



# securityManager

## Release Notes

Version 2.3.1

Copyright 2009

Der rechtmäßige Erwerb der sdi.suite Softwareprodukte und der zugehörigen Handbücher berechtigt den Lizenznehmer zur Nutzung dieser Gegenstände entsprechend den Lizenzbedingungen.

Jede nicht vertragsgemäße Vervielfältigung, Veräußerung oder Verwendung der Software oder dieses Handbuches ist nicht gestattet und wird ggf. strafrechtlich verfolgt.

Gewährleistung / Haftungsausschluss

Obwohl die vorliegenden Release Notes mit aller Sorgfalt erstellt wurde, können Fehler im Detail nicht ausgeschlossen werden. Die con terra GmbH übernimmt keine Haftung für Schäden, die aus der Anwendung dieser Release Notes oder der Software entstehen.

Herausgeber

con terra  
Gesellschaft für Angewandte Informationstechnologie mbH  
Martin-Luther-King-Weg 24  
48155 Münster  
Tel +49 (0)251.7474-0  
Fax +49 (0)251.7474-100  
conterra@conterra.de  
www.conterra.de

# Inhaltsverzeichnis

1 Einführung	1
2 What's new?	2
Neu in 2.3.1	2
Neu in 2.3.0	2
3 Bekannte Probleme und Hinweise	4

# 1 Einführung

Das Release 2.3.1 des securityManager der sdi.suite beinhaltet gegenüber seiner Vorgängerversion weitere funktionale Verbesserungen, zahlreiche neue Funktionen und wichtige Bugfixes.

Das vorliegende Dokument enthält einen Überblick über Änderungen und Erweiterungen ab der Version 2.0 sowie eine Auflistung bekannter Probleme.

## 2 What's new?

### Neu in 2.3.1

#### **Zugriff auf geschützte Dienste mit HTTP Authentication**

- > Zugriff auf geschützte Dienste per HTTP Basic Authentication – Erstellen eines Gates ist nicht mehr zwingend erforderlich  
(Weitere Informationen im Installationshandbuch unter „Konfiguration der zu schützenden Dienste im WSS“)
- > Direktes Einladen geschützter Dienste in Applikationen, die HTTP Authentication unterstützen, z.B. ESRI ArcMap.

### Neu in 2.3.0

#### **Schutz von ArcGIS Server 9.3 Diensten**

- > Schutz von ArcGIS Server SOAP Diensten der *Version 9.3* (SOAP über HTTP/POST).
- > *Räumliche Berechtigungen* neben WMS, WFS und ArcIMS nun auch für ArcGIS Server MapServer.
- > Berechtigung für unterschiedliche *Zugriffsoperationen* für GeoDataServer und MapServer

#### **Schutz von Web Coverage Services (WCS)**

- > Schutz von *Coverages*, die durch einen WCS der Versionen 1.0, 1.1 und 1.1.1 zur Verfügung gestellt werden.

#### **Nutzer-Administration**

- > Im Administrator wurde die Rolle des *Gruppenadministrators* eingeführt, der nur die Benutzer seiner Gruppe verwalten kann. Der Super-Administrator kann weiterhin alle Benutzer verwalten.
- > Benutzer, die mit dem Administrator verwaltet werden, können ihr Profil anpassen und z. B. ihr *Passwort ändern*.
- > Nutzer können sich selbst am Administrator *registrieren* und ihre Profildaten eingeben.

#### **licenseManager**

- > Über das Gateway können Dienste, die mit dem *sdi.suite licenseManager 2.3* geschützt sind, eingeladen werden.

### **Anonyme Nutzer**

- > Nutzer können sich für die Anfrage geschützter Dienste beim Gateway *anonym anmelden* und mit definierten Standard-Rollen und –Rechten auf den Dienst zugreifen.

### **Schutz mehrerer Dienste mit dem WSS**

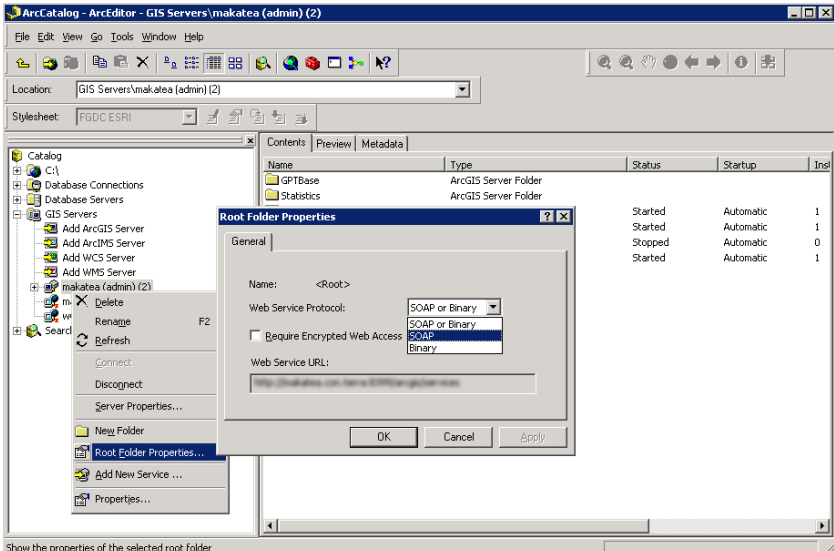
- > Mit einer WSS (Web Security Service) Instanz können *beliebig viele Dienste* abgesichert werden.

### **Installation & Konfiguration**

- > Vereinfachte Installation und Konfiguration von WAS, PDP und Administrator als *eine* Applikation
- > Konfiguration eines WSS über *Web-basierte Oberfläche*

## 3 Bekannte Probleme und Hinweise

Die folgende Liste enthält die zum Zeitpunkt der Freigabe der Version 2.3 bekannten Probleme und Hinweise:

Komponente	Beschreibung
Unterstützung ArcGIS Server	<p>Um ArcGIS Server Dienste mit dem securityManager schützen und dann mit ArcMap nutzen zu können, muss der ArcGIS Server im „SOAP-only“ Modus betrieben werden. Dies kann über ArcCatalog und eine administrative ArcGIS Server Verbindung eingestellt werden.</p>  <ul style="list-style-type: none"> <li>- ArcCatalog öffnen, ArcGIS Server Verbindung wählen, rechte Maustaste, Auswahl „Root Folder Properties“</li> <li>- Im gleichnamigen Dialog unter Web Service Protocol „SOAP“ wählen</li> <li>- 2x mit OK bestätigen</li> </ul>
Sichtbarkeit von Veränderungen im LDAP; Anzeige im securityManager Administrator	<p>Um Änderungen im LDAP im securityManager Administrator zu visualisieren, man sich neu beim securityManager Administrator anmelden.</p>
ArcIMS und räumliche	<p>Wird ein Recht mit räumlicher Einschränkung erzeugt und der Operator "within" gewählt, so ist zwingend die</p>

### 3 Bekannte Probleme und Hinweise

Einschränkung	Definition eines negativen Buffers erforderlich. Durch das Buffering kann es bei stark verzerrenden Koordinatentransformationen zu invaliden Geometrien kommen, wodurch die Abfragen komplett geblockt werden. Hier muss im Einzelfall geprüft werden, ob und wo Berechtigungsgeometrien angepasst werden müssen.
Verwendung des HTML-Client für geschützte ArcIMS Dienste	Die Verwendung des ArcIMS HTML Client wird für geschützte ArcIMS Dienste unterstützt, es muss jedoch die Datei ArcIMSParam.js angepasst werden. Die Standard-URL des ArcIMS Dienstes muss durch die URL des Gates ersetzt werden. Dies ist nur sinnvoll, wenn vordefinierte Gates verwendet werden oder Gates dynamisch durch eine Erweiterung des HTML Clients geöffnet werden.
Räumliche Einschränkung für ArcIMS Dienste	Damit die räumliche Einschränkung für ArcIMS funktioniert, ist es erforderlich, in der AXL-Datei des Dienstes die Parameter „FeatureCRS“ und „FilterCRS“ korrekt zu setzen.
Mehr als ein Rechteset (Policyset) pro Service	Werden pro Service mehr als ein Rechteset angelegt, so kommt es immer zu einer negativen Autorisierungsentscheidung (Anfrage wird abgelehnt), da keine eindeutige Entscheidung getroffen werden kann. Es darf immer nur ein Rechteset pro Service (URL) definiert werden.
Wertigkeit zwei Rechte	Werden zwei Rechte definiert, die auf einen Nutzer anwendbar sind, ist es wichtig, die korrekte Reihenfolge im securityManager Administrator (im Dialog „Rechteset“) festzulegen. Beispiel: Es wird ein Recht definiert, dass allen Nutzer Zugriff auf einen WMS gewährt, allerdings mit Copyright-Einschränkung. Für eine Nutzergruppe „registriert“ wurde ein weiteres Recht für diesen WMS definiert, dass den Zugriff OHNE Copyright-Einschränkung gewährt. Bei Rechte sind gültig wenn Nutzer der Gruppe „registriert“ den WMS zugreifen, es wird immer das erste anwendbare Recht benutzt. Um zu verhindern, dass die Nutzer der Gruppe „registriert“ den gleichen Copyright-Vermerk sehen wie alle anderen, muss dieses Recht im Administration zuoberst aufgeführt werden.
Fehler beim Speichern von Rechten bei Oracle XE	Tritt bei gleichzeitiger Speicherung von Rechten (z.B. im ArcGIS Server Dialog) ein Fehler auf und wird Oracle 10g XE als Benutzerverwaltung verwendet, so ist dies auf einen Oracle Fehler zurückzuführen. Zur Behebung muss folgende



### 3 Bekannte Probleme und Hinweise

	<p>SQL-Anweisung ausgeführt werden (ohne Gewähr):</p> <pre>ALTER SYSTEM SET PROCESSES=150 SCOPE=SPFILE</pre> <p>Im Anschluss Oracle neu starten. Weitere Informationen hierzu finden sich unter:</p> <p><a href="http://forums.oracle.com/forums/thread.jspa?messageID=1255542">http://forums.oracle.com/forums/thread.jspa?messageID=1255542</a></p>
Schutz von Diensten, die ihrerseits nur über HTTPS zugegriffen werden können.	<p>Dies wird vom securityManager unterstützt, allerdings sind Anpassungen des Tomcat erforderlich, unter dem die securityManager Komponenten betrieben werden. Die Schritte zur Anpassung sind:</p> <ul style="list-style-type: none"><li>- Zertifikat der HTTPS Quelle (= URL des Dienstes) kopieren und lokal speichern (z.B. mit Internet Explorer); Format: DER-codiert-binär X.509 (.CER)</li><li>- Importieren in den globalen Zertifikatsspeicher der JRE/JDK-Installation, die von Tomcat verwendet wird (/JRE/lib/security/CA.certs)</li></ul> <p>Beispielbefehl zum Importieren (Standard-Passwort: changeit):</p> <pre>keytool -import -alias zielzertifikatname -file mycertificate.cer -keystore c:\Programme\Java\jdk1.5.0_11\jre\lib\security\cacerts</pre> <ul style="list-style-type: none"><li>- Tomcat neu starten</li></ul>
Keine räumlichen Berechtigungen für ArcGIS Server Cached MapServices	<p>Derzeit werden im Gegensatz zu Standard-MapServices räumliche Berechtigungen für ArcGIS Server <i>Cached</i> MapServices ignoriert. Die Unterstützung räumlicher Berechtigungen für solche Dienste ist für eine spätere Version vorgesehen.</p>
Räumliche Berechtigungen bei Verwendung von WMS 1.3	<p>GetMap-Anfragen an geschützte WMS, die gemäß WMS Spezifikation 1.3 gestellt werden, können dazu führen, dass ggf. mit dem securityManager definierte räumliche Einschränkungen nicht korrekt angewendet werden. Es wird empfohlen, auf die Verwendung von räumlichen Einschränkungen bei WMS 1.3 Diensten zu verzichten, bzw. die Unterstützung der Version 1.3 zu unterbinden.</p>