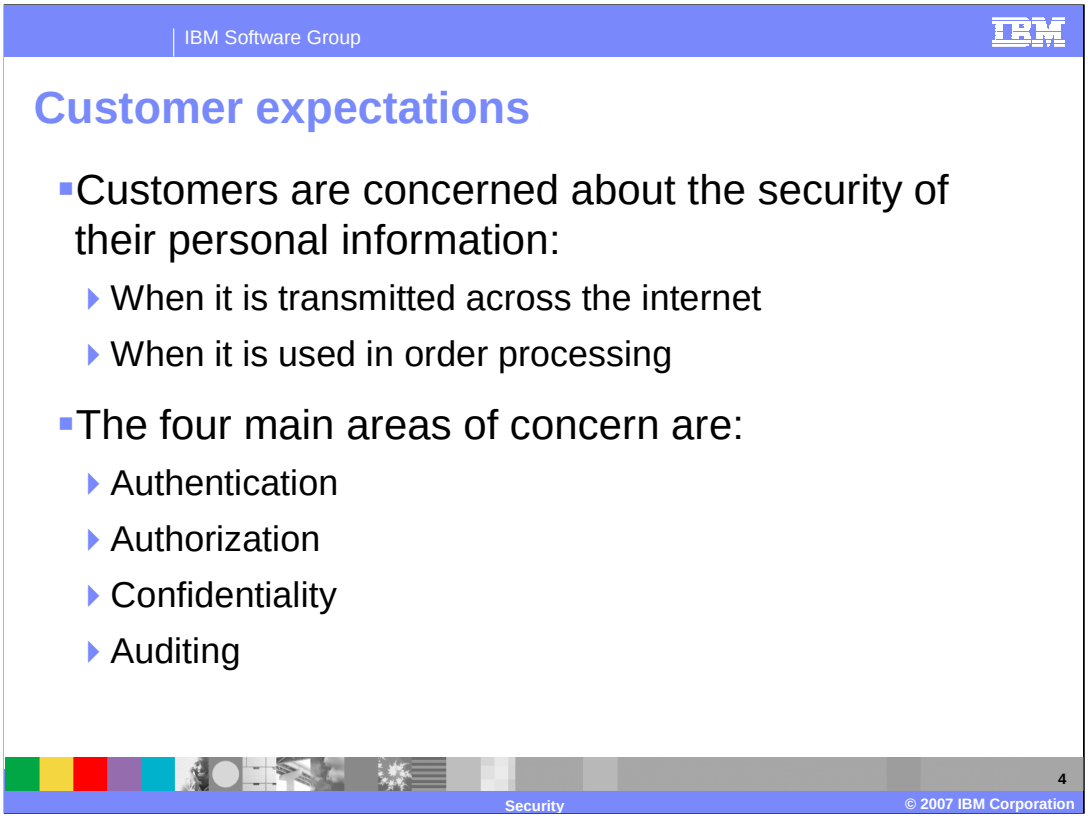
- General security considerations for an e-commerce site
- Security features provided by WebSphere Commerce
- Configure site security for WebSphere Commerce

This presentation discusses general security considerations for an e-commerce site. It also discusses security features provided by WebSphere Commerce and how to configure site security for WebSphere Commerce.



Your business model will determine some of your security policies for you. For example, if you have a business-to-customer store you would want the checkout flow to be secure. The only place where you would have sensitive data being transferred would be in that part of the application. However if you have a business-to-business store, you would want the whole site to be secure.

You will want to develop a strong password policy for your site. A good password policy will make it more difficult, if not impossible, to guess passwords quickly.

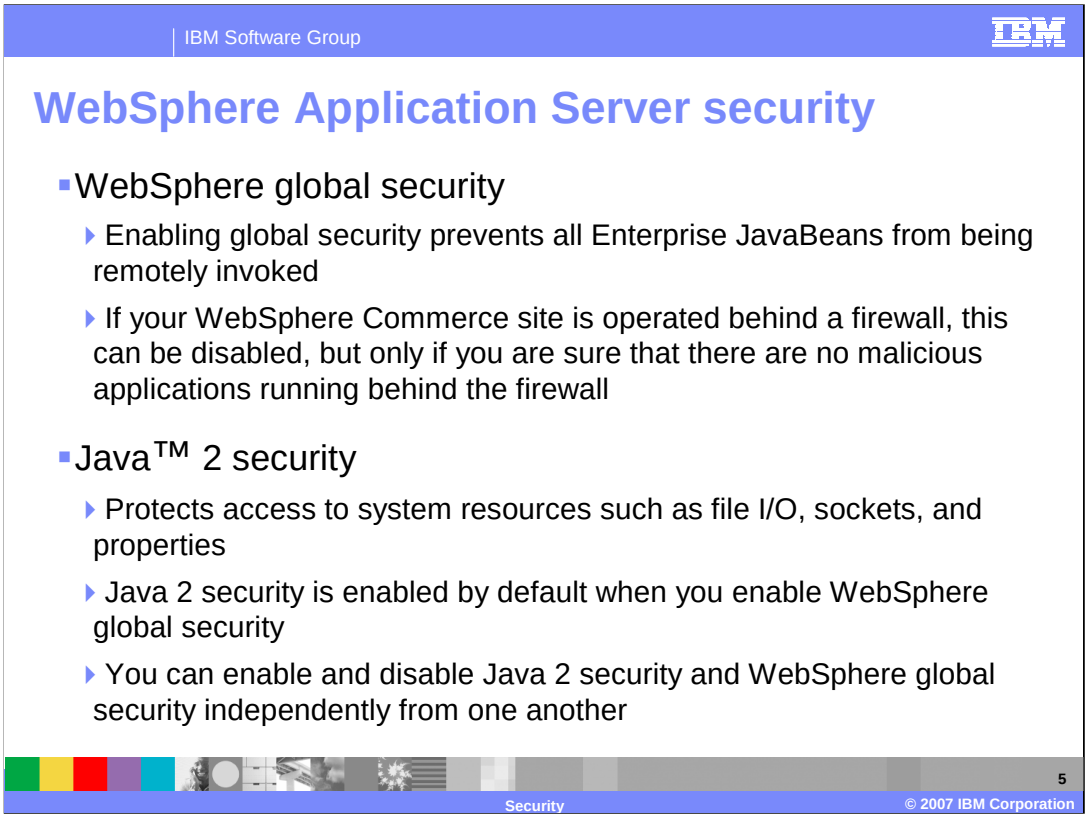


Customers want to feel safe and know that all the personal information required to make a purchase is safe in two cases. First, when their data is transmitted over the Internet. Second, they want to be sure that while their order is processing their data is safe. In the first case, the customer wants to be sure that somebody snooping on their network cannot get their data. In the second case, the customer wants to be sure that in order processing (for example credit card validation) their personal information is not susceptible to being compromised.

There are four main areas of concern. Authentication involves establishing trust between the site and the users. Users must be validated against a registry to ensure that they are who they say they are. The information in that registry, such as passwords, must be secure. Authorization controls access to resources. This will allow users to only access or manipulate data that they have been given permission to.

The main goal of confidentiality is to be sure that all data is secure when it is being transmitted or stored. Encrypting data is one of many ways that confidentiality is enforced.

Auditing involves logging security and access violations and analyzing what happened in the case of a violation.



There are two orthogonal components to enabling WebSphere Application Server security.

Enabling global security prevents all Enterprise JavaBeans from being remotely invoked. If your WebSphere Commerce site is operated behind a firewall, this can be disabled, but only if you are sure there are no malicious applications running behind the firewall.

Enabling Java 2 security protects access to system resources such as file I/O, sockets and properties. Java 2 security is enabled by default when you enable WebSphere global security. You can enable and disable Java 2 security and WebSphere global security independently from one another.

In general, any additional layer of security will degrade performance. WebSphere Application Server security and Java 2 security should only be enabled if absolutely necessary. If you plan to enable this security, you should take into account additional hardware requirements for your systems (such as more memory)

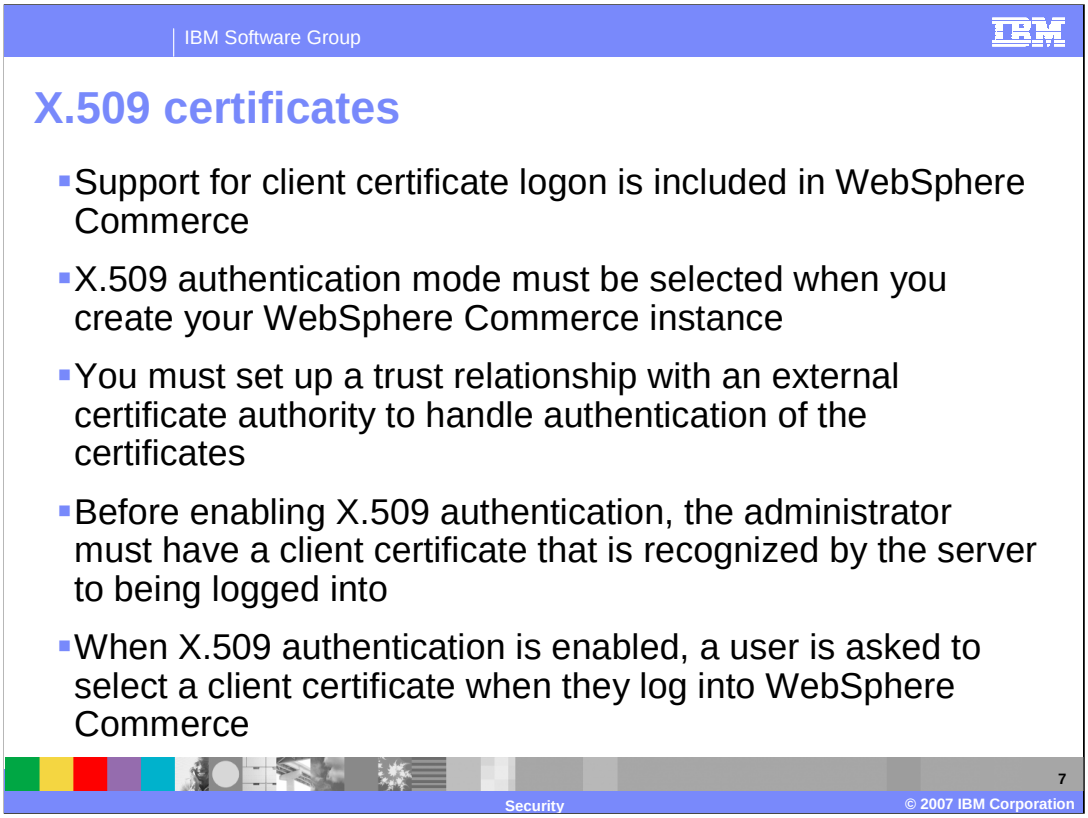
For more information on WebSphere Application Server security, see the WebSphere Application Server Information Center.

Web server SSL

- SSL protocol encrypts data from a user's computer to the WebSphere Commerce site's server
- If a SSL certificate is not from a trusted authority, the user's browser issues a warning
- To make sure that the communication between the two is through SSL, use this URL:
  - https://***host_name***:*port_number*/webapp/PaymentManager where ***host_name*** is your WebSphere Commerce Payments server machine name, and *port_number* is 5433 (by default)
- If you directly launch the WebSphere Commerce payments user interface, communication is not through SSL:
  - http://***host_name***:*port_number*/webapp/PaymentManager where ***host_name*** is your WebSphere Commerce Payments server machine name, and *port_number* is 5432 (by default)

When the browser requests an SSL protected page, the browser will identify the server as a trusted entity and will pass encryption key information back and forth between itself and the server. On any subsequent SSL protected requests, the information flowing between the browser and the server will be encrypted.

The SSL certificate is issued to the server by a certificate authority authorized by the government. If you are still using WebSphere Commerce payments, it is recommended that you use SSL when connecting WebSphere Commerce to WebSphere Commerce payments for security reasons.



When creating a WebSphere Commerce instance, select the Authentication Mode. The Authentication Mode is either Basic or X.509. The default is Basic authentication, which is logon authentication using a login ID and password. To activate logon authentication using X.509 certificates, select X.509 authentication.

Error messages are displayed when a user's X.509 certificate has been revoked by a site, or when a client certificate does not contain the necessary information to guarantee that the customer is unique in WebSphere Commerce.

Only the information found in the CERT_X509 table is taken from the certificate. However, customer address information could be taken from the X.509 client certificate, if it is available.

Salted passwords

- A salt is a random string used in the generation of passwords
- Salts should be unique for each user
- By using a salt if two users have the same password, the encrypted string in the database will look different
- In WebSphere Commerce each user's salt is stored in the USERREG table in the salt column

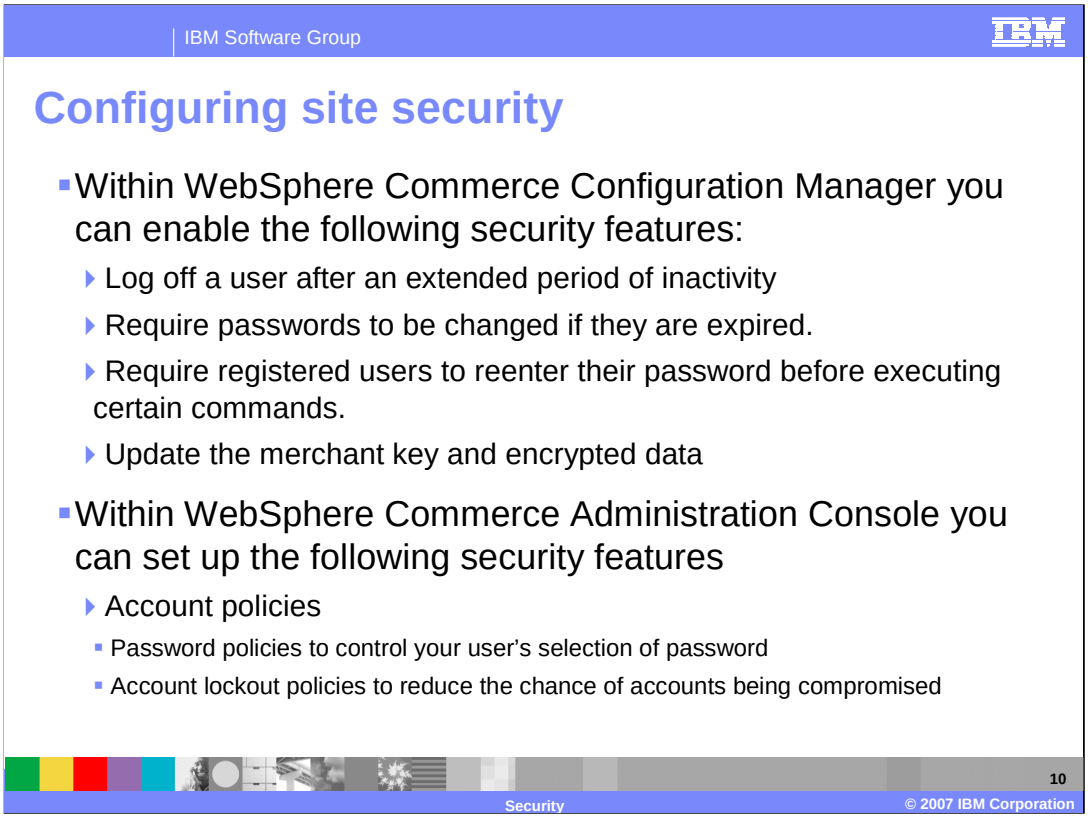
The main purpose of a salt is to add more security to storing passwords. By using a salt when encrypting a password, two users that have the same password will not have the same encrypted string as their password. In this manner, if a vendor gains access to the database, they will not be able to tell if multiple users have the same password.

Cross site scripting protection

- If enabled, this feature rejects any request that has parameters that have been designated not allowable
- You can override this protection on a per command basis
- By default cross site scripting protection is enabled
- This feature is configured in the WebSphere Commerce configuration file
- As this protection is a restrictive feature, take extreme caution in configuring it

When you enable cross-site scripting protection, this feature rejects any user requests that contain attributes (parameters) or strings that are designated as not allowable. You can also exclude commands from cross-site scripting protection by allowing the values of specified attributes for that particular command to contain prohibited strings. Cross-site scripting protection is enabled by default.

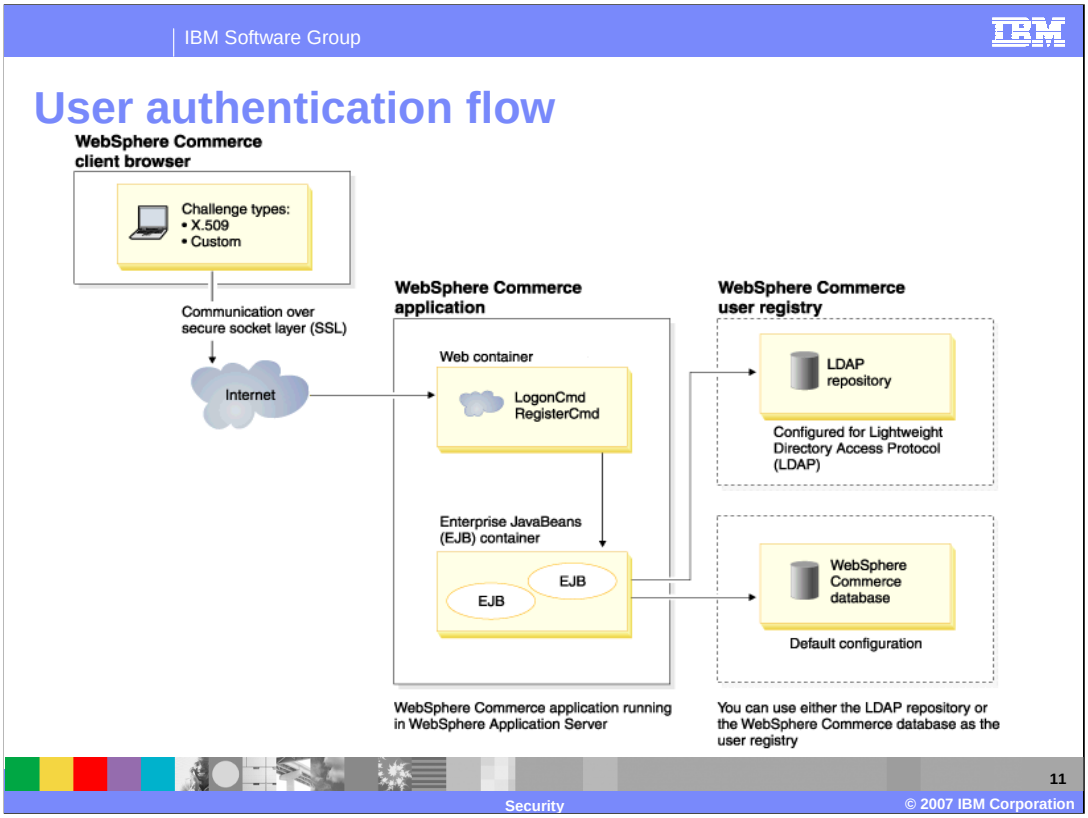
Cross-site scripting protection is a restrictive feature such that it will restrict the execution of commands based on its configuration. The feature does not check what attributes or strings have been defined as prohibited. Therefore, when configuring it, ensure that the prohibited attributes are not those used by the commands and that the prohibited strings are not values that are passed to the commands. Use extreme caution when configuring this feature.



To enhance the security of your WebSphere Commerce site, you can enable any of the following features in WebSphere Commerce Configuration Manager.

Log off a user that is inactive for an extended period and request they log back on to the system, using the Login Timeout node. You can require users to change their passwords when they are logging in to the system for the first time, using the Password Invalidation node. You can update encrypted data such as passwords, credit card information, and the merchant key in a WebSphere Commerce database, using the Database Update Tool node. You can require users to enter their passwords if they are running requests that run designated commands, using the Password Protected Commands node.

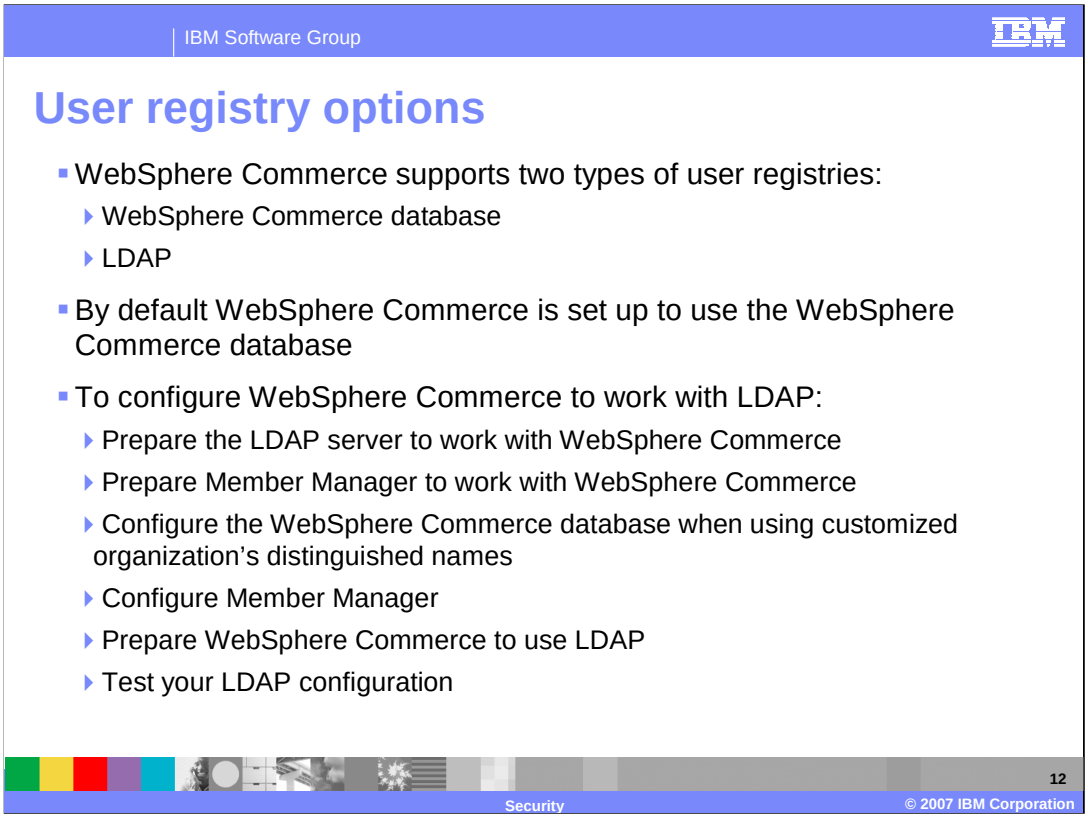
Within the WebSphere Commerce Administration Console you can also set up account policies, password policies and account lockout policies to reduce the change of accounts being compromised.



User authentication flow works like this: the user will be given a challenge to prove that this user is a registered user; this could be providing an X.509 certificate or a username and password.

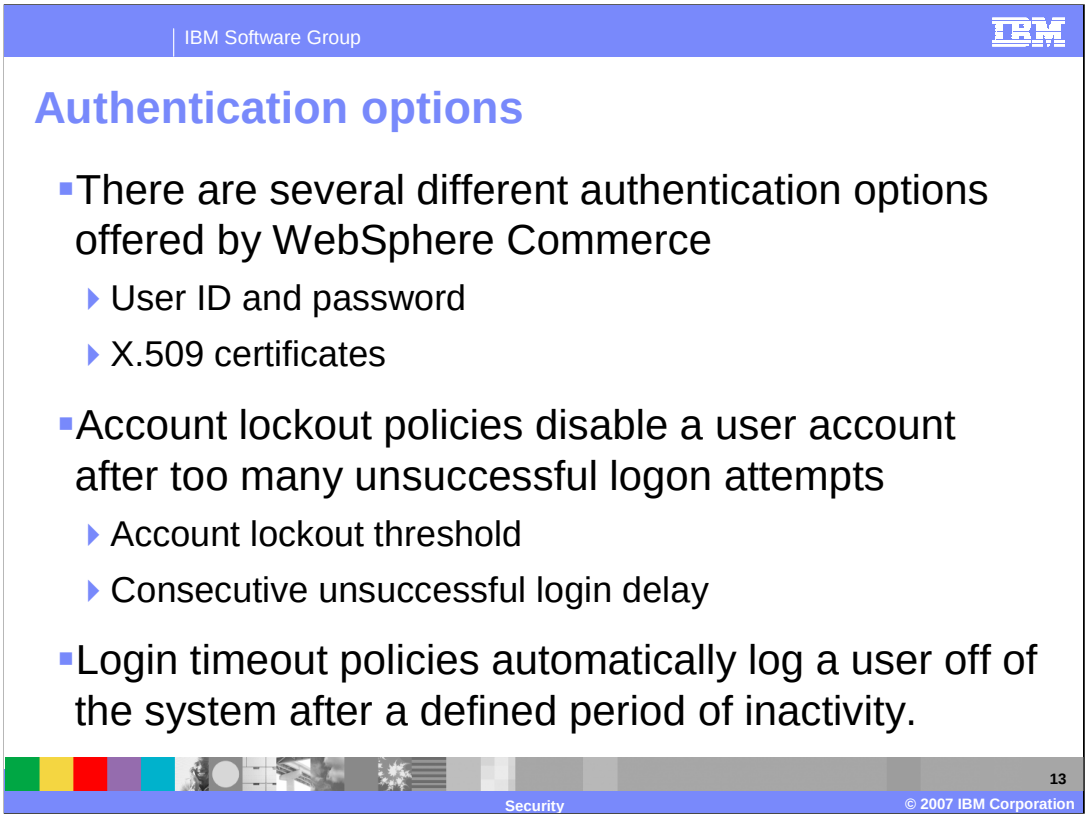
Once the user has provided the information that the challenge required, WebSphere Commerce will validate the provided information against a user registry.

User registries are repositories that contain user information and user authentication information (for example passwords). WebSphere Commerce supports registries based on two different types of domains: the WebSphere Commerce database and LDAP. LDAP servers are commonly used in single sign on environments.



Configuring WebSphere Commerce to work with LDAP is not a trivial task. When WebSphere Commerce is configured to use LDAP, the member and member subsystem tables are still populated.

To see more information on LDAP configurations, see WebSphere Commerce Information Center for Configuring directory services with WebSphere Commerce.



WebSphere Commerce supports X509 certificates or a user ID and password for authentication. This option is defined at instance creation using the Configuration Manager. Do not enable the X.509 authentication mechanism until you have obtained a certificate for your site administrators.

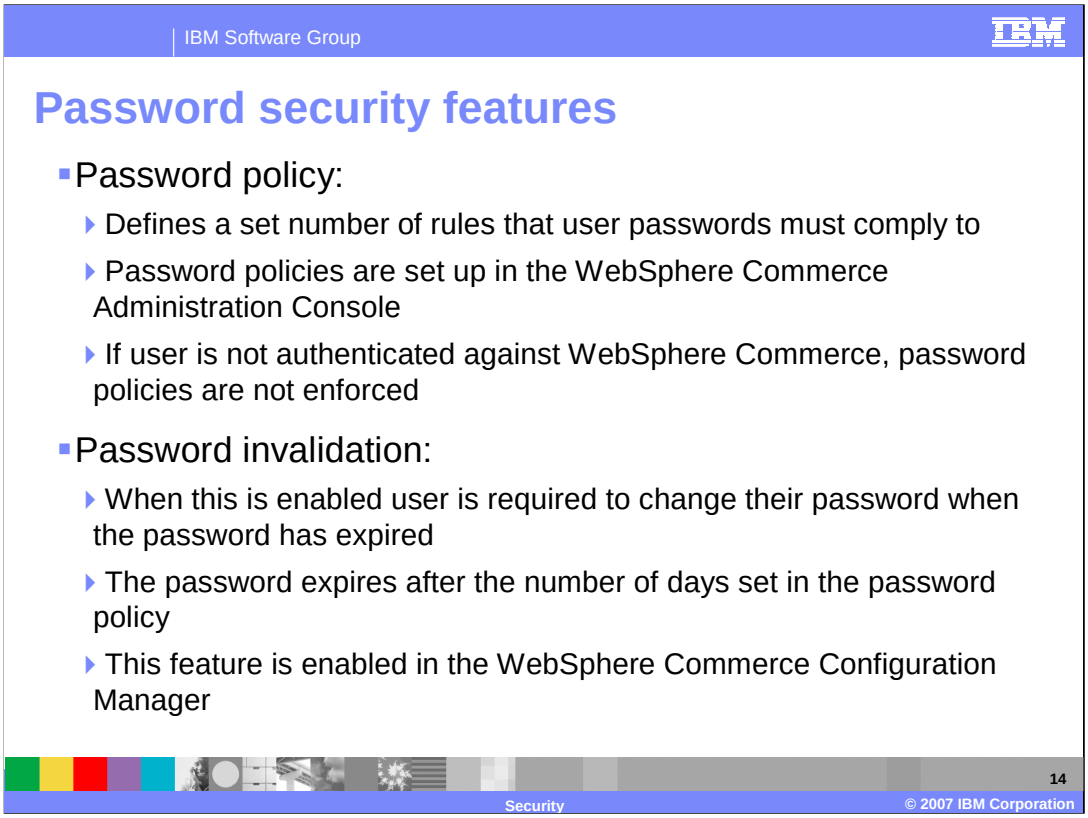
Account lockout policies are specified using the WebSphere Commerce Administration Console.

You can set the account lockout threshold to disable a user account after the set number of invalid login attempts.

You can also set the consecutive unsuccessful login delay. This is the amount of time that a user will not be able to login after two failed login attempts. The delay will increase by the configure value with every additional consecutive failure

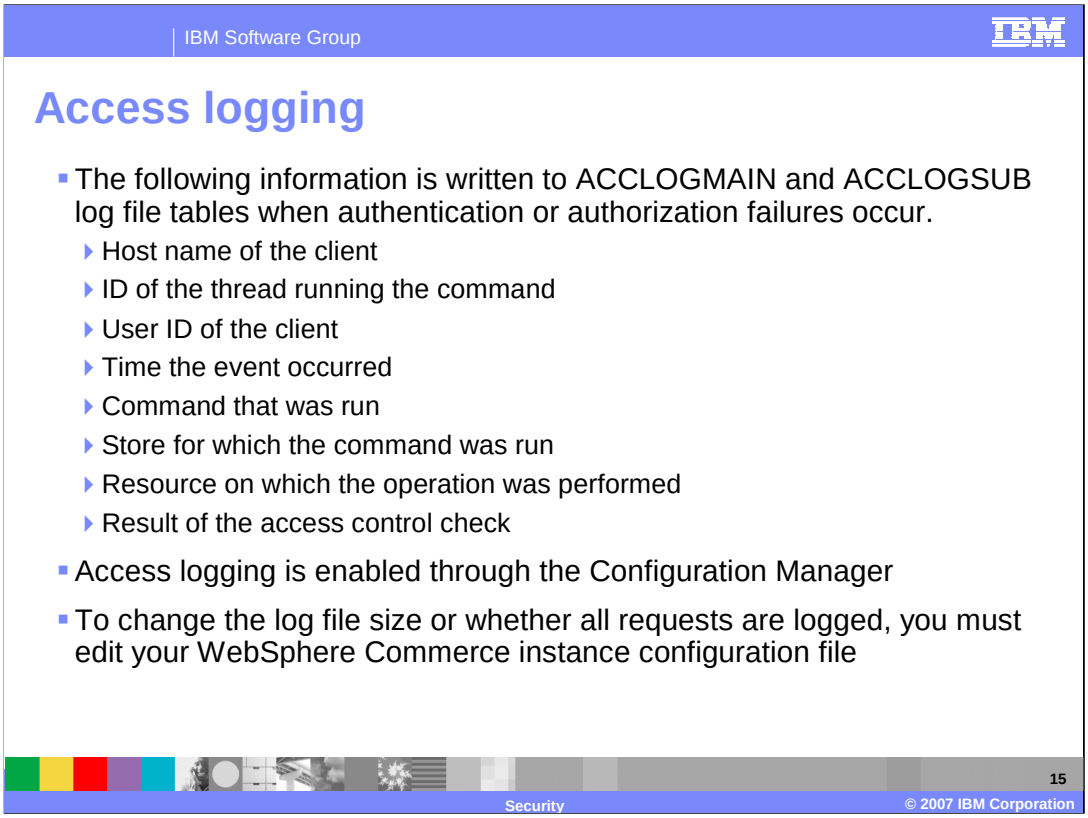
For information about creating account lockout policies, see the WebSphere Commerce V6 information center on setting up an account lockout policy. These policies are one part of an account policy. Password policies are the other part.

Login timeout policies are configured using the Configuration Manager. By default, a timeout policy of 30 minutes is in effect.



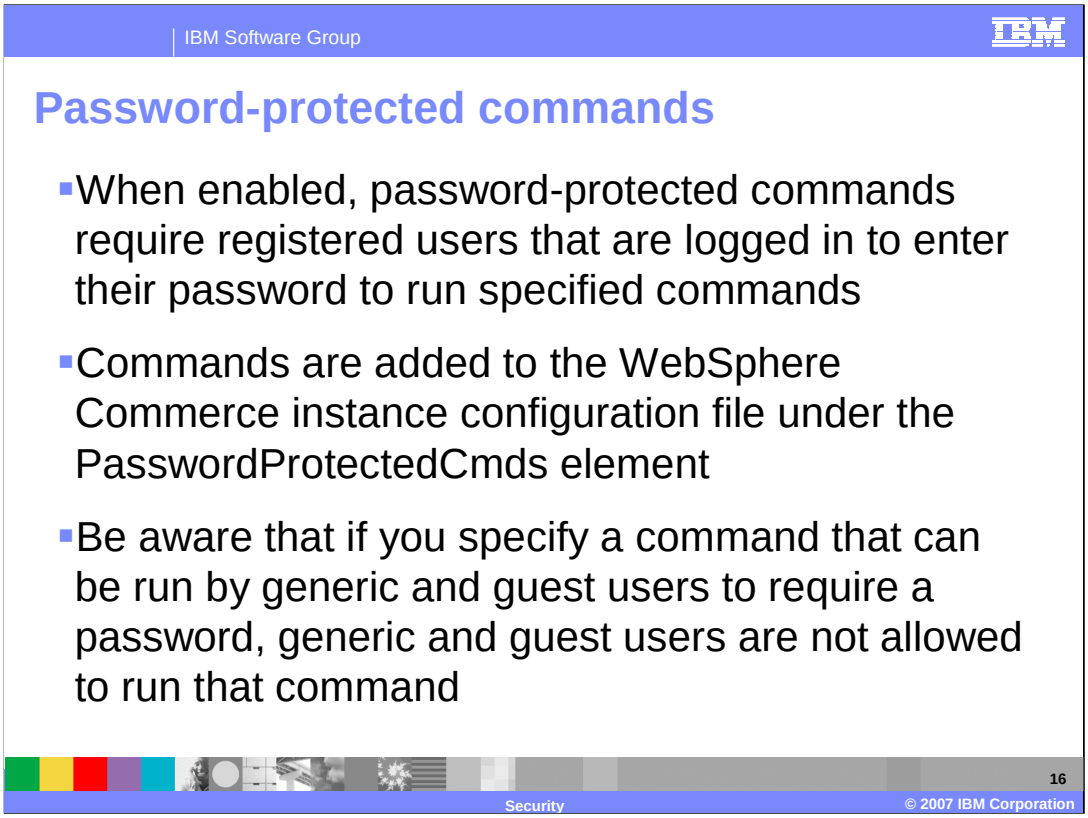
You can configure your password policy to enforce rules that have maximum occurrence of consecutive characters, instances of any character and lifetime of the passwords. The password policy can also enforce rules that have a minimum number of alphabetic characters, number of numeric characters and length of password. You cannot delete a password policy that is in use.

Password policies are part of an account policy. These are defined using the WebSphere Commerce Administration Console. The password invalidation feature can be enabled or disabled using the Configuration Manager. The length of time after which a password becomes invalid is defined as part of a password policy.



When enabled, the access logging feature logs either all incoming requests to the WebSphere Commerce Server or only the requests resulting in access violations. Examples of access violations are authentication failure or insufficient authority to run a command. When enabled, access logging allows a WebSphere Commerce administrator to quickly identify security threats to the WebSphere Commerce system.

The slide shows all the information that will be written to the ACCLOGMAIN and ACCLOGSUB log file tables when authentication or authorization failures occur. Access logging is enabled through the Configuration Manager. To change the log file size or whether all requests are logged, you must edit your WebSphere Commerce instance configuration file.



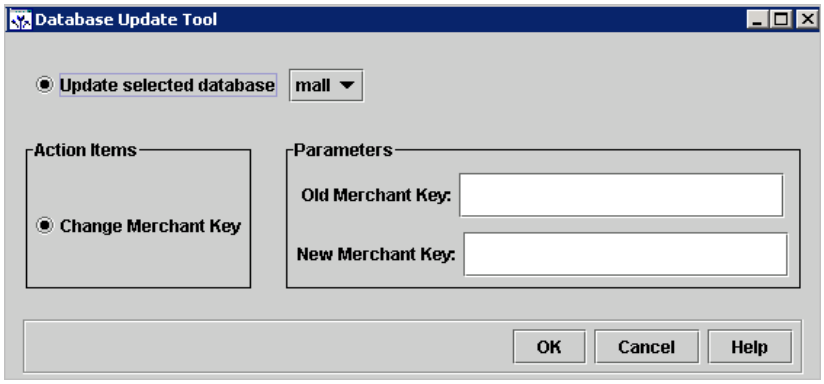
When the password-protected commands feature is enabled, WebSphere Commerce requires registered users who are logged onto WebSphere Commerce to enter their password before continuing a request that runs designated WebSphere Commerce commands.

When you configure password-protected commands, be aware of the consequences of specifying a command that can be run by generic and guest users. Configuring such commands as password-protected will prevent generic and guest customers from running them.

For information about enabling the password protected commands feature, see enabling password protected commands in the WebSphere Commerce V6 Information Center.

Merchant key migration

- If you suspect your merchant key has been compromised, you can update the merchant key
- You can migrate to a new merchant key using WebSphere Commerce Configuration Manager Update Database tool:
  - This is only available to use if the merchant key is in the instance.xml file



You can change the merchant key and update the encrypted data using the command line tool, MigrateEncryptedInfo. This utility supports two ways of specifying the values of the merchant keys. One is to provide the actual values of the old and new merchant keys as command line arguments. The other is to retrieve the values through the Key Locator Framework using MigrateEncryptedInfo.

The database update tool in configuration manager will update the merchant key and update all encrypted data in the database (for example passwords and credit card numbers.)

To run the Database Update tool first open Configuration Manager, and then expand the Instance Properties for your instance. Next, expand the database section for your instance and right click on your database and select Database Update Tool. Select the database to update and enter the old and new merchant keys. Click on OK to update the key and encrypted data. Once it has finished running, restart your WebSphere Commerce server.

Recommended courses

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

- 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 training paths for the skill or certification you want to explore.

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_Security.ppt

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

Access, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Enterprise JavaBeans, Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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.

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.

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.