Oracle® WebCenter Sites

Installation Guide for the Gadgets Application

11*g* Release 1 (11.1.1)

February 2012

ORACLE®

Oracle® WebCenter Sites Installation Guide for the Gadgets Application, 11*g* Release 1 (11.1.1)

Primary Author: Tatiana Kolubayev

Contributing Author: Melinda Rubenau

Contributor: Igor Dzyuba, Eric Gandt

Table of

Contents

About This Guide 5
Audience 5
Related Documents 6
Conventions 6
Third-Party Libraries 6

1 Installation Overview 7
Oracle WebCenter Sites: Gadgets Application 8
Prerequisites for Installing the Gadgets Application 10
Mappings Worksheet 12

2 Installation Options 17
Selecting an Identity Provider 18
Installing the Gadgets Application with Its Native Identity Provider 18
Installing the Gadgets Application with a New or Existing LDAP Server 18

3 Installing the Gadgets Application via the Configuration Tool 21
Overview of the Gadgets Application Configuration Tool 22
Installing the Gadgets Application Graphically 22
Installing the Gadgets Application Silently 27

4 Installing the Gadgets Application Manually 31
Overview of the Manual Installation Process 32
Encrypting Passwords Manually 32
Installing the Gadgets Application 33
Gadgets Application Configuration Files 34
log4j.properties 35
cos_facilities.xml 35
registry_client.properties 35
Java Key Store (JKS) 35

sslproxy.properties 36
gsoauthkey.pem. 37
zoo.properties 37
jmemcached.properties 38
schema_import.properties 39
user_runtime.xml 39
Configuring the Gadgets Application to Use the LDAP Identity Provider 39

5 Post-Installation Steps 41
Overview 42
If the Community Application is Installed 42
Configuring Security 42
Securing Ports 42
Creating Certificates, JKS, and Private Keys 42
Specifying OAuth Consumer Credentials. 43
Enabling Shindig Features. 43
Verifying the Gadgets Application Installation 44
Enabling the Gadgets Application 46
Registering the Gadgets Application 46
Authorizing Users to Work with the Gadgets Application's Interfaces 47
Next Steps 50

6 Adding Sample Gadgets 51
Prerequisites for Installing Sample Gadgets 52
Installing the Sample Gadgets 53

About This Guide

This guide describes the process of installing Oracle WebCenter Sites: Gadgets, an application designed to display gadgets on websites.

Applications discussed in this guide are former FatWire products. Naming conventions are the following:

- *Oracle WebCenter Sites* is the current name of the product previously known as *FatWire Content Server.* In this guide, *Oracle WebCenter Sites* is also called *WebCenter Sites*.
- *Oracle WebCenter Sites: Gadgets* is the current name of the application previously known as *FatWire Gadget Server.* In this guide, *Oracle WebCenter Sites: Gadgets* is also called *Gadgets*.
- *Oracle WebCenter Sites: Community* is the current name of the application previously known as *FatWire Community Server.* In this guide, *Oracle WebCenter Sites: Community* is also called *Community.*
- *Oracle WebCenter Sites: Web Experience Management Framework* is the current name of the environment previously known as *FatWire Web Experience Management Framework.* In this guide, *Oracle WebCenter Sites: Web Experience Management Framework* is also called *WEM Framework*.

The Gadgets application integrates with Oracle WebCenter Sites according to specifications in the *Oracle WebCenter Sites 11g Release 1 (11.1.1.x) Certification Matrix*. For additional information, see the release notes for the Gadgets application. Check the WebCenter Sites documentation site regularly for updates to the *Certification Matrix* and release notes.

Audience

This guide is for installation engineers and anyone else who has expertise with Oracle WebCenter Sites and the process of installing enterprise-level software. Users of this guide should also be familiar with the Oracle WebCenter Sites Advanced interface, especially mirror publishing. Also required is experience with the Oracle WebCenter Sites: Web Experience Management Framework, the process of registering applications with WebCenter Sites, and authorizing users to access the applications.

Related Documents

For more information, see the following documents:

- *Oracle WebCenter Sites Developer's Guide*
- *Oracle WebCenter Sites Administrator's Guide for the WEM Framework*
- *Oracle WebCenter Sites User's Guide for the Gadgets Application*
- *Oracle WebCenter Sites Developer's Guide for Creating Gadgets*

Conventions

The following text conventions are used in this guide:

- **Boldface** type indicates graphical user interface elements that you select.
- *Italic* type indicates book titles, emphasis, or variables for which you supply particular values.
- `Monospace` type indicates file names, URLs, sample code, or text that appears on the screen.
- **`Monospace bold`** type indicates a command.

Third-Party Libraries

Oracle WebCenter Sites and its applications include third-party libraries. For additional information, see *Oracle WebCenter Sites 11gR1: Third-Party Licenses*.

Chapter 1

Installation Overview

- Oracle WebCenter Sites: Gadgets Application
- Prerequisites for Installing the Gadgets Application
- Mappings Worksheet

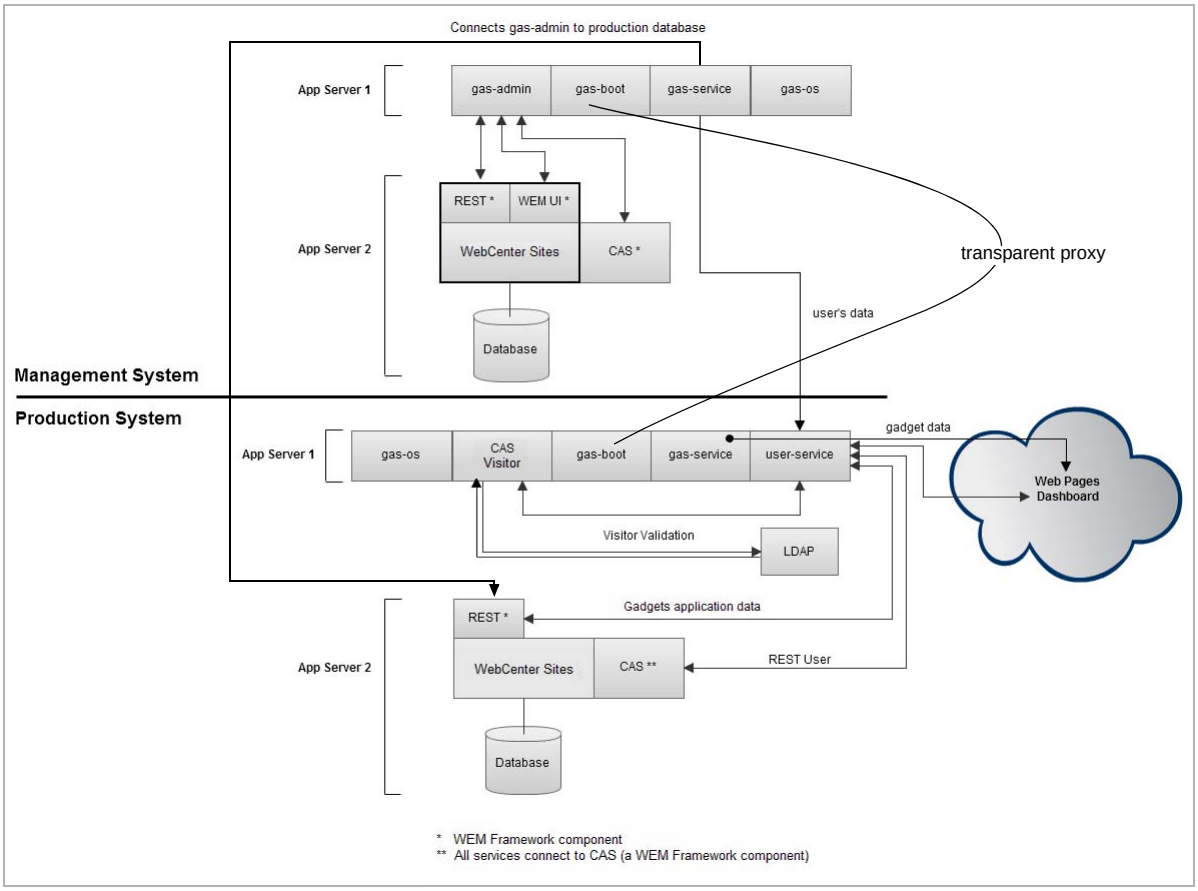
Oracle WebCenter Sites: Gadgets Application

The Gadgets application is a gadget container whose component web applications are installed on a management system and production system, as shown in Figure 1.

Note

In this guide, the term “production system” means “delivery system.”

Figure 1: The Gadgets Application Installation



The management system hosts the following component web applications: `gas-admin`, `gas-boot`, `gas-service`, and `gas-os`. The management system is a WebCenter Sites installation running the Oracle WebCenter Sites: Web Experience Management (WEM) Framework, which includes Representational State Transfer services (REST), Central Authentication Service (CAS), and the WEM Admin interface.

The production system hosts the following component web applications: `gas-os`, CAS for visitors, `gas-boot`, `gas-service`, and `user-service`. The production system is a WebCenter Sites installation running the WEM Framework, which includes CAS and REST services. The production system does not require the WEM Admin interface. The LDAP server can be configured to replace the native authentication system used by the WEM Framework.

Descriptions for the components of the Gadgets application are as follows:

- The `gas-os` component is an OpenSocial container, which provides a reference implementation for the OpenSocial standard. `gas-os` provides the code to render gadgets, proxy requests, handle REST and RPC requests, and enable visitor discovery with OAuth. The `gas-os` component is capable of rendering OpenSocial gadgets in a web browser.
- `gas-admin` is the Gadgets application's interface. As shown in Figure 1, it runs on the management system.

  The `gas-admin` component is used to register gadgets for display on site visitors' dashboards. Installing the Gadgets Samples Module provides several gadgets out-of-the-box that can be registered to the `gas-admin` component. The sample gadgets are: List, RSS, ThumbList, and SlideShow. Gadgets with OAuth support can be personalized by visitors and/or retrieve a visitor's personalized data from their OAuth Service Providers.

  The `gas-admin` component specifies a predefined user, which is a WebCenter Sites general administrator (`fwadmin`, by default) who belongs to the `RESTAdmin` group. Real users derive their access rights to the Gadgets application through the general administrator's membership in the `RESTAdmin` group, making it unnecessary to add the real users to any REST group.

  Interface functions in `gas-admin` are protected by the roles GeneralAdmin, SiteAdmin, and Designer. If a role does not exist, it is created during the installation process. Each role grants its user access to the `gas-admin` component and exposes a set of interface functions commensurate with the role.

  The `gas-admin` component provides one of two interfaces, depending on the site to which it is assigned:

  - On `{cs_site}`, `gas-admin` displays its Global Gadget Catalog interface, which is protected by the GeneralAdmin role and therefore accessible only to general administrators. The global gadget catalog is used to centrally store gadgets and distribute them to sites that run the Gadgets User interface.
  - On sites other than `{cs_site}`, `gas-admin` displays its Gadgets User interface, which provides the site gadget catalog for registering gadgets locally, provides a dashboard to contain the gadgets, and offers options for deploying registered gadgets to the website. Which interface functions are displayed to a user depends on the user's role.
- The `gas-boot` component manages production services and communication between the production and management systems. The `gas-boot` component provides a caching service based on `jmemcached`. It also provides a registry service based on Apache ZooKeeper. ZooKeeper maintains a centralized configuration file that defines how the components communicate with each other, which eliminates the need to configure each component individually. **Single-server installations require only one instance of gas-boot (the production instance).**
- The `gas-service` component handles gadget data.

  On the management system, `gas-service` provides the JavaScript API to support the `gas-admin` interface and user interactions. For example, when a user invokes an interface function, `gas-admin` sends the user's request to the `gas-service` component, which sends the request to the production system REST layer, which retrieves the requested information from the production system database. The information is displayed in the `gas-admin` interface.

On the production system, `gas-service` serves gadgets to web pages tagged with gadget configuration code. The `gas-service` component maintains the gadget registry, provides gadget code for download, and serves JavaScript API requests from the gadgets to provide them with data.

- The `user-service` component handles visitor data. It serves requests related to visitors, such as registration and editing of visitor profiles. In this manner, `user-service` keeps track of visitors' profile data and collects such information as author IDs, display names, and images.

When the Gadgets application's components are installed, the Gadgets application's asset types are installed in the WebCenter Sites' databases. The asset types are used to define gadgets (including the Gadgets application's sample gadgets, which must be installed separately), and provide the infrastructure for the Gadgets application, such as the dashboard, site visitor account storage, and the skins for the Gadgets application's interface.

Prerequisites for Installing the Gadgets Application

Anyone installing the Gadgets application must have expertise with WebCenter Sites, the WEM Admin interface, and the process of installing enterprise-level software. Before installing the Gadgets application, complete the following checklist:

- Verify that you have the `Gadget_Server_v1.1.zip` file.
- Review the Gadgets application release notes for the latest information about supported platforms and procedures for installing the Gadgets application.
- Read this guide to determine your installation options:
  - The Gadgets application can be installed to work with either its native identity provider (the database used by the WEM Framework) or an LDAP identity provider.
  - The Gadgets application can be installed via the Configuration Tool or manually. Installing the Gadgets application via the Configuration Tool is recommended.
  - The Gadgets application can be installed on dual-server systems or single servers.

    Note

    Single-server installations are supported only for development purposes.

    A dual-server installation consists of two physically separate machines, one hosting the management environment, the other hosting the production environment. A single-server installation consists of a single machine hosting both the management and production environments. This guide is written for dual-server installations. Instructions for single-server installations are provided in this guide, as necessary.
  - Unless noted otherwise, all mention of the `cas` component refers to visitor `cas`.
- The Gadgets application requires two dedicated application servers: one application server for its management instances and one for its production instances.

Management and production systems must be fully functional WebCenter Sites installations.

- The general administrator used throughout this guide must be a member of the `RestAdmin` security group on both the management and production systems. Users of the Gadgets application will connect to the Gadgets interfaces through the general administrator, as explained on page 9.
- On the content management system, mirror the following sites to the production system:
  - `{cs_site}`, which you can either create or select to host the Global Gadget Catalog interface
  - Sites other than `{cs_site}`, which you can either create or select to host the Gadgets User interface

Note

Once you have installed and registered the Gadgets application, you will assign the application to the mirrored sites on the production system such that a given site runs either the Global Gadget Catalog interface or the Gadgets User interface, as described above. Additional information about assigning the Gadgets application is available in "Authorizing Users to Work with the Gadgets Application's Interfaces," on page 47.

- On the production system, enable searches as follows: Start the Lucene search engine. Configure search indexing, using the steps in the "Public Site Search" chapter of the *Oracle WebCenter Sites Developer's Guide*.
- On Unix systems, enable rendering of gadgets by adding the `-Djava.awt.headless=true` JVM parameter to `JAVA_OPTS` on both the management and production application servers used by the Gadgets application.
- To ensure an efficient installation process, use the worksheet on page 12 to pre-record information that you will be prompted to enter during the installation process.

In addition to installation instructions, this guide provides you with instructions for installing sample gadgets on the FirstSiteII sample site (with **StoreDemoData** enabled). For instructions, see Chapter 6, "Adding Sample Gadgets."

Mappings Worksheet

Use Table 1 as a worksheet to record the information you will provide during the installation process. Properties are listed in the order in which they appear in the dialogs of the Configuration Tool. They are named exactly as they appear in the default configuration files of the Gadgets application.

Note

The Gadgets application uses encrypted passwords (as well as unencrypted passwords when an LDAP server is installed). Enter passwords as follows:

- If you choose to run the Configuration Tool, enter passwords in plain text. They will be encrypted automatically by the Configuration Tool.
- If you choose to install manually:
  - Enter encrypted passwords, obtained from the encryption utility provided with the Gadgets application. See "Encrypting Passwords Manually," on page 32.
  - LDAP users, enter both the encrypted and unencrypted versions of `{ldap_user_password}`. You will specify the *encrypted* version in the `gas_registry_schema.xml` file and the *unencrypted* version in `deployerConfigContext.xml`, located in the visitor `cas` component (`cas/WEB-INF/classes/deployerConfigContext.xml`).

Table 1: Mappings Worksheet

Property	Required	Description	Your Value
`{management_cs_ip}`	✓	IP address or host name of the WebCenter Sites management system (which contains the WEM Admin interface)	
`{management_cs_port}`	✓	Port for the management WebCenter Sites application	
`{management_cs_context_root}`	✓	Context root for the management WebCenter Sites application	
`{cs_management_username}`	✓	User name for a WebCenter Sites general admin with full REST permissions (default, `fwadmin`) to the WebCenter Sites management system	
`{cs_management_password}`	✓	Password for the above WebCenter Sites user `{cs_management_username}`	
`{management_cs_cas_ip}`	✓	IP address or host name for CAS on the WebCenter Sites management system	
`{management_cs_cas_port}`	✓	CAS port on the WebCenter Sites management system	

Table 1: Mappings Worksheet *(continued)*

Property	Required	Description	Your Value
{management_cs_cas_context_root}	✓	CAS context root on the WebCenter Sites management system.	
{production_cs_ip}	✓	IP address or host name of the WebCenter Sites production system	
{production_cs_port}	✓	Port for the production WebCenter Sites application	
{production_cs_context_root}	✓	Context root for the production WebCenter Sites application	
{cs_production_username}	✓	User name for a WebCenter Sites general admin with full REST permissions (default, fwadmin) to the production WebCenter Sites application	
{cs_production_password}	✓	Password for above user {cs_production_username}	
{production_cs_cas_ip}	✓	IP address or host name for CAS on the production WebCenter Sites system	
{production_cs_cas_port}	✓	CAS port on the production WebCenter Sites system	
{production_cs_cas_context_root}	✓	CAS context root on the production WebCenter Sites system.	
{cs_site}	✓	Site where the Gadgets application's asset types and Global Gadget Catalog interface will be enabled (must be a site that exists on both the management and production WebCenter Sites applications). It is the same site that you created (or selected) and mirrored on page 11. This is a site to which you will assign the Gadgets application once you have registered the application with WebCenter Sites.	
{management_gas_ip}	✓	IP address or host name for the Gadgets application's management system	
{management_gas_port}	✓	Port for the Gadgets application on the management system	
{production_gas_ip}	✓	IP address or host name for the Gadgets application's production system	
{production_gas_port}	✓	Port for the Gadgets application on the production system	

Table 1: Mappings Worksheet *(continued)*

Property	Required	Description	Your Value
{GASHOME}	✓	Path to the directory under which the Gadgets application will be installed and the following subdirectories will be created: logs, storage, data, install. (For single-server installations, only one {GASHOME} is required.)	
{gas_production_ldap_ip}	When using LDAP	IP address or host name for the LDAP server for the Gadgets application's production system	
{gas_production_ldap_port}	When using LDAP	Port for the LDAP server for the Gadgets application's production system	
{ldap_basedn}	When using LDAP	Base DN for the Gadgets application (example dc=fatwire,dc=com)	
{ldap_username}	When using LDAP	User name with administrative permissions to the given Base DN	
{ldap_user_password}	When using LDAP	Password of administrative user {ldap_username}. **Note**: If you plan to install the Gadgets application via the Configuration Tool, enter the unencrypted password. If installing manually, enter both the encrypted ***and*** unencrypted versions of the password.	
{gasvisitor_username}	✓	Visitor name of the Gadgets application, used as the default visitor when one is logged in. This is also the security user for the Gadgets application.	
{gasvisitor_password}	✓	Password for above visitor {gasvisitor_username}. **Note:** If you plan to install the Gadgets application via the Configuration Tool, a random and complex password is automatically created. If installing manually, it is strongly recommended that you create a complex password.	
{mailhost_ip}	✓	IP address or host name of the mail server	
{mailhost_port}	✓	Port on which the mail server is listening (normally 25)	
{use_mail_account_to_send_mail}	✓	Must be set to true or false	

Table 1: Mappings Worksheet *(continued)*

Property	Required	Description	Your Value
`{email_from_account}`	✓	Email address from which to send mail	
`{sender_email_account}`	Only when `{use_mail_account_to_send_mail}` is true	User name used to log in to the SMTP server	
`{sender_email_password}`	Only when `{use_mail_account_to_send_mail}` is true	Password for the above email account `{sender_email_account}`	

Chapter 2

Installation Options

- Selecting an Identity Provider
- Installing the Gadgets Application with Its Native Identity Provider
- Installing the Gadgets Application with a New or Existing LDAP Server

Selecting an Identity Provider

The Gadgets application can be installed to work with either its native identity provider (the database used by the WEM Framework) or an LDAP identity provider. The Gadgets application can be installed via the Configuration Tool or manually. The Configuration Tool is preferred, as it prompts you for installation parameters (listed on page 12) and encrypts passwords automatically. If you select the LDAP option, the Configuration Tool will configure the Gadgets application's components to use the LDAP identity provider.

Note

Before continuing, ensure that you have completed the following steps:

- Prepared for the installation process as described in "Prerequisites for Installing the Gadgets Application," on page 10.
- Filled out the installation worksheet (page 12).
- You have carefully chosen the type of identity provider to enable. Once the Gadgets application is installed, it cannot be configured to use a different identity provider.

Installing the Gadgets Application with Its Native Identity Provider

In this type of installation, users are authenticated by default against the database used by the WEM Framework. Install the Gadgets application using instructions in one of the following chapters:

- Chapter 3, "Installing the Gadgets Application via the Configuration Tool":
  - "Installing the Gadgets Application Graphically," on page 22
  - "Installing the Gadgets Application Silently," on page 27
- Chapter 4, "Installing the Gadgets Application Manually"

Installing the Gadgets Application with a New or Existing LDAP Server

Using LDAP as the Gadgets application's identity provider is recommended if you wish to share user accounts between the Community application and the Gadgets application, or a third-party application and the Gadgets application.

1. Do one of the following:
   - If you are using a new LDAP server, install and configure a supported LDAP server, listed in the Gadgets application release notes. Continue to step 2.
   - To set up an existing LDAP server, create a new Base DN to provide for the Gadgets application visitors. Complete the steps below, starting with step 2.

2. Create an `ldif` file with the following information, replacing the `{ldap_basedn}` parameter with the value for your system (you can import multiple users by copying the `# add user` section for each user):

```
dn: {ldap_basedn}
objectclass: dcObject
objectclass: organization
dc: fatwire
description: OpenLDAP pre_gas_setup
o: Fatwire Software

dn: cn=<user_name>,{ldap_basedn}
objectClass: inetOrgPerson
objectClass: top
userPassword: <user_password>
cn: <user_name>
sn: <user_name>
displayName: <user_name>
description: <user_description>
```

3. Import the created `ldif` file.
4. In LDAP, create a default visitor user with the following credentials: `{gasvisitor_username}` and `{gasvisitor_password}`. This visitor will be used by default for anonymous visitors.
5. You are ready to install the Gadgets application. For instructions, see one of the following chapters:
   - Chapter 3, "Installing the Gadgets Application via the Configuration Tool":
     - "Installing the Gadgets Application Graphically," on page 22
     - "Installing the Gadgets Application Silently," on page 27
   - Chapter 4, "Installing the Gadgets Application Manually"

Chapter 3

Installing the Gadgets Application via the Configuration Tool

- Overview of the Gadgets Application Configuration Tool
- Installing the Gadgets Application Graphically
- Installing the Gadgets Application Silently

Overview of the Gadgets Application Configuration Tool

The Configuration Tool guides you through the installation process for the Gadgets application by prompting you for installation parameters (listed on page 12) and automatically encrypting all passwords that must be encrypted. If you choose the LDAP option, the Configuration Tool will enable the Gadgets application's components to use the LDAP identity provider.

The Configuration Tool provides the following installation options:

- Installing the Gadgets Application Graphically
- Installing the Gadgets Application Silently

Note

Before continuing, ensure that you have completed the following steps:

- Prepared for the installation process as described in "Prerequisites for Installing the Gadgets Application," on page 10.
- Filled out the installation worksheet (page 12).
- If you plan to use an LDAP identity provider, you have set up the LDAP server as shown on page 18.

Installing the Gadgets Application Graphically

For dual-server installations, complete the following steps on both the management and production systems unless otherwise noted. Notes for single-server installations are provided where necessary:

1. Unzip the `Gadget_Server_v1.1.zip` file.

   Ex. `/u01/Downloads/GS`

2. Copy the `gasmanagement` and `gasproduction` folders to the `gs_Configure` folder.

3. Creating the home directory: The home directory is where logs, monitoring data, and ZooKeeper data will be stored for the Gadgets application. The path to this directory will be the value for `{GASHOME}` throughout this guide.

   Ex. `/u01/software/GS`

   - If you wish to have the Configuration Tool create the home directory, skip this step and continue with step 4.
   - If you wish to create the home directory, note the following:
     - On management and production systems, we recommend using the same path.
     - On single-server installations, only one `{GASHOME}` is necessary. In this `{GASHOME}` directory we recommend using two separate paths – one for management logs and one for production logs.

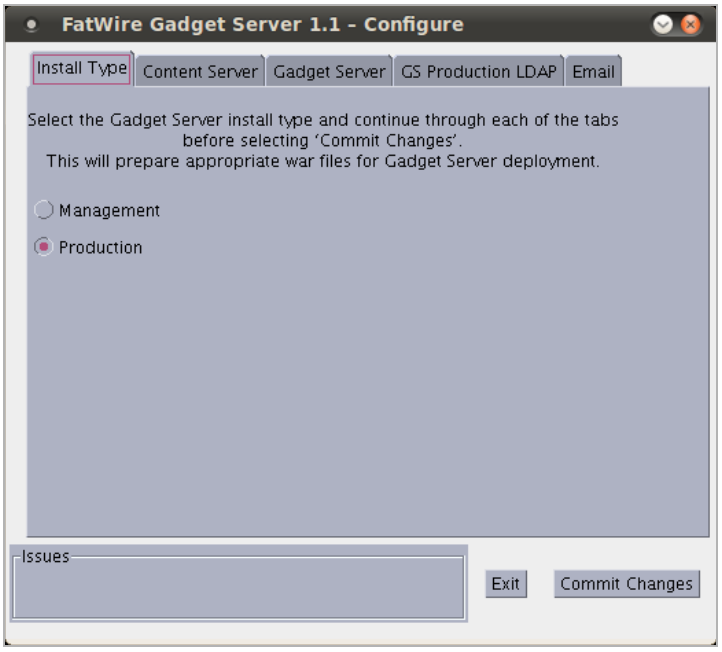
4. Configure two application servers for the Gadgets application:
   - Dual-server installations: One application server is for the production system, for the Gadgets application production components; the other is for the management system, for the Gadgets application management components.
   - Single-server installations: One application server is for the Gadgets application production components; the other is for the Gadgets application management components.
5. Set `JAVA_HOME` to the `jdk` folder of the version of Java that will be used. The Java version must be 1.6 or higher.

   Ex. `export JAVA_HOME=/opt/jdk1.6.0_20`
6. If installing on a Unix environment, ensure that the `bash` shell and `sed` stream editor are installed and located in the `PATH` environment variable.
7. Install the Gadgets application:
   a. Run the `configureGS.sh` or `configureGS.bat` script.

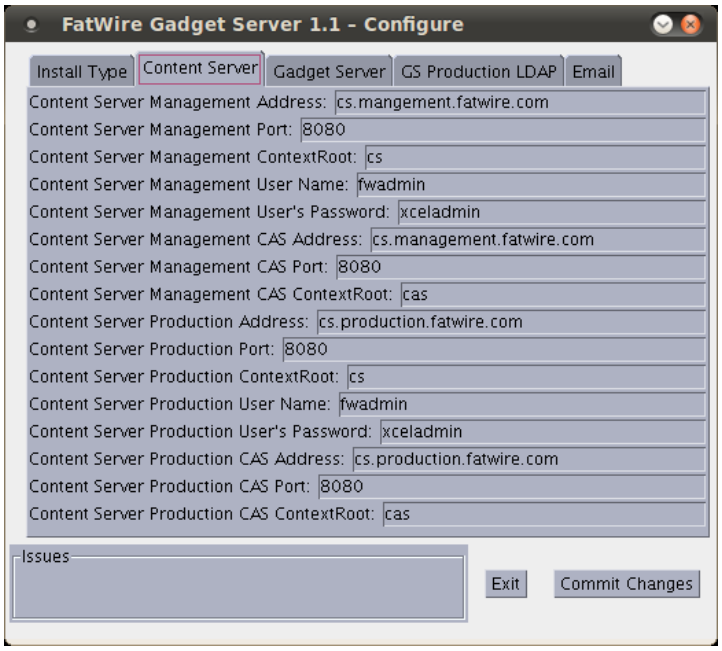
   Note

   On Unix, the `DISPLAY` environment variable must be set. For example:
   `export DISPLAY=10.120.19.21:0.0`

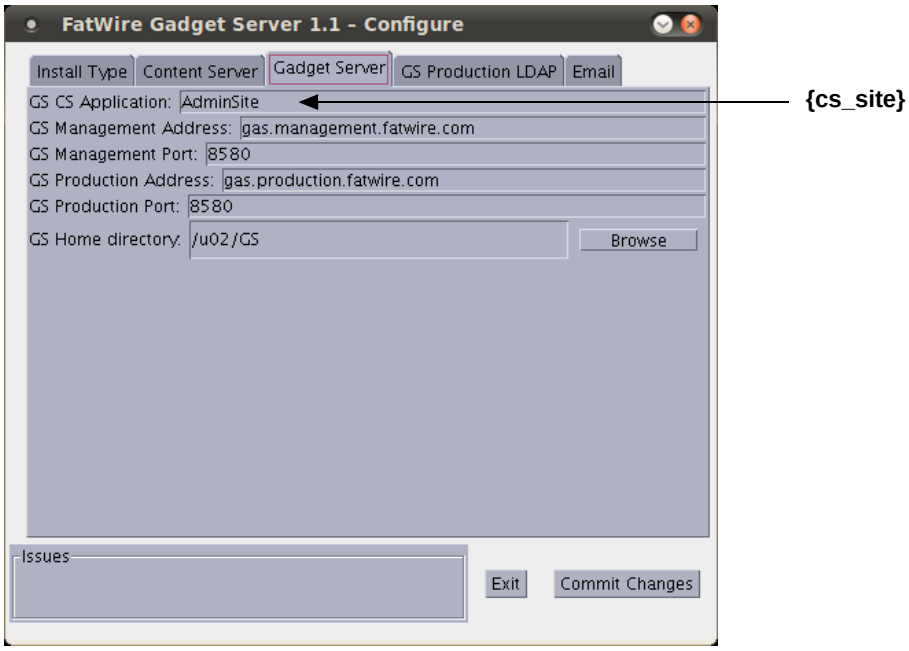
   b. On the **Install Type** tab, select **Management** if you are installing on the management application server, or **Production** if you are installing on the production application server.



c. On the **Sites** tab (**Content Server**), enter the values from your mappings worksheet (page 12).

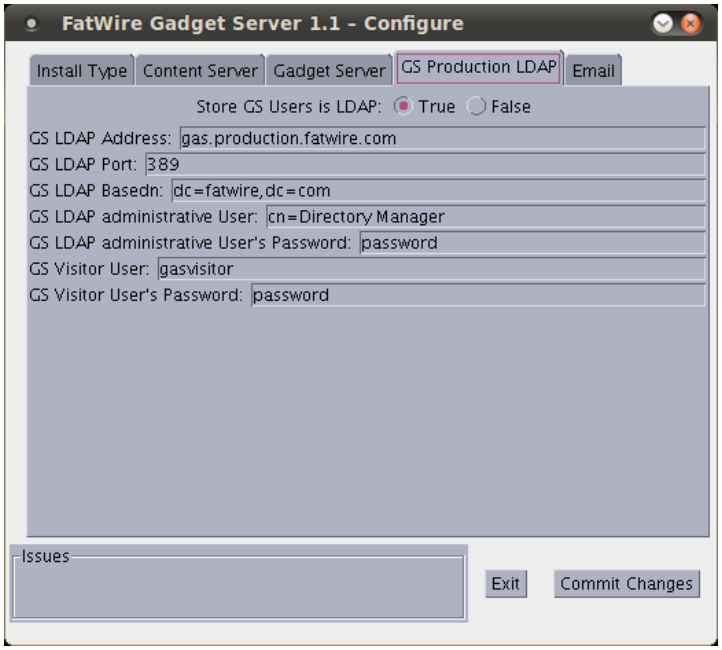


d. On the **Gadgets** tab (**Gadget Server**), enter the values from your mappings worksheet. You can either enter the value for `{GASHOME}` (see step 3), or browse to the directory.



e. On the **GS Production LDAP** tab, do one of the following:

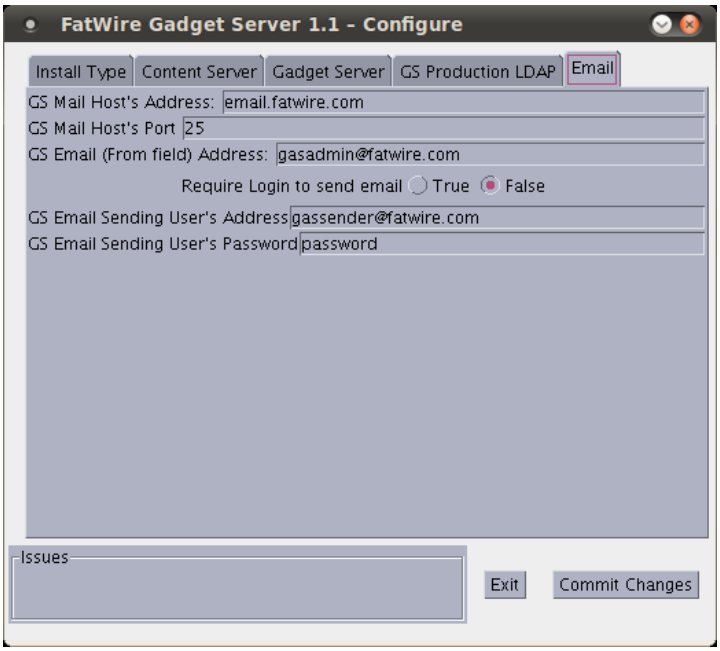
- If you are not using LDAP, set “Store GS Users in LDAP” to **False**. The fields “GS Visitor User” and “GS Visitor User’s Password” are pre-populated (if necessary you can supply your own values). Continue to the next step.
- If you are using LDAP, set “Store GS Users in LDAP” to **True** and enter the values from your mappings worksheet. **Complete this step on both the management and production systems.**



f. Click the **Email** tab:

1) Enter the values from your mappings worksheet. Set "Require Login to send email" to the value of `{use_mail_account_to_send_mail}`.

2) Click **Commit Changes**.



g. After the Configuration Tool has completed configuring the Gadgets application, click **OK**.

h. Deploy the Gadgets application `WAR` files at `{GASHOME}/install`, first on the production application server, then on the management application server (as required by boot order):

- Dual-Server installations: On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-boot`, `gas-os`, and `gas-service`.
- Single-Server installations: On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-os`, and `gas-`

`service`. (Deploy `gas-boot` only on the production application server. `gas-boot` is not used on the management environment.)

8. Once the `WAR` files are deployed, proceed to Chapter 5, "Post-Installation Steps" to secure and verify your installation, register the Gadgets application, and authorize its users.

Installing the Gadgets Application Silently

For dual-server installations, complete the following steps on both the management and production systems unless otherwise noted. Notes for single-server installations are provided where necessary:

1. Unzip the `Gadget_Server_v1.1.zip` file.

   Ex. `/u01/Downloads/GS`

2. Copy the `gasmanagement` and `gasproduction` folders to the `gs_Configure` folder.

3. Creating the home directory: The home directory is where logs, monitoring data, and ZooKeeper data will be stored for the Gadgets application. The path to this directory will be the value for `{GASHOME}` throughout this guide.

   Ex. `/u01/software/GS`

   - If you wish to have the Configuration Tool create the home directory, skip this step and continue with step 4.
   - If you wish to create the home directory, note the following:
     - On management and production systems, we recommend using the same path.
     - On single-server installations, only one `{GASHOME}` is necessary.

4. Configure two application servers for the Gadgets application:
   - On dual-server installations, one application server is for the production system, for the Gadgets application production components; the other is for the management system, for the Gadgets application management components.
   - On single-server installations, one application server is for the Gadgets application production components; the other is for the Gadgets application management components.

5. Create a `GSsettings.ini` file, which is required for running the Configuration Tool in silent mode. The `GSsettings.ini` file can be created either manually or from the `GSsettings.ini` of a previous installation. Both methods are provided below.

   Single-Server Installations

   Create one `GSsettings.ini` file.

   To create `GSsettings.ini` manually

   a. Open a blank file named `GSsettings.ini` in a text editor and add the following properties:

1) Add all properties from your mappings worksheet (page 12), in the format `<property>=<value>` (one property per line).

   Ex. `{cs_management_username}=fwadmin`
   `{cs_management_password}=xceladmin`

> **Note**
>
> All '=' characters within a property value must be prefixed with a backslash (`'\'`).
>
> **Ex.** `{ldap_username}=cn\=Directory Manager`
>
> `{ldap_basedn}=dc\=fatwire,dc\=com`

2) Add the `InstallationProductType` property and set it to either `MANAGEMENT` or `PRODUCTION` depending on your system.

b. Save the changes.

To create `GSsettings.ini` from a previous installation

a. Copy the `GSsettings.ini` file located in the Gadgets application Configuration Tool directory of the previous installation.

b. Open the copied `GSsettings.ini` in a text editor and make the following changes, ensuring that all `'='` characters within a property value are prefixed with a backslash (`'\'`), as noted above:

1) Replace the values of the listed properties with the values in your mappings worksheet (page 12).

2) Change the value of `InstallationProductType` to `MANAGEMENT`, `PRODUCTION`, or `SINGLESERVER` depending on your system.

c. Save your changes.

6. Copy the `GSsettings.ini` file to the directory of the Gadgets application Configuration Tool.
7. Set `JAVA_HOME` to the `jdk` folder of the version of Java that will be used. The Java version must be 1.6 or higher.

   Ex. `export JAVA_HOME=/opt/jdk1.6.0_20`
8. If installing on a Unix environment, verify that the `bash` shell and `sed` stream editor are installed and located in the `PATH` environment variable.
9. Run the Configuration Tool in silent mode:

   - Dual-server installations: Run the `configureGS.sh` or `configureGS.bat` script on both the management and production systems, adding the `–Dsilent` option to specify silent mode. For example:

     `configureGS.sh -Dsilent`
   - Single-server installations: Run the `configureGS.sh` or `configureGS.bat` script on the system containing both the management and production environments. For example:

     `configureGS.sh -Dsilent`

10. After the Configuration Tool has completed configuring the Gadgets application, deploy the Gadgets application `WAR` files at `{GASHOME}/install`. Deploy the files first on the production application server, then on the management application server (as required by boot order):
    - Dual-Server installations – On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-boot`, `gas-os`, and `gas-service`.
    - Single-Server installations – On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-os`, and `gas-service`. (Deploy `gas-boot` only on the production application server. `gas-boot` is not used on the management environment.)
11. Once the `WAR` files are deployed, proceed to Chapter 5, "Post-Installation Steps" to secure and verify your installation, register `gas-admin`, and authorize its users.

Chapter 4

Installing the Gadgets Application Manually

- Overview of the Manual Installation Process
- Encrypting Passwords Manually
- Installing the Gadgets Application
- Configuring the Gadgets Application to Use the LDAP Identity Provider

Overview of the Manual Installation Process

The manual process for installing the Gadgets application requires you to:

1. Manually encrypt passwords (shown on this page).
2. Install the Gadgets application by configuring various property files for its components and deploying the components (page 33).
3. Configure the Gadgets application's components to use the LDAP identity provider (page 39), if you have set up an LDAP server.

Encrypting Passwords Manually

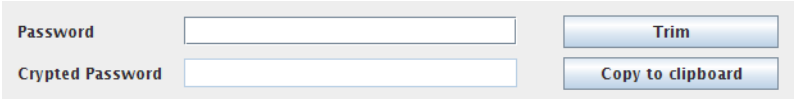
Before installing the Gadgets application, encrypt all passwords as described in "Mappings Worksheet," on page 12 and record them in the worksheet (Table 1, on page 12).

To encrypt passwords

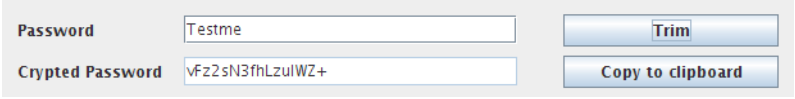
1. Run the following command:

   ```
   java -jar gs-password-encryptor-1.1.jar
   ```

2. Enter your password into the "Password" field and click **Trim**:



   The encrypted password is displayed in the 'Crypted Password' field. For example, `Testme` is entered as the password; the encrypted password is displayed in the "Crypted Password" field.



3. When you have encrypted all passwords that require encryption and filled out the worksheet, you are ready to install the Gadgets application. Continue with "Installing the Gadgets Application," on page 33.

Installing the Gadgets Application

Note

Before continuing, ensure that you have completed the following steps:

- Prepared for the installation process as described in "Prerequisites for Installing the Gadgets Application," on page 10.
- Filled out the worksheet (Table 1, on page 12), using encrypted passwords obtained from the utility described on page 32.
- If you plan to use an LDAP identity provider, you have set up the LDAP server as shown on page 18.

To manually install the Gadgets application

For dual-server installations, complete the following steps on both the management and production systems unless otherwise noted. Notes for single-server installations are provided where necessary:

1. Configure two application servers for the Gadgets application:
   - Dual-server installations: One application server is on the production system for the Gadgets application production components; the other is on the management system for the Gadgets application management components.
   - Single-server installations: One application server is for the Gadgets application production components; the other is for the Gadgets application management components.
2. Create a home directory where the logs, monitoring data, and ZooKeeper data will be stored for the Gadgets application. The path to the home directory will be the value for `{GASHOME}` throughout this guide. On management and production systems, we recommend using the same path. On single-server installations, only one `{GASHOME}` is necessary.

   Ex. `/u01/software/GS`
3. Create a directory under `{GASHOME}` for ZooKeeper data.

   Ex. `/u01/software/GS/data`
4. Create a directory under `{GASHOME}` for monitoring the data of the Gadgets application.

   Ex. `/u01/software/GS/storage`
5. Create a directory under `{GASHOME}` for logs.

   Ex. `/u01/software/GS/logs`
6. Unzip the Gadgets application's components.
7. Configure the files that are listed in Table 2, on page 34 and described on the referenced pages.
8. If you have set up an LDAP server as shown on page 18, configure the Gadgets application's components to use the LDAP identity provider. For instructions, see page 39.

9. Deploy the Gadgets application WAR files first on the production application server, then on the management application server (as required by boot order), as follows:
   - Dual-Server installations – On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-boot`, `gas-os`, and `gas-service`.
   - Single-Server installations – On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-os`, and `gas-service`. (Deploy `gas-boot` only on the production application server. `gas-boot` is not used on the management environment.)
10. You have completed the installation process. Go to Chapter 5, "Post-Installation Steps" to secure and verify your installation, register `gas-admin`, and authorize its users.

Gadgets Application Configuration Files

Table 2 lists the components for the Gadgets application, their configuration files, and the pages on which configurable parameters are described.

Table 2: The Gadgets Application Configuration Files

System	Gadgets Application Components	Configuration File	For Parameters, See ...
Management and Production	All GS components	/WEB-INF/classes/ log4j.properties	page 35
	gas-service	/WEB-INF/classes/ cos_facilities.xml	page 35
		/WEB-INF/classes/ registry_client.properties	page 35
	gas-os	/WEB-INF/classes/ cos_facilities.xml	page 35
		/WEB-INF/classes/ registry_client.properties	page 35
		/WEB-INF/classes/ gsoauthkey.pem	page 37
	gas-boot[a]	/WEB-INF/classes/ Java Key Store (JKS)	page 35
		/WEB-INF/classes/ sslproxy.properties	page 36
		/WEB-INF/classes/ zoo.properties	page 37
		/WEB-INF/classes/ jmemcached.properties	page 38
Production	gas-boot	/WEB-INF/classes/ gas_registry_schema.xml	page 12 (Table 1)
		/WEB-INF/classes/ schema_import.properties	page 39
	user-service	/WEB-INF/classes/ cos_facilities.xml	page 35
		/WEB-INF/classes/ registry_client.properties	page 35
		/WEB-INF/classes/ user_runtime.xml	page 39
	cas (visitor)	same files as user-service	
Management	gas-admin	/WEB-INF/classes/ cos_facilities.xml	page 35
		/WEB-INF/classes/ registry_client.properties	page 35

a. On single-server installations, `gas-boot` is not used on the management environment.

log4j.properties

Configure this file as follows for all components listed in Table 2, on page 34.

Property	Value	Your Value
log4j.appender.logfile.file	{GASHOME}	
log4j.appender.logfile.MaxFileSize	10MB	
log4j.appender.logfile.MaxBackupIndex	5	

cos_facilities.xml

Configure this file as follows for the components specified in Table 2, on page 34:

Bean	Key	Value	Your Value
storage	storageFolder	{GASHOME}	

registry_client.properties

Configure this file as follows for the components specified in Table 2, on page 34

Property	Value	Your Value
zookeeper.server.host	{management_gas_ip} for management components {production_gas_ip} for production components	
zookeeper.server.port	2181 **Note:** Do not change this value.	

Java Key Store (JKS)

Single-Server Installations

Configure only the production gas-boot component. All URLs that point to gas-boot must point to the production gas-boot (the management gas-boot is not used).

Configuring gas-boot instances on management and production starts with the RSA SSL key integration. The Java Key Store file contains the RSA key and must be identical on both the production and management instances of gas-boot. Filename and password information for the Java Key Store are configured in the sslproxy.properties file.

On the management system, `gas-boot` does not store configurations, but only proxies requests (for configurations) coming from management components to the production `gas-boot`. The production `gas-boot` serves the request with actual data from the ZooKeeper. Management components connect to management `gas-boot`, which then connects to production `gas-boot` via an SSL tunnel. The SSL tunnel properties are in the following files: JKS, `sslproxy.properties`, `zoo.properties`, and `jmemcached.properties`.

The Gadgets application ships with the default JKS (`cert.jks`) containing an RSA key. The Gadgets application also ships with a default `sslproxy.properties` file configured with the `cert.jks` file name and password information. The default key may be used, but should be regenerated for security reasons.

Note

When using SSL, the preferred method is to ensure that a valid signed certificate is present and can be accepted by both the management and production servers. Alternatively, you can create your own JKS with RSA key, using the following command:

```
<JAVA_HOME>/bin/keytool -genkey -alias sslproxy -keysize
  2048 -validity 936500 -keyalg RSA -dname "<dname>" -
  keypass <keypass> -storepass <storepass> -keystore
  <jks_filename>
```

The following example uses default values from the `sslproxy.properties` file:

```
keytool -genkey -alias sslproxy -keysize 2048 -validity
  936500 -keyalg RSA -dname "CN=fatwire" -keypass
  fatwire -storepass fatwire -keystore cert.jks
```

sslproxy.properties

Single-Server Installations

Configure `sslproxy.properties` for only the production instance of `gas-boot` (the management instance is not used).

The `sslproxy.properties` file must be reconfigured only if you customized the Java Key Store (page 35). The `sslproxy.properties` file must be identical on the management and production instances of `gas-boot` and its parameters must specify the same values that were used to generate the Java Key Store file (page 35).

- If you generated the Java Key Store file, enter the parameter values that you used to generate the file.
- If you used the default Java Key Store (`cert.jks`), do not modify the default `sslproxy.xml` file.

The `sslproxy.xml` file contains the following parameters:

- `ssl.cert=<Java_Key_Store_filename>`
- `ssl.keypass=<keypass>`

- `ssl.storepass=<storepass>`
- `ssl.dname=<distinguished_name>`

By default they are set as follows (to match the parameters that were used to generate the default `cert.jks` file):

- `ssl.cert=cert.jks`
- `ssl.keypass=fatwire`
- `ssl.storepass=fatwire`
- `ssl.dname=CN=fatwire`

gsoauthkey.pem

This is an SSL private key file. The `gas-os` component uses this key as a default for OAuth gadgets lacking their own consumer credentials. The `gas-os` component ships with a default private key file. For security reasons we recommend generating a custom key for each `gas-os` instance (management and production). Generating a custom private key for `gas-os` requires the OpenSSL tool to be installed. Many Linux distributions come with pre-compiled OpenSSL packages. Windows binaries can be found at `http://www.openssl.org/related/binaries.html`.

To generate a custom SSL private key for OAuth:

1. Create a `gskey.pem` file by executing the following command:

   ```
   openssl req -newkey rsa:1024 -days 365 -nodes -x509 -keyout
      gskey.pem -out gskey.pem -subj /CN=GadgetServerKey
   ```

2. Convert the previously generated certificate from the `gskey.pem` file to PKCS#8 format in the `gsoauthkey.pem` file.

   ```
   openssl pkcs8 -in gskey.pem -out gsoauthkey.pem -topk8 -nocrypt
      -outform PEM
   ```

3. Copy the newly generated `gsoauthkey.pem` file into the `gas-os/WEB-INF/classes` directory. Overwrite the previous directory, if it exists.

zoo.properties

Single-Server Installations

Configure `zoo.properties` for only the production instance of `gas-boot` (the management instance is not used).

Configure this file as follows for the `gas-boot` management and production components, specified in Table 2, on page 34:

- `dataDir`: Replace `{GASHOME}` with the value for your system.
- `tempClientPort`: Either specify the port that is temporarily used to start the ZooKeeper component, or keep the default value.
- `clientPort`: Either specify the port on which the ZooKeeper component starts, or keep the default value.

- `sslClientPort`: Either specify the port used by the ZooKeeper SSL connections, or keep the default value.

  Note

  For dual-server installations, the value of `sslClientPort` must be the same on both the management and production systems. This port must also be opened on any firewall between management and production. The default value `4181` is appropriate for most installations.

- `sslHost`: Specify the production server host.

jmemcached.properties

Single-Server Installations

Configure `jmemcached.properties` for only the production instance of `gas-boot` (the management instance is not used).

Configure this file as follows for the `gas-boot` management and production components, specified in Table 2, on page 34:

- `jmemcached.port`: Either specify the port on which the Java memory cache manager starts, or keep the default value.
- `jmemcached.sslport`: Either specify the port that is used by the Java memory cache manager SSL connections, or keep the default value.

  Note

  For dual-server installations, the value of `jmemcached.sslport` must be the same on both the management and production systems. This port must also be opened on any firewall between management and production. The default value `22322` is appropriate for most installations.

- `jmemcached.sslHost:` Specify the production server host.

schema_import.properties

Configure this file as follows for the `gas-boot` production component, specified in Table 2, on page 34:

Property	Description	Value	Your Value
`importOnStart`	Controls whether the `gas_registry_schema.xml` file is re-imported into `ZooKeeper` on server startup.	`true`, to pick up changes to the schema file	
`cleanIfExists`	Controls whether a value is cleaned from the existing schema in `ZooKeeper` before the new schema is imported.	`true`, to pick up changes to the schema file	

user_runtime.xml

This file must be identical for both the `cas` and `user-service` components. Set `{cs_site}` in the `siteName` bean to the value that you specified in the worksheet on page 12. If you are setting up an LDAP identity provider, you must also complete the next section, "Configuring the Gadgets Application to Use the LDAP Identity Provider."

Configuring the Gadgets Application to Use the LDAP Identity Provider

Note

Complete the steps in this section if you have set up a supported LDAP server as shown in "Installing the Gadgets Application with a New or Existing LDAP Server," on page 18.

To enable the LDAP identity provider

1. In the visitor `cas` and `user-service` components, modify the `user_runtime.xml` file as follows:

   `WEB-INF/classes/user_runtime.xml`

Bean	Property	LDAP
`wemIdentityProvider`	`enabled`	`false`
	`defaultProvider`	`false`
`ldapIdentityProvider`	`enabled`	`true`
	`defaultProvider`	`true`

2. Back up `deployerConfigContext.xml` in `cas/WEB-INF` and rename `deployerConfigContext_onlyLDAP.xml` to `deployerConfigContext.xml` to allow CAS to pick up changes.
3. In the **new** `cas/WEB-INF/deployerConfigContext.xml` file, set the following LDAP properties:

   `cas/WEB-INF/classes/deployerConfigContext.xml`

Bean	Key	Value
`LdapPrincipalProvider`	`searchBase`	`{ldap_basedn}` `Ex.dc=fatwire,dc=com`
`LdapAuthenticationHandler`	`searchBase`	`{ldap_basedn}` `Ex.dc=fatwire,dc=com`
`LdapContextSource`	`urls`	`{gas_production_ldap_ip}` `{gas_production_ldap_port}`
	`userDn`	`{ldap_username}` `Ex. cn=Directory Manager`
	`password`	`{ldap_user_password}` **Note**: Enter the unencrypted password.
`LdapPersonAttributeDao`	`baseDN`	`{ldap_basedn}` `Ex.dc=fatwire,dc=com`

4. Once you have enabled the LDAP identity provider, deploy the Gadgets application `WAR` files first on the production application server, then on the management application server (as required by boot order):
   - Dual-Server installations – On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-boot`, `gas-os`, and `gas-service`.
   - Single-Server installations – On the production application server, deploy `gas-boot`, `gas-os`, `gas-service`, `user-service`, and visitor `cas`. On the management application server, deploy `gas-admin`, `gas-os`, and `gas-service`. (Deploy `gas-boot` only on the production application server. `gas-boot` is not used on the management environment.)
5. You have completed the installation process. Go to Chapter 5, "Post-Installation Steps" to secure and verify your installation, register `gas-admin`, and authorize its users.

Chapter 5

Post-Installation Steps

- Overview
- If the Community Application is Installed
- Configuring Security
- Enabling Shindig Features
- Verifying the Gadgets Application Installation
- Enabling the Gadgets Application

Overview

Having installed the Gadgets application, you are ready to secure your installation and verify your installation by testing the URLs of the Gadgets application's components. You will then register the `gas-admin` component with the WebCenter Sites management system, authorize yourself, and authorize others to use `gas-admin`.

If the Community Application is Installed

Verify that Zookeeper and JMemcached in `cos-boot` and `gas-boot` are using different ports.

Configuring Security

Recommended security measures are the following:

- Securing Ports
- Creating Certificates, JKS, and Private Keys
- Specifying OAuth Consumer Credentials

Securing Ports

- The following ports should be accessible only from the local machine, to decrease the possibility of leaking information:
  - ZooKeeper port (`2181`, by default). This port is configured in the `clientPort` property of the `gas-boot/WEB-INF/classes/zoo.properties` file.
  - JMemcached port (`11211`, by default). This port is configured in the `jmemcached.port` property of the `gas-boot/WEB-INF/classes/jmemcached.properties` file.
- Open the following SSL `gas-boot` ports on the delivery host:
  - ZooKeeper SSL port (`4181`, by default). This port is configured in the `sslClientPort` property of the `gas-boot/WEB-INF/classes/zoo.properties` file.
  - JMemcached SSL port (`22322`, by default). This port is configured in the `jmemcached.sslport` property of the `gas-boot/WEB-INF/classes/jmemcached.properties` file.

Creating Certificates, JKS, and Private Keys

- Create a custom JKS (Java Key Storage) with custom RSA key in the `gas-boot` component. For instructions, see "Java Key Store (JKS)," on page 35.

Note

The file (`cert.jks`, by default) must be identical for both `gas-boot` instances.

- Create a custom Private Key, `gsoauthkey.pem` for the `gas-os` component. For instructions, see "gsoauthkey.pem," on page 37.

Note

We recommend creating two `gsoauthkey.pem` files, one for each of the `gas-os` components.

Specifying OAuth Consumer Credentials

Consumer credentials are the consumer key and consumer secret (for definitions and other information, see the *Oracle WebCenter Sites User's Guide for the Gadgets Application*). Specify the following sets of consumer credentials in the `gas-boot/WEB-INF/classes/gas_registry_schema.xml` file:

Bean	Key	Default Value	Your Value
`gasProductionOSOAuthSecret_private`	`consumer.key`	`gadgetPrivateConsumer`	
	`consumer.secret`	`gadgetPrivateSecret`	
`gasProductionOSOAuthSecret_public`	`consumer.key`	`gadgetPublicConsumer`	
	`consumer.secret`	`gadgetPublicSecret`	

Enabling Shindig Features

Gadgets that are either developed for *iGoogle* or use *iGoogle* features may require you to enable extra Shindig features for the Gadgets application in order for those gadgets to render properly. If you enable these Shindig features, the Gadgets application downloads the third-party libraries necessary for rendering the gadgets that require them from the Shindig website. **For the Gadgets application to download the necessary third-party libraries, you must have access to the internet.**

If you wish to enable additional Shindig features for the Gadgets application, you must uncomment the following lines in the `gas-os/WEB-INF/classes/gas_features.txt` file in both `gas_os` components (management and production):

```
# features/analytics/feature.xml
# features/com.google.gadgets.analytics/feature.xml
# features-extras/org.jquery.core-1.4.2/feature.xml
```

Note

Once the additional Shindig features are enabled, restart both the management and production application servers for the changes to take effect.

Verifying the Gadgets Application Installation

You will verify your installation by testing the URLs of the Gadgets application's components.

Note

URLs in this section are used only to verify that the Gadgets application is correctly installed; they must not be used to invoke the Gadgets application for content management operations. The Gadgets application must be accessed from WebCenter Sites.

1. Start the WebCenter Sites' application server before starting the application servers for the Gadgets application. **The production application servers must be fully started before the management application servers are started.**
2. Verify the following components:
   a. Verify the visitor `cas` component:

      `http://{production_gas_ip}:{production_gas_port}/cas/login`

      Ex. `http://gas.production.fatwire.com:8580/cas/login`

      A successful connection displays the CAS login form. Sign in as `{gasvisitor_username}`/`{gasvisitor_password}`. If the user name and password are valid, the "Log In Successful" message is displayed.

   b. Verify the `user-service` component:

      A successful connection displays the "`Welcome to User Service`" message:

      `http://{production_gas_ip}:{production_gas_port}/user-service`

      Ex. `http://gas.production.fatwire.com:8580/user-service`

   c. Verify the `gas-service` components:

      A successful connection displays the "`Welcome to GS Service`" message.

      - To verify the management `gas-service`, open the following URL:

        `http://{management_gas_ip}:{management_gas_port}/gas-service`

        Ex. `http://gas.management.fatwire.com:8580/gas-service`

      - To verify the production `gas-service`, open the following URL:

        `http://{production_gas_ip}:{production_gas_port}/gas-service`

        Ex. `http://gas.production.fatwire.com:8580/gas-service`

   d. Verify the `gas-os` components:

      A successful connection displays the "Welcome to GS OpenSocial Container" message.

      - To verify the management `gas-os`, open the following URL:

        `http://{management_gas_ip}:{management_gas_port}/gas-os`

Ex. `http://gas.management.fatwire.com:8580/gas-os`

- To verify the production `gas-os`, open the following URL:

  `http://{production_gas_ip}:{production_gas_port}/gas-os`

  Ex. `http://gas.production.fatwire.com:8580/gas-os`

e. Verify the `gas-admin` component:

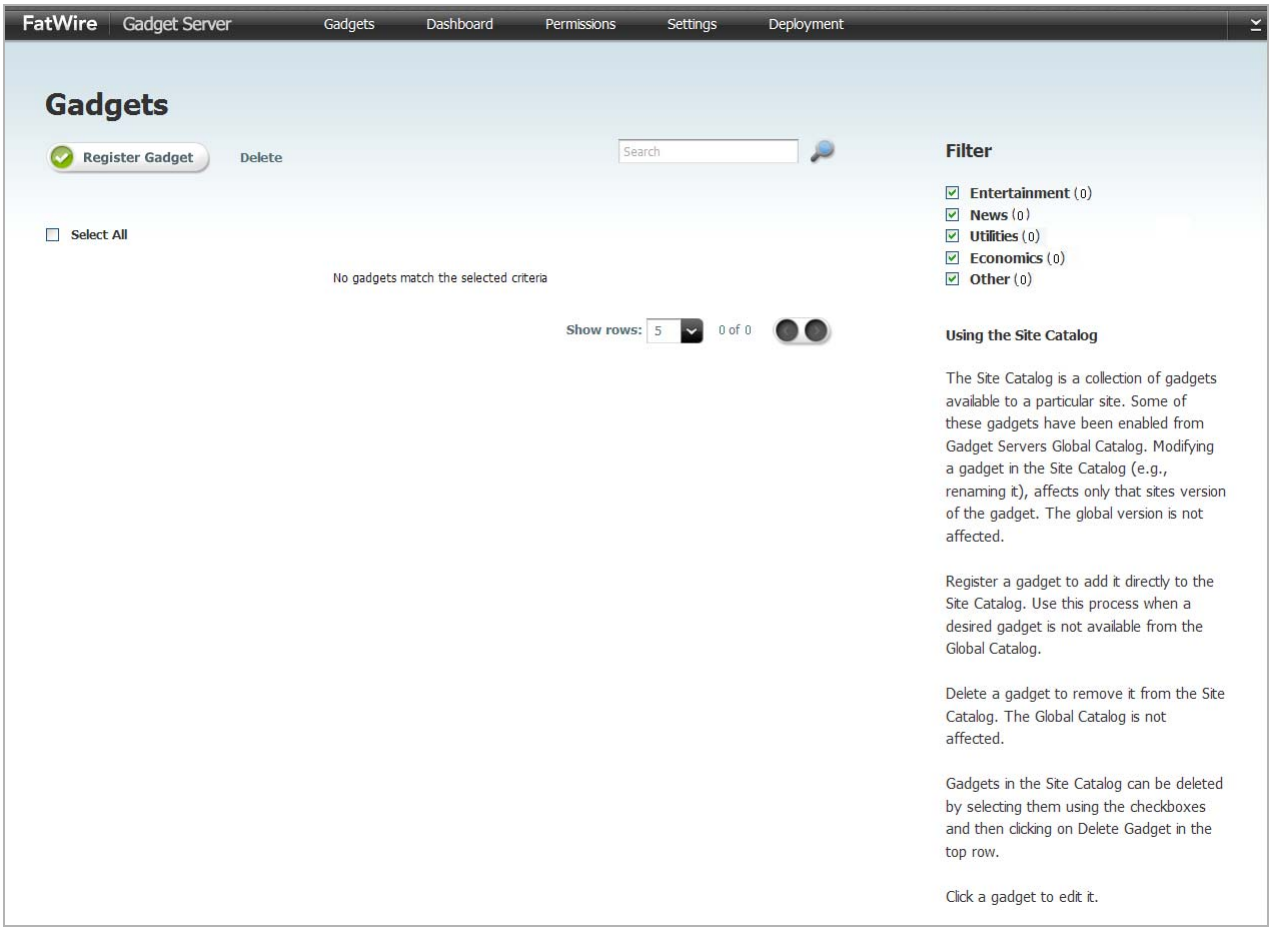
1) Log in to the Gadgets interface as a general administrator:

```
http://{management_gas_ip}:{management_gas_port}/gas-
   admin/start.jsp?siteid=<site_name>
```

Ex. `http://gas.management.fatwire.com:8580/gas-admin/start.jsp?siteid=FirstSiteII`

2) In the CAS login form, sign in as a general administrator (`fwadmin`/`xceladmin` by default).

3) Open the Gadgets application. Its user interface is displayed:



3. When all tests have been successfully completed, continue to the next section to register the Gadgets application with WebCenter Sites.

Enabling the Gadgets Application

- Registering the Gadgets Application
- Authorizing Users to Work with the Gadgets Application's Interfaces

Registering the Gadgets Application

In this section, you will register the management Gadgets application in order for it to be recognized by WebCenter Sites. Registration displays the Gadgets application icon on the WebCenter Sites login page and applications bar; lists the application on the **Apps** page of the WEM Admin interface, and enables the WEM Framework to render the application's interface.

To register the Gadgets application

1. On the management system, log in to WebCenter Sites as a general administrator (the default credentials are `fwadmin/xceladmin`):
   a. Use the following URL:

      `http://<server>:<port>/<context>/login`

      where `<server>` is the host name or IP address of the server running WebCenter Sites, and `<context>` is the name of the web application that was deployed on `<server>`. Depending on how the system was set up, you may also need to include the port number.
   b. Access **AdminSite**.
2. Open the WebCenter Sites Admin interface and register the Gadgets application:
   a. On the **Admin** tab, select **Site** > **AdminSite**.
   b. Create an asset of type `FW_View` with the following values:
      - **Name**: `GaSView` (or a name of your own choice)
      - **Parent Node**: `frame1`
      - **View Type**: `Iframe`
      - **Source Url**: `http://{management_gas_ip}:{management_gas_port}/gas-admin/WemContext.gas`
   c. Create an asset of type `FW_Application` with the following values:
      - **Name**: `GS` (or a name of your own choice)
      - **Icon URL**: `wemresources/images/icons/apps/GadgetServer.png` ()
      - **Active Icon URL**: `wemresources/images/icons/apps/GadgetServerActive.png`
      - **Layout type**: `Layout Renderer`
      - **Layout URL**: `wemresources/layout/admin.html`
   d. Add the new asset of type `FW_View` as an associated view by selecting it from the **History** tab (located on the tree in the left-hand panel) and clicking **Add Selected Items**. Click **Save Changes**.

3. Verify that the Gadgets application is listed in the WEM Admin interface:
   a. Open the WEM Admin interface (on AdminSite).
   b. Click **Apps** in the menu bar, and check that the Gadgets application is listed on the **Apps** page. Keep this page open.
4. Continue to the next section to authorize access to the Gadgets application's interfaces.

Authorizing Users to Work with the Gadgets Application's Interfaces

Detailed information about user authorization is available in the *Oracle WebCenter Sites User's Guide for the Gadgets Application*. For a quick start, follow the steps below:

To authorize users to work with Gadgets application's interfaces

1. Assign the Gadgets application to `{cs_site}`:
   a. Starting with the "Apps" page of the WEM Admin interface (in the menu bar, click **Apps**), mouse over the Gadgets application's name and select **Manage App**.
   b. In the "Manage App" screen, click **Assign to Sites**.
   c. Select `{cs_site}` to run the Global Gadget Catalog interface.
   d. Select the GeneralAdmin role for the Gadgets application.
2. Assign the Gadgets application to a site other than `{cs_site}` to run the Gadgets User interface.

   Note

   To assign the Gadgets application to sites other than `{cs_site}`, you must first create or select the sites on the management system, then mirror the sites to the production system.

   a. In the menu bar, click **Apps**.
   b. Mouse over the Gadgets application name and select **Manage App**.
   c. In the "Manage App" screen, click **Assign to Sites**.
   d. Select the desired site, other than `{cs_site}`, on which you wish to run the Gadgets User interface.
   e. Select the following roles for the Gadgets application: GeneralAdmin, SiteAdmin, and Designer.
3. Authorize users to access the Gadgets application's interfaces. In this step you will assign users to `{cs_site}` or the site(s) running the Gadgets User interface, and assign to each user at least one of the roles that was assigned to `gas-admin`. (Sharing at least one role to an application and a user on the same site grants the user access to the application on that site):
   a. In the menu bar, select **Sites**.
   b. Mouse over the site to which the Gadgets application is assigned and select **Manage Site Users**.

c. In the "Manage Site Users" screen, complete one or both of the following steps, as necessary:

- To assign roles to an existing site user, mouse over the user's name and select **Assign Roles to User**.
- To assign a user to the site and assign roles to the user, click **Assign Users** > *select the name of the user you wish to assign to the site* > **Continue**.

d. In the "Assign Roles to User" screen, select at least one of the following roles: **GeneralAdmin**, **SiteAdmin**, **Designer**, (see Table 3 for permissions associated with each role).

Table 3: Gadgets application's permissions and roles

Permissions	Gadgets Application Roles		
	GeneralAdmin	SiteAdmin	Designer
Enable the Gadgets application's Global Gadget Catalog Interface	✓		
Enable the Gadgets application's User Interface	✓	✓	
Register Gadgets to Global Gadget Catalog	✓		
Register Gadgets to a Site Gadget Catalog	✓	✓	
Remove Gadgets from the Global Gadget Catalog	✓		
Remove Gadgets from a Site Gadget Catalog	✓	✓	
Enable Gadgets for a Site Gadget Catalog	✓		
Modify Gadget Metadata	✓	✓	
Add Default Gadgets to the Dashboard	✓	✓	✓
Modify the Dashboard's Default Layout	✓	✓	✓
Modify the Dashboard's Default Color Theme	✓	✓	✓
Authorize a Domain	✓	✓	✓
Configure Appearance Settings for Gadgets	✓	✓	✓
Deploy the Dashboard "Tag"	✓	✓	✓
Deploy an Individual Gadget's "Tag"	✓	✓	✓

Table 3: Gadgets application's permissions and roles

Permissions	Gadgets Application Roles		
	GeneralAdmin	SiteAdmin	Designer
Modify the Deployed Dashboard's Defaults	✓	✓	✓

4. Click **Save and Close**.

> **Note**
>
> Verify that the site administrator is a member of the `REST` security group `SiteAdmin_AdminSite`. For instructions on adding a user to a group, see the *Oracle WebCenter Sites Administrator's Guide for the WEM Framework*.

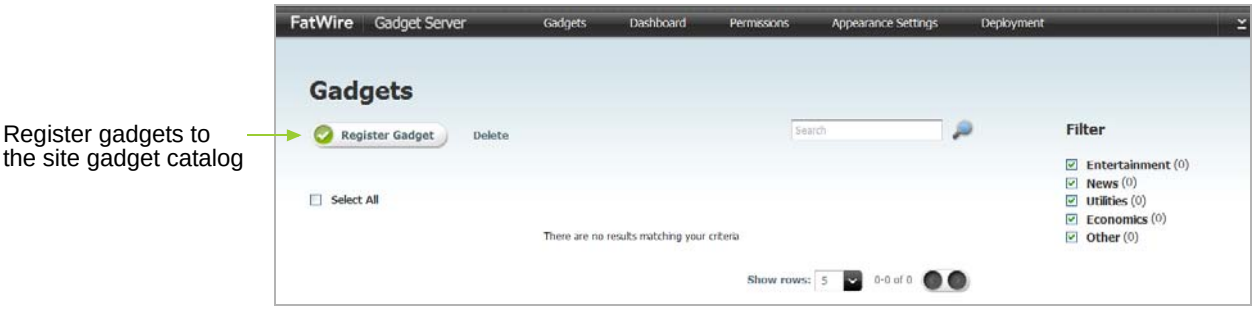
5. Verify the user's access to the Gadgets application:
   a. Log in to WebCenter Sites as one of the new Gadgets application's users.
   b. If the user is a general administrator, access the global gadget catalog by selecting `{cs_site}` and the Gadgets application icon:

   - If the user is not a general administrator, select the site running the Gadgets User interface and click the Gadgets application icon:

6. Your interface is one of the following:

- If you selected `{cs_site}`, the Global Gadget Catalog interface is displayed:

- If you selected a site other than `{cs_site}` to which `gas-admin` is assigned, the Gadgets User interface is displayed:



Next Steps

- If you wish to install sample gadgets, continue to Chapter 6, "Adding Sample Gadgets."
- For information and instructions about using the Gadgets application, see the *Oracle WebCenter Sites User's Guide for the Gadgets Application*.

Chapter 6

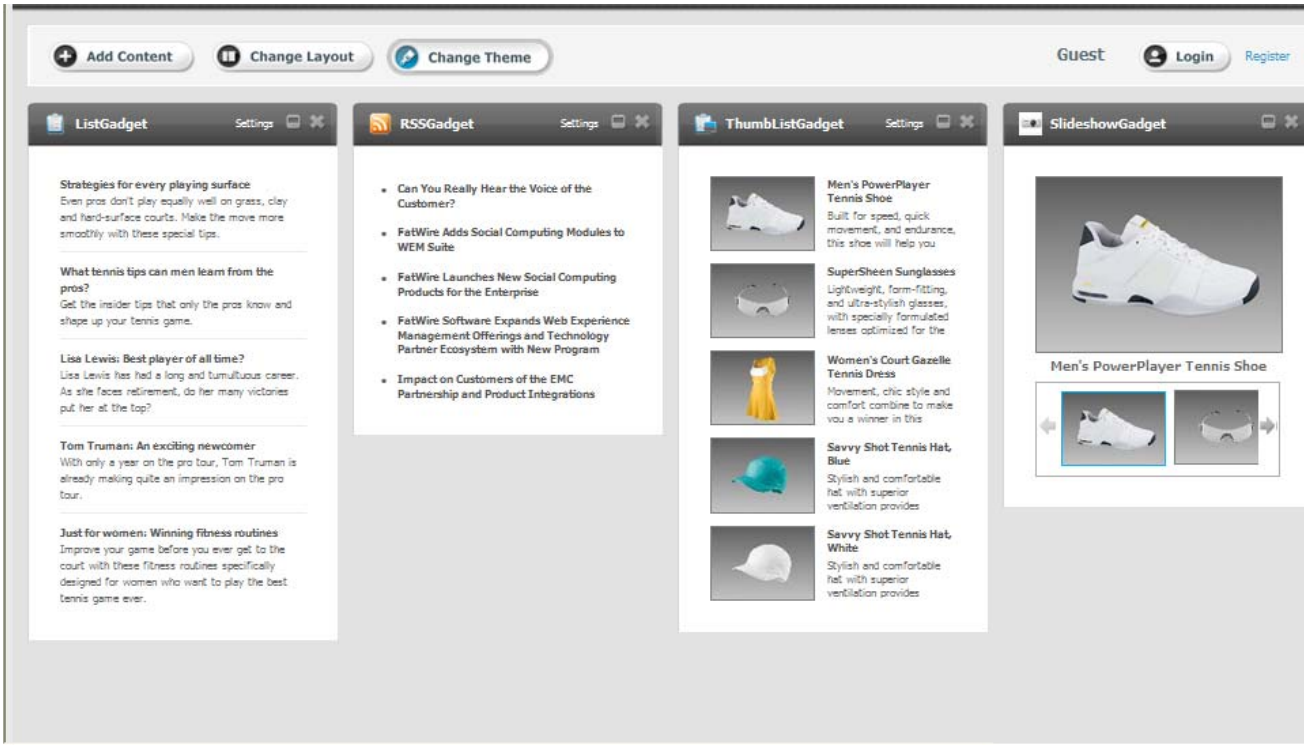
Adding Sample Gadgets

- Prerequisites for Installing Sample Gadgets
- Installing the Sample Gadgets

Prerequisites for Installing Sample Gadgets

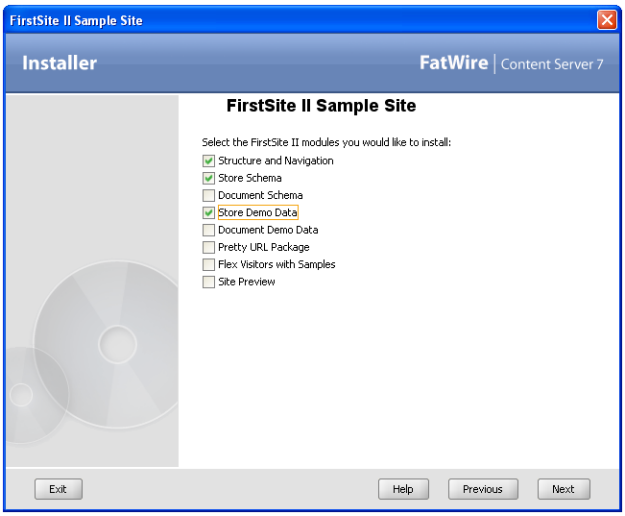
WebCenter Sites ships with the following sample gadgets:

ListGadget, RSSGadget, ThumbListGadget, and SlideshowGadget.



The sample gadgets must be installed on the FirstSite II sample site. The site must be enabled to store demo data. If your management WebCenter Sites system does not have FirstSite II, do the following:

Prepare a WebCenter Sites system running FirstSite II with **Store Demo Data** enabled (as shown in the figure below).



After installing the sample gadgets on your newly prepared WebCenter Sites system (see "Installing the Sample Gadgets"), you will publish FirstSite II to the WebCenter Sites management system.

Installing the Sample Gadgets

Installing sample gadgets installs the following components:

- `FW_CSGadget` asset type (used to create gadgets)
- Sample gadgets (assets of type `FW_CSGadget`)
- Templates for rendering the gadgets
- Assets that provide content for the sample gadgets. The assets are instances of FirstSite II asset types.

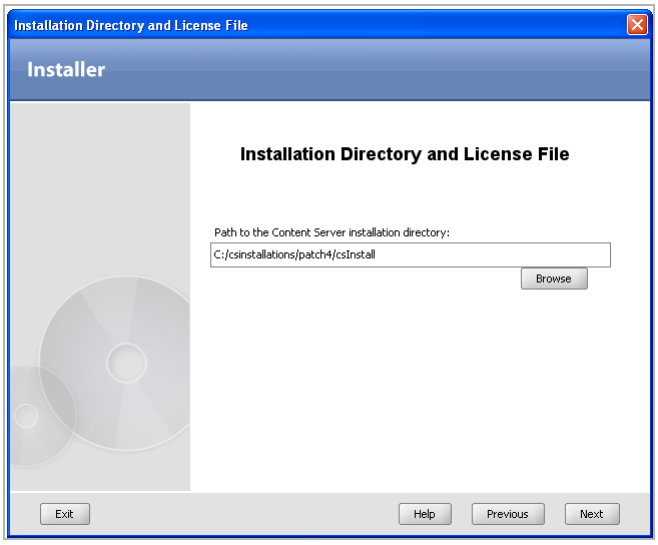
To install sample gadgets

1. Ensure that prerequisites on page 52 are satisfied.
2. Extract the installation file named `GadgetServer_v1.1.zip` to the host machine. Extracting this zip file creates a subdirectory named `GS_Samples`.

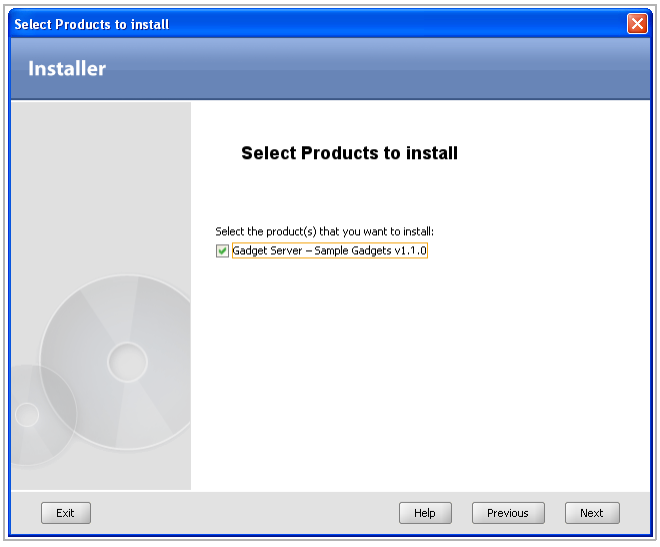
> **Note**
>
> Do not change the name of this subdirectory or any of its subdirectories, and be sure to retain the archived directory structure. Otherwise, the installer will fail.

3. Run the Gadgets application Integration Installer script:
   - Windows: `gsInstall.bat`
   - Unix: `gsInstall.sh`
4. In the "Welcome" screen, click **Next**.

5. In the “Installation Directory and License File” screen, enter the path to your WebCenter Sites installation directory.



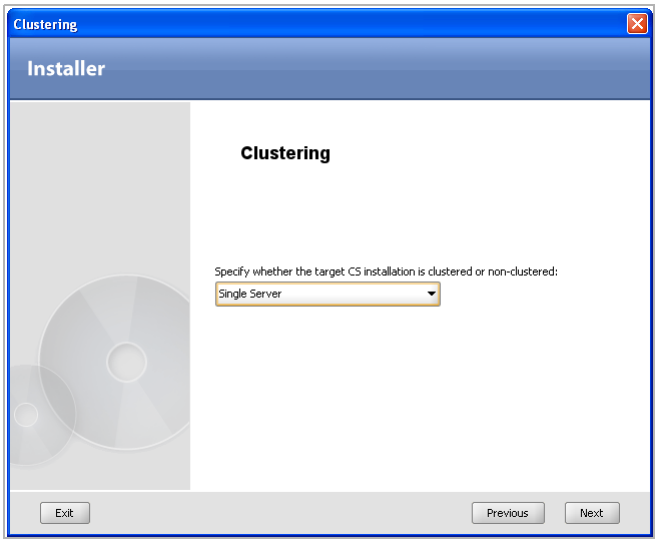
6. Select **Sample Gadgets**.



The following components will be installed:

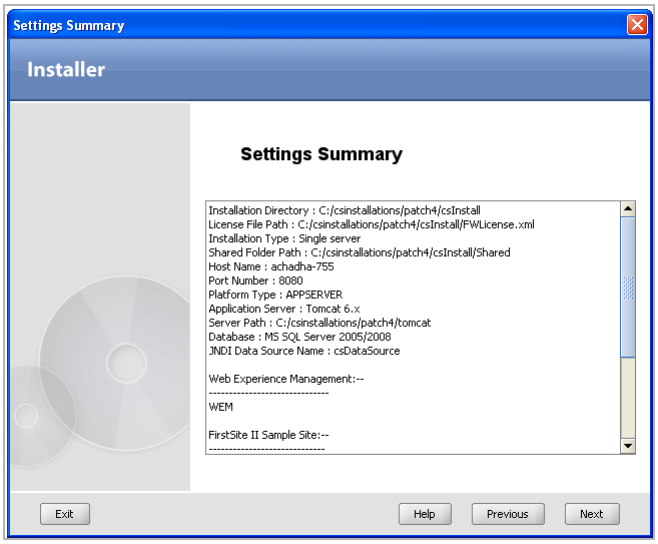
- `FW_CSGadget` asset type (used to create gadgets)
- Sample gadgets (assets of type `FW_CSGadget`)
- Templates for rendering the gadgets
- Assets that provide content for the sample gadgets. The assets are instances of FirstSite II asset types.

7. In the “Clustering” screen, indicate whether you are installing the sample gadgets on a single server or a secondary cluster member. Click **Next**.

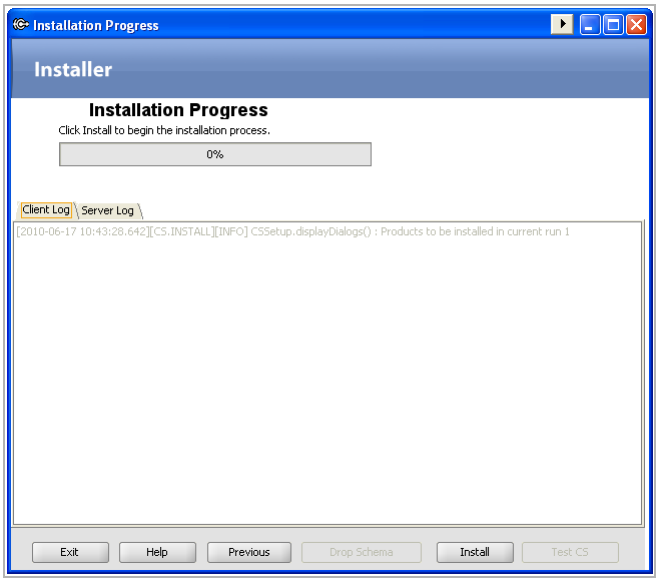


8. In the “Enter Gadgets Information” screen, select either **http** or **https**, and then enter the host name and port number of your Gadgets application installation.

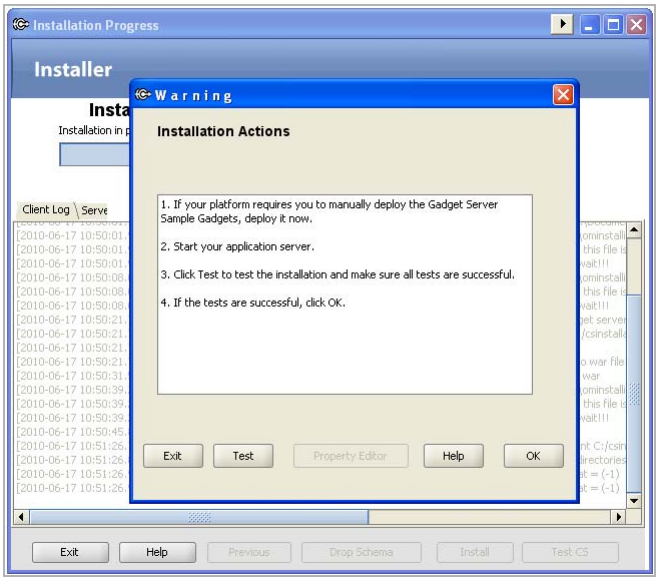
9. Click **Next**.



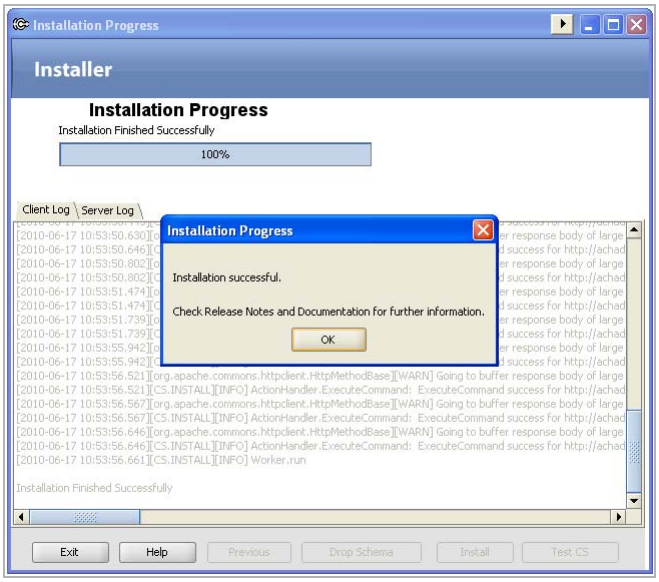
10. Click **Install** to begin the installation.



11. When the “Installation Actions” dialog box opens, start your WebCenter Sites installation, and click **Test** to test your WebCenter Sites installation. Click **OK**.



12. When the installation is complete, click **OK**.



13. Register the sample gadgets in either the Gadgets application’s global gadget catalog or site gadget catalog. For instructions, see “Registering Gadgets” in the *Oracle WebCenter Sites User’s Guide for the Gadgets Application.*

Note

Gadget registration requires you to enter the gadgets’ descriptor URLs. To obtain the URLs, follow the instructions below.

To obtain the sample gadgets' descriptor URLs:

a. Log in to the WebCenter Sites Advanced interface with the credentials of a general administrator (for example, `fwadmin/xceladmin`).

b. Select the FirstSite II sample site.

c. In the button bar, click **Search**.

The list of asset types is displayed. Make sure that the **CS-Based Gadget** asset type is included in this list:

Search

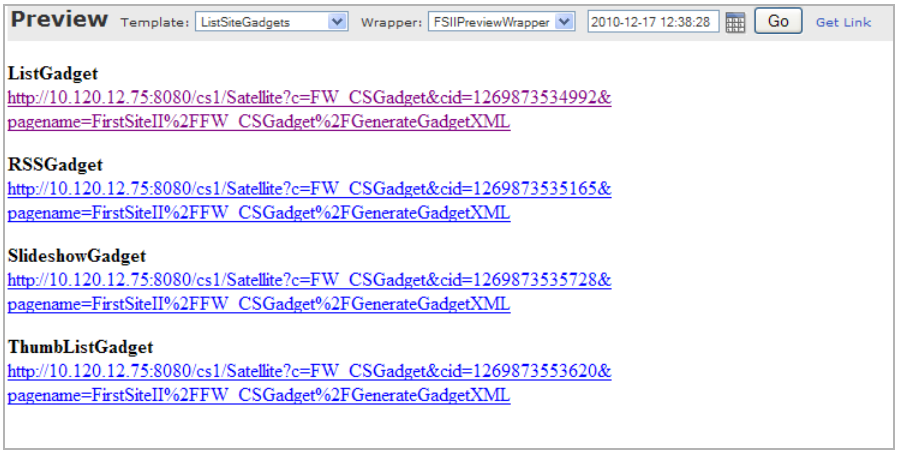
Type	Name	
Attribute Editor	Find Attribute Editor	(Advanced search)
Content Attribute	Find Content Attribute	(Advanced search)
Content Definition	Find Content Definition	(Advanced search)
Content Filter	Find Content Filter	(Advanced search)
Content Parent Definition	Find Content Parent Definition	(Advanced search)
Content Parent	Find Content Parent	(Advanced search)
Content	Find Content	(Advanced search)
CS-Based Gadget	Find CS-Based Gadget	(Advanced search)
CSElement	Find CSElement	(Advanced search)
Document Attribute	Find Document Attribute	(Advanced search)
Document Definition	Find Document Definition	(Advanced search)
Document Filter	Find Document Filter	(Advanced search)
Document Parent Definition	Find Document Parent Definition	(Advanced search)
Document Parent	Find Document Parent	(Advanced search)
Document	Find Document	(Advanced search)
Media Attribute	Find Media Attribute	(Advanced search)
Media Definition	Find Media Definition	(Advanced search)
Media Filter	Find Media Filter	(Advanced search)
Media Parent Definition	Find Media Parent Definition	(Advanced search)
Media Parent	Find Media Parent	(Advanced search)
Media	Find Media	(Advanced search)
Page	Find Page	(Advanced search)
SiteEntry	Find SiteEntry	(Advanced search)
StyleSheet	Find StyleSheet	(Advanced search)
Template	Find Template	(Advanced search)
Visitor Attribute	Find Visitor Attribute	(Advanced search)

1) In the list of asset types, click **Find CS-Based Gadget**.

2) In the "Search for FW_CSGadget" screen, click **Search**.

3) Preview any of the sample gadget assets.

4) In the "Template" field, select **ListSiteGadgets** to display the list of gadget descriptor URLs:



Preview Template: ListSiteGadgets Wrapper: FSIIPreviewWrapper 2010-12-17 12:38:28 Go Get Link

ListGadget
http://10.120.12.75:8080/cs1/Satellite?c=FW_CSGadget&cid=1269873534992&pagename=FirstSiteII%2FFW_CSGadget%2FGenerateGadgetXML

RSSGadget
http://10.120.12.75:8080/cs1/Satellite?c=FW_CSGadget&cid=1269873535165&pagename=FirstSiteII%2FFW_CSGadget%2FGenerateGadgetXML

SlideshowGadget
http://10.120.12.75:8080/cs1/Satellite?c=FW_CSGadget&cid=1269873535728&pagename=FirstSiteII%2FFW_CSGadget%2FGenerateGadgetXML

ThumbListGadget
http://10.120.12.75:8080/cs1/Satellite?c=FW_CSGadget&cid=1269873553620&pagename=FirstSiteII%2FFW_CSGadget%2FGenerateGadgetXML

Once you successfully register the sample gadgets, they are displayed as thumbnails on either the global gadget catalog or a site gadget catalog, depending on how you registered the gadgets. For example:

For more information about sample gadgets and creating custom gadgets, see the *Oracle WebCenter Sites Developer's Guide for Creating Gadgets.*