



# Helix Security Manager

## Quick Start Guide

Updated April 26, 2007



## RealNetworks, Inc.

2601 Elliott Avenue, Suite 1000  
Seattle, WA 98121  
U.S.A.

<http://www.real.com>

<http://www.realnetworks.com>

©2007 RealNetworks, Inc. Patents pending. All rights reserved. RealNetworks, RealPlayer, RealProducer, RealAudio, RealVideo, the Real logo, Helix, Helix DNA and the Helix logo are either trademarks or registered trademarks of RealNetworks, Inc. in the United States of America and other countries.

All other trade names, trademarks, or registered trademarks are trade names, trademarks or registered trademarks of their respective companies.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of RealNetworks, Inc.



## Pre-Requisites

1. Basic knowledge of Helix Server which is already installed and running.
2. Java (J2SE) 1.4.2\_13 or later is installed (java.sun.com).
3. Helix Server and Security Manager are recommended to be on two separate machines.
  - a. Unix or Linux: (Note: Paths are for reference only, not mandatory.)
    - i. Helix Security Manager: /opt/real/hsm
    - ii. JBOSS: /opt/real/hsm/jboss-4.02
    - iii. Helix Server: /opt/real/hus
  - b. Windows
    - i. JBOSS: C:\Program Files\Real\Helix Security Manager\jboss-4.02\
    - ii. Helix Server: C:\Program Files\Real\Helix Server\

## Installation and Configuration

**STEP 1.** Extract the compressed Security Manager file which contains the Server Adapter and URL Processor compressed files. Then extract each of these files into separate subfolders.

For Unix or Linux extraction, use a command such as the following:

```
tar-xvzf sds-secmgr-11.0.0.87.tar.gz  
cd sds-secmgr.11.0.0.87  
mkdir -p path_to_security_manager  
tar-C path_to_security_manager-xvzf url-processor-11.0.0.87.tar.gz
```

For Windows, open file with an Extraction tool such as WinZip:

```
Open sds-secmgr-11.0.0.87.tar.gz, then url-processor-11.0.0.87.tar.gz  
Extract url-processor-11.0.0.87.tar.gz to path_to_security_manager
```



**STEP 2.** Copy the Security Adapter file to the Helix Server Plugin directory. Be sure to extract the plug-in that corresponds to the platform running the Helix Server. [daucplin.so=linux/solaris or daucplin.dll=windows]

For Unix or Linux extraction use a command such as the following:

```
tar -xzvf sds-serveradapter-11.0.0.87.tar.gz  
cd serveradapter-11.0.0.87/linux-2.4-glibc23-i686  
cp daucplin.so path_to_helix_server/Plugins
```

For Windows, open file with an Extraction tool such as WinZip:

```
Open secmgr-serveradapter-11.0.0.87.tar.gz and extract daucplin.dll from  
win32-i386-vc7 folder to path_to_helix_server\Plugins
```

**STEP 3.** Enable the Security Adapter by adding configuration information into the rmserver.cfg to secure content.

```
<List Name="DAUCPlugin">  
  <Var Enabled="1"/>  
  <Var TokenFileName="path_to_helix_server/tokens.txt"/>  
  <Var DefaultToken="token1"/>  
  <Var KeyExpiryTime="30"/>  
  <Var UseFullURL="0"/>  
  <Var AuthLogging="1"/>  
  <Var AuthLogStyle="7"/>  
  <Var AuthLogFileName="path_to_helix/Logs/dauc.log"/>  
  <Var LogRollSize="2"/>  
  <Var UseUserAlerts="1"/>  
  <Var AllowanceDefault="Deny"/>  
</List>
```

**STEP 4.** Move the Security Adapter license file to the Helix Server license directory. This file comes via email in the form of a zip file. The license file needs to be extracted from the zip file then moved as a .lic file.

**STEP 5.** Copy the same license file to the JBOSS directory on the Security Manager machine.

**STEP 6.** Restart Helix Server from command line or from Web Administrator pages.



**STEP 7.** Modify the Security Manager configuration file (secmgr-config.xml) with the following examples, which can be customized for further integration.

1. Change LicenseFileName to match full location of License File (path\_to\_jboss/file.lic)
2. Change MAC Address to match Network Card of JBoss Server
3. Set DefaultToken (token1)
4. Set Key Name (token1)
5. Set Key Value (1234567890)
6. Ensure only 1 Key is available to start

**STEP 8.** Create tokens.txt to reside on the Helix Server to certify against links from the URL Processor by using the same token name.

Fill in the new file with the following, then save:  
token1:1234567890

**STEP 9.** Start Security Manager by running the script from the command line:

```
Unix or Linux: cd path_to_jboss/bin/  
                ./secmgrstart.sh  
Windows:      cd path_to_jboss\bin\  
                secmgrstart.bat
```

**STEP 10.** Attempt to access sample file on Helix Server with Security Adapter configured. If the Security Adapter plug-in is working, then the request will be denied since the link has not been sent through the Security Manager.

**STEP 11.** Open URL <http://secmgrIP:8080/urlprocessor> then insert the following variables:

```
URL= http://serverIP:HTTPport/ramgen/realvideo10.rm  
Tokenname= token1  
Life= 0  
Debug= false  
Click Send to Servlet
```



## Next Steps

**STEP 12.** If the clip plays, then the Server and Security Manager are functioning as expected.

**STEP 13.** The final step is to create a Web Portal that mimics the inserted URL that is placed into the Security Manager (see chapter 6, “Generating Secure URLs” in the Helix Security Manager Guide).