Oracle® Retail Macro Space Planning

Security Guide
Release 14.1

E59552-01

December 2014

ORACLE

Oracle® Retail Macro Space Planning Security Guide, Release 14.1

E59552-01

Primary Author: Max Goltyakov

Contributors:

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

Send Us Your Comments

Oracle Retail Macro Space Planning, Security Guide, Release 14.1

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at www.oracle.com.

Preface

This document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate Oracle Retail applications. Installation and configuration are covered in more detail in the Macro Space Planning Installation Guide, which covers the Macro Space Management and the In-Store Space Collaboration products.

This document is intended for administrators, developers, and system integrators who perform the following functions:

- Document specific security features and configuration details for the above mentioned products, in order to facilitate and support the secure operation of the Oracle Retail Product and any external compliance standards.
- Guide administrators, developers, and system integrators on secure product implementation, integration, and administration.

We assume that the readers have general knowledge of administering the underlying technologies and the application.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Retail Macro Space Planning Release 14.1 documentation set:

Macro Space Planning

- *Macro Space Planning Installation Guide*
- *Macro Space Planning Data Model*

Macro Space Management

- *Macro Space Management Release Notes*
- *Administration Module User Guide*
- *Configuration Module User Guide*
- *Data Importer User Guide*
- *Fixture Studio User Guide*
- *Merchandiser User Guide*
- *Planner User Guide*
- *Product Studio User Guide*

- *Report Designer User Guide*

In-Store Space Collaboration

- *ISSC User Guide*
- *ISSC Mobile User Guide*

My Oracle Support

See also the following documents on My Oracle Support

- *Oracle Retail Macro Space Management: Implementing Customizable Buttons in Planner (Doc ID: 19528731.1)*
- *Oracle Retail Macro Space Management: Configuring the Master Plangram Mapping (Doc ID: 1952876.1)*

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 14.1) or a later patch release (for example, 14.1.1). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times **not** be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part

number, with a higher-numbered suffix. For example, part number E123456-**02** is an updated version of a document with part number E123456-**01**.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Documentation is packaged with each Oracle Retail product release. Oracle Retail product documentation is also available on the following Web site:

http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html

(Data Model documents are not available through Oracle Technology Network. These documents are packaged with released code, or you can obtain them through My Oracle Support.)

Documentation should be available on this Web site within a month after a product release.

Conventions

Navigate: This is a navigate statement. It tells you how to get to the start of the procedure and ends with a screen shot of the starting point and the statement "the Window Name window opens."

```
This is a code sample
    It is used to display examples of code
```

1

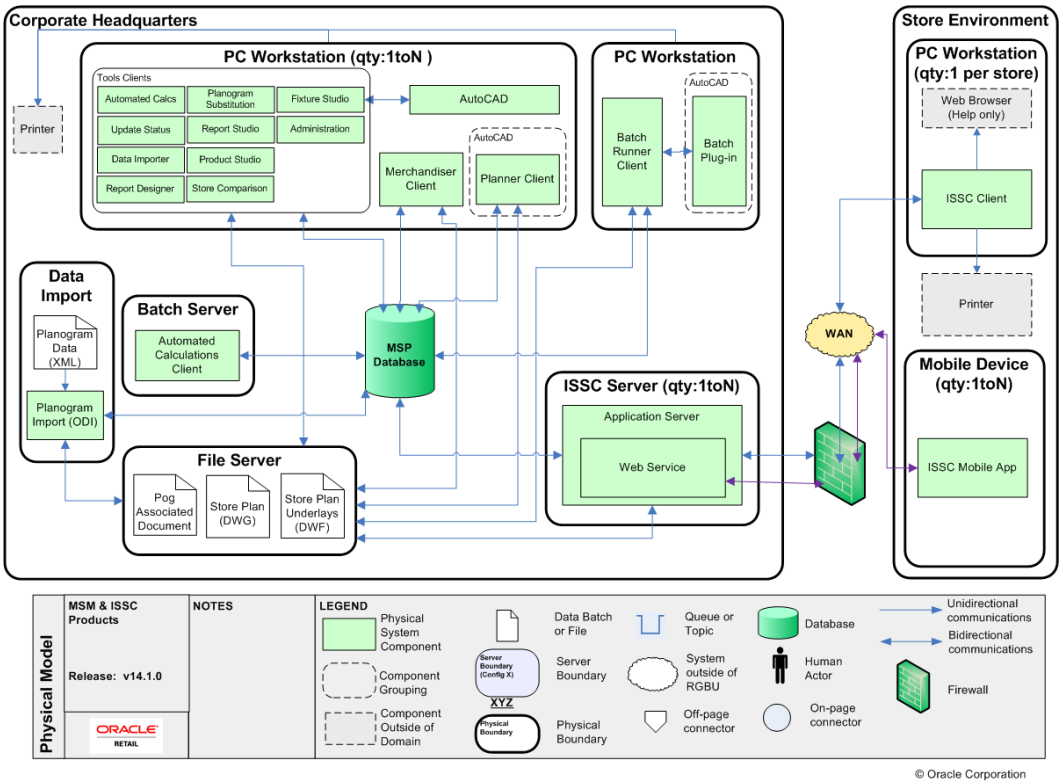
Overview of Security Features

This Security Guide covers a group of products that make up the Oracle Space Planning Suite of applications. The products are:

- Macro Space Management (MSM)
- In-Store Space Collaboration (ISSC)

These products offer solutions to very different retail business requirements and are meant to operate in different environments. In order to achieve consistency and simplify implementation, the core security aspects are shared between the products. The MSM product is a standalone product that has all the necessary administrative and functional applications and tools. The ISSC does not have any administrative tools and therefore is dependent on MSM in order to configure and administer the product's security.

Space Planning Physical Deployment



© Oracle Corporation

MSM is primarily used within the Corporate Headquarters environment. It is a suite of productivity applications supported by administrative, configuration and automation tools. It is the responsibility of the retailer to ensure the MSM suite is only accessible by highly privileged users.

The ISSC product is built upon the client-server architecture and is primary made for usage within the store environment. The desktop and mobile device clients are usually deployed within the stores. The clients interact with the application server, which is located in the Corporate Headquarters. The communication channel between the server

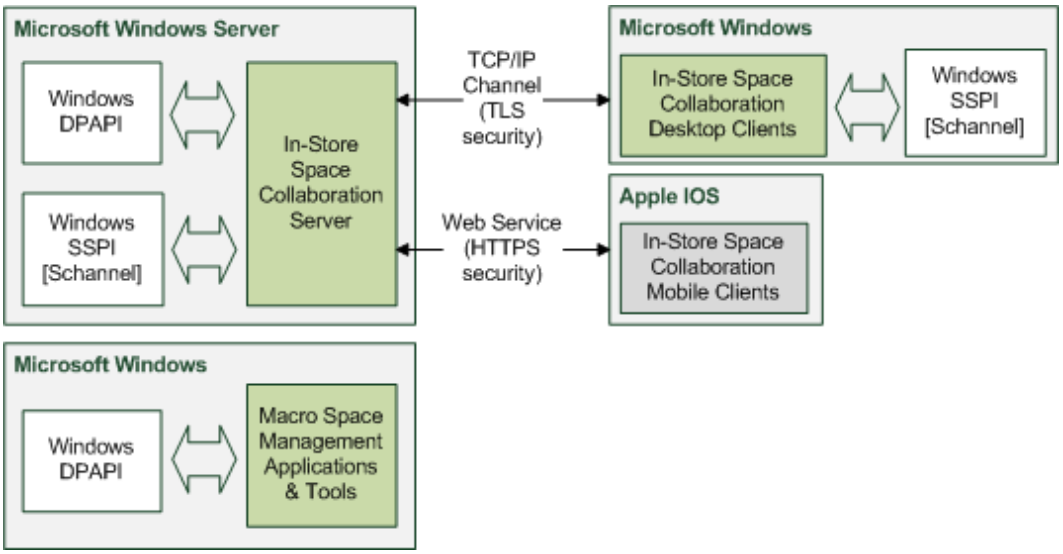
and the clients is protected by a secure communication mechanism. It is the responsibility of the retailer to restrict access to the ISSC desktop and mobile clients.

Data is imported into the database through the use of the MSM functionality. This mainly consists of dedicated data import solutions. An example is the Planogram Data Import solution which makes use of Oracle Data Integrator. The import tools assume the data to be imported is from a trusted source. It is the retailer's responsibility to ensure the integrity of the import data and to secure access to the import files on the servers.

MSM and ISSC share the same database server and therefore large parts of configuration and security are shared. The MSM Administration module is the main method used for Space Planning security configuration.

The application, file and database servers are intended to be deployed in a corporate data centre environment, with computer and physical access restricted to the machines.

Space Planning Security Architecture



At the application level, the products leverage Windows operating system technologies in order to protect sensitive data and communication channels. The database credentials are protected with the help of the Data Protection Application Programmable Interface (DPAPI).

In ISSC, the secure communication is handled through the use of the functionality exposed by the Microsoft .NET framework, which in turn leverages the Windows operating system aspects. Detailed secure communication configuration is done through the use of the operating system tools.

Dependent Applications

The following link is for the Oracle products that the Space Planning products have dependencies on:

Oracle Database Security Guide 12c Release (12.1)

The following link is for the Oracle products that the Macro Space Management product has dependencies on:

Fusion Middleware Developer's Guide for Oracle Data Integrator (11.1.1.7)

The following link is for the Oracle products that the In-Store Space Collaboration product has dependencies on:

Fusion Middleware Mobile Developer's Guide for Oracle Application Development Framework

Discussion of Dependencies on Underlying Platform

Products within the Space Planning Suite operate in the Microsoft Windows environments. The products make use of the available operating systems security features where possible.

- The ISSC secure communication leverages the Windows Schannel functionality. The detailed configuration of the Schannel is carried out using the Windows operating system tools.

  Note: The ISSC Server to desktop client communication only supports the TLS 1.0 protocol.

  Refer to the Secure Channel link in the Microsoft documentation on how to configure the Schannel in Windows.
- The ISSC server makes use of the X509 certificates in order to establish a successful connection between the server and the clients. The management and protection of the certificates is handled via the Windows Certificate Store, which is administered using the Microsoft Management Console (MMS). Refer to the Certificates link in the Microsoft documentation for additional information.
- Microsoft .NET Framework 4.0 (Full Profile). Refer to the Installing .NET Framework link in the Microsoft documentation for additional information.
- Autodesk AutoCAD 2013 or 2014 – this is used by the MSM Planner application. Planner is integrated within the AutoCAD environment. It makes use of the AutoCAD secure bundle loading mechanism, which tightly controls loading of the application code. Refer to the AutoCAD documentation for further information about the security aspects it offers.
- Microsoft Visual Basic run-time environment – this is built into the Windows operating system but if required a redistribution pack can be obtained from Microsoft.
- Microsoft Visual C++2010 run-time environment – this is built into the Windows operating system, but if required, a redistribution package can be obtained from Microsoft.

It is responsibility of the retailer to ensure that the underlying platform dependencies are kept up to date with the latest patches and security fixes distributed by Microsoft and Autodesk.

2

Installation Overview

The MSM product is intended to be used in the corporate data centre within a LAN environment. The pool of users is relatively small, but those users usually have the highest privileges. The ISSC product is intended to be used across the internet. The pool of users is dependent on the number of site seats required, thus can be a large number. The majority of ISSC users usually have low privileges.

Installing an Infrastructure Component

Microsoft Windows

The Space Planning products operate within the Microsoft Windows Environment. It is the retailer's responsibility to ensure the Microsoft Operating System is kept up to date with the latest security fixes. Listed below are the security hardening guides published by Microsoft:

Microsoft Windows Server 2008 Security Baseline

http://technet.microsoft.com/en-us/library/cc514539.aspx

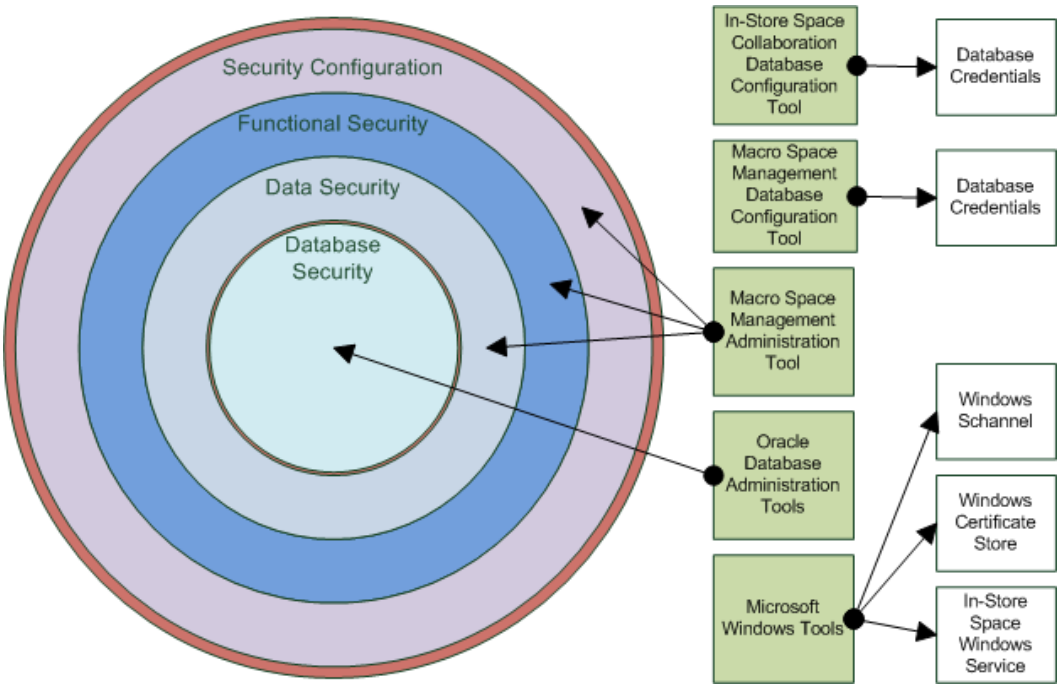
Microsoft Windows 7 Security Baseline

http://technet.microsoft.com/en-us/library/ee712767.aspx

Installing the Product

Refer to the Macro Space Planning Installation Guide for information regarding installation of Macro Space Management and In-Store Space Collaboration.

Post Installation Configuration



The figure above illustrates the collection of tools involved in configuring security in the Space Planning products. The MSM Administration tool plays the central role in configuring core application security aspects like user authentication and authorization.

Each product has its own dedicated database configuration tool. The tool associates the database credentials with the Windows account of the user which is intended to run the product.

The remaining Space Planning security configuration is carried out using standard Windows tools, as listed below:

1. Windows Schannel configuration – use the Group Policy Object Editor to define the SSL Configuration Settings. Refer to the Prioritizing Schannel Cipher Suites link in the Microsoft documentation for additional information.
2. Certificate Store configuration – use the Certificates Snap-In within the Microsoft Management Console (MMS) to manage the certificates store. Refer to the Add the Certificates Snap-In to an MMC link in the Microsoft documentation for additional information.
3. ISSC Service configuration – use the Services configuration tool. Refer to the Macro Space Planning Installation Guide for additional information.

For usage of the Space Planning configuration tools refer to the Space Planning Installation Guide. For the instructions on how to use the Windows tools refer to the documentation published by Microsoft.

In-Store Space Collaboration Server Strengthening

The ISSC Server installs and runs as a Windows service. The service is configured to log on as a *Local System* account. This is a built-in account which has high privileges. It is advisable to change the account under which the service runs under to an account with tighter security permissions, immediately after installation.

Refer to the Oracle Retail Macro Space Planning Installation Guide for additional information.

Macro Space Management Database Configuration

Run the MSM database configuration tool in order to setup the database credentials. This needs to be carried out for *each* MSM user's Windows account. The database credentials are saved to a configuration file in the private space allocated to the Windows account that the product will be running with. The location is as follows:

`%USERPROFILE%\AppData\Local\Oracle Retail\MSM\Config\Connections.Config`

The MSM database credentials do not support Windows roaming profiles. Refer to the Macro Space Planning Installation Guide for additional information regarding installation.

In-Store Space Collaboration Database Configuration

Run the ISSC database configuration tool in order to setup the database credentials. The tool is used to setup the database connection information for the ISSC Server. The credentials can be configured at either machine-specific or user-account-specific protections. These protection levels are explained further in the table below, in relation to the database configuration tool's options.

	Windows Account Option	
	Current User (Logged in User)	**Built-in User**
Protection level	User-account specific	Machine-specific
Description	Access tied to a specific Windows account. The credentials can only be read by the Windows account to which the credentials are assigned to. This is the safest option from the security point of view.	Shared access to credentials. The credentials can be read by any Windows account on the machine. This is not a safe option and is only in place to allow running of the ISSC Server Service under the default built-in Windows accounts.
Credentials storage location	%USERPROFILE%\AppData\Local\Oracle Retail\ISSC\Config\Connections.Config	%SystemDrive%\ProgramData\Oracle Retail\ISSC\Config

The ISSC database credentials do not support Windows roaming profiles.

> **Note**: It is recommended to use the user-account specific protection option only, as it offers the strongest protection of the database credentials.

When attempting to configure the ISSC database credentials, it might be needed to run the Database Configuration Tool under different Windows credentials, i.e. the credentials that match the Windows account under which the ISSC Service is intended to be run under.

The following options can be used to achieve this:

- Use the Windows Run as different user execution option. This is accessed by holding down the Shift key and then right-clicking on the Database Configuration Tool icon.
- Use the Windows Run as command-line tool.

Refer to the Macro Space Planning Installation Guide for additional information regarding installation.

Application Users Configuration

Space Planning comes with a pre-installed application user. The user is created during the database scripts execution and is set to expire on first use. The purpose of this default user is to allow configuration of the application security, via the MSM Administration application.

Initiate the user by logging into the Administration application. When prompted to change the password, assign a new password. The password must comply with the default passwords policy. Refer to the Password Policy Configuration section below for more information.

In-Store Space Collaboration Desktop Secure Communication

The ISSC product supports secure communication between the server and the desktop client. This is enabled by default, but requires additional configuration in order for it to work. This is done through the use of the application configuration files, located on the server and the client sides.

Server Configuration

The server supports secure communication by presenting the desktop client with a valid X509 certificate which validates the server's identity. The certificates are managed and stored in the Windows Certificate Store. The server's configuration must be set to point to the certificates in the Certificate Store.

The application configuration file is called RFServer.exe.config and is located in the ISSC Server installation folder.

```
<!--General ISSC Server settings-->
<applicationSettings>
  <RFServer.My.MySettings>
    <setting name="Secure_Connection" serializeAs="String">
      <value>True</value>
    </setting>
    <setting name="Connection_Port" serializeAs="String">
      <value>7001</value>
    </setting>
    <setting name="Certificate_Store_Location" serializeAs="String">
      <value>CurrentUser</value>
    </setting>
    <setting name="Certificate_Store_Name" serializeAs="String">
      <value>Personal</value>
    </setting>
    <setting name="Certificate_Find_Value" serializeAs="String">
      <value>CN=</value>
    </setting>
    <setting name="Certificate_Find_Type" serializeAs="String">
      <value>SubjectDistinguishedName</value>
    </setting>
  </RFServer.My.MySettings>
</applicationSettings>
</configuration>
```

There are a number of settings available that allow the server locate the required X509 certificate within the Certificate Store.

The following steps should be carried out:

1. Setup the server X509 certificate in the Certificate Store. Refer to the Import a Certificate link in the Microsoft documentation for additional information. A valid server X509 certificate and the associated private keys are required for secure communication via TLS.
2. Check the *Secure Connection* is enabled (this should be the default value).

   Set the *Certificate Store Location* value to indicate the location of the certificate store.

The options are:

- CurrentUser
- LocalMachine

The Current User offers the greatest level of security as it is tied to the current user's Windows account. Only the account in question is allowed to access the protected area used to manage the sensitive data like private keys. The LocalMachine location is the certificate store assigned to the local machine. It is accessible by all the Windows accounts on the machine, but is restricted to the local machine usage only.

3. Set the *Certificate Store Name* value to indicate the name of the certificate store.

   The options are:

   - TrustedPublisher – directly trusted publishers
   - Root – trusted root certificate authorities (CAs)
   - Personal – personal certificates
   - CertificateAuthority – intermediate certificate authorities

   The default value is Personal. The personal certificates are usually certificates that have been explicitly issued to the machine the ISSC Server is running on and therefore act as valid prove of identity for the machine.

   Refer to the Display Certificate Stores link in the Microsoft documentation for additional information.

4. Set the *Certificate Find Value* and *Certificate Find Type*. The find type allows to specify the search criteria to be used and has the following options:

   - SubjectName
   - SubjectDistinguishedName
   - SerialNumber
   - SubjectKeyIdentifier

   The default setting is SubjectDistinguishedName. Set the find value based on the certificate information being searched. This is the value that is used to locate the certificate. The find value must match the certificate's value as stored in the find type.

   For example,

   ```
   Certificate Subject Field = 'cn=ISSCServer, ou=example.ou=com'
   ```

   Then using `SubjectDistinguishedName` as find type would require the find value to be `'cn=ISSCServer, ou=example.ou=com'`

> **Note**: It is crucial to get the certificate configuration correct as failure to locate a valid certificate will prevent the ISSC Server from starting.

Desktop Client Configuration

The client application must have secure communication switched on in order to establish a secure connection with the ISSC Server. This is done through the usage of an application configuration file called ISSCClient.exe.config, which is located in the ISSC Client installation folder.

```
<setting name="Secure_Connection" serializeAs="String">
       <value>True</value>
</setting>

<setting name="Validate_Server_Certificate" serializeAs="String">
       <value>True</value>
</setting>

<setting name="Check_Revoked_Certificates" serializeAs="String">
       <value>True</value>
</setting>
```

All the secure communication settings are enabled by default.

In-Store Space Collaboration Mobile Secure Communication

ISSC offers a mobile solution which is primary used for store compliance. The ISSC Mobile application communicates with the ISSC Server via a Web Service. The communication channel between the app and the service is protected using standard web HTTPS protection. The Web Service is built upon the Microsoft Windows Communication Framework (WCF) and is hosted within the ISSC Server Windows Service.

Server

The ISSC Mobile functionality is disabled by default. The functionality is enabled and secured using the application configuration file. The application configuration file is located in the ISSC Server installation folder and is called RFServer.exe.config.

The settings used to configure the service are located in the *<system.serviceModel>* section. The configuration file comes pre-configured with the secure and unsecure versions of the serviceModel sections. Both versions are disabled and therefore need to be enabled by using standard xml notation. It is recommended to use the secure version of the configuration. The secure section enables the HTTPS secure communication by enabling transport security.

Once the secure section is enabled, the remaining section is to bind a certificate to the port being used for the Web Service communication. The port defaults to 8080. Refer to the Space Planning Installation Guide for additional information.

Client

The ISSC Mobile App is distributed as a Mobile Application Archive (MAA). Therefore, the application itself is configured and compiled by the retailer. The ISSC Mobile application is built upon the Oracle Application Development Framework (ADF). Usage of the domain whitelist security feature in order to control access to the device is recommended.

Refer to the Fusion Middleware Mobile Developer's Guide for Oracle Application Development Framework documentation for additional information.

3

Technical Overview of the Security Features

Security features of the Application

Authentication

The Space Planning products use a common mechanism to configure and enforce authentication. Authentication is carried out internally at the application level. There is no support for any external authentication systems e.g. LDAP.

The application user's credentials are stored in the database. The user's passwords are stored in a hashed form. The available hash algorithms are SHA-256, SHA-384 and SHA-512.

Password Policy Configuration

Space Planning is installed with the following default password policy settings:

Policy Group	Policy Item	Value
Failed Log-in	Number of login attempts before suspending	5
	Number of minutes account will be suspended	60
Password Complexity	Minimum password length	7
	Maximum password length	30
	Minimum number of upper case characters	1
	Minimum number of lower case characters	1
	Minimum number of numeric characters	1
	Minimum number of extended characters	0
Password Expiry	Password expiry period (days)	90
	Lock (days past expiration)	14
Password History	Number of passwords to keep	4
	Number of days to keep passwords	97
Excluded Passwords	*Empty*	

The level of protection offered by the settings above can be strengthened even further either by manually changing the values or by selecting a pre-defined 'Max' level option.

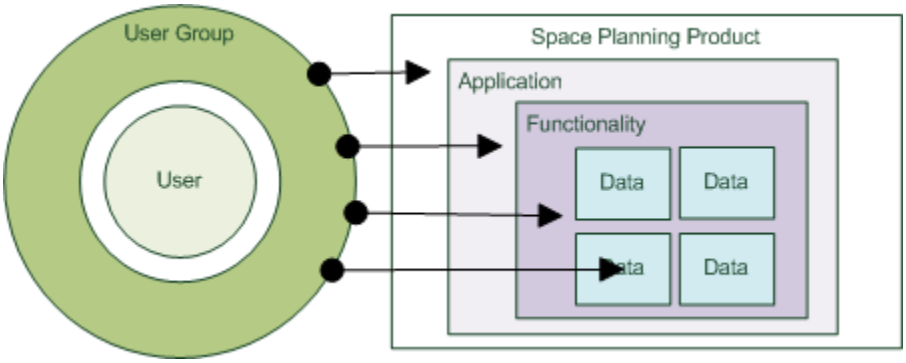
The extended characters list is as follows:

`	~	!	@	#	$	%	^	&	*	(	)	_	-	+	=
{	}	[	]	\	|	:	;	"	'	<	>	,	.	?	/

Configure the password policy to comply with the standards defined by your business.

Authorization

The Space Planning products authorization mechanism operates at different levels. The level to be used is dependent on the product and functionality in use.



In Space Planning, each application user belongs to an application user group. The authorization model revolves around assigning appropriate permissions to the user group.

The following access levels restrictions are available:

1. **Application level (functional security)**

   Restricts access to an application part of the MSM or the ISSC product. The products are configured with predefined default permissions in order to ensure that access is only provided to those user groups that require them for their normal day to day operations.

2. **Functional level (functional security)**

   Restricts access to functionality within the application. This level of restriction is lightly used in the MSM products. The ISSC product offers detailed functionality restriction.

3. **Business data level (data security)**

   Restricts access to business level data e.g. a store plan. This is shared between the MSM and ISSC products.

4. **Database level (database security)**

   Restricts access to database objects. This is achieved through the use of database roles and synonyms.

Refer to the Administration Module User Guide for information on how to configure functional and data security.

In-Store Space Collaboration

The ISSC product offers a very granular level of functional security implementation. The restrictions can be applied anywhere from application level to a specific graphical user interface element or even an actions carried out by users. By default, only the *In-Store* user group has full access to the functionality in the ISSC desktop and mobile clients.

If there is a requirement to give other user groups access to the ISSC product, then the changes to the functional security would need to be made directly in the database. This is because; currently there are not graphical user interface tools to do this. The configuration would involve some or all of the tables listed below:

- avttb_user_group – the user group the application user belongs to. The user group is given permissions to the functionality
- avttb_user_group_type – holds additional information for the user group
- avttb_message_control – the functional elements that require to be given permissions to
- avttb_message_user_group_link – defines the permissions between the user group and the functionality

The ISSC product has a limited data security lockdown for the product hierarchical tree. The user groups can be given permissions to access *top level* product groups only. The configuration would involve the following tables:

- avttb_user_group - the user group the application user belongs to. The user group is given permissions to the functionality
- avttb_user_group_product_link – defines permissions between the product hierarchical items and the user group. Need to use a top level product item, i.e. the one that has no parents defined.

Refer to the Standard Data Model document which describes these tables in more detail.

Encryption and Hashing

The database credentials are protected using the security technologies exposed by the Windows operating system. The encryption and decryption of the credentials is handled using the Data Protection Application Programming Interface (DPAPI). The DPAPI interface handles management and protection of the encryption keys. The encrypted credentials are secured using user or machine level protection. The user level protection ties the credentials to a specific Windows account. The machine level protection ties the credentials to the machine itself. The required level of protection depends on the Space Planning Suite product and its usage. The encrypted credentials are stored in a protected location. The protected credentials cannot be used in a roaming scenario as they are tied to a specific Windows account or the machine itself.

The database credentials are configured using a specialized Database Configuration tool which is distributed with each Space Planning Suite product. Refer to Macro Space Planning Installation Guide for instructions on how to use the Database Configuration Tool.

The application user passwords are handled using a hashing technique. The following hashing algorithms are supported: SHA-256, SHA-384 and SHA-512. This applies to MSM and ISSC products and is configured using the MSM Administration Module.

The MSM Planogram Import solution makes use of Oracle Data Integrator (ODI). Refer to the Fusion Middleware Developer's Guide for Oracle Data Integrator for more information on the encryption and hashing for the ODI.

The following cipher technologies are recommended by Oracle:

- Cipher algorithms: AES (>=128 bit)
- Hash algorithms: SHA-1
- Key Exchange algorithms: Diffie Hellman (>=2048 bits)

4

Application Administration

Roles and Permissions

The Space Planning products are distributed with a predefined set of user groups. Each user group is assigned permission levels that are relevant to the tasks to be carried out by that user group.

When making changes to the roles and permissions, it is important to use the Principle of Least privilege when adjusting the permissions to protect your database from accidental modification or unauthorized access. Only assign privileges that are required to carry out the tasks by the users of the role.

Macros Space Management Roles

The MSM product has the following default user groups and permissions assigned to it:

User Group	Application
Admin	Admin Automation Planogram Studio Planner Planogram Substitution Data Importer Report Designer Product Studio Report Studio Fixture Studio
Floor Layout	Planner Report Studio
Merchandizer	Planner Planogram Studio Report Studio

In-Store Space Collaboration Roles

The ISSC product has only has single user group called

User Group	Application
In-Store	ISSC

Database Roles

The Space Planning database is protected using roles and synonyms database features. The table in Appendix C demonstrates the default roles and how they map to the applications they are intended to be used by.

The default application roles mentioned in the previous sections do not all directly map to the database roles. It is advised to create applications roles that are relevant to your business process and then assign them appropriate database role. It is important to get the mapping correct between the application and database roles, in order to ensure the application users would be able to perform their day to day tasks.

The ISSC Server only has a single database role. There are no default database roles defined for the Oracle Data Integrator MSM solution.

5

Extended Customization

Customizable SQL Functionality

Space Planning products offer an ability to configure specific functionality through the use of Custom SQL. The main purpose of the Custom SQL is to allow the implementers to adapt the functionality in order to meet specific business requirements. The Custom SQL usage varies from product to product.

Examples of the use of custom SQL are:

- Adapt property data to be displayed based on items selected in a hierarchical tree, for example merchandise properties.
- Configure reports to be displayed
- Annotation information

The Custom SQL is configured using various interfaces, which require some level of power user permissions set in order to access them. If the customization is found to be present in a non-administrative application, then it will be disabled by default and would need to be explicitly enabled. Usually, permissions are enabled using the MSM Administration application.

In ISSC, majority of the Custom SQL functionality cannot be configured via a graphical user interface and this would need to be altered directly in the database. The changes are usually made in the avttb_custom_sql table.

It is important to note that care must be taken:

- When enabling Custom SQL functionality as it is a very powerful functionality and must only be accessible by authorized personnel
- When constructing Custom SQL, because its output could potentially be displayed to the end user
- When making changes directly in the database
- When writing error handlers, make sure all database cursors are properly closed to prevent cursor snarfing
- When reporting errors, replace generated error messages such as exceptions with laconic messages to prevent accidental information leaks about your system to the end user (actual error messages may be written to a protected system log)

> **Note**: When making changes to Custom SQL, it might be necessary to adjust permissions assigned to the database role which will be used to execute the SQL. This is because the pre-defined database roles are configured to work with the default distributed Custom SQL only. Use the Principle of Least Privilege when adjusting the permissions to protect your database from accidental modification or unauthorized access.

It is the responsibility of the retailer to ensure that their Custom SQL code is safe and is executed under the proper privileges.

Macro Space Planning Customizable Buttons

The MSM product contains an AutoCAD based application called Planner. The Planner application has built-in customizable buttons functionality, which allows execution of bespoke database procedures via the graphical user interface elements. This enables creation of custom solutions to business process problems or steps.

This customizable buttons functionality is very flexible and powerful. Therefore, it requires a high level of expertise in order to be created and configured. Being custom functionality, it would require separate testing phases and tightly controlled security permissions. Refer to the Customizable Buttons White paper for further guidance. It is highly advisable to follow the guidance specified in the White Paper.

A

Appendix: Checklists

Secure Deployment Checklist - Macro Space Planning

1. Microsoft Windows hardening
2. Space Planning database users configuration
3. Database credentials configuration
4. Default application user configuration
5. Space Planning application users configuration
6. Space Planning functional security configuration
7. Space Planning data security configuration

Secure Deployment Checklist - In-Store Space Collaboration

Server

1. Microsoft Server Windows hardening
2. Microsoft Secure Communication hardening
3. ISSC Server Windows service account
4. ISSC Server database credentials configuration
5. ISSC Server secure communication configuration

Client

1. Microsoft Windows hardening
2. Microsoft Secure Communication hardening
3. ISSC Client secure communication configuration

Space Planning Database Roles

Database Role	Administration	Automated Calculations	Data Importer	Fixture Studio	Merchandiser	Planner	Planogram Substitution	Product Studio	Report Designer	Store Comparison	Report Studio	Update Status	Batch Runner
Application Administrator	X	X	X	X	X	X	X	X	X	X	X	X	X
IT Help Desk	X	X	X	X	X	X	X	X	X	X	X	X	X
Merchandising Manager			X		X	X	X	X	X	X	X		
Merchandising Planner					X	X	X	X		X	X		
Product Data Steward								X					
Store Planner					X	X				X	X		
Store Planning Manager				X	X	X			X	X	X		

Database Role	Administration	Automated Calculations	Data Importer	Fixture Studio	Merchandiser	Planner	Planogram Substitution	Product Studio	Report Designer	Store Comparison	Report Studio	Update Status	Batch Runner
Automation		x	x									x	x

The table above lists the default database roles distributed for the use in the MSM product. Each role is configured to be used by a specific number of application(s).

The ISSC product only has a single database role defined called *ISSC Server*. Users of this role are intended to be ISSC Desktop Client and ISSC Mobile applicarion users.