Disabling Global Security in Single Server and ND environments

Disabling Global security in the Single Server or Base environment

This section discusses only how to turn off Global security on WebSphere Application Server.

____ 1. Start the WebSphere Application Server administrative console by clicking `http://yourhost.domain:9090/admin` after starting the WebSphere Application Server. Log in with a predefined administrative ID and password (this is typically the server user ID specified when you configured the user registry).

____ 2. Click **Security > Global Security** and set the **Enabled** flag to **OFF** so that security gets disabled upon a server restart.

____ 3. Before restarting the server, log off the administrative console. You can log out by clicking **Log off** at the top menu bar.

____ 4. Stop the server by going to the command line in the WebSphere Application Server /bin directory and issuing the following command on one continuous line:

```
stopServer server1 -username <user_id> -password <password>
```

UNIX system: `/opt/WebSphere/AppServer/bin/stopServer.sh server1 –username <user_id> -password <password>`

____ 5. Issue the following command to restart the server : `startServer <server_name>`

UNIX system: `/opt/WebSphere/AppServer/bin/startServer.sh server1`

Disabling global security in the Network Deployment environment

____ **1.** Start the WebSphere Application Server administrative console by clicking `http://yourhost.domain:9090/admin` after starting the WebSphere Application Server. Log in with a predefined administrative ID and password (this is typically the server user ID specified when you configured the user registry).

____ **2.** Click **Security > Global Security** and set the **Enabled** flag to **OFF** so that security gets disabled upon a server restart and click **Save** so that the configuration is saved to the repository.

____ 3. Issue a force file sync command from the administrative console to push a copy of the new configuration to all of the running node agents. Failure for a node agent to get the security enabled configuration causes it to fail to communicate with the Deployment Manager due to lack of access (security is not enabled). To force a file synchronization on any specific node, issue the following command from the administrative console:

__ a. Go to **System Administration > Nodes** and select the check box beside all of the nodes. You do **not** need to select the Deployment Manager Node. Click **Full Resynchronize** to ensure the file synchronization has occurred. The status might indicate that the nodes already are synchronized. Once synchronization has been initiated, continue refreshing the view until the status displays as **Synchronized** for all nodes.

____ 4. Stop all processes including the Deployment Manager, node agents, and application servers.

__ a. Stop the application servers by clicking **Servers > Application Servers**, clicking each application server process, and clicking **Stop**.

__ **b.** Stop the node agents by clicking **System Administration > Node Agents**, clicking on each node agent process, and clicking **Stop**. If you have problem to stop the node agent, follow the steps down below in Network Deployment part of **How to disable Global security if using the Administrative Console fails to do it** section.

__ c. Stop the Deployment Manager by clicking **System Administration > Deployment Manager** and clicking **Stop**.

____ 5. Once all processes are stopped, manually restart the Deployment Manager and all node agents from the command line.

__ a. Restart the Deployment Manager process. You can do this by going to the Deployment Manager installation/bin directory and issue the command:

```
startManager.bat
```

UNIX system: `startManager.sh`

__ b. Restart all node agent processes by going to the node agent installation /bin directory and issuing the command:

```
startNode.bat
```

UNIX system: `startNode.sh`

____ 6. If any node agent fails to restart, manually resynchronize the configuration by going to the physical node and running the client nodeSync command. This client logs into the Deployment Manager and pulls down all of the configuration files to the Node Agent. To perform the manual resynchronization, complete the following:

__ a. If the Node Agent is started but not communicating with the Deployment Manager, stop the Node Agent by issuing a `stopServer` command. If security is enabled on this node agent, issue the following command:

```
stopNode -username <administrative_user_name> -password
<administrative_password>
```

__ a. Next, issue the command: `syncNode CELL_HOST 8879 -username <administrative_user_name> -password <administrative_password>`

CELL_HOST is the host name where the Deployment Manager resides. The port **8879** is the default SOAP connector port. If that port number is changed, specify the changed port. The `<administrative_user_name>` is the administrative user configured for the user registry.

__ b. Restart the node agent by issuing the following command: `startNode`

____ 7. Restart all application servers on each node agent. Start the servers by going back into the **Administrative Console Servers > Application Servers** and selecting the servers that you want to start. Click **Start**.

____ 8. If you go to **System Management > Nodes** and the status of the node is Unknown, go to that node, manually stop the node agent, perform configuration synchronization, and restart the node agent.

__ a. To stop the node agent, issue the command:

```
stopNode -username <administrative_user_name> -password
<administrative_password>
```

__ b. Perform configuration synchronization, by issuing the command:

```
syncNode CELL_HOST 8879 -username <administrative_user_name> -
password <administrative_password>
```

The CELL_HOST is the host name where the Deployment Manager resides. Port **8879** is the default SOAP connector port. If the post number is changed, specify the changed port. The `<administrative_user_name>` is the administrative user configured for the user registry.

__ c. To start the node agent, issue the command

```
startNode
```

UNIX system: `startNode.sh`

Security Problem Determination

If you encountered a problem, check the WebSphere Application Server `/logs/server_name/SystemOut.log` file for hints about the problems that occurred. There are no special requirements to view this log. It is located in the *installation_directory*/logs/*applicationServerName* directory, and by default is named `SystemOut.log`.

Network Deployment environment: If you have any problems restarting the node agents or application servers, review the output logs in the `WAS/logs/nodeagent` or WAS `/logs/server_name` directory, respectively.

There are two techniques that you can use to view the log for an application server.

____ 1. View the JVM log from the administrative console.

__ a. Start the administrative console.

__ b. Click **Troubleshooting > Logs and Trace** in the console navigation tree. To view the logs for a particular server, click on the server name to select it, and then click **JVM Logs**.

__ c. Select the runtime tab.

__ d. Click **View** corresponding to the log you want to view.

____ 2. View the log from the machine where they are stored.

__ a. Go to the machine where the logs are stored.

__ b. Open the file in a text editor or drag and drop the file into an editing and viewing program.

➢ ***Did security appear to initialize properly?***

A lot of security code is visited during initialization. So you will likely see problems there first if the problem is configuration related. The following sequence of messages generated in the SystemOut.log indicates normal code initialization of an application server in which the security service has started successfully. You can check the following message "Security `enabled false`" to see if security is indeed turn off.

This sequence will vary based on the configuration, but the messages are similar:

```
SASRas        A JSAS0001I: Security configuration initialized.
SASRas        A JSAS0002I: Authentication protocol: CSIV2/IBM
SASRas        A JSAS0003I: Authentication mechanism: SWAM
SASRas        A JSAS0004I: Principal name: MYHOSTNAME/aServerID
SASRas        A JSAS0005I: SecurityCurrent registered.
SASRas        A JSAS0006I: Security connection interceptor initialized.
SASRas        A JSAS0007I: Client request interceptor registered.
SASRas        A JSAS0008I: Server request interceptor registered.
SASRas        A JSAS0009I: IOR interceptor registered.
NameServerImp I NMSV0720I: Do Security service listener registration.
SecurityCompo A SECJ0242A: Security service is starting
UserRegistryI A SECJ0136I: Custom Registry:com.ibm.ws.security.registry.nt.NTLocalDomainRegistryImpl
has been initialized
SecurityCompo A SECJ0202A: Admin application initialized successfully
SecurityCompo A SECJ0203A: Naming application initialized successfully
SecurityCompo A SECJ0204A: Rolebased authorizer initialized successfully
SecurityCompo A SECJ0205A: Security Admin mBean registered successfully
SecurityCompo A SECJ0243A: Security service started successfully

SecurityCompo A SECJ0210A: Security enabled false
```

If none of these steps solves the problem, check to see if the problem has been identified and documented using the links in **Troubleshooting security configurations** section of the Websphere Application Server Information Center:
`http://publib.boulder.ibm.com/infocenter/ws51help/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_trouble.html`

If you do not see a problem that resembles yours, or if the information provided does not solve your problem, contact **IBM support** for further assistance**:**

`http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg21145599`

How to disable Global security if using the Administrative Console fails to do it

How to disable global security by using wsadmin

- ***Single Server environment:***

  If your server does not restart after you enable global security, you can disable security by using the following steps:

____ 1. Go to your `<installation_root>\AppServer\bin` directory and execute the following command:

```
wsadmin -conntype NONE
```

At the `wsadmin>` prompt, enter `securityoff` and then type `exit` to return to a command prompt.

____ 2. Stop and restart the server with security disabled to check any incorrect settings through the administrative console. From the <installation_root>/AppServer/bin:

stopServer <server_name>

startServer <server_name>

UNIX system: restart the server with these commands:

```
cd /opt/WebSphere/AppServer/bin
./stopServer.sh –username <user_id> -password <password>server1;
./startServer.sh server1
```

- ***Network Deployment environment:***

____ 1. Go to your `<installation_root>\DeploymentManager\bin` directory and execute the following command:

```
wsadmin -conntype NONE
```

At the `wsadmin>` prompt, enter `securityoff` and then type `exit` to return to a command prompt.

____ 3. Restart the Deployment Manager process. You can do this by going to the Deployment Manager installation/bin directory and issue the command:

```
startManager.bat -username <administrative_user_name> -password
<administrative_password>
```

Or `startManager.sh` command on **UNIX** system.

____ 4. If you go to **System Management > Nodes** and the status of the node is Unknown, go to that node, manually stop the node agent, perform configuration synchronization, and restart the node agent.

__ a. To stop the node agent, issue the command:

`stopNode -username <administrative_user_name> -password <administrative_password>` command.

__ b. Perform configuration synchronization, by issuing the command:

```
syncNode CELL_HOST 8879 -username <administrative_user_name> -
password <administrative_password>
```

The CELL_HOST is the host name where the Deployment Manager resides. Port **8879** is the default SOAP connector port. If the post number is changed, specify the changed port. The `<administrative_user_name>` is the administrative user configured for the user registry. To start the node agent, issue the `startNode` command.

UNIX system: `/opt/WebSphere/AppServer/bin/stopNode.sh -username <administrative_user_name> -password <administrative_password>`

/opt/WebSphere/AppServer/bin/startNode.sh

Reference:

- **WebSphere Application Server Information Center Version 5**

http://www-306.ibm.com/software/webservers/appserv/infocenter.html

- **IBM WebSphere V5.0 Security Handbook**

http://www.redbooks.ibm.com/redbooks/SG246573.html

Trademarks and Disclaimers

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

IBM
IBM(logo)
e(logo)business
Tivoli
iSeries
pSeries
xSeries
zSeries
OS/400
AIX
CICS
OS/390
Informix
Cloudscape
DB2 Universal Database
IMS
WebSphere
MQSeries
DB2
Lotus

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

the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both. Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are

trademarks of Intel Corporation in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Other company, product and service names may be trademarks or service marks of others.

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 and/or changes in the product(s) and/or program(s) 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 (e.g., 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.

This page is left intentionally blank.