



IBM Software Group

# IBM® WebSphere® Application Server V7

*Security in a flexible management environment*



@business on demand.

© 2008 IBM Corporation  
Updated September 24, 2008

This presentation will explain security in the new flexible management model introduced in WebSphere Application Server Version 7. It will explain how it is enabled and considerations involved when accessing secured servers in this environment.

## Agenda

- Enabling security in a flexible management environment
- Accessing secured components



This presentation provides an overview of security in the flexible management environment. It looks at enabling security in this environment and then at accessing secured components.

## Section

# ***Enabling security in a flexible management environment***



This section describes how to enable security in a flexible management environment.

## Enabling flexible management security

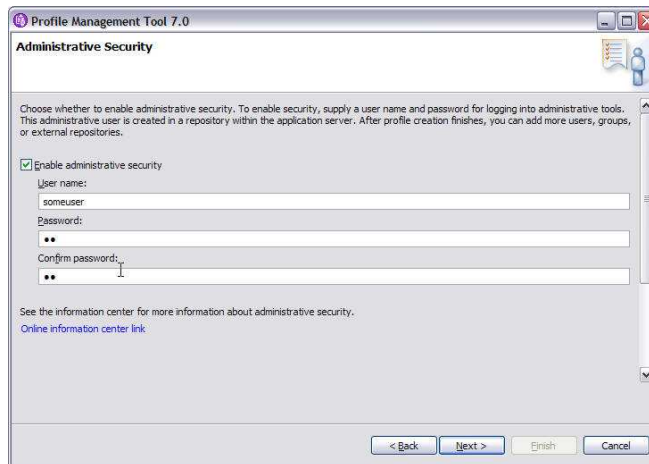
- Enabling security is very similar to the way administrative security is enabled for servers in WebSphere Application Server V6.1
- When security can be enabled:
  - ▶ During profile creation
  - ▶ After the profile has been created
- How security can be enabled:
  - ▶ Using profile creation
  - ▶ Using the administrative console
  - ▶ Using wsadmin
- Security **must** be enabled before registration with administrative agent or job manager



Enabling security in a flexible management environment is very similar to the way administrative security is enabled for servers in a WebSphere Application Server Version 6.1 environment. Just as in Version 6.1, security can be enabled during or after profile creation. However, in a flexible management environment, if security is to be enabled, it must be enabled before registration with the administrative agent or job manager.

## Enabling flexible management security

- Administrative security can be enabled from the Profile Management Tool during profile creation



The screenshot shows the 'Administrative Security' dialog box in the Profile Management Tool 7.0. The dialog has a title bar with the text 'Profile Management Tool 7.0' and standard window controls. The main content area is titled 'Administrative Security' and contains the following text: 'Choose whether to enable administrative security. To enable security, supply a user name and password for logging into administrative tools. This administrative user is created in a repository within the application server. After profile creation finishes, you can add more users, groups, or external repositories.' Below this text is a checked checkbox labeled 'Enable administrative security'. Underneath the checkbox are three input fields: 'User name:' with the text 'someuser', 'Password:', and 'Confirm password:'. At the bottom of the dialog are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. A small icon of a person is visible in the top right corner of the dialog box.

This page shows security being enabled during profile creation. It is the same panel used to enable administrative security for other WebSphere servers. The same procedures used to enable administrative security for WebSphere servers with wsadmin or the administrative console also apply in a flexible management environment.

## Section

# ***Accessing secured components***



This part of the presentation discusses considerations that must be made when accessing secured components in a flexible management environment.

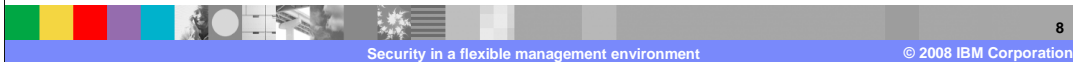
## Accessing secured components

- Accessing secured servers in a flexible management environment is similar to the way administrative security is enabled for servers in WebSphere Application Server V6.1
- In a flexible management environment, security must be considered when accessing:
  - ▶ Job manager
  - ▶ Administrative agent
  - ▶ Application server
- Each of the above can have a different username password that must be used

In a network deployment environment, a single username and password is used to access all systems. In a flexible management environment each job manager, administrative agent, and application server can have a different username and password combination.

## Security considerations

- Starting a secured server does not require *username* and *password*
- Accessing a secured server through the administrative console or wsadmin does require *username* and *password*
- Stopping a secured server does require *username* and *password*

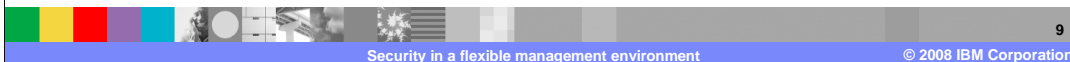


This page briefly describes when security must be considered for a server. No username or password is required to start a server – even if it is security enabled. Administrative access, for example using the administrative console or wsadmin, to a secured server always requires a username and password. Stopping a secured server also requires a username and password. Some implications of the above are shown on the next few slides.



## Administrative agent security considerations

- If administrative agent has administrative security enabled:
  - ▶ Must provide username and password for administrative agent when registering an application server node with administrative agent
- If application server has administrative security enabled:
  - ▶ Must provide username and password for that server when registering with the administrative agent
- Sample command:
  - ▶ `registerProfile.bat <all normal parameters>`
  - ▶ `-username <adminagent_username> -password`
  - ▶ `<adminagent_password> -nodeusername`
  - ▶ `<base_node_username> -nodepassword`
  - ▶ `<base_node_password>`



If the administrative agent is secured, then the username and password for the administrative agent will need to be given when registering a base node. If the base node is secured, then the username and password for the base node will also need to be given when the base node is registered. Additional keyword parameters are provided in the registerProfile command to support this.

## Job manager security considerations

- If job manager has administrative security enabled:
  - ▶ Must provide username and password for job manager when registering an application server node with the job manager
- If administrative agent has administrative security enabled:
  - ▶ Must provide username and password for administrative agent when registering with the job manager
- Sample commands for starting wsadmin and doing registration:
  - ▶ `wsadmin.bat -profileName <adminagent_profile_name> -user <adminagent_username> -password <adminagent_password>`
  - ▶ `AdminTask.registerWithJobManager('[-port 9943 -user <jobmgr_username> -password <jobmgr_password> -managedNodeName <managed_node_name>]')`

10

Security in a flexible management environment

© 2008 IBM Corporation

If the job manager is secured, then the username and password for the job manager will need to be given when registering a base node. If the administrative agent is secured, then the username and password for the administrative agent will also need to be given when the base node is registered with the job manager. The username and password for the administrative agent are specified on the command line to wsadmin. The username and password for the job manager are specified as parameters to the AdminTask.registerWithJobManager command.

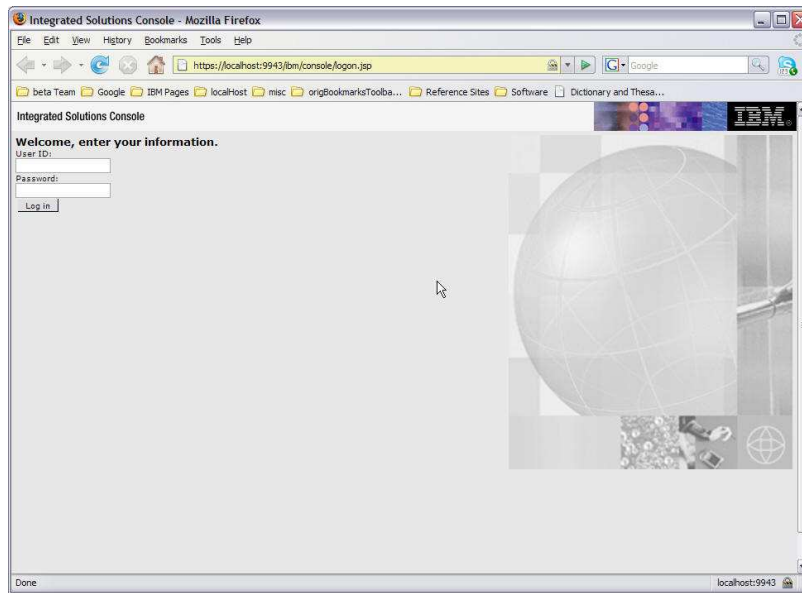
## Job manager security considerations

- Scenario:
  - ▶ You want to submit a job from the job manager to an application server in a managed node
  - ▶ Administrative security is enabled on the job managed and the application
- In this case, credentials for both the job manager and the application server need to be provided
  - ▶ Username and password for job manager need to be entered to access job manager through the job manager console
  - ▶ Username and password for application server need to be sent with other information when job is submitted



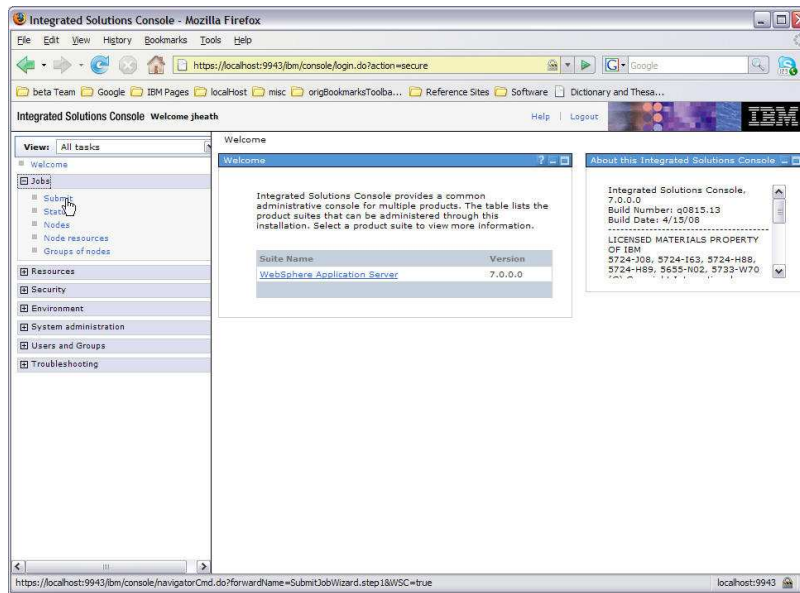
If both the job manager and the managed node have security enabled, then you will need to provide both sets of security credentials to submit a job to the application server in the managed node. To access the job manager's administrative interfaces, like the administrative console, you need to provide the job manager's username and password. To submit the job to the application server, you need to provide the application server's username and password.

## Flexible management security



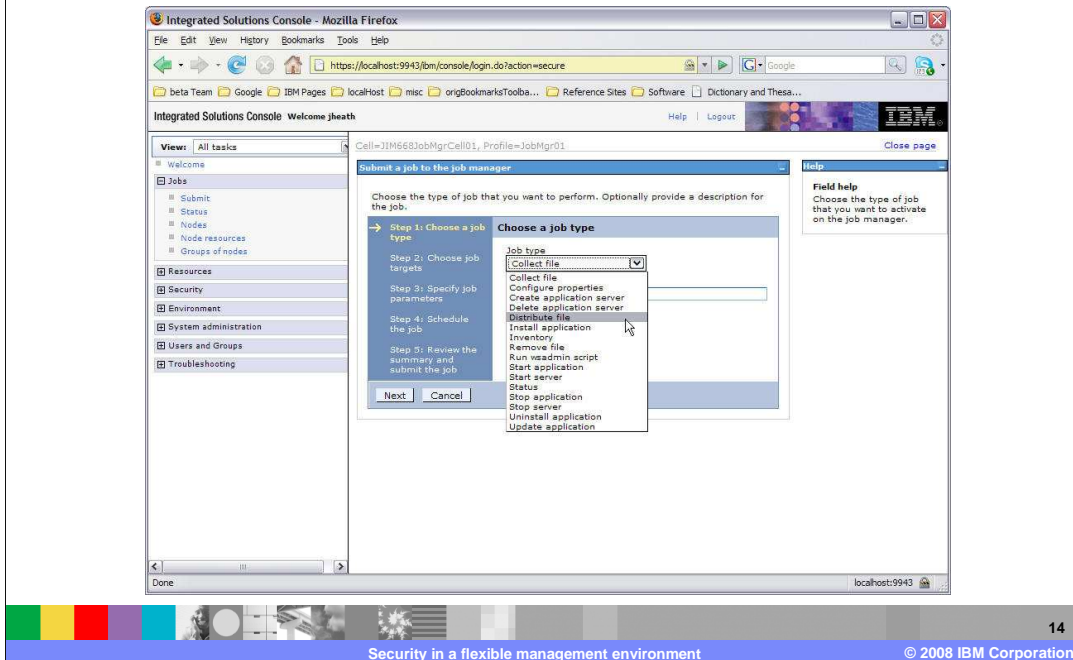
If administrative security is enabled on the job manager, you need to provide the administrative user ID and password to authenticate to the job manager's console.

## Flexible management security



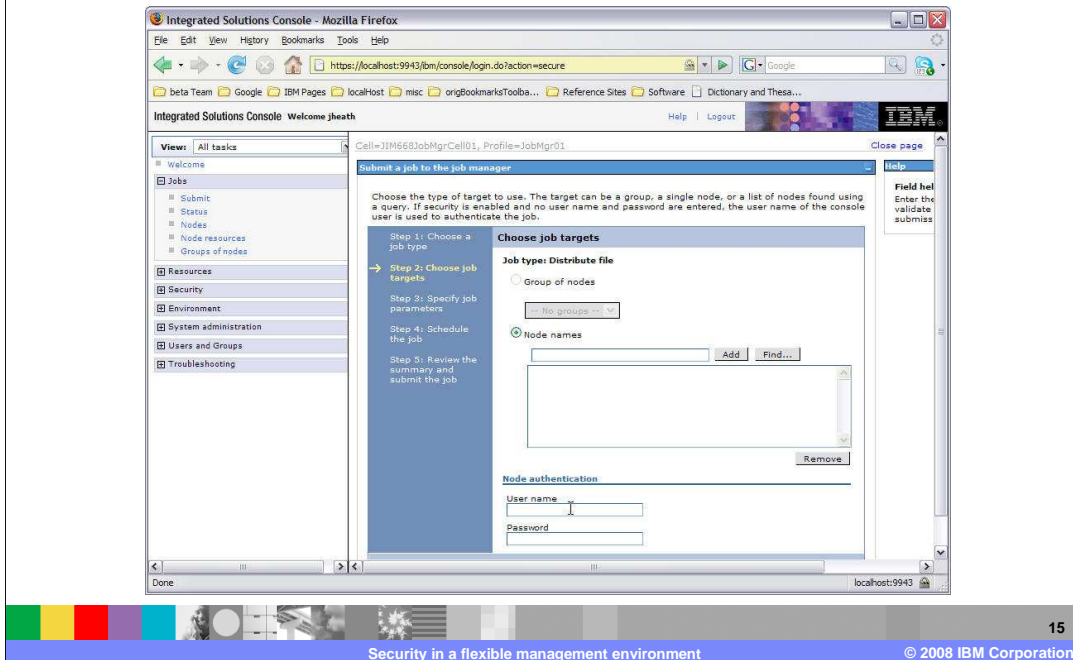
You can use the job manager's console to submit a job to the managed application server. In the left navigation menu, expand Jobs and then select Submit.

## Flexible management security



There are several different types of flexible management jobs that you can submit to the application server. In this case, assume that you want to send a file to the system where the application server is running, so you choose the “Distribute file” job type.

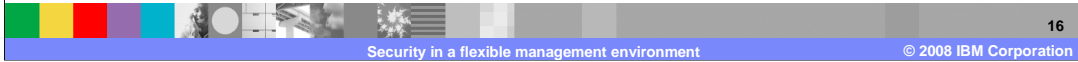
## Flexible management security



On the panel, you configure the target node where you are submitting your job. Near the bottom of the panel are fields to provide authentication information for the node. This is where you need to provide the administrative security username and password for the application server in the managed node.

## Section

# *Summary*



This section contains a summary of security considerations for flexible management.



## Summary

- Enabling security in a flexible management environment is similar to enabling administrative security in other WebSphere environments
- Unlike the network deployment environments, each server in a flexible management environment might have its own username and password



In many ways, security in a flexible management environment is similar to administrative security in a network deployment environment. Access to a secured server is allowed by passing the username and password. However, unlike the network deployment environments where a single username and password will allow access to all servers, in a flexible management environment, each server might have its own username and password.

## 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\\_WASv7\\_FlexMgtSecurity.ppt](mailto:iea@us.ibm.com?subject=Feedback_about_WASv7_FlexMgtSecurity.ppt)

This module is also available in PDF format at: [..\\WASv7\\_FlexMgtSecurity.pdf](..\\WASv7_FlexMgtSecurity.pdf)



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

A current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

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 NON-INFRINGEMENT. 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.

© Copyright International Business Machines Corporation 2008. All rights reserved.

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.

