

### HOW TO CONFIGURE XMII 11.5.1 BUILD 63 AND IIS 6.0 FOR HTTPS

#### Applies to:

Configuring SAP xApp Manufacturing Integration and Intelligence (SAP xMII 11.5.1 build 63) and IIS 6.0 for https.

#### Summary

This paper outlines the process of configuring SAP xMII and IIS to use https. This document assumes that a certification authority is setup on the network and the logged in user has the necessary rights to perform all steps. This example that may not apply to all circumstances, certain steps may differ depending on security configurations specific to a network. All paths are relative to the Java SDK version 1.4.2\_07.

#### Author Bio

Jamie Cawley has worked for Lighthammer Software since September 2004 supporting and doing application development for the Lighthammer CMS product. Since the SAP acquisition of Lighthammer in July 2005 Jamie has become a Sr. Support Consultant for SAP xMII. He is also involved in the testing and development of several of the composite applications being developed with the xMII product

## Table of Contents

Requesting A Certificate In IIS .....	3
Changing The Security Server.....	4
Exporting The SSL Certificate From IIS .....	4
Configuring The XMI Security Manager For SSL .....	4
Configuring The Java Web Start For SSL .....	6
Troubleshooting .....	7
Copyright.....	9

## Requesting A Certificate In IIS

Open IIS ( start – run – type: inetmgr – click ok)

Expand the tree under the computer name and expand the Web Sites folder.

Right click on the Web Site designated for xMII and choose properties.

Choose the Directory Security tab and choose Server Certificate.

Click Next and choose “Create a new certificate” and then click Next.

Choose “Send the request immediately...” and click Next.

Fill in a name, leave the bit length to 1024 and Click Next.

Fill in requested information, Organization and Organization Unit, and click Next.

The Common name will need to match the name entered in for the Security Server of xMII. See section “Changing the Security Server” for more information.

If the entry is

`https://computername.test.com/LHSecurity`

the Common name should be

`computername.test.com`

Click Next and fill in the Geographical Information and then click Next again.

Leave port 443 as the port for SSL to use and click Next.

Choose the appropriate Certification authority and click Next.

Verify the information entered and click Next.

Click Finish.

Click OK to close the Web Site Properties dialog.

## Changing The Security Server

On the server open the menu using `http://localhost/Lighthammer/Menu.jsp`

Choose Security Services then choose Security Server

Verify that the entry for Security Server includes the 's' in 'https'

`https://computername.test.com/LHSecurity`

Click Save if any changes were made.

## Exporting The SSL Certificate From IIS

Open IIS ( start – run – type: `inetmgr` – click ok)

Expand the tree under the computer name and expand the Web Sites folder.

Right click on the Web Site designated for xMII and choose properties.

Choose the Directory Security tab and choose View Certificate.

Choose the Details tab.

Click the "Copy to file..." button.

Click Next.

Choose "No, do not export the private key" and click Next.

Choose "DER encoded binary X.509 (.CER)" and click Next.

Click Browse and choose a directory and file name and click Save and then click Next.

Click Finish and then OK. Close the remaining dialog windows.

## Configuring The XMI Security Manager For SSL

In order for Secure Sockets Layer (SSL) communications to take place, you must import your server's certificate into the Java Virtual Machine (JVM) on which the Security Manager is running. This step establishes a trust between the client and the server application. These steps will assume that the version of the java sdk is 1.4.2\_07 and is installed on the c drive.

To import the SSL certificate into the JVM Truststore, complete the following steps:

Open a command prompt: start – run type: `cmd` click OK.

Change the directory to `C:\j2sdk1.4.2_07\bin`

Run the following command to do this: `cd C:\j2sdk1.4.2_07\bin`

Run the following command:

```
keytool -import -file <path to cert> -keystore <path to the JRE cacerts file> -alias <name to store cert>
```

where

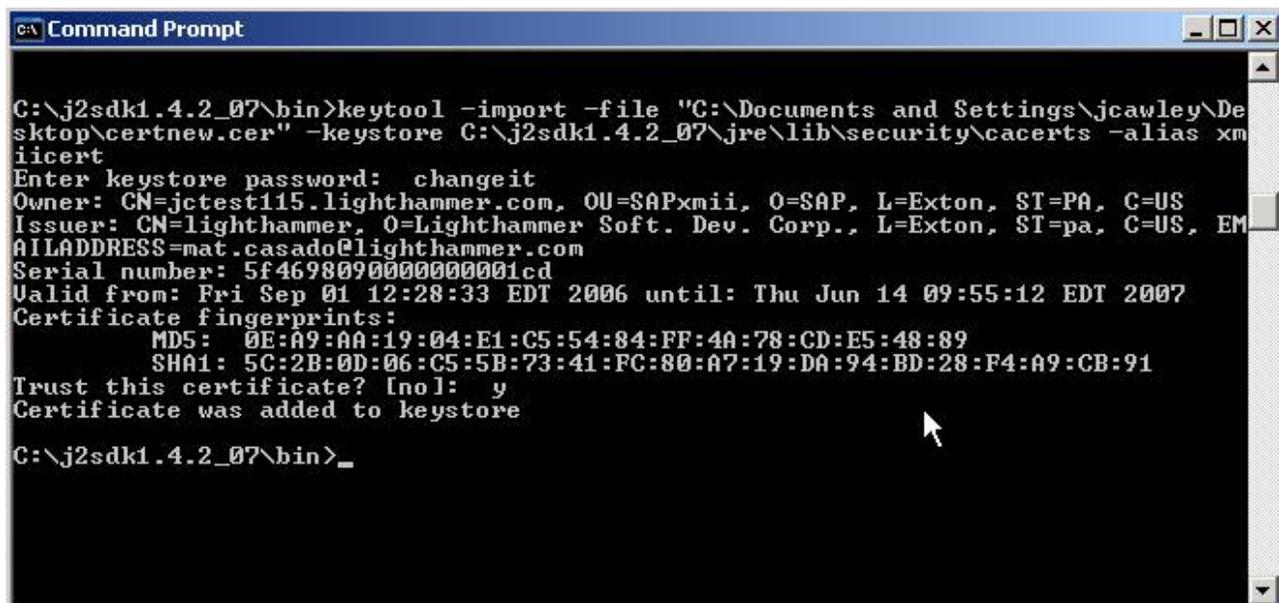
**file** is the path to the SSL certificate

**keystore** is the location of the JVM's CACERT file (the list of trusted certificates for the JVM)

**alias** is the name you want to use to store the certificate

Example:

```
keytool -import -file "C:\certnew.cer" -keystore C:\j2sdk1.4.2_07\jre\lib\security\cacerts -alias certServerName
```



```
C:\j2sdk1.4.2_07\bin>keytool -import -file "C:\Documents and Settings\jcawley\Desktop\certnew.cer" -keystore C:\j2sdk1.4.2_07\jre\lib\security\cacerts -alias xmiiicert
Enter keystore password: changeit
Owner: CN=jctest115.lighthammer.com, OU=SAPxmii, O=SAP, L=Exton, ST=PA, C=US
Issuer: CN=lighthammer, O=Lighthammer Soft. Dev. Corp., L=Exton, ST=pa, C=US, EMAILADDRESS=mat.casado@lighthammer.com
Serial number: 5f4698090000000001cd
Valid from: Fri Sep 01 12:28:33 EDT 2006 until: Thu Jun 14 09:55:12 EDT 2007
Certificate fingerprints:
    MD5: 0E:A9:AA:19:04:E1:C5:54:84:FF:4A:78:CD:E5:48:89
    SHA1: 5C:2B:0D:06:C5:5B:73:41:FC:80:A7:19:DA:94:BD:28:F4:A9:CB:91
Trust this certificate? [no]: y
Certificate was added to keystore

C:\j2sdk1.4.2_07\bin>_
```

You will then be prompted for a password, the password should be "changeit" without the quotes.

You will then be prompted to "Trust this certificate?" type "y" without the quotes.

Restart the application server that is hosting the SAP xMII Security Manager.

Start – Run type: services.msc click OK.

Choose ServletExec-xMII and click restart.

## Configuring The Java Web Start For SSL

In order for Secure Sockets Layer (SSL) communications to take place between Java Web Start, which runs Business Logic Services, and the server the certificate will need to be imported into the JRE Truststore on the client machine. This is only necessary for machines used for building transactions in Business Logic Services. This will be similar to the previous step but the directory paths will differ. These steps will also assume that the version of the java sdk is 1.4.2\_07 and is installed on the c drive.

Open a command prompt on the machine that will be used to develop transactions: start – run type: *cmd* click OK.

Change the directory to C:\Program Files\Java\j2re1.4.2\_07\bin

Run the following command to do this: *cd C:\Program Files\Java\j2re1.4.2\_07\bin*

Run the following command:

```
keytool -import -file <path to cert> -keystore <path to the JRE cacerts file> -alias <name to store cert>
```

where

**file** is the path to the SSL certificate

**keystore** is the location of the JVM's CACERT file (the list of trusted certificates for the JVM)

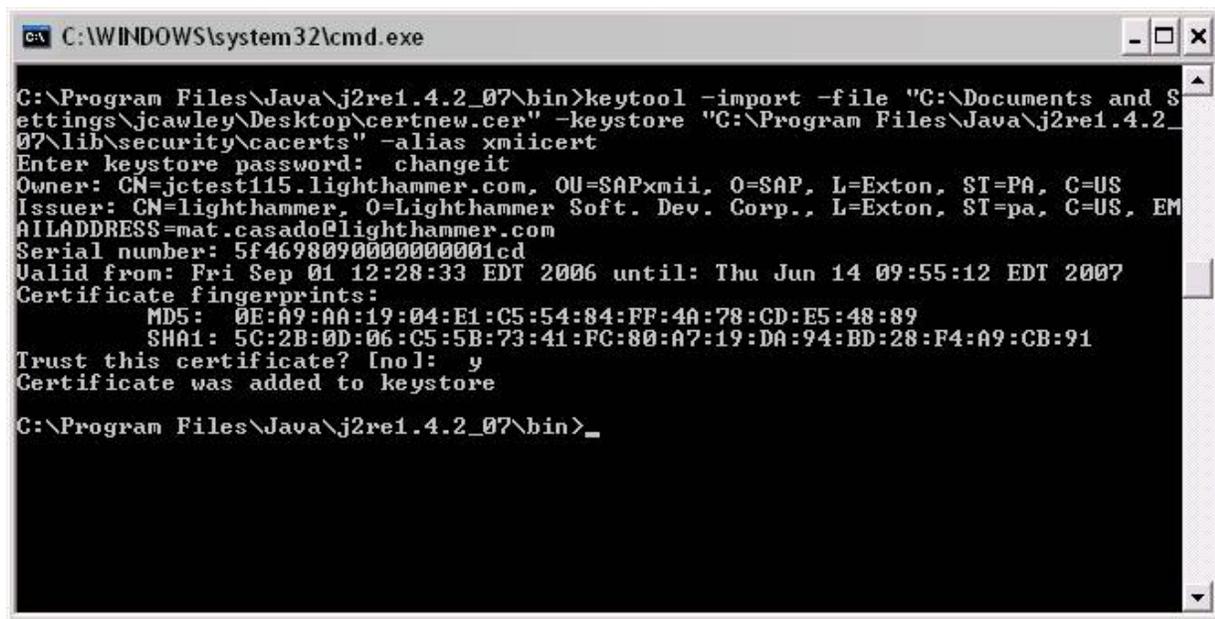
**alias** is the name you want to use to store the certificate

Example:

```
keytool -import -file "C:\certnew.cer" -keystore "C:\Program Files\Java\j2re1.4.2_07\lib\security\cacerts" -alias certServerName
```

You will then be prompted for a password, the password should be "changeit" without the quotes.

You will then be prompted to "Trust this certificate?" type "y" without the quotes.



```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Java\j2re1.4.2_07\bin>keytool -import -file "C:\Documents and Settings\jcauley\Desktop\certnew.cer" -keystore "C:\Program Files\Java\j2re1.4.2_07\lib\security\cacerts" -alias xmiicert
Enter keystore password: changeit
Owner: CN=jctest115.lighthammer.com, OU=SAPxmii, O=SAP, L=Exton, ST=PA, C=US
Issuer: CN=lighthammer, O=Lighthammer Soft. Dev. Corp., L=Exton, ST=pa, C=US, EMAILADDRESS=mat.casado@lighthammer.com
Serial number: 5f4698090000000001cd
Valid from: Fri Sep 01 12:28:33 EDT 2006 until: Thu Jun 14 09:55:12 EDT 2007
Certificate fingerprints:
    MD5: 0E:A9:AA:19:04:E1:C5:54:84:FF:4A:78:CD:E5:48:89
    SHA1: 5C:2B:0D:06:C5:5B:73:41:FC:80:A7:19:DA:94:BD:28:F4:A9:CB:91
Trust this certificate? [no]: y
Certificate was added to keystore
C:\Program Files\Java\j2re1.4.2_07\bin>_
```

## Troubleshooting

Two common errors that may be received:

### 1. Receiving the error “No host available, all connections are down”



This can be caused from an incorrect security server or the certificate was not correctly imported into the JVM Truststore. If `https://servername.domain.com/LHSecurity` will not resolve then verify that the path of the security server is correct. Otherwise verify that the certificate was imported into the JVM Truststore and is correct. The command

```
keytool -list -keystore <path to the JRE cacerts file>
```

can be used to verify that the certificate exists

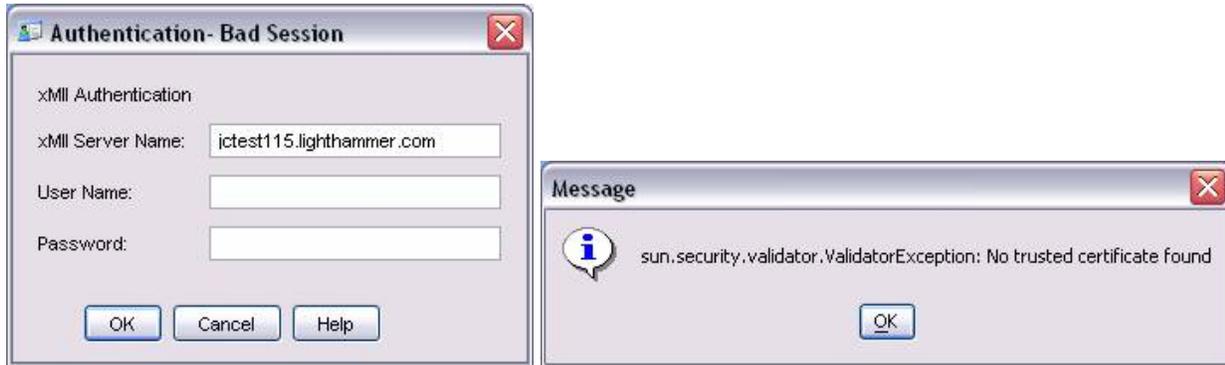
```
CA\ Select Command Prompt
C:\j2sdk1.4.2_07\bin>keytool -import -list -keystore C:\j2sdk1.4.2_07\jre\lib\se
curity\cacerts
Enter keystore password: changeit

Keystore type: jks
Keystore provider: SUN

Your keystore contains 32 entries

equifaxsecureebusinessca, Jul 23, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 64:9C:EF:2E:44:FC:C6:8F:52:07:D0:51:73:8F:CB:3D
verisignclass1g3ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
verisignclass2g2ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): 2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
verisignclass4ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5): 1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
verisignclass3g3ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
entrustglobalclientca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 9A:77:19:18:ED:96:CF:DF:1B:B7:0E:F5:8D:B9:88:2E
gtcybertrustglobalca, May 10, 2002, trustedCertEntry,
Certificate fingerprint (MD5): CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB
entrustgsslca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 9D:66:6A:CC:FF:D5:F5:43:B4:BF:8C:16:D1:2B:A8:99
verisignclass1ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): 97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
thawtepersonalbasicca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
verisignclass1g2ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
entrustsslca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): DF:F2:80:73:CC:F1:E6:61:73:FC:F5:42:E9:C5:7C:EE
thawtepersonalfreemailca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): 1E:74:C3:86:9C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
xmiicert, Sep 1, 2006, trustedCertEntry,
Certificate fingerprint (MD5): 0E:A9:AA:19:04:E1:C5:54:84:FF:4A:78:CD:E5:48:89
verisignclass3ca, Oct 24, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
gtcybertrustca, May 10, 2002, trustedCertEntry,
```

## 2. Receiving the error “bad session” and “no trusted certificate found” when attempting to access business logic services



Verify that you are running xMII version 11.5.1 build 63 or greater. This can be found on the xMII main menu under Support - About

Otherwise verify that the certificate was imported into the JRE Truststore and is correct. The command `keytool -list -keystore <path to the JRE cacerts file>`

can be used to verify that the certificate exists

```

C:\Program Files\Java\j2re1.4.2_07\bin>keytool -list -keystore "C:\Program Files\Java\j2re1.4.2_07\lib\security\cacerts"
Enter keystore password: changeit

Keystore type: jks
Keystore provider: SUN

Your keystore contains 33 entries

verisignclass1g3ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
equifaxsecurebusinessca, Jul 23, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 64:9C:EF:2E:44:FC:C6:8F:52:07:D0:51:73:8F:CB:3D
verisignclass2g2ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): 2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
verisignclass4ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5): 1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
verisignclass3g3ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
testqa, Apr 6, 2006, trustedCertEntry,
Certificate fingerprint (MD5): 04:14:2D:F9:F7:40:DE:7B:BA:58:66:31:39:45:CC:DD
entrustglobalclientca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 9A:77:19:18:ED:96:CF:DF:1B:B7:0E:F5:8D:B9:88:2E
gtecybertrustglobalca, May 10, 2002, trustedCertEntry,
Certificate fingerprint (MD5): CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB
entrustgsslca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 9D:66:6A:CC:FF:D5:F5:43:B4:BF:8C:16:D1:2B:A8:99
thawtepersonalbasicca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
verisignclass1ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): 97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
verisignclass1g2ca, Jun 15, 2004, trustedCertEntry,
Certificate fingerprint (MD5): DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
thawtepersonalfreemailca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): 1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
entrustsslca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): DF:F2:80:73:CC:F1:E6:61:73:FC:F5:42:E9:C5:7C:EE
xmlicert, Sep 1, 2006, trustedCertEntry,
Certificate fingerprint (MD5): 0E:A9:AA:19:04:E1:C5:54:84:FF:4A:78:CD:E5:48:89
verisignclass3ca, Oct 24, 2003, trustedCertEntry,
```

## Copyright

© Copyright 2006 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided "as is" without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.