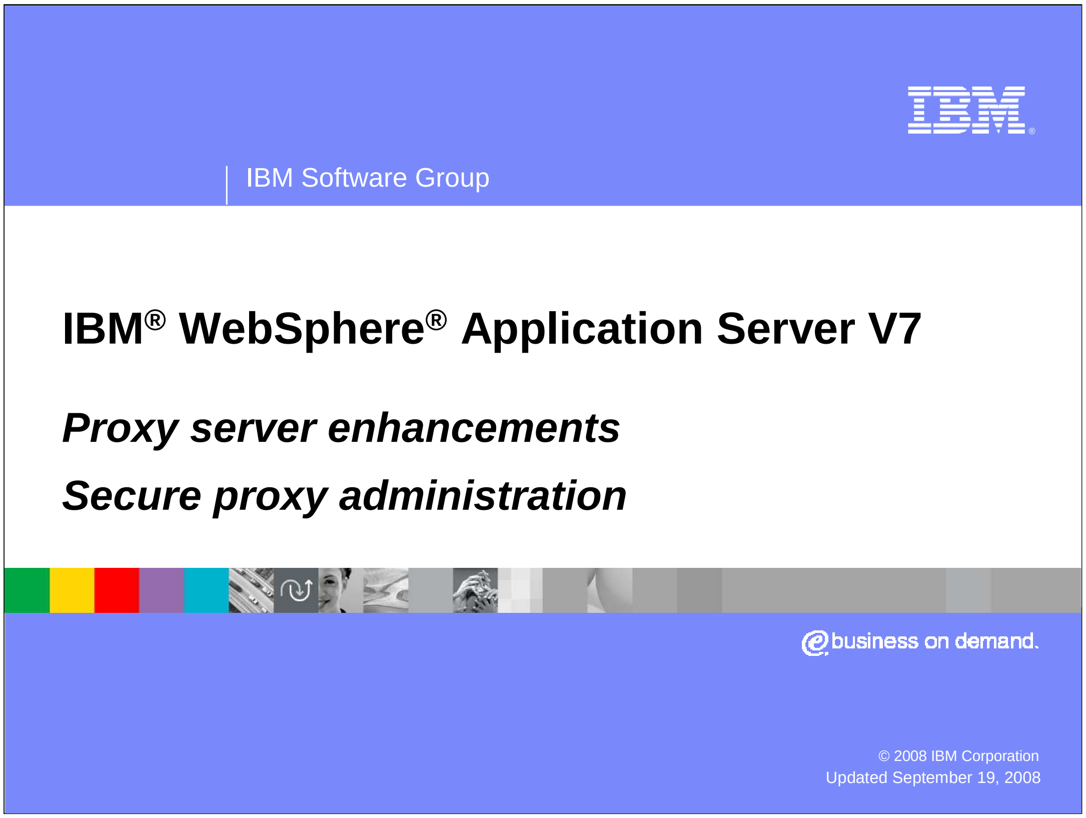


IBM Software Group

IBM® WebSphere® Application Server V7

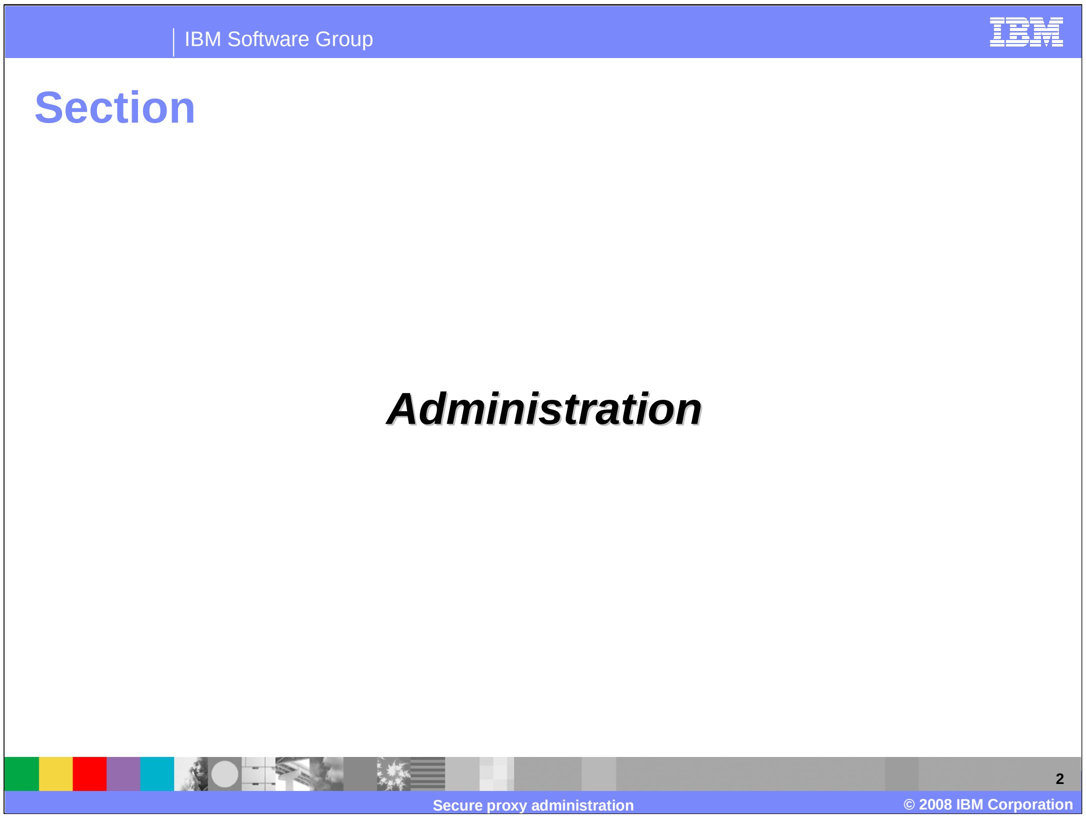
Proxy server enhancements

Secure proxy administration

business on demand.

Updated September 19, 2008

This presentation discusses the secure proxy server administration as found in IBM WebSphere Application Server V7.

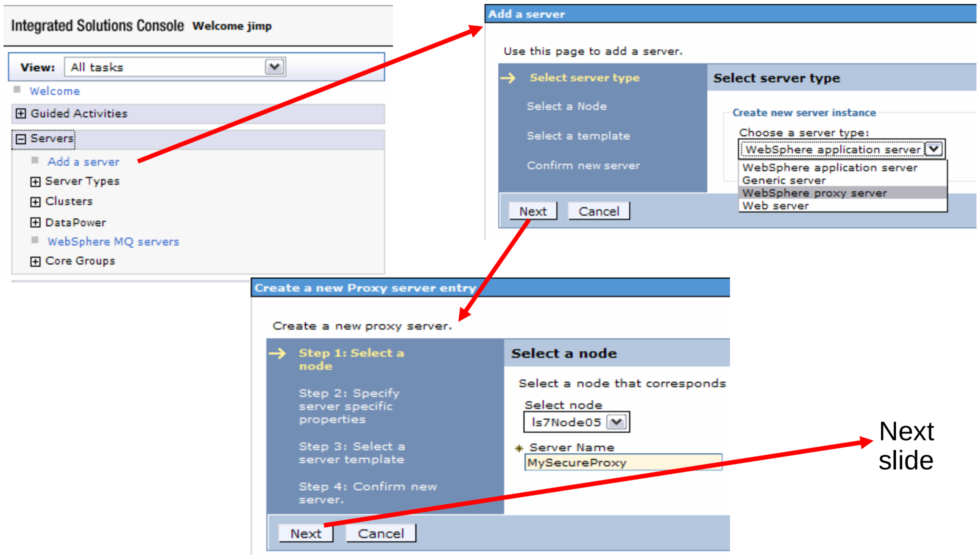


Section

Administration

The next section presents administering a secure proxy server with the administrative agent and scripting.

Create DMZ proxy server (console)



Add a server

Use this page to add a server.

Select server type

Create new server instance

Choose a server type: WebSphere application server

Create a new Proxy server entry

Create a new proxy server.

Step 1: Select a node
Step 2: Specify server specific properties
Step 3: Select a server template
Step 4: Confirm new server.
Next
Cancel

Select a node

Select a node that corresponds

Select node: ls7Node05

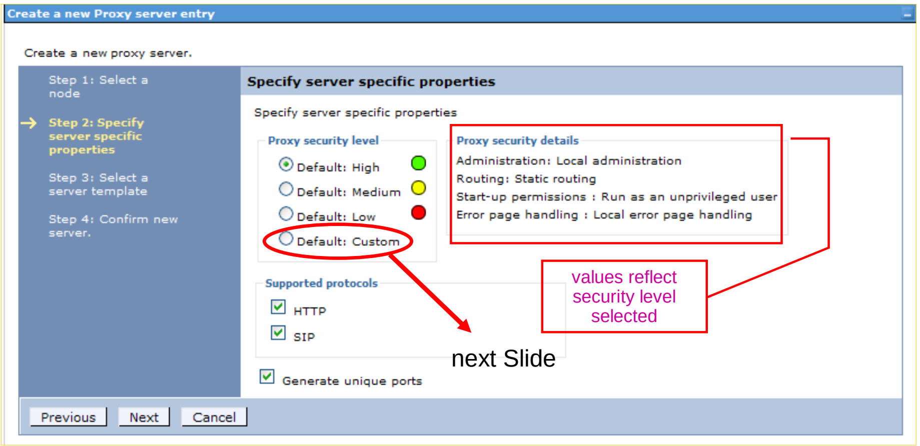
* Server Name: MySecureProxy

Next slide

There are two ways to create a secure proxy server. The first is with the profile management tool. The second is with the console in the administrative agent. Notice that you use the administrative client to create or maintain a classical proxy server and a classical proxy server cannot be converted to a secure proxy server. In a similar manor, a secure proxy cannot be converted to a classical proxy server.

This slide demonstrates using the administrative agent’s console to create a secure proxy. This console and the wizard have the same layout as the administrative client. Here you select the *add a server* wizard under *servers* in the left menu. Next select *WebSphere proxy server* from the pull down list. After selecting a node to host the secure proxy, you proceed to the next slide.

Select security level



Create a new Proxy server entry

Create a new proxy server.

Step 1: Select a node

→ Step 2: Specify server specific properties

Step 3: Select a server template

Step 4: Confirm new server.

Specify server specific properties

Specify server specific properties

Proxy security level

● Default: High 🟢

○ Default: Medium 🟡

○ Default: Low 🔴

○ Default: Custom

Proxy security details

Administration: Local administration

Routing: Static routing

Start-up permissions : Run as an unprivileged user

Error page handling : Local error page handling

Supported protocols

☑ HTTP

☑ SIP

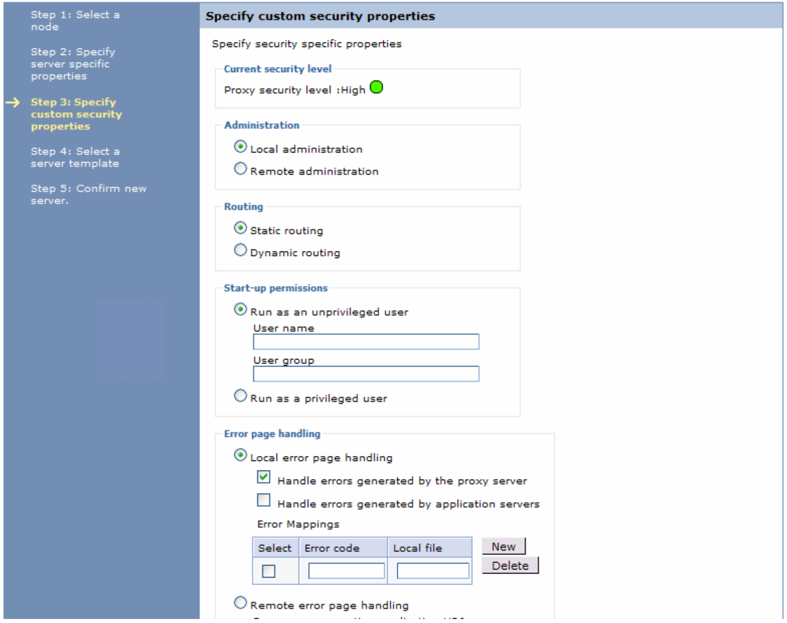
☑ Generate unique ports

values reflect security level selected

next Slide

On this panel you can select one of the default security configurations or you can select custom to decide to set each of the four security components yourself. The three predefined security levels were discussed earlier. The corresponding values for each of the four selectable security components discussed earlier are shown to the right. The high security button is selected here and you can see the associated values: local Administration or local SOAP, static routing, run as unprivileged and local error page handling. For completeness, the custom screen is shown on the next slide. To get to the custom screen select the “Default: Custom” button and click next.

Specify custom security properties



Step 1: Select a node

Step 2: Specify server specific properties

→ Step 3: Specify custom security properties

Step 4: Select a server template

Step 5: Confirm new server.

Specify custom security properties

Specify security specific properties

Current security level

Proxy security level :High ●

Administration

● Local administration

○ Remote administration

Routing

● Static routing

○ Dynamic routing

Start-up permissions

● Run as an unprivileged user

User name

User group

○ Run as a privileged user

Error page handling

● Local error page handling

☑ Handle errors generated by the proxy server

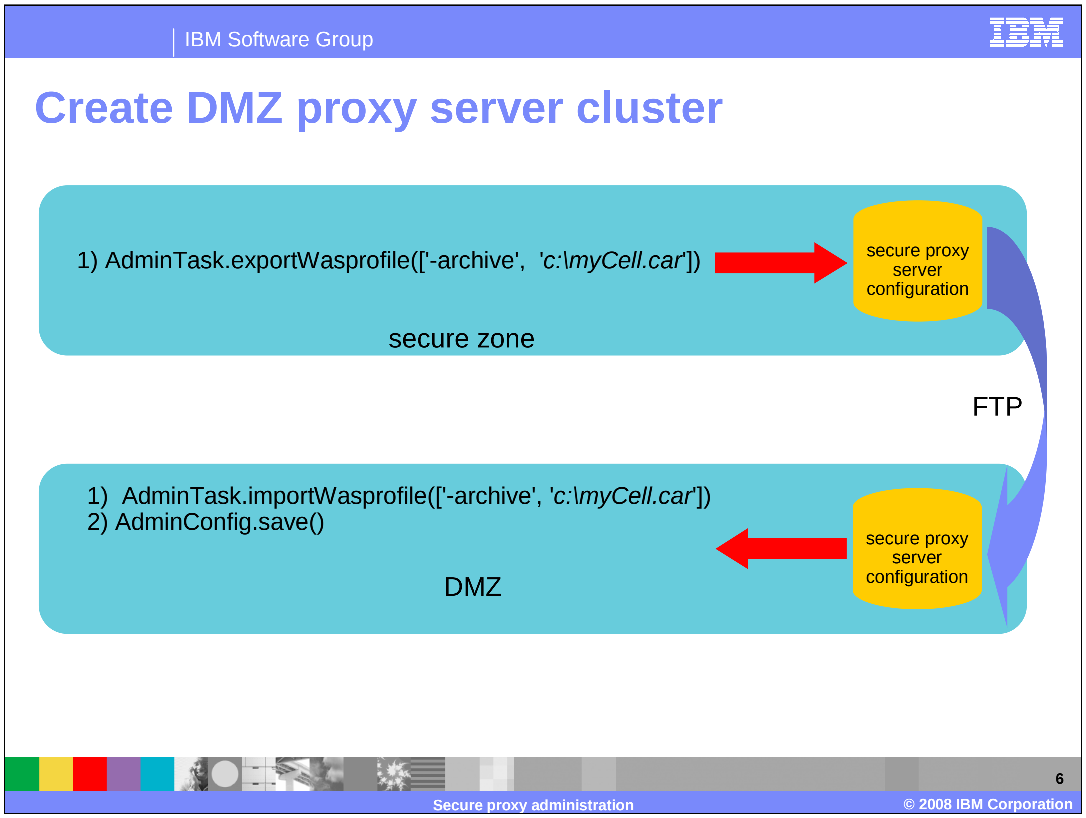
☐ Handle errors generated by application servers

Error Mappings

Select	Error code	Local file
☐		

○ Remote error page handling

This is the custom security level screen in the *create a secure proxy* wizard. You can get to a similar screen for maintenance later. You can see the possible selections for each of the four configurable security components. Now that you have defined a new proxy server, it is time to create it on the next slide.



IBM Software Group

Create DMZ proxy server cluster

1) AdminTask.exportWasprofile(['-archive', '*c:\myCell.car*'])

secure proxy server configuration
secure zone
FTP
secure proxy server configuration
DMZ

1) AdminTask.importWasprofile(['-archive', '*c:\myCell.car*'])
2) AdminConfig.save()

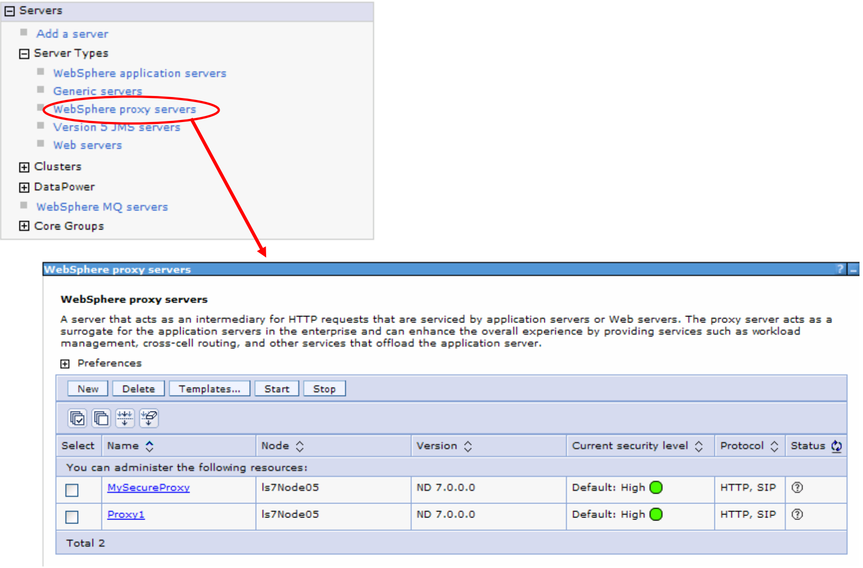
6

Secure proxy administration

© 2008 IBM Corporation

This slide shows creating managing a secure proxy server without an administrative agent in the DMZ and the proxy server requires local SOAP. What you have to do is use scripting to create a file containing the command to create a secure proxy server. Move these commands to the target host in the DMZ where you have installed the reduced capability WebSphere V7 libraries. Finally, using scripting again, you create the secure proxy in the DMZ. One side effect of this is you create a fully functioning ghost copy of the secure proxy server in the secure zone and this is a good thing. You never need to start the ghost copy but you can use the console of the administrative agent to administer your secure proxy and follow the same process to perform the changes.

Change security level (administrative console)



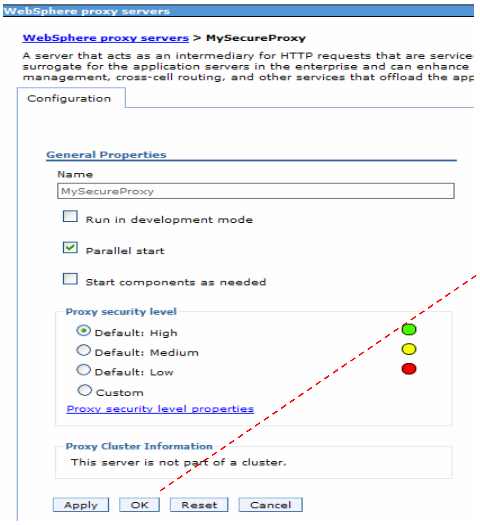
WebSphere proxy servers

A server that acts as an intermediary for HTTP requests that are serviced by application servers or Web servers. The proxy server acts as a surrogate for the application servers in the enterprise and can enhance the overall experience by providing services such as workload management, cross-cell routing, and other services that offload the application server.

Select	Name	Node	Version	Current security level	Protocol	Status
You can administer the following resources:						
☐	MySecureProxy	ls7Node05	ND 7.0.0.0	Default: High ●	HTTP, SIP	?
☐	Proxy1	ls7Node05	ND 7.0.0.0	Default: High ●	HTTP, SIP	?
Total 2						

This slide and the next show how to manage a secure proxy server, in particular how to manage the security levels. Again in the administrative agents console select “Servers -> Server Types -> WebSphere proxy servers”. Then click on your proxy server, in this case “MySecureProxy”.

Change security level (continued)



WebSphere proxy servers

WebSphere proxy servers > MySecureProxy

A server that acts as an intermediary for HTTP requests that are service surrogate for the application servers in the enterprise and can enhance management, cross-cell routing, and other services that offload the app

Configuration

General Properties

Name

MySecureProxy

□ Run in development mode

☑ Parallel start

□ Start components as needed

Proxy security level

● Default: High 🟢

○ Default: Medium 🟡

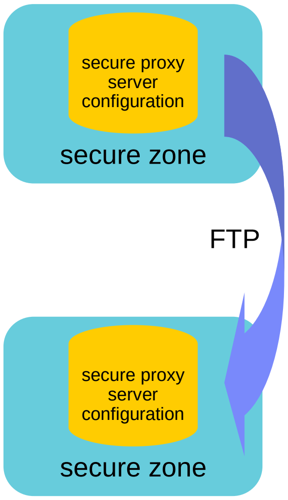
○ Default: Low 🔴

○ Custom

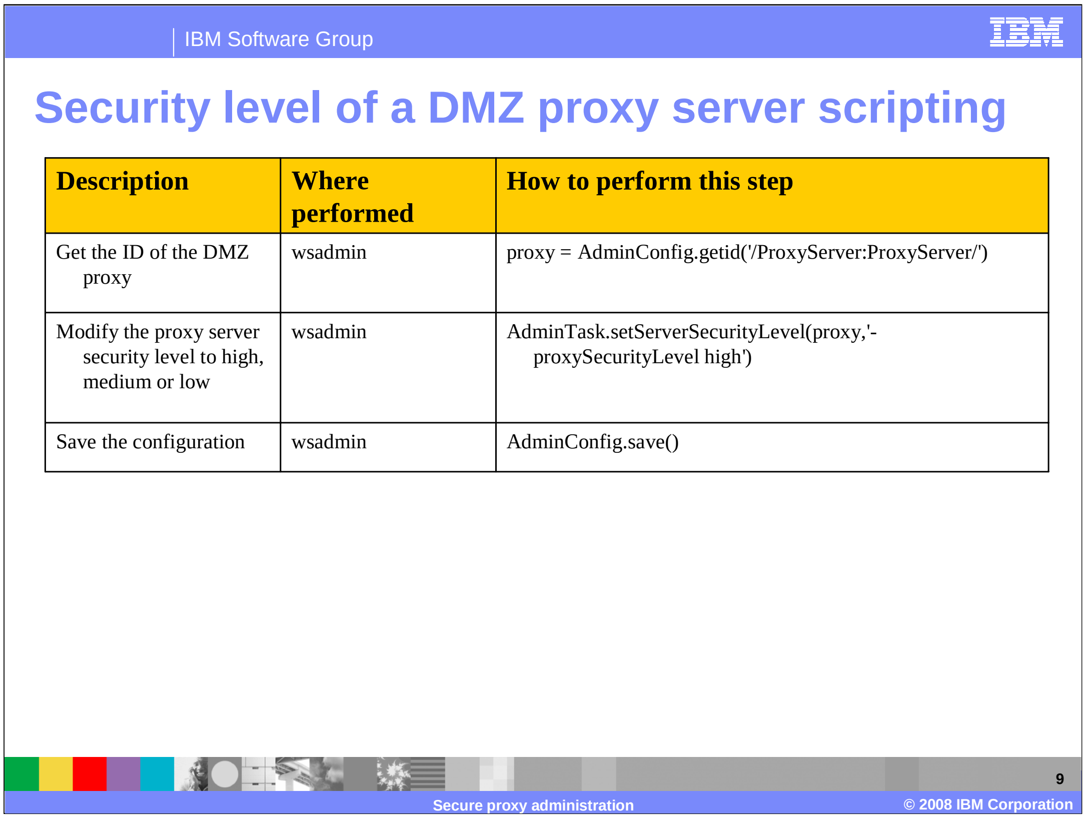
Proxy security level properties

Proxy Cluster Information

This server is not part of a cluster.


secure proxy server configuration
secure zone
FTP
secure proxy server configuration
secure zone

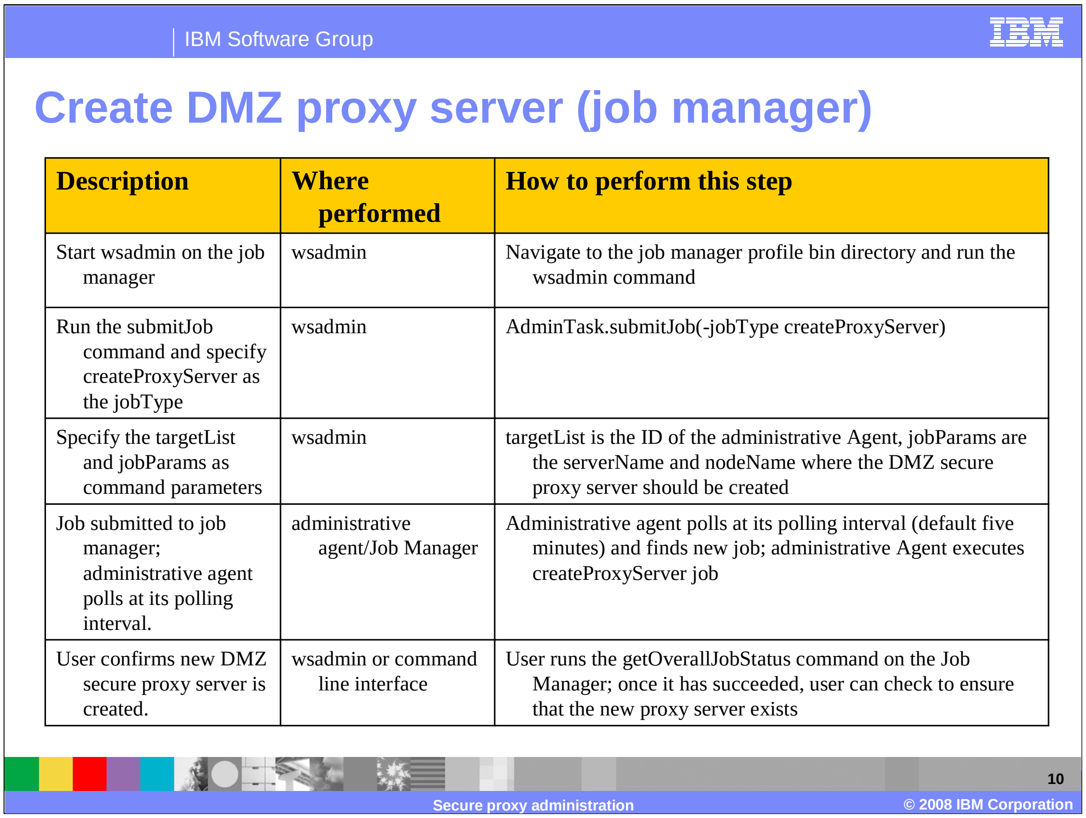
Modify the security level as required, if you select custom you will get the same options you viewed during secure proxy server creation. Here again this slides assumes you are working in the secure zone and the proxy server requires local SOAP so you have to use scripting and FTP again to cause the change to actually happen.



Security level of a DMZ proxy server scripting

Description	Where performed	How to perform this step
Get the ID of the DMZ proxy	wsadmin	proxy = AdminConfig.getid('/ProxyServer:ProxyServer/')
Modify the proxy server security level to high, medium or low	wsadmin	AdminTask.setServerSecurityLevel(proxy,'-proxySecurityLevel high')
Save the configuration	wsadmin	AdminConfig.save()

This chart shows the wsadmin steps you use to change the default security level of a secure proxy server. On the right column are the script commands. As always if the security level of the secure proxy server requires local SOAP you need to issue these commands on the host where the secure proxy resides.



IBM Software Group

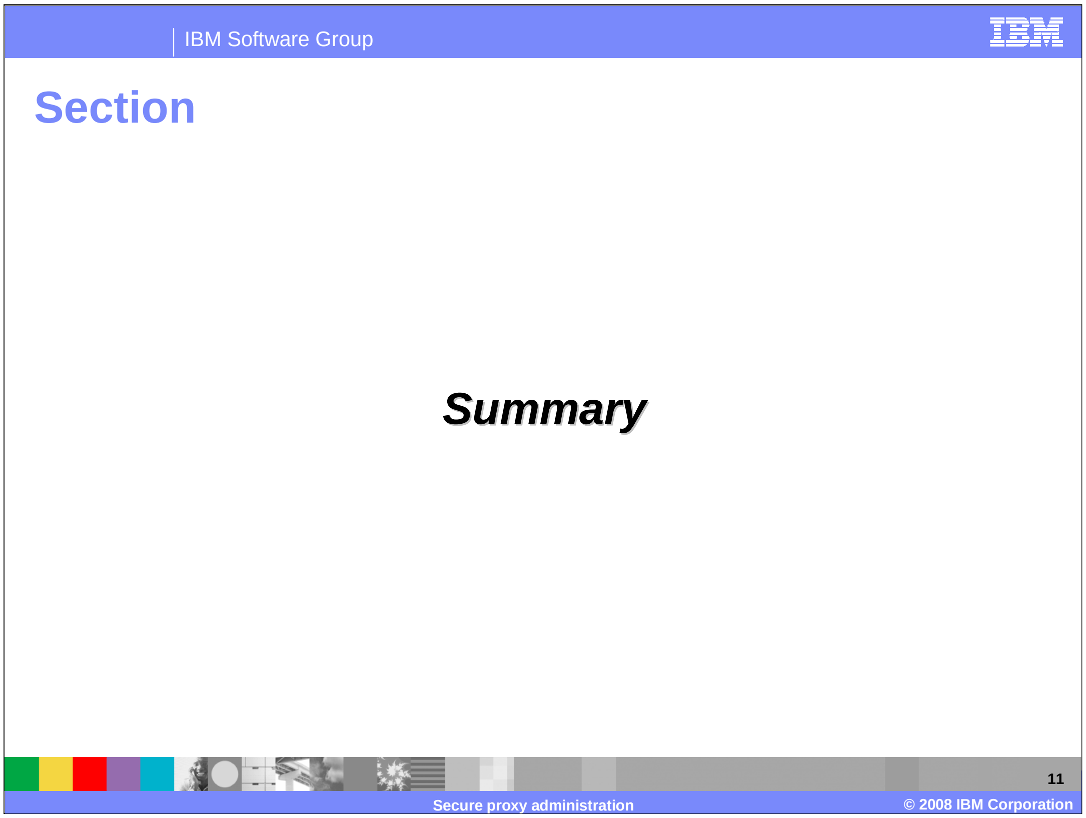
Create DMZ proxy server (job manager)

Description	Where performed	How to perform this step
Start wsadmin on the job manager	wsadmin	Navigate to the job manager profile bin directory and run the wsadmin command
Run the submitJob command and specify createProxyServer as the jobType	wsadmin	AdminTask.submitJob(-jobType createProxyServer)
Specify the targetList and jobParams as command parameters	wsadmin	targetList is the ID of the administrative Agent, jobParams are the serverName and nodeName where the DMZ secure proxy server should be created
Job submitted to job manager; administrative agent polls at its polling interval.	administrative agent/Job Manager	Administrative agent polls at its polling interval (default five minutes) and finds new job; administrative Agent executes createProxyServer job
User confirms new DMZ secure proxy server is created.	wsadmin or command line interface	User runs the getOverallJobStatus command on the Job Manager; once it has succeeded, user can check to ensure that the new proxy server exists

10

Secure proxy administration

As a final example of administering to a proxy server, here is an example of using the job manager to create a secure proxy server. The administrative agent used here is required to be on the same host as the destination secure server. Any intervening network firewalls need to allow communication between the job manager and the administrative agent. The pull semantics of the administrative agent helps make this secure, but this configuration might not meet your security requirements.



IBM Software Group

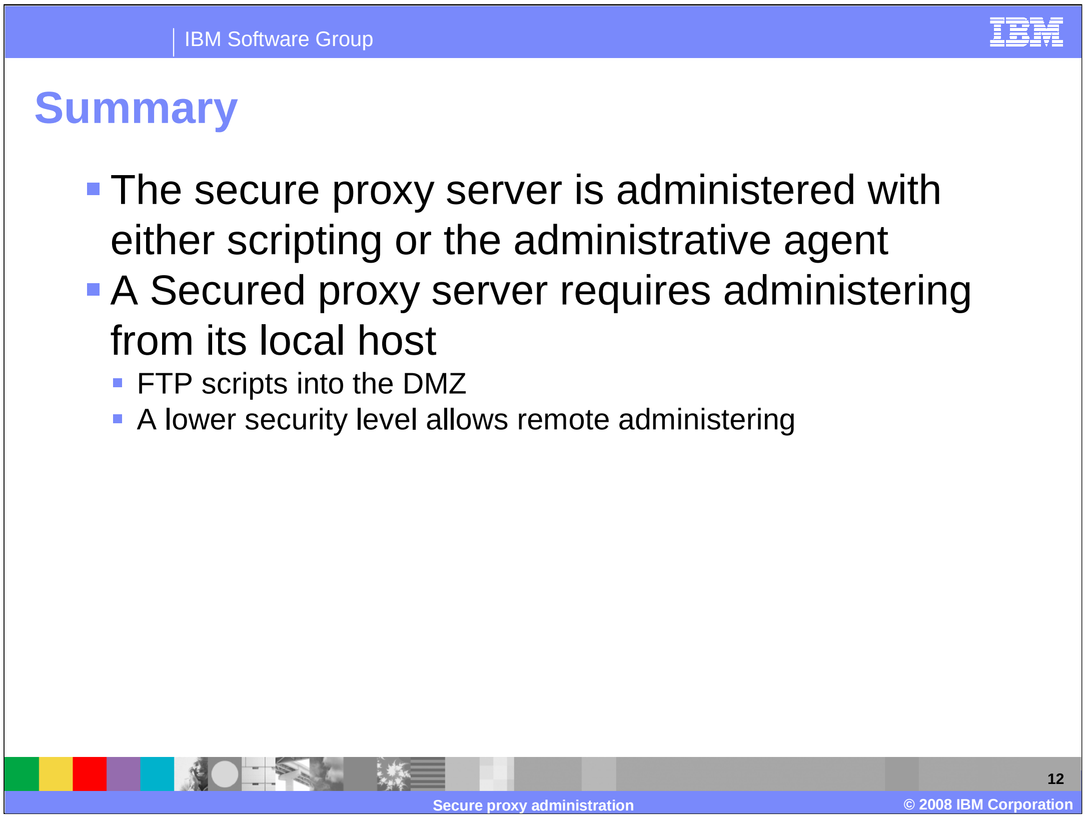
Section

Summary

11

Secure proxy administration

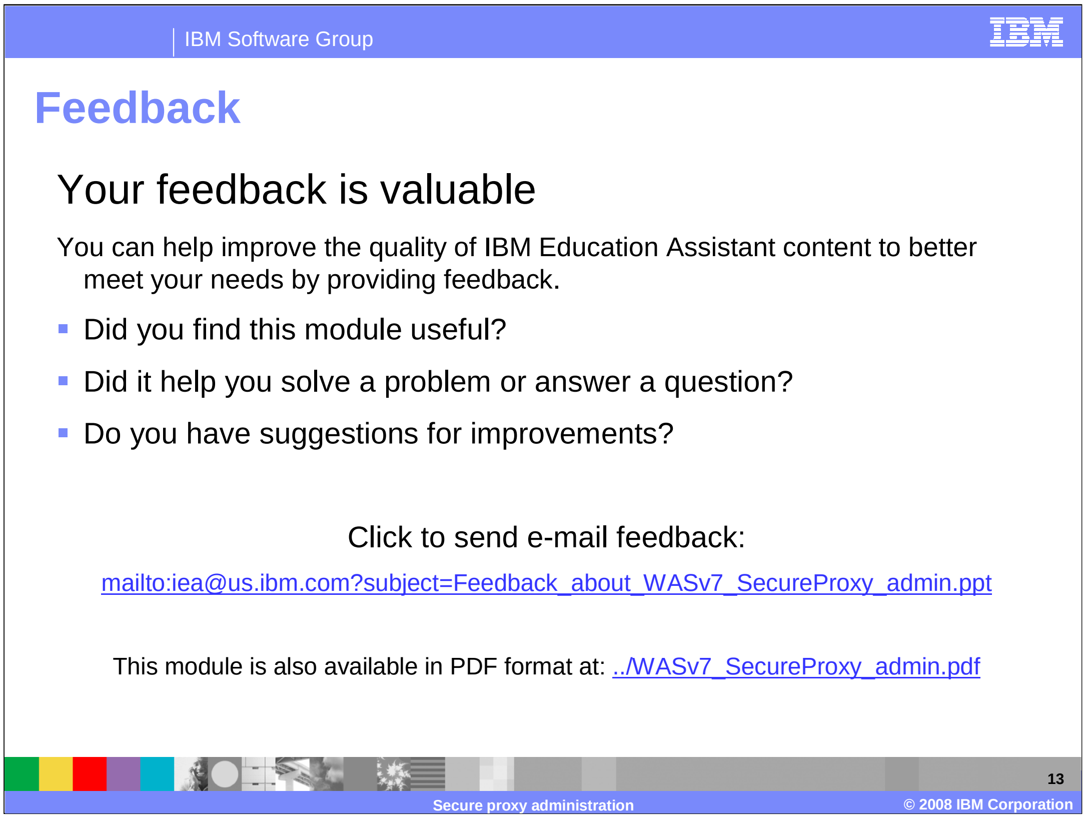
The following slide summarizes the secure proxy server.



Summary

- The secure proxy server is administered with either scripting or the administrative agent
- A Secured proxy server requires administering from its local host
  - FTP scripts into the DMZ
  - A lower security level allows remote administering

Administration of a secure proxy server is different from other parts of WebSphere. Scripts can be created that you are responsible for moving into a DMZ and running there. Alternately, you can administer a secure proxy server locally or if you chose a lower security option, you can administer a secure proxy server from a remote host.



Feedback

Your feedback is valuable

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

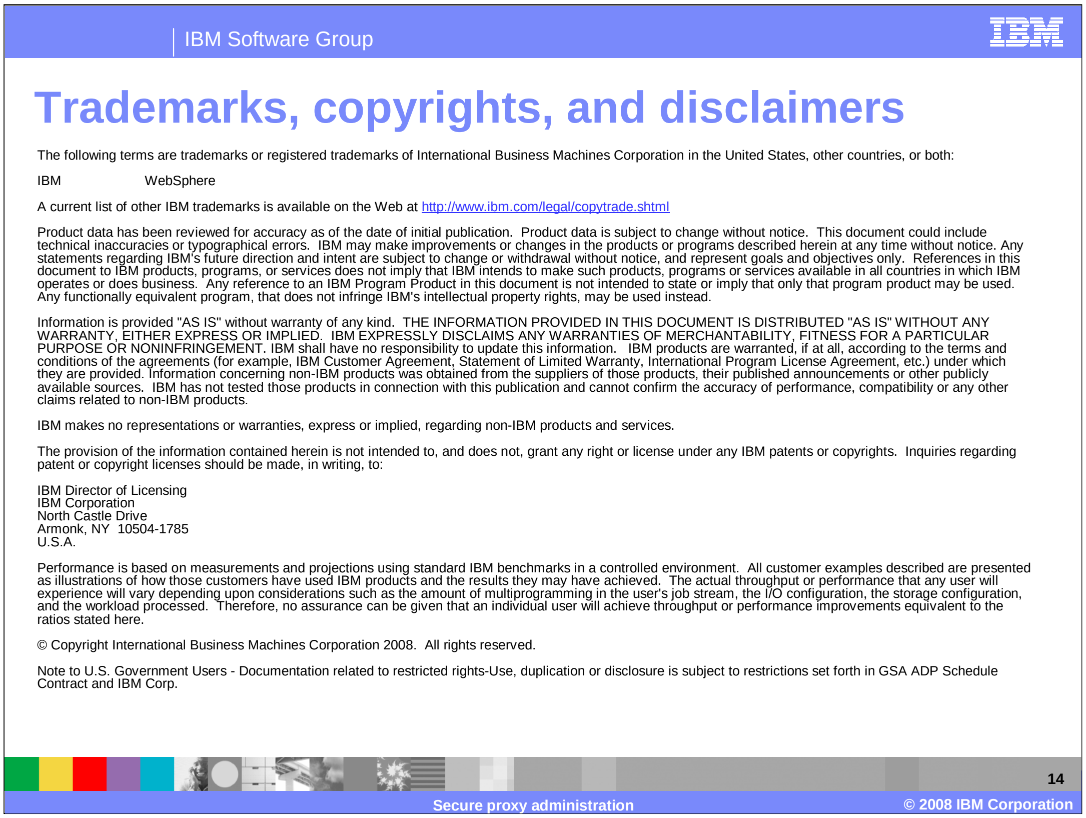
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASv7_SecureProxy_admin.ppt

This module is also available in PDF format at: ../WASv7_SecureProxy_admin.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 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.