



Version 3.0

Copyright 2010

The lawful acquisition of the sdi.suite software products and its associated handbooks entitles the license holder to use the products in accordance with the terms and conditions of the license.

Any duplication, resale or use of either the software or this handbook in a manner that does not comply with the terms and conditions of the license is strictly forbidden and may result in criminal proceedings.

Warranty/ Disclaimer

Although this handbook has been produced with all due care, errors in detail cannot be excluded. con terra GmbH shall not be liable in any way whatsoever for any damage occurring as a result of using either this handbook or the associated software.

Published by

con terra
Gesellschaft für Angewandte Informationstechnologie mbH
Martin-Luther-King-Weg 24
48155 Münster
Tel +49 (0)251.74745-0
Fax +49 (0)251.74745-2111
conterra@conterra.de
www.conterra.de

System Requirements

The purpose of the sdi.suite securityManager is to organise access rights to services and data in service-based spatial data infrastructures. Access is restricted to authorised users, thus securing recognition of use agreements and preventing unauthorised use.

This document describes the necessary steps that need to be taken to install and configure the system. For further information and help, please contact support@conterra.de.

The following sections contain descriptions of the installation process and the administration of the securityManager. The installation guide is optimised for installations under Windows, using Apache Tomcat as both servlet container and web server. securityManager can also be installed and operated under Unix or Linux.

Runtime Environment

The securityManager requires a pre-installed web server with a servlet/JSP container as a runtime environment. The following products are supported.

Operating System

The following operating systems are supported:

- > Windows Server 2008 32bit/64bit
- > Windows Server 2003 32bit/64bit
- > Windows XP Professional SP 3
- > Linux 64-bit Kernel 2.6
- > Linux 32-bit Kernel 2.6

Servlet Container

The applications making up the securityManager are Java web applications, which run in a servlet container, such as Apache Tomcat.

Recommended products and versions:

- > Tomcat 5.5.x [5.5.27+] with JDK 1.5.x [1.5.0_21+], 32bit or JDK 1.5.x [1.5.0_20+] 64-bit
- > Tomcat 6.0.x [6.0.20+] with JDK 1.6.x [1.6.0_16+], 32bit or JDK 1.6.x [1.6.0_15b03+] 64-bit

Database Management System

The securityManager bases its user and access management on an internal database.

Recommended products and versions:

- > Oracle 11 Enterprise
- > Oracle 10g
- > Oracle 10.2.0 XE
- > PostgreSQL 8.4
- > MS SQL 2008+
- > MySQL 4.1+

Browsers

The following browsers are supported:

- > Firefox Version 3.5
- > Microsoft Internet Explorer Version 8.0
- > Microsoft Internet Explorer Version 7.0

Web Server (optional)

Any HTTP server (e.g. Apache) can be used for the web server. The only requirement is that Apache Tomcat is integrated as the servlet/JSP engine. Apache Tomcat can also be used directly as a web server.

Mail SMTP Server (optional)

An SMTP server is required for sending self-registration e-mails. This function is not available with LDAP-based user management.

Web Feature Service For Spatial Authorisation (optional)

In order to use spatial authorisation in securityManager it is necessary to install a WFS service that supports WFS Version 1.0.0. This can be, for instance, ArcIMS with a WFS connector (version 9.2 or higher with Service Pack 2), a WFS based on ArcGIS Server, version 9.3 or higher, or Geoserver WFS, version 1.5 or higher (open source, available from <http://docs.codehaus.org/display/GEOS/Home>). The service must provide the geometry data (area geometries), to be used for the spatial authorisation.



Languages

All components of the securityManager support user interfaces in multiple languages. This distribution contains German and English language files.

Prerequisites

The following conditions must be satisfied for both operation and installation:

HTTPS connector must be activated

The web server that is in use must support access via HTTPS; this generally requires an SSL certificate. A brief manual for Apache Tomcat 5.5 has been included with this documentation (see: '**Fehler! Verweisquelle konnte nicht gefunden werden.**').

Please also note that at runtime, the default trust manager instance of Tomcat, which is valid throughout the process, is exchanged for a trust manager that does not validate the certification chain. This means that the certification path of server certificates is not checked when HTTPS connections are set up but are generally assumed to be valid.

Since the altered trust manager instance within the general Tomcat process has global validity, you should not run other web applications in the same Tomcat process if these require the security functions of the default trust manager or when these make use of a trust manager. Only web applications that do not use a trust manager or that do not require the restricted security functions can be run in the same Tomcat process.

The reason for installing the trust manager is to minimise the administration entailed in incorporating new services to be protected. If this is not in line with the security criteria of your environment, it is possible to prevent the installation of the trust manager by way of a simple configuration. Should you wish to do this, please get in touch with us.

Support for UTF-8

The servlet engine (or web server) must support UTF-8 encoding (in the case of Tomcat 5.5 this has to be set manually; see also the instructions contained in 'Setting Up UTF-8 Support (Tomcat 5.5 only)' at the end of this document).



Management system for users and permissions

The management of users and authorisations can either reference a database or is based on LDAP (read-only), while the management of rights always references a database.

Database for users and rights

A database, in which users and rights are stored, must be created on one of the supported DBMS, and be available for installation. This database must be accessible by the web server via JDBC at runtime (INSERT, UPDATE, DELETE, SELECT)

User management with LDAP/ADS

As an alternative to managing users by way of a database, securityManager also supports existing LDAP/ADS directory services for the purpose of user management. If LDAP/ADS user management is selected, securityManager integrates it as reading only, i.e. LDAP/ADS users can be viewed with the securityManager Administrator but not modified. Similarly, for the purpose of authentication, the user data of the connected LDAP/ADS system is accessed as reading only. The administration of the user information must then be performed using an external tool, and not one supplied with securityManager. For further information on setting up and using LDAP/ADS, please consult the User Guide.

The following are supported:

- > LDAP v2 und v3
- > Microsoft Active Directory Server (ADS)
 - Logging in to ADS with simple bind
 - Logging in to ADS with Kerberos

The securityManager can authenticate itself in existing LDAP systems using "simple bind", which conveys a user's "distinguishedName" (DN) and password to the LDAP system.

Memory Settings

Depending on the servlet engine used, the memory allocation may need to be increased. The following values are recommended (parameters may have to be added; this can be done in the same way as with proxy parameter settings):



- > „-Xms256m“ – minimum memory allocated by the JVM (256 MByte)
- > „-Xmx512m“ – maximum memory allocated by the JVM (512 MByte; this value is for guidance only – if a high load is expected and there are many services requiring protection, this value should be increased in accordance with the available hardware).
- „-XX:MaxPermSize=256m“ – maximum memory allocated by the JVM for static variables and classes (256 MByte)