



Agito Security Center for SharePoint

Installation Guide

June 2011

Index

- 1 About the Product 3**
 - 1.1 Trial Version 3**
- 2 Prerequisites 4**
 - 2.1 Software Prerequisites 4**
 - 2.2 Hardware Prerequisites 4**
 - 2.3 Permissions 4**
- 3 Installing Standard Reports Package..... 5**
- 4 Configuring Database 7**
- 5 Installing and Configuring Import Service..... 9**
 - 5.1 System Configuration for Import 12**

1 About the Product

Agito Security Center for SharePoint is Microsoft SharePoint plug-in which introduces control and centralized management of your SharePoint environment. The solution enforces compliance with security policies, enables audit trails and gives you control over your SharePoint portal. Agito Security Center for SharePoint is consisted from:

- Reports which enable comprehensive overview and control over your SharePoint environment.
- Notifications for violations of security policies. Providing a way to identify and fix them in time.
- Change tracking and audit trails.
- Self-service processes for managing your SharePoint environment. Significantly relieving IT department and lowering maintenance costs.

Key functionalities:

- Supports Microsoft SharePoint 2007 and Microsoft SharePoint 2010.
- Comprehensive overview of SharePoint portal user permissions and accesses.
- Permissions reports contain inherited permissions, permission levels and permission trail showing you how the user got the permission (directly, via Active Directory group or via SharePoint group). With this information you don't only see who has access but also how the user gained access.
- All permissions are logged according to the schedule defined in the central administration (daily, weekly, monthly) while at the same time recording changes in permissions and other SharePoint data (site structure, features, ...).
- Overview of the list, site and portal sizes.
- Overview of the active SharePoint features.
- Overview of SharePoint workflow defined approvers.
- Overview of site permissions levels.
- Advanced view of portal size and growth over time.
- Advanced view of user permissions based on business intelligence reports.

For more information please visit www.agito.si.

1.1 Trial Version

Agito Security Center for SharePoint is treated as a trial version until a proper license key is entered. Licensing of Agito Security Center for SharePoint is based on domain users, where trial version is a fully functional version limited to displaying 15 users. Since the trial version is fully functional all users from Active Directory are imported but only 15 of them will have full information visible on the reports.

You can continue to use the same database as in trial version after a license key has been entered. All users' information will be updated automatically on the next import.

For more information about licensing and pricing please visit www.agito.si.

2 Prerequisites

2.1 Software Prerequisites

Agito Security Center for SharePoint Standard Reports requires:

- Microsoft SharePoint 2010 or Microsoft SharePoint Foundation
- SQL Server 2008 or SQL Server 2008 R2, any edition

MOSS 2007 or WSS 3.0 is not supported by this version. If you require Agito Security Center for SharePoint 2007, please contact us by email: support@agito.si or by telephone: +386 1 242 5670.

Database for Agito Security Center for SharePoint can be installed on the same database instance as SharePoint database.

2.2 Hardware Prerequisites

No other hardware is required other than hardware required by Microsoft SharePoint 2010.

2.3 Permissions

Before installing Agito Security Center for SharePoint please review the permissions required for installing and using the solution.

Permissions for installing Agito Security Center for SharePoint:

- User needs to be SharePoint Farm Administrator.
- User need to be local administrator on a server where Microsoft SharePoint 2010 or Microsoft SharePoint foundation is running.

Service permissions:

- SharePoint farm account needs to have enough rights on SQL Server 2008 R2 instance to create a new database or you must provide SQL Server account to create and access the Agito Security Center for SharePoint Database.

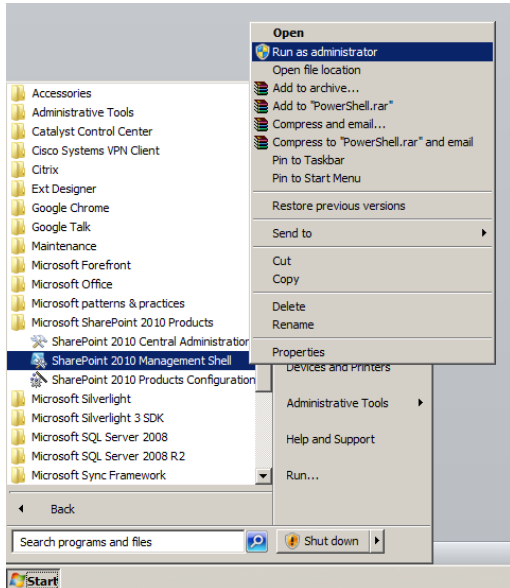
User permissions:

- User requires read-only permissions to the site where reports will be installed. User access is configured through central administration and no additional changes are required directly on the database. Please see user manual for more details.

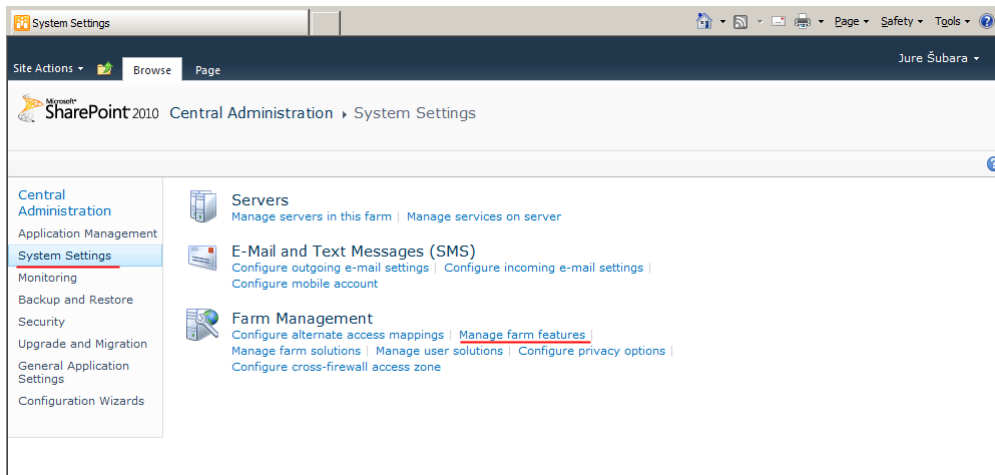
3 Installing Standard Reports Package

Follow these steps to install the standard reports package:

1. Copy the "SecurityCenter.wsp" file to one of the servers hosting SharePoint farm.
2. On the server hosting SharePoint farm open select "Start -> All Programs -> Microsoft SharePoint 2010 Products" and right click on "SharePoint 2010 Management Shell -> Run as Administrator".



3. In command prompt change to the folder containing "SecurityCenter.wsp" file
4. Run command: `"stsadm -o addsolution -filename SecurityCenter.wsp"`
5. Run command: `"stsadm -o deploysolution -name SecurityCenter.wsp -immediate -allowgacdeployment"`
6. Click "Start -> All Programs -> Microsoft SharePoint 2010 Products -> SharePoint 2010 Central Administration".
7. In Central Administration click "System Settings -> Manage Farm Features".

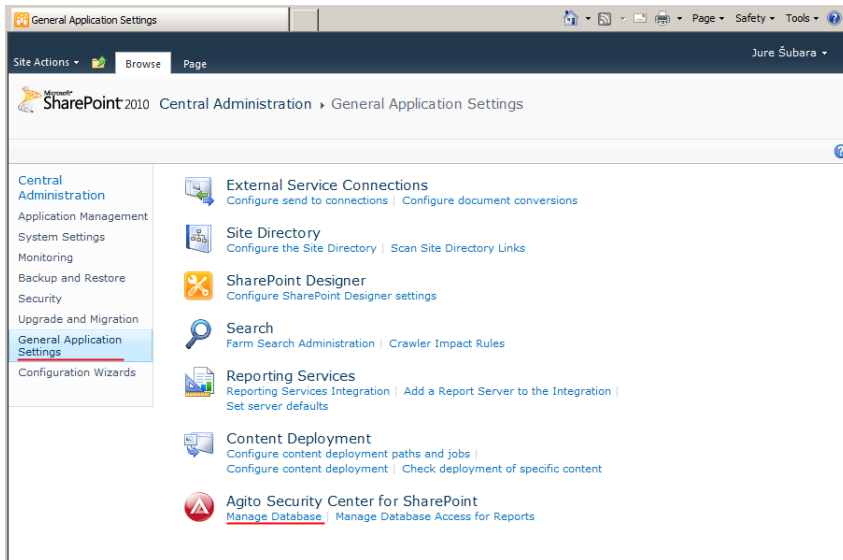


8. Make sure that the feature Agito Security Center for SharePoint is activated.

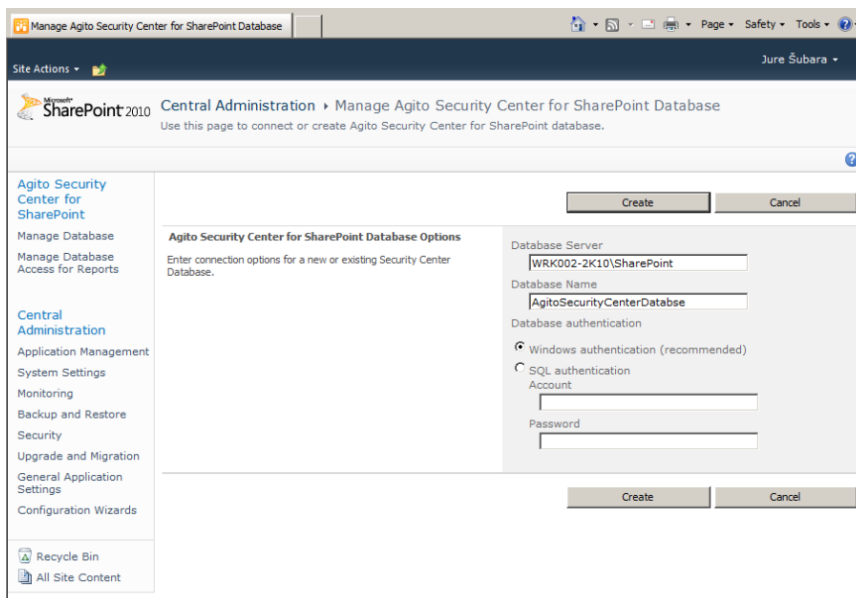
4 Configuring Database

After deploying the Security Center for SharePoint on your portal the database has to be created and configured. To do this, please follow these steps:

1. Open "SharePoint 2010 Central Administration".
2. Click "General Application Settings -> Manage Database".



3. Enter the name of the SQL Server where the database for Agito Security Center for SharePoint will be created and enter the name of the database. You must also configure authentication information for accessing the database. The database will be automatically created by clicking on "Create" button.



Important: If windows authentication is selected make sure that the SharePoint Database account has enough privileges on the specified SQL server to create a new database.

Important: If windows authentication is selected the Import Service will access the database with SharePoint Farm account. This account requires read, write and execute privileges on the created database.

4. Go to "General Application Settings" and click "Manage Database Access for Reports" to configure user access for viewing the reports.
5. Configure access for viewing the data in the reports. You can use either SQL authentication or Windows Authentication.
 - a. If SQL authentication is selected the reports will be automatically configured to access the data with entered SQL Server user credentials.
 - b. If Windows authentication is selected, every listed AD user and/or AD group will be able to see the data in the reports.
6. Connection configuration in the reports and access to the SQL Server is automatically configured. Access to the SQL Server, either for SQL user or for AD users and/or groups, is configured by giving the users or groups a special report role in the Agito Security Center for SharePoint database.

The screenshot shows the 'Manage Database Access for Reports' page in the SharePoint 2010 Central Administration console. The page title is 'Report User Access'. It contains a section for 'SQL user for accessing the Agito Security Center for SharePoint Database' with a warning that the user must be able to change the connection string. Below this, there are two radio button options: 'Use SQL User Access' (which is selected) and 'Use Windows Access'. The 'Use SQL User Access' option has input fields for 'Username:' and 'Password:'. The 'Use Windows Access' option has an input field for 'Windows Account:'. A 'Cancel' button is located at the bottom right of the configuration area.

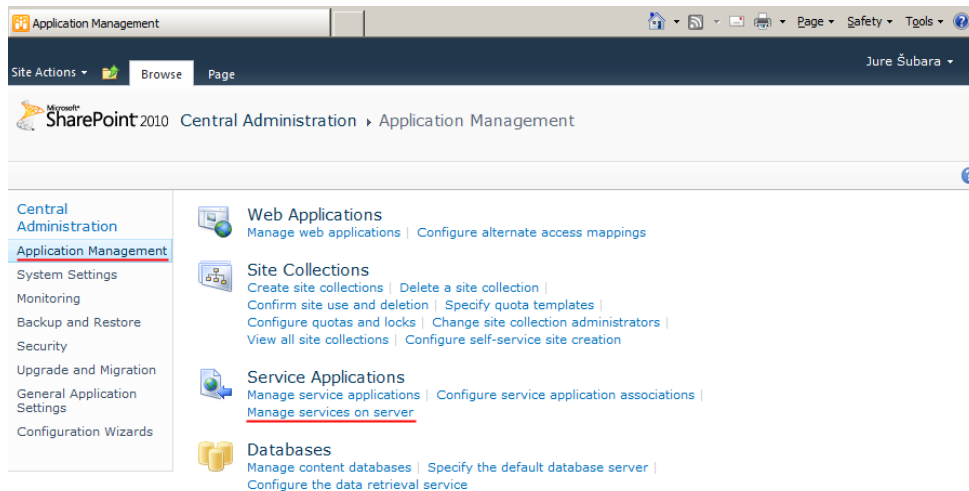
Important: If SQL User Access is selected every user will be able to see the username and password of the SQL user in the report's connection configuration.

Important: If SQL User Access is changed or if authentication type has changed Agito Security Center for SharePoint feature has to be deactivated and reactivated so that changes will be reflected in the reports.

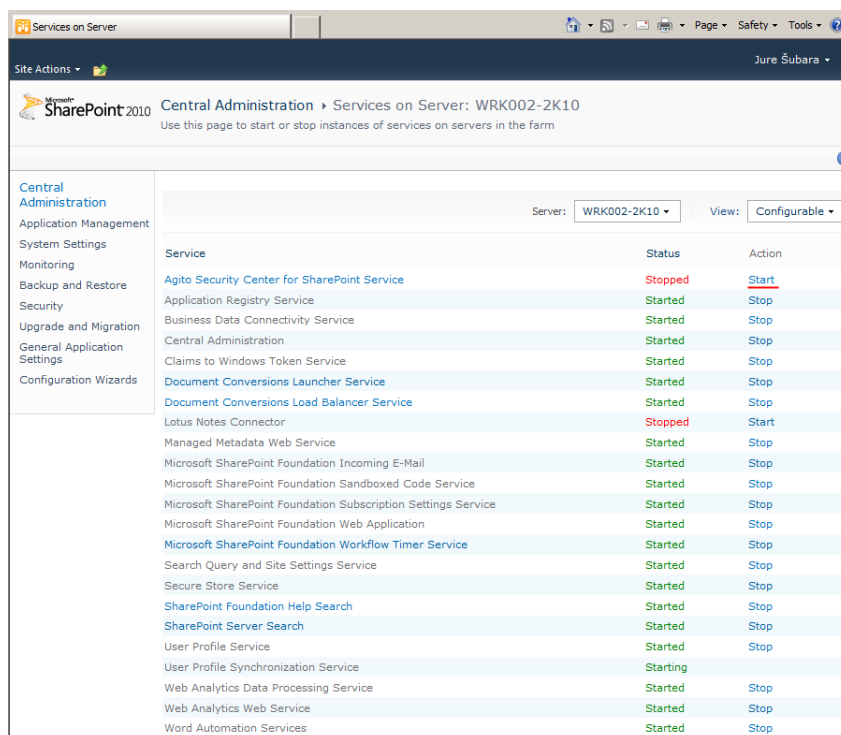
5 Installing and Configuring Import Service

Import Service handles daily imports of SharePoint structures and permissions into its own database. To configure Import Service please follow these steps:

1. Open "SharePoint 2010 Central Administration".
2. Click "System Settings -> Manage Farm Features" and make sure that the feature "Agito Security Center for SharePoint - Import Service" is activated.
3. Go to "Application Management -> Manage services on server" page.



4. Start the "Agito Security Center for SharePoint Service".



5. Configure Import Service:

a. Active Directory Export Settings:

- Enter the LDAP path in format "LDAP://domain" where your Active Directory can be accessed.
- If the SharePoint Job account doesn't have full read access to the Active Directory or you want to use other account to access Active Directory, select "Use specific user account for Active Directory Access" and fill in the account information

b. Job Scheduling settings:

- Select when to run the Import Service. The recommended settings are "Daily" in the time when SharePoint is at lowest use, e.g. 1 AM.

c. History log settings:

- By checking this setting, the job will write very detailed history log. It is recommended to check this option if you have problems with Import Service. Log can be viewed on Job History page.

d. Select Web Applications for import:

- Select the Web Applications for Import Service should gather the data.

The screenshot shows the configuration page for the Agito Security Center for SharePoint Service. The page is divided into several sections:

- Service Status:** Shows the current status of the service. Service Status: Running, Job Enabled: Enabled, Last run: 6/30/2011 2:54 PM, Job Status: Online.
- Active Directory Export Settings:** Set if Active Directory users and groups should be imported, and settings needed to access the active directory data. LDAP: LDAP://mycompany. There is a checkbox for "Use specific user account for Active Directory Access" which is currently unchecked. Below it are fields for "User name:" and "Password:".
- Job Scheduling settings:** Set when the import of SharePoint data to Agito Security Center for Sharepoint will occur. There are three radio button options: "Daily" (selected), "Weekly", and "Monthly". The "Daily" option has a time picker set to "Starting every day between 12 AM and no later than 12 AM".
- History log settings:** Settings related to history logging. There is a checkbox for "Write Extensive History Log" which is currently unchecked.
- Select Web Applications for import:** Select the web applications for import. There are two checkboxes: "SharePoint Central Administration v4" (unchecked) and "SharePoint - 80" (checked).
- Set Agito Security Center for SharePoint Database:** Settings for connecting to the Agito Security Center for SharePoint Database. Manage database instance: AgitoSecurityCenterDatabase.
- Job Details:** Details of the Job running Agito Security Center for SharePoint Import. Security Center Import Job.

At the bottom of the page, there are "Save" and "Cancel" buttons.

6. Click on "Save" button and then on "Start" button.

7. Click on "Security Center Import Job" to create initial import of the data.

8. Click on "Run Now" to import the initial data. Data will be periodically updated based on the configured job schedule.

The screenshot shows the 'Edit Timer Job' interface in SharePoint 2010 Central Administration. The page title is 'Agito Security Center for SharePoint Import Job'. The interface is divided into several sections:

- Timer Links:** Timer Job Status, Scheduled Jobs, Running Jobs, Job History, Job Definitions.
- Central Administration:** Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Configuration Wizards.
- Job Properties:**
 - Job Title:** Agito Security Center for SharePoint Import Job
 - Job Description:** (Empty)
 - Job Properties:** This section lists the properties for this job.
 - Web application: N/A
 - Last run time: 6/30/2011 1:14 PM
 - Recurring Schedule:** Use this section to modify the schedule specifying when the timer job will run. Daily, weekly, and monthly schedules also include a window of execution. The timer service will pick a random time within this interval to begin executing the job on each applicable server. This feature is appropriate for high-load jobs which run on multiple servers on the farm. Running this type of job on all the servers simultaneously might place an unreasonable load on the farm. To specify an exact starting time, set the beginning and ending times of the interval to the same value.
 - This timer job is scheduled to run:**
 - Minutes
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - Starting every day between:** 12 AM and 00
 - and no later than:** 12 AM and 00
- Buttons:** Run Now, Disable, OK, Cancel.

9. You can check "Running Jobs" or "Job History" to view status of the job.

5.1 System Configuration for Import

Agito Security Center for SharePoint uses Distributed Transaction Coordinator or DTC which has to be configured properly and running.

To configure DTC please read the instructions on Microsoft's web site:
[http://technet.microsoft.com/en-us/library/cc753510\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753510(WS.10).aspx).