SAS Publishing

SAS Web Infrastructure Kit 1.0
AdministratorÕs Guide

The Power to Know.

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2004. *SAS® Web Infrastructure Kit 1.0: Administrator's Guide*. Cary, NC: SAS Institute Inc.

SAS Web Infrastructure Kit 1.0: Administrator's Guide

SAS Institute Inc., SAS Campus Drive, Cary, North Carolina 27513.

April 2004

SAS Publishing provides a complete selection of books and electronic products to help customers use SAS software to its fullest potential. For more information about our e-books, e-learning products, CDs, and hard-copy books, visit the SAS Publishing Web site at **support.sas.com/pubs** or call 1-800-727-3228.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

SAS® Web Infrastructure Kit 1.0: Administrator's Guide

This SAS Web Infrastructure Kit Administrator's Guide provides instructions for carrying out the administrative tasks that are required in order to fully implement the portal Web application for your organization.

Note: In this guide, "portal Web application" is a generic term that refers to either of the following:

- the SAS Portal Web Application Shell, which is a portal−like Web application shell that is included in the SAS Web Infrastructure Kit and is used by other SAS Web applications, or
- the SAS Information Delivery Portal, which (when installed with the SAS Web Infrastructure Kit) fully implements the capabilities of the SAS Portal Web Application Shell.

The guide includes the following chapters:

- Installation and Migration provides additional setup information for authentication and initial metadata, an installation checklist to help you verify that you have correctly installed the portal Web application and other required software, guidance for deploying the portal Web application and its components, and information about how to reconfigure your initial portal Web application installation.
- Portal Environment provides a description of the portal environment, including the portal Web application and the associated administrative and development tools.
- Administration Tools provides a description of the administration tools used by the portal administrator, including metadata administration and deployment tools.
- Security provides guidelines for setting up portal security, including user registration, assigning users to groups, and setting up authorization (access control) for portal Web application content.
- Deployment provides instructions for deploying the SAS Foundation Services, SAS servers, and custom−developed portlets that are needed to support your portal Web application implementation.
- Content provides instructions for adding content to the portal Web application so that it will be available to portal users. Content types might include Web applications, files, SAS Information Maps, links, packages, portlets, syndication channels, SAS Stored Processes, SAS publication channels, and SAS Reports.

For information about how to use the Web Infrastructure Kit to develop your own custom applications, or to customize and extend the features of the SAS Information Delivery Portal, see the *Web Infrastructure Kit Developer's Guide*.

For information about using the portal Web application, see the online Help that is provided in the application's user interface.

Installation

The procedures in this guide assume that you have successfully installed the portal Web application shell. Detailed installation instructions are provided with the SAS Web Infrastructure Kit and SAS Information Delivery Portal software. There are two methods by which you might have performed your installation:

- **Project Install:** A project install is performed using SAS project directories and a planning worksheet. The planning worksheet is used as input to the SAS Software Navigator and the SAS Configuration Wizard. For this type of install, you should follow the customized instructions that are generated based on your plan. The customized instructions will direct you to specific steps in this guide as needed. For more information about project installs, refer to the SAS Intelligence Architecture: Planning and Administration Guide.
- **Basic Install:** A basic install is performed without the use of planning worksheets and SAS project directories. For this type of install, you should follow all of the pre−installation, installation, and post−installation steps that are provided in the `wik_readme.html`.

The following sections in this chapter provide further details to help you customize, complete, and verify your installation:

- **User Authentication Setup**. When you installed the portal Web application, you had the opportunity to choose whether user authentication would be performed by the SAS Metadata Server's or the Web server's authentication provider.

  If you chose the SAS Metadata Server's authentication provider, then you set up an authentication provider: host, LDAP, or Microsoft Active Directory Server. If you did not choose to set up the host authentication provider, that is, if you chose to set up an alternative authentication provider (LDAP or Microsoft Active Directory Server) for the SAS Metadata Server, then the `wik_readme.html` instructed you to follow the setup steps in one of the following sections:

  - Setting up LDAP Server Authentication
  - Setting up Microsoft Active Directory Server Authentication

  If you chose the Web server's authentication provider, then the `wik_readme.html` instructed you to follow the setup steps in the following section:

  - Setting up Web Server (Trusted Realm) Authentication

  The default installation uses the host authentication provider for the SAS Metadata Server and follows the instructions in Setting up Host Authentication.
- **Initial Security and Initial Metadata**. When you installed the portal Web application, you set up initial users and groups for security. You can also choose to run the `*.sas` files to load initial metadata for the portal Web application. For details, see Default Security Installation and Loading Initial Metadata.
- **Installation Verification**. To verify and ensure correct installation, refer to Verifying Your Portal Installation and use the checklist to verify that all of the steps in the installation process have been successfully completed. The checklist includes important technical details that are critical to the operation of the portal Web application.
- **Log Output**. To debug problems with the portal Web application, you can monitor the portal Web application log file. To modify the priority level of messages or the location of the log file, see Modifying the Logging Output Information and Location .
- **Server Startup**. After you verify your installation is set up correctly, ensure that you start your servers in the appropriate order. For details, see Starting the Servers.
- **Installation Reconfiguration**. To reconfigure specific features of your portal Web application, you can re−run the Web Infrastructure Kit installation and change your initial parameters.

Note: It is recommended that the base path for the Xythos WFS WebDAV server be a blank value.

You can use the Web Infrastructure Kit installation program to reconfigure the following parameters:

- **Authentication Type**. You can reconfigure the portal Web application to use a different type of authentication, either SAS Metadata Server or Web server authentication.
- **User Names and Passwords**. You can reconfigure the SAS user and password information.
- **Installation Directories**. You can reconfigure where configuration files are stored.
- **Xythos WFS WebDAV server location or base path**. You can reconfigure the Xythos WFS WebDAV server configuration information.
- **Locales**. You can reconfigure which locale is supported by the portal Web application.

After you re−run the install program, you must re−run the configure_wik.bat utility and re−deploy the WAR files.

- **Distributed Environment**. The Web applications that are included in the SAS Web Infrastructure Kit are designed to operate in a tiered environment using various servers, each of which can run on a separate machine. To help you get the applications up and running, the steps in this procedure will result in an initial installation in which all of the required servers and applications are running on the same machine.

  After the SAS Web Infrastructure Kit is successfully installed on a single machine, you can move the applications and servers in order to implement a distributed environment. For additional information, see Redistributing Applications and Servers.

You can now begin to understand and administer the portal Web application. For a summary of administration tasks, see Administering the Portal Web Application.

If you are not using the Web server's authentication provider for user authentication, when users access the portal Web application, you can display a Public Kiosk for users to access before they log in to the portal Web application. For details, see Administering the Public Kiosk.

Installation

Setting Up Host Authentication

To understand authentication for the SAS Metadata Server and other IOM servers, see the topics "Initial Authentication on a Metadata Server" and "Additional Authentication" in the SAS Intelligence Architecture: Planning and Administration Guide. To understand the portal Web application environment when using host authentication, see Understanding the SAS Metadata Server (Host Authentication). To enable the portal's SAS Metadata Server to authenticate your users against the host authentication provider and authorize the users with the SAS Metadata Server's Authorization Facility, you must set up the appropriate security on your host authentication provider and SAS Metadata Server as follows:

- If you have used the project install to install the portal Web application, you already have the SAS Metadata Server set up and initial users and groups defined. In addition, you must follow Step 4 in this section, For Distributed Server Access, Add Additional Credentials.
- If you have used the basic install to install the portal Web application:

    1. Add the initial users to the host operating system.
    2. Set up and start the SAS Metadata Server.
    3. Add the initial users and required groups to the SAS Metadata Server.
    4. For Server Access, Add Additional Credentials.

Step 1: Add the Initial Users to the Host Operating System

To set up the host authentication provider, you must add the following individual and shared accounts to the host operating system:

- *SAS (Required for Unix and z/OS only):* Add an individual account for the SAS user and a shared account for the SAS group. For example, specify the user ID `sas` and the password `Admin123`, and specify the shared ID `sas` (or `sasgrp` on z/Os) and the password `Admin123`.
- *SAS Administrator (Required):* Add an individual account for the SAS Administrator user. For example, specify the user ID `sasadm` and the password `Admin123`. (Note: You did not enter information for this user during the install program.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS Trusted User (Required):* Add an individual account for the SAS Trusted user. For example, specify the user ID `sastrust` and the password `Trust123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS Web Administrator (Required):* Add an individual account for the SAS Web Administrator user. For example, specify the user ID `saswbadm` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program) For the following Windows systems, give this account the specified user rights:

    - On Windows NT and 2000: Act as part of the Operating System.
    - On all Windows versions: Log on as a batch job.
- *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in

the install program.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.

Step 2: Set up the SAS Metadata Server

To set up your SAS Metadata Server, see the setup instructions in the SAS 9.1 Metadata Server: Setup Guide. The following list provides specific additions (for each step) for the portal Web application's SAS Metadata Server setup.

1. Create directories for the metadata server, repository manager, and repositories as described in the *SAS 9.1 Metadata Server: Setup Guide*.
2. Set directory and file access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Give the SAS user permissions for this directory.
3. Set system access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*.
4. Set server configuration options in an omaconfig.xml file as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Ensure that the omaconfig.xml file contains the security setting `<OMA AUTHCHCK="INHERIT"/>`. For example:

   ```
   <OMAconfig>
     <OMA AUTHCHCK="INHERIT"/>
   </OMAconfig>
   ```
5. Configure special users in adminUsers.txt and trustedUsers.txt files as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note 1: In the adminUsers.txt file, add an entry for the SAS Administrator. For Windows systems, this entry must be fully qualified with the Windows domain or machine name. In addition, to grant unrestricted access to this user (so that the user can locate users to load metadata), place an asterisk in the first character position of the fully qualified user ID.

   Note 2: In the trustedUsers.txt file, add an entry for the SAS Trusted User. For Windows systems, this entry must be fully qualified with the Windows domain or machine name.
6. Start the Metadata Server as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: When creating the script for starting the SAS Metadata Server:

   - specify the same SAS Metadata Server port number that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - specify the correct path for sas.exe.

Step 3: Add Initial Users and Groups to the SAS Metadata Server

To set up security on the SAS Metadata Server, add the initial users and groups to the SAS Metadata Server. To add new users, follow these steps:

1. **Set up the SAS Management Console profile**. Start SAS Management Console, and create a new profile and metadata repository. Use the following values when answering prompts:

   - **Machine Name**: Assign the same machine that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_HOST$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - **Port**: Assign the same port that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - **Add Repository**: If you are creating a new repository, it must be a foundation repository. Assign the same repository name that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_REPOSITORY$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
2. **Add or Modify Users on the SAS Metadata Repository**. For host authentication, each user must have access to login credentials for all the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

   A user with administrative permissions can manually create user definitions in the metadata repository. Log in to SAS Management Console as the SAS Administrator and create the user definitions with the User Manager plug−in. If you have already created a user definition for one of these users as part of another install, do not create it again; instead, modify the login definitions as specified. For details about defining SAS users, see Defining a User in the *SAS Management Console: User's Guide*.

   The User Manager requires you to enter the following fields when you define or modify a new user and login definition:

   Name
   Specifies the name of the user.
   User ID
   The fully−qualified user ID for the login credentials of the user.
   Password
   Specifies the password for the user ID.
   Authentication Domain
   The logical grouping that associates logins and resources.
   For example:

   - **Name:** `SAS Administrator`
   - **User ID**: `SAS Administrator`
   - **Password**: `Admin123`
   - **Authentication Domain**: **`DefaultAuth`**

   Add new user definitions for the following users and associated user IDs:

- **SAS Administrator**: Add a new user and login definition for the SAS Administrator. You did not enter information for this user during the install program. From the User Manager, fill in the user and login definitions field as follows:
  a. General tab.
  Name: `SAS Administrator`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  · **User ID**: `Raleigh\sasadm`
  · **Password**: `Admin123`
  · **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- **SAS Trusted User**: Add a new user and login definition for the SAS Trusted User using the information you provided in the install program. You must use the exact user ID, password, and name entered in the install program and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Trusted User`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  · **User ID**: `RALEIGH\sastrust`
  · **Password**: ,`Admin123`
  · **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- **SAS Web Administrator**: Add a new user and login definition for the SAS Web Administrator (portal administrator) user using the information you provided in the install program. You must use the exact user ID, password, and name entered in the install program and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Web Administrator`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  · **User ID**: `RALEIGH\saswbadm`
  · **Password**: `Admin123`
  · **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- **SAS Guest**. Add a new user and login definition for the SAS Guest user using the information you provided in the install program. You must use the exact user ID, password, and name entered in the install program and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Guest`

b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `RALEIGH\sasguest`
- **Password**: `Guest123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Demo User**: Add a new user and login definition for the SAS Demo User using the information you provided in the install program. For example, for the user definition:

a. General tab.
Name: `SAS Demo User`

b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `RALEIGH\sasdemo`
- **Password**: `Demo123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **Add the initial portal Web application groups to the repository and add the necessary users to those groups.** If you have already created a group definition for one of these groups as part of another install, do ***not*** create it again. However, you will need to make sure that all the specified users have been added to the group.

  - **SAS General Servers**: Add a new group definition for the SAS General Servers group, specifying the name `SAS General Servers`. Add a group login definition that specifies the login credentials for the SAS General Servers account that you defined on the host authentication provider. You must use the exact user ID and password entered in the install program and in Step 1. For example, for the group definition:

  a. General tab.
  Name: `SAS General Servers`

  b. Logins tab. For the initial login definition, fill in the fields as follows:

  - **User ID**: `RALEIGH\sassrv`
  - **Password**: `Admin123`
  - **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

  Add the SAS Trusted User as a group member of the SAS General Servers group.

◊ **Portal Admins**: Add a new group definition for portal Web application administrators specifying the name `Portal Admins`. Add the SAS Web Administrator user as a group member.
◊ **Portal Demos**:. Add a new group definition for Portal Demos specifying the name `Portal Demos`. Add the SAS Demo User as a group member.

For details about defining users and groups, see the SAS Management Console User Manager Help, and refer to Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

The administrator only needs to create the user definitions for the user in the metadata repository. The first time the user logs in to the portal, the portal Web application automatically creates a profile definition in the metadata repository.

Step 4: For Server Access, Add Additional Credentials

If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account).

Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, the account must have the following user right:

- "Log on as a batch job" user right

If the server uses a different authentication process than the SAS Metadata Server, you must set up an additional user or group (shared) login definition (credentials) for the user on the SAS Metadata Server. For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains.

To set up valid server credentials, for each server, do one of the following:

- **If the server runs on the same operating system and requires the same credentials as the SAS Metadata Server**, ensure that the following users can authenticate against the authentication provider for the server's machine:

  ♦ *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`.
  ♦ *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program) For the following Windows systems, give this account the specified user rights:

    ◊ On Windows NT and 2000: Act as part of the Operating System.
    ◊ On all Windows versions: Log on as a batch job.
  ♦ *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and

password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.

- *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.

If your server is defined in the default authentication domain, the SAS Metadata Server uses credential caching to retrieve the appropriate credentials for the server; you do not need to specify an additional login on the SAS Metadata Server.

Note: If your server is defined in an additional authentication domain but runs in the same operating system (and uses the same credentials) as the SAS Metadata Server, use SAS Management Console to re−configure your server definition to specify the default authentication domain (DefaultAuth) for the authentication domain.

- **If the server runs on a different operating system than the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

  - **individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**.

    1. Ensure that the following users can authenticate against the authentication provider for the server:
       - *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`. On Windows, give this user the "Log on as a batch job" user right.
       - *SAS General Servers (Required):* Add an individual account for the SAS General Servers group credentials, for example specifying the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program)

         For the following Windows systems, give this account the specified user rights:

         - On Windows NT and 2000: Act as part of the Operating System.
         - On all Windows versions: Log on as a batch job.
       - *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.
       - *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.
    2. Set up an additional login definition for the SAS General Servers group, SAS Guest, and SAS Demo User on the SAS Metadata Server.

       Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

· For example, for the SAS General Servers group, define an additional login definition and fill in the fields as follows::
  - **User ID**: `RALEIGH\sassrv`
  - **Password**: `Admin123`
  - **Authentication Domain**: **`ServerAuth`**

  Note:

  - If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the IOM_DOMAIN property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory)).
  - If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must re−configure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

· For example, for the SAS Guest user, define an additional login definition and fill in the fields as follows::
  - **User ID**: `RALEIGH\sasguest`
  - **Password**: `Guest123`
  - **Authentication Domain**: **`ServerAuth`**

  Note:

  - If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the IOM_DOMAIN property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory)).
  - If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must re−configure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

· For example, for the SAS Demo User, define an additional login definition and fill in the fields as follows::
  - **User ID**: `RALEIGH\sasdemo`
  - **Password**: `Demo123`
  - **Authentication Domain**: **`ServerAuth`**

  Note:

  - If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of

the IOM_DOMAIN property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory)).

- If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must re−configure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

- **set up a shared account on the authentication provider and associated group (shared) login for a SAS group definition (that contains the SAS user) on the SAS Metadata Server**. For all servers, determine existing or set up a new set up a shared account on the server's authentication provider.

  Use SAS Management Console to set up or add to a SAS group that contains:

  - the shared account as a group (shared) login of the SAS group.

    Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.
  - the user as a member of the SAS group. The user will then use the group (shared) login credentials to access the servers.

  For details about defining SAS groups, see Defining a Group in the *SAS Management Console: User's Guide*.

To add additional users for host authentication, see Adding Users.*Installation*

Setting Up LDAP Authentication

To understand authentication, see "Initial Authentication on a Metadata Server" and "Additional Authentication" in the SAS Intelligence Architecture: Planning and Administration Guide. To understand the portal Web application environment when using LDAP authentication, see Understanding the SAS Metadata Server (LDAP Authentication). To enable the portal Web application's SAS Metadata Server to authenticate your users against an LDAP server and authorize the users with the SAS Metadata Server's Authorization Facility, you must set up security as follows:

- If you have used the project install to install the portal Web application, you already have the SAS Metadata Server set up and the appropriate users and groups defined. To enable authentication with LDAP:

    1. Set up the LDAP server.
    2. Add the required users to the LDAP server.
    3. Add the required users to the host system.
    4. Set up the SAS Metadata Server startup script to enable LDAP authentication.
    5. Add or modify users and groups on the SAS Metadata Server.
    6. For server access, add additional credentials.
    7. Ensure that all users specify the appropriate LDAP authentication provider domain when they log in to the portal Web application.
- If you have used the basic install to install the portal Web application:

    1. Set up the LDAP server.
    2. Add the required users to the LDAP server.
    3. Add the required users to the host system.
    4. If not already configured, set up the SAS Metadata Server.
    5. Set up the SAS Metadata Server Startup Script to Enable LDAP Authentication.
    6. Add or modify users and groups on the SAS Metadata Server.
    7. For server access, add additional credentials.
    8. Ensure that all users specify the appropriate LDAP authentication provider domain when they log in to the portal Web application.

Step 1: Set Up the LDAP Server

To authenticate users against an LDAP server, you must set up an LDAP directory server. For details, see Setting Up an LDAP Directory Server in the *SAS Integration Technologies Administrator's Guide (LDAP)*.

Step 2: Add the Required Users to the LDAP Server

To enable LDAP authentication, you must add the initial portal Web application users to the LDAP server. Each directory entry in the `ou=People` organizational unit should look like the following. The bold items are those that are different for each user.

```
dn: cn=username, distinguished name for person context
cn: username
description: user description
mail: user email address
objectclass: inetorgperson
objectclass: person
```

```
sn: short name of the user
uid: user's portal login ID
userpassword: login password
```

Create a person entry for the following users:

- *SAS Administrator (Required):* Add a person entry for the SAS Administrator user, for example specifying the user ID `sasadm` and the password `Admin123`. (Note: You did not enter information for this user during the install program.)
- *SAS Trusted User (Required):* Add a person entry for the SAS Trusted User, for example specifying the user ID `sastrust` and the password `Trust123`. (Note: You must use the exact user ID and password entered in the install program.)
- *SAS Web Administrator (Required):* Add a person entry for the SAS Web Administrator user, for example specifying the user ID `saswbadm` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program.)
- *SAS Guest (Required):* Add a person entry for the SAS Guest user, for example specifying the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program.)
- *SAS Demo User (Optional):* Add a person entry for the SAS Demo User, for example specifying the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program.)

Manually creating an entry in the directory for each portal Web application user can be time consuming. Creating and importing an LDIF file simplifies the process and also provides a backup file of portal Web application users.

For further details about setting up person entries on an LDAP directory server, see Adding Person Entries to the Directory in the *SAS Integration Technologies Administrator's Guide (LDAP)*

Step 3: Add the Required Users to the Host System

Add the following user and shared accounts to the host operating system:

- *SAS (Required for Unix and z/OS only):* Add an individual account for the SAS user and a shared account for the SAS group. For example, specify the user ID `sas` and the password `Admin123`, and specify the shared ID `sas` (or `sasgrp` on z/Os) and the password `Admin123`.
- *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program.) For the following Windows systems, give this account the following user rights:
    - ♦ On Windows NT and 2000: Act as part of the Operating System
    - ♦ On all Windows versions: Log on as a batch job

Step 4: If Not Already Configured, Set Up the SAS Metadata Server

To set up your SAS Metadata Server, see the setup instructions in the SAS 9.1 Metadata Server: Setup Guide. The following list provides specific additions (for each step) for the portal Web application SAS Metadata Server setup.

1. Create directories for the metadata server, repository manager, and repositories as described in the *SAS 9.1 Metadata Server: Setup Guide*.
2. Set directory and file access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Give the SAS user permissions for this directory.
3. Set system access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*.
4. Set server configuration options in an omaconfig.xml file as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Ensure that the omaconfig.xml file contains the security setting `<OMA AUTHCHCK="INHERIT"/>`. For example,

   ```
   <OMAconfig>
     <OMA AUTHCHCK="INHERIT"/>
   </OMAconfig>
   ```
5. Configure special users in `adminUsers.txt` and `trustedUsers.txt` files as described in the *SAS 9.1 Metadata Server: Setup Guide* .

   Note 1: In the adminUsers.txt file, add an entry for the SAS Administrator. For Windows systems, this entry must be fully qualified with the Windows domain or machine name. In addition, in order to grant unrestricted access to this user (so that the user can locate users to load metadata), place an asterisk in the first character position of the fully qualified user ID.

   Note 2: In the trustedUsers.txt file, add an entry for the SAS Trusted User. For Windows systems, this entry must be fully qualified with the Windows domain or machine name.

Step 5: Set Up the SAS Metadata Server Startup Script to Enable LDAP Authentication

To enable the SAS Metadata Server to authenticate users against an LDAP server, you must configure the SAS Metadata Server startup command to enable LDAP authentication.

To create a startup command for the SAS Metadata Server, see Start the Metadata Server in the *SAS 9.1 Metadata Server: Setup Guide* .

Note: When creating the script for starting the SAS Metadata Server:

- specify the same SAS Metadata Server port number that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- specify the correct path for `sas.exe`.

To enable the SAS Metadata Server to authenticate against LDAP:

1. **Set environment variables for LDAP**. You can set the environment variables as system level environment variables or as part of your server startup script as follows:

```
LDAP_PORT=  <port number for LDAP>LDAP_BASE=  <base DN to use.
           For example: o=my company,c=US>
LDAP_HOST=  <host name of the machine running LDAP>
LDAP_PRIV_DN=  <privileged DN that is
              allowed to search for users.
              For example, cn=useradmin>
LDAP_PRIV_PW=  <password for LDAP_PRIV_DN>
LDAP_IDATTR=   <person entry LDAP attribute
              that stores the user ID >
```

2. **specify an authentication provider domain option for LDAP authentication**. Specify the authentication provider domain option in the startup command for the SAS Metadata Server as follows:

   ```
   -authpd "ldap:LDAPAuthProv"
   ```

   When you configure user credentials on the SAS Metadata Server, you must specify the same domain (e.g., `LDAPAuthProv`) that you specify in the SAS Metadata Server startup script.

The following SAS Metadata Server startup file shows the additional options in bold type:

```
@echo on
title OMS-5555
set omsport=5555

set LDAP_HOST=cia2.na.abc.com
set LDAP_PORT=3456
set LDAP_BASE=o=portal.test
set LDAP_IDATTR=uid
set LDAP_PRIVDN=cn=root
set LDAP_PRIVPW=mypassword

"C:\Program Files\SAS\SAS System\9.1\sas.exe" -memsize 0 -nologo
-nosplash -noterminal -objectserver  -objectserverparms
"protocol=bridge port=%omsport% instantiate
classfactory=2887E7D7-4780-11D4-879F-00C04F38F0DB" -log
"C:\Portal2.0.1Files\Open Metadata Server\OMR5555.log"
-authpd "ldap:LDAPAuthProv"
```

Step 6: Add or Modify Users and Groups on the SAS Metadata Server

You must add the initial users and initial groups to the SAS Metadata Server. To add new users:

1. **Set up the SAS Management Console profile**. Start SAS Management Console, and create a new profile and metadata repository. Use the following values when answering prompts:

   - Assign the same machine that you specified when you ran the install program. If you do not remember what value you specified, check the value of the `$SERVICES_OMI_HOST$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - Assign the same port that you specified when you ran the install program. If you do not remember what value you specified, check the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - If you are creating a new repository, it must be a foundation repository.

- Assign the same repository name that you specified when you ran the install program. If you do not remember what value you specified, check the value of the `$SERVICES_OMI_REPOSITORY$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

2. **Add users to the SAS Metadata Repository**. For LDAP server authentication, each user must have access to login credentials for all the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

   A user with administrative permissions can manually create user definitions in the metadata repository. Log in to SAS Management Console as the SAS Administrator and create the user definitions with the User Manager plug−in. If you have already created a user definition for one of these users as part of another install, do not create it again; instead, modify the login definitions as specified. For details about defining SAS users, see Defining a User in the *SAS Management Console: User's Guide*.

   The User Manager requires you to enter the following fields when you define a new user and login definition:

   Name
   specifies the name of the user.
   User ID
   specifies the fully qualified user ID for the login credentials of the user. If you are authenticating against LDAP, you must specify the user ID in the format `userID@AUTHPROVIDERDOMAIN`.
   Password
   specifies the password for the user ID.
   Authentication Domain
   specifies the logical grouping that associates logins and resources together.
   For example:

   - **Name:** `SAS Administrator`
   - **User ID**: `sasadm@LDAPAuthProv`
   - **Password**: `Admin123`
   - **Authentication Domain**: **`DefaultAuth`**

   Add new user definitions for the following users and associated user IDs:

   - **SAS Administrator**: Add a new or modify an existing user definition for the SAS Administrator. You did not enter information for this user during the install program. For example, for the user definition:
     a. General tab.
     Name: `SAS Administrator`
     b. Logins tab. For the initial login definition, fill in the fields as follows:

     · **User ID**: `sasadm@LDAPAuthProv`
     · **Password**: `Admin123`
     · **Authentication Domain**: **DefaultAuth**

     Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - **SAS Trusted User**: Add a new or modify an existing user definition for the SAS Trusted User using

the information you provided in the install program. You must use the exact user ID and password entered in the install program and in Step 2. For example, for the user definition:

a. General tab.
Name: `SAS Trusted User`
b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `sastrust@LDAPAuthProv`
- **Password**: `Admin123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Web Administrator**: Add a new or modify an existing user definition for the SAS Web Administrator using the information you provided in the install program. You must use the exact user ID, password, and name entered in the install program and in Step 2. For example, for the user definition:

a. General tab.
Name: `SAS Web Administrator`
b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `saswbadm@LDAPAuthProv`
- **Password**: `Admin123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Guest**: Add a new or modify an existing user definition for the SAS Guest using the information you provided in the install program. You must use the exact user ID and password entered in the install program and in Step 2. For example, for the user definition:

a. General tab.
Name: `SAS Guest`
b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `sasguest@LDAPAuthProv`
- **Password**: `Admin123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Demo User**: Add a new user definition for the SAS Demo User using the information you provided in the install program. For example, for the user definition:

a. General tab.
Name: `SAS Demo User`
b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `sasdemo@LDAPAuthProv`
- **Password**: `Demo123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `ortalConfigure` subdirectory of the setup directory).

3. **Add the required and demo portal Web application groups to the repository and add the necessary users to those groups.** If you have already created a group definition for one of these groups as part of another install, do ***not*** create it again. However, you will need to make sure that all the specified users have been added to the group.

   - **SAS General Servers**: Add a new group definition for the SAS General Servers group, specifying the name `SAS General Servers`. Add a group login definition that specifies the login credentials for the SAS General Servers account that you defined on the host authentication provider. For example, for the group definition:

     a. General tab.
     Name: `SAS General Servers`
     b. Logins tab. For the initial login definition, fill in the fields as follows:

     - **User ID**: `sassrv`
     - **Password**: `Admin123`
     - **Authentication Domain**: **`DefaultAuth`**

     Note: Specify the default authentication domain that you specified when you ran the install program. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

     Add the SAS Trusted User to the SAS General Servers group.
   - **Portal Admins**: Add a new group definition for portal Web application administrators specifying the name `Portal Admins`. Add the SAS Web Administrator user as a group member.
   - **Portal Demos**: Add a new group definition for Portal Demos specifying the name `Portal Demos`. Add the SAS Demo User as a group member.

The administrator only needs to create the user definitions for the user in the metadata repository. The first time the user logs in to the portal Web application, the portal Web application automatically creates a profile definition in the metadata repository.

Step 7: For Server Access, Add Additional Credentials

If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account).

Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, the account must have the following

user right:

- "Log on as a batch job" user right

If the server uses a different authentication process than the SAS Metadata Server, you must set up an additional user or group (shared) login definition (credentials) for the user on the SAS Metadata Server. For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains. To set up valid server credentials, for each server, do one of the following:

- **If the server uses the same authentication process as the SAS Metadata Server**, ensure that the following users can authenticate against the authentication provider for the server's machine:
  - *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`. On Windows, give this user the "Log on as a batch job" user right.
  - *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program.)

    For the following Windows systems, give this account the specified user rights:

    - On Windows NT and 2000: Act as part of the Operating System.
    - On all Windows versions: Log on as a batch job.
  - *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.
  - *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.

  If your server is defined in the default authentication domain, the SAS Metadata Server uses credential caching to retrieve the appropriate credentials for the server; you do not need to specify an additional login on the SAS Metadata Server.

  Note: If your server is defined in an additional authentication domain but runs on the same operating system (and uses the same credentials) as the SAS Metadata Server, use SAS Management Console to reconfigure your server definition to specify the default authentication domain (DefaultAuth) for the authentication domain.
- **If the server uses a different authentication process than the SAS Metadata Server**, set up credentials for the servers in one of the following ways:
  - **Set up an individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server as follows**:

    1. Ensure that the following users can authenticate against the authentication provider for the server:
       - *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`.
       - *SAS General Servers (Required):* Add an individual account for the SAS General Servers group credentials, for example specifying the user ID `sassrv` and the

password `Admin123`. (Note: You must use the exact user ID and password entered in the install program.)

For the following Windows systems, give this account the specified user rights:

- On Windows NT and 2000: Act as part of the Operating System.
- On all Windows versions: Log on as a batch job.

· *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.

· *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program.) On Windows, give this user the "Log on as a batch job" user right.

2. Set up an additional login definition for the SAS General Servers group, SAS Guest, and SAS Demo User on the SAS Metadata Server.

Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

· For example, for the SAS General Servers group, define an additional login definition and fill in the fields as follows::

- **User ID**: `RALEIGH\sassrv`
- **Password**: `Admin123`
- **Authentication Domain**: **`ServerAuth`**

Note:

♦ If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the `$IOM_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

♦ If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

· For example, for the SAS Guest user, define an additional login definition and fill in the fields as follows::

- **User ID**: `RALEIGH\sasguest`
- **Password**: `Guest123`
- **Authentication Domain**: **`ServerAuth`**

Note:

- If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the IOM_DOMAIN property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory)).
- If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

· For example, for the SAS Demo User, define an additional login definition and fill in the fields as follows::

- **User ID**: `RALEIGH\sasdemo`
- **Password**: `Demo123`
- **Authentication Domain**: **`ServerAuth`**

Note:

- If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the IOM_DOMAIN property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory)).
- If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

- **set up a shared account on the authentication provider and associated group (shared) login for a SAS group definition (that contains the SAS user) on the SAS Metadata Server**. For all servers. determine existing or set up a new set up a shared account on the server's authentication provider.

  Use SAS Management Console to set up or add to a SAS group that contains:

  ◊ the shared account as a group (shared) login of the SAS group.

  Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

  ◊ the user as a member of the SAS group. The user will then use the group (shared) login credentials to access the servers.

  For details about defining SAS groups, see Defining a Group in the *SAS Management Console: User's Guide*.

Step 8: Ensure That All Users Specify the Appropriate LDAP Authentication Provider Domain when They Log In to the Portal Web Application

When a user logs in to the portal Web application, they must specify the LDAP domain that was configured in the SAS Metadata Server startup command and in the user definitions on the SAS Metadata Server. For example:

```
user ID: saswbadm@LDAPAuthProv
password:  Admin123
```

Test your initial portal Web application authentication and authorization setup by logging in to the portal Web application.

To add additional users for LDAP authentication, see Adding Users (LDAP Authentication).

Installation

Setting Up Microsoft Active Directory Authentication

To understand the portal Web application environment when using Microsoft Active Directory authentication, see Understanding the SAS Metadata Server (Microsoft Active Directory Authentication. To enable the portal Web application's SAS Metadata Server to authenticate your users against an Microsoft Active Directory server and authorize the users with the SAS Metadata Server's Authorization Facility, you must set up security as follows:

- If you have used the project install to install the portal Web application, you already have the SAS Metadata Server set up and the appropriate users and groups defined. To enable authentication with Microsoft Active Directory:

    1. Set up the Microsoft Active Directory server.
    2. Add the required users to the Microsoft Active Directory server.
    3. Add required users to the host system.
    4. Set up the SAS Metadata Server startup script to enable Microsoft Active Directory Authentication.
    5. Add or modify users and groups on the SAS Metadata Server.
    6. For server access, add additional credentials.
    7. Ensure that all users specify the appropriate domain when they log in to the portal Web application.
- If you have used the basic install to install the portal Web application:

    1. Set up the Microsoft Active Directory server.
    2. Add the required users to the Microsoft Active Directory server.
    3. Add required users to the host system.
    4. If not already configured, set up the SAS Metadata Server.
    5. Set up the SAS Metadata Server startup script to Enable Microsoft Active Directory authentication.
    6. Add or modify users and groups on the SAS Metadata Server.
    7. For server access, add additional credentials.
    8. Ensure that all users specify the appropriate domain when they log in to the portal Web application.

Step 1: Set Up the Microsoft Active Directory Server

To authenticate users against a Microsoft Active Directory server, you must set up a Microsoft Active Directory server. Ensure that the appropriate user credentials are set up on a Microsoft Active Directory server. For details, see the Microsoft Active Directory home page on the Microsoft Web site.

Step 2: Add the Required Users to the Microsoft Active Directory Server

To enable Microsoft Active Directory authentication, you must add the initial users to the Microsoft Active Directory server. Create a person entry for the following user:

- *SAS Administrator (Required):* Add a person entry for the SAS Administrator user, for example , specifying the user ID `sasadm` and the password `Admin123`. (Note: You did not enter information for this user during the install program.)
- *SAS Trusted User (Required):* Add a person entry for the SAS Trusted User, for example, specifying the user ID `sastrust` and the password `Trust123`. (Note: You must use the exact user ID and password that was

entered in the install program wizard.)
- *SAS Web Administrator (Required):* Add a person entry for the SAS Web Administrator user, for example specifying the user ID `saswbadm` and the password `Admin123`. (Note: You must use the exact user ID and password that was entered in the install program wizard.)
- *SAS Guest (Required):* Add a person entry for the SAS Guest user, for example specifying the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password that was entered in the install program wizard.)
- *SAS Demo User (Optional):* Add a person entry for the SAS Demo User, for example specifying the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password that was entered in the install program wizard.)

Manually creating an entry for each portal Web application user can be time consuming. Creating and importing an LDIF file simplifies the process and also provides a backup file of portal Web application users.

Step 3: Add Required Users to the Host System

Add the following user account to the host operating system:

- *SAS (Required for Unix and z/OS only):* Add an individual account for the SAS user and a shared account for the SAS group. For example, specify the user ID `sas` and the password `Admin123`, and specify the shared ID `sas` (or `sasgrp` on z/Os) and the password `Admin123`.
- *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program wizard) For the following Windows systems, give this account the following user rights:

    - On Windows NT and 2000: Act as part of the Operating System.
    - On all Windows versions: Log on as a batch job.

Step 4: If Not Already Configured, Set up the SAS Metadata Server

To set up your SAS Metadata Server, see the setup instructions in the SAS 9.1 Metadata Server: Setup Guide. The following list provides specific additions (for each step) for the portal Web application SAS Metadata Server set up.

1. Create directories for the metadata server, repository manager, and repositories as described in the *SAS 9.1 Metadata Server: Setup Guide*.
2. Set directory and file access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Give the SAS user permissions for this directory.
3. Set system access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*.
4. Set server configuration options in an omaconfig.xml file as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Ensure that the omaconfig.xml file contains the security setting `<OMA AUTHCHCK="INHERIT"/>`. For example:

```
<OMAconfig>
  <OMA AUTHCHCK="INHERIT"/>
</OMAconfig>
```

5. Configure special users in adminUsers.txt and trustedUsers.txt files as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note 1: In the adminUsers.txt file, add an entry for the SAS Administrator. For Windows systems, this entry must be fully qualified with the Windows domain or machine name. In addition, to grant unrestricted access to this user (so that the user can locate users to load metadata), place an asterisk in the first character position of the fully qualified user ID.

   Note 2: In the trustedUsers.txt file, add an entry for the SAS Trusted User. For Windows systems, this entry must be fully qualified with the Windows domain or machine name.

Step 5: Set Up the SAS Metadata Server Startup Script to Enable Microsoft Active Directory Authentication

To enable the SAS Metadata Server to authenticate users against a Microsoft Active Directory server, you must configure the SAS Metadata Server startup command to allow Microsoft Active Directory authentication.

To create a startup command for the SAS Metadata Server, see Start the Metadata Server as described in the *SAS 9.1 Metadata Server: Setup Guide*.

Note: When creating the script for starting the SAS Metadata Server:

- specify the same SAS Metadata Server port number that you specified when you ran the install program wizard. if you do not remember which value you specified, check the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- specify the correct path for `sas.exe`.

To enable the SAS Metadata Server to authenticate against Microsoft Active Directory, follow these steps:

1. Set environment variables for the Microsoft Active Directory server. You can set the environment variables as system level environment variables or as part of your server startup script as follows:

   ```
   AD_PORT=  <port number for
                  Microsoft Active Directory>
   AD_HOST=  <host name of the machine
                  running Microsoft Active Directory>
   ```

2. Specify an authentication provider domain option for Microsoft Active Directory authentication. Specify the authentication provider domain option in the startup command for the SAS Metadata Server as follows:

   ```
   -authpd "ADIR:<your Windows domain>"
   ```

   When you configure user credentials on the SAS Metadata Server, you must specify the same domain (e.g. your Windows domain) that you specify in the SAS Metadata Server startup script.

The following SAS Metadata Server startup file shows the additional options in bold type:

```
@echo on
title OMS−5555
set omsport=5555
set AD_HOST=cia2.na.abc.com
set AD_PORT=3456
"C:\Program Files\SAS\SAS System\9.1\sas.exe" −memsize 0 −nologo
−nosplash −noterminal −objectserver  −objectserverparms
"protocol=bridge port=%omsport% instantiate
classfactory=2887E7D7−4780−11D4−879F−00C04F38F0DB" −log
"C:\Portal2.0.1Files\Open Metadata Server\OMR5555.log"
−authpd "adir:WINNT"
```

Step 6: Add or Modify Users and Groups on the SAS Metadata Server

You must add the initial users and groups to the SAS Metadata Server. To add new users:

1. **Set up the SAS Management Console profile**. Start SAS Management Console, and create a new profile and metadata repository. Use the following values when answering prompts:

   - Assign the same machine that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_HOST$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - Assign the same port that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - If you are creating a new repository, it must be a foundation repository.
   - Assign the same repository name that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_REPOSITORY$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
2. **Add Users to the SAS Metadata Repository**. For Microsoft Active Directory Server authentication, each user must have access to login credentials for all the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

   A user with administrative permissions can manually create user definitions in the metadata repository. Log in to SAS Management Console as the SAS Administrator and create the user definitions with the User Manager plug−in. If you have already created a user definition for one of these users as part of another install, do not create it again; instead, modify the login definitions as specified. For details about defining SAS users, see

   Defining a User in the *SAS Management Console: User's Guide*.

   The User Manager requires you to enter the following fields when you define a new user and login definition:

   Name
   specifies the name of the user.
   User ID

specifies the fully qualified user ID for the login credentials of the user. If you are authenticating against a Microsoft Active Directory, you must specify the user ID in the format `userID@<your Windows network domain>`

Password

specifies the password for the user ID.

Authentication Domain

specifies the logical grouping that associates logins and resources together.

For example:

- **Name**: `SAS Administrator`
- **User ID**: `sasadm@`***`your Windows Domain`***
- **Password**: `Admin123`
- **Authentication Domain**: **`DefaultAuth`**

Add new user definitions for the following users and associated user IDs:

- **SAS Administrator**: Add a new user definition for the SAS Administrator. You did not enter information for this user during the install program. For example, for the user definition:
  a. General tab.
  Name: `SAS Administrator`
  b. Logins tab. For the initial login definition, fill in the fields as follows:
     - **User ID**: `sasadm@`*`your Windows Domain`*
     - **Password**: `Admin123`
     - **Authentication Domain**: **`DefaultAuth`**

     Note: Specify the default authentication domain that you specified when you ran the install program wizard. if you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- **SAS Trusted User**: Add a new user definition for the SAS Trusted User using the information you provided in the install program wizard. You must use the exact user ID and password entered in the install program wizard and in Step 2. For example, for the user definition:
  a. General tab.
  Name: `SAS Trusted User`
  b. Logins tab. For the initial login definition, fill in the fields as follows:
     - **User ID**: `RALEIGH\sastrust`
     - **Password**: `Admin123`
     - **Authentication Domain**: **`DefaultAuth`**

     Note: Specify the default authentication domain that you specified when you ran the install program wizard. if you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- **SAS Web Administrator**: Add a new user definition for the SAS Web Administrator using the information you provided in the install program wizard. You must use the exact user ID and password entered in the install program Wizard and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Web Administrator`

b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `saswbadm@your Windows Domain`
- **Password**: `Admin123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program wizard. if you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Guest**. Add a new user definition for the SAS Guest using the information you provided in the install program wizard. You must use the exact user ID and password entered in the install program Wizard and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Guest`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  - **User ID**: `sasguest@your Windows Domain`
  - **Password**: `Guest123`
  - **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- **SAS Demo User**: Add a new user definition for the SAS Demo User using the information you provided in the install program wizard. For example:

  a. General tab.
  Name: `SAS Demo`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  - **User ID**: `sasdemo@your Windows Domain`
  - **Password**: `Demo123`
  - **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- **Add the required and demo portal Web application groups to the repository and add the necessary users to those groups.** If you have already created a group definition for one of these groups as part of another install, do ***not*** create it again. However, you will need to make sure that all the specified users have been added to the group.

  ◊ **SAS General Servers**: Add a new group definition for the SAS General Servers group, specifying the name `SAS General Servers`. Add a group login definition that specifies the login credentials for the SAS General Servers account that you defined on the host

authentication provider. You must use the exact user ID and password entered in the install program and in Step 1. For example, for the group definition:

a. General tab.
Name: `SAS General Servers`
b. Logins tab. For the initial login definition, fill in the fields as follows:

- **User ID**: `sassrv`
- **Password**: `Admin123`
- **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

Add the SAS Trusted User to the SAS General Servers group.

◊ **Portal Admins**: Add a new group definition for portal Web application administrators specifying the name `Portal Admins`. Add the SAS Web Administrator user as a group member.

◊ **Portal Demos**: Add a new group definition for Portal Demos specifying the name `Portal Demos`. Add the SAS Demo User as a group member.

For details about defining users and groups, see the SAS Management Console User Manager Help, and refer to Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

The administrator only needs to create the user definitions for the user in the metadata repository. The first time the user logs in to the portal Web application, the portal Web application automatically creates a profile definition in the metadata repository.

Step 7: For Server Access, Add Additional Credentials

If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account).

Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, the account must have the following user right:

- "Log on as a batch job" user right

If the server uses a different authentication process than the SAS Metadata Server, you must set up an additional user or group (shared) login definition (credentials) for the user on the SAS Metadata Server. For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains. To set up valid server credentials, for each server, do one of the following:

- **If the server uses the same authentication process as the SAS Metadata Server**, ensure that the following users can authenticate against the authentication provider for the server's machine.

    - *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`. On Windows, give this user the "Log on as a batch job" user right.
    - *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program wizard.)

      For the following Windows systems, give this account the specified user rights:

        - On Windows NT and 2000: Act as part of the Operating System.
        - On all Windows versions: Log on as a batch job.
    - *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.
    - *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.

  If your server is defined in the default authentication domain, the SAS Metadata Server uses credential caching to retrieve the appropriate credentials for the server; you do not need to specify an additional login on the SAS Metadata Server.

  Note: If your server is defined in an additional authentication domain but runs on the same operating system (and uses the same credentials) as the SAS Metadata Server, use SAS Management Console to reconfigure your server definition to specify the default authentication domain (DefaultAuth) for the authentication domain.
- **If the server uses a different authentication process than the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

    - **set up an individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**.

        1. Ensure that the following users can authenticate against the authentication provider for the server:
            - *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`.
            - *SAS General Servers (Required):* Add an individual account for the SAS General Servers group credentials, for example specifying the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program wizard.)

              For the following Windows systems, give this account the specified user rights:

                - On Windows NT and 2000: Act as part of the Operating System.
                - On all Windows versions: Log on as a batch job.
            - *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You

must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.

2. Set up an additional login definition for the SAS General Servers group, SAS Guest, and SAS Demo User on the SAS Metadata Server.

   Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

   Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

   - For example, for the SAS General Servers group, define an additional login definition and fill in the fields as follows:
     - **User ID**: `RALEIGH\sassrv`
     - **Password**: `Admin123`
     - **Authentication Domain**: **`ServerAuth`**

     Note:

     - If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the `$IOM_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
     - If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

   - For example, for the SAS Guest user, define an additional login definition and fill in the fields as follows:
     - **User ID**: `RALEIGH\sasguest`
     - **Password**: `Guest123`
     - **Authentication Domain**: **`ServerAuth`**

     Note:

     - If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for

the SAS Workspace and SAS Stored Process Server, use the value of the `$IOM_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- ♦ If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

· For example, for the SAS Demo User, define an additional login definition and fill in the fields as follows:

- **User ID**: `RALEIGH\sasdemo`
- **Password**: `Demo123`
- **Authentication Domain**: **`ServerAuth`**

Note:

- ♦ If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the `$IOM_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
- ♦ If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

♦ **set up a shared account on the authentication provider and associated group (shared) login for a SAS group definition (that contains the SAS user) on the SAS Metadata Server**. For all servers, determine existing or set up a new set up a shared account on the server's authentication provider.

Use SAS Management Console to set up or add to a SAS group that contains:

◊ the shared account as a group (shared) login of the SAS group.

Note: If the SAS OLAP Server authenticates against an alternate provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

◊ the user as a member of the SAS group. The user will then use the group (shared) login credentials to access the servers.

For details about defining SAS groups, see Defining a Group in the *SAS Management Console: User's Guide*.

Step 8: Ensure That All Users Specify the Appropriate Domain When They Log In to the Portal Web Application

When a user logs in to the portal Web application, they must specify the Microsoft Active Directory domain that was configured in the SAS Metadata Server startup command and in the user definitions on the SAS Metadata Server. For example:

```
user ID: saswbadm@WINNT
password:  Admin123
```

Test your initial portal Web application authentication and authorization setup by logging in to the portal Web application.

To add additional users for Microsoft Active Directory authentication, see Adding Users (Microsoft Active Directory Authentication).*Installation*

Setting Up Web Server Authentication

To understand Web server authentication and additional server authentication, see the topics "Initial Authentication on a Mid−Tier Server" and "Additional Authentication" in the SAS Intelligence Architecture: Planning and Administration Guide. To understand the portal Web application environment when using Web server (trusted realm) authentication, see Understanding the SAS Metadata Server (Web Server Authentication). To enable the portal's SAS Metadata Server to trust your users as already authenticated (by the web server) and then authorize the users with the SAS Metadata Server authorization facility, you must do the following:

- If you have used the project install to install the portal Web application, you already have the SAS Metadata Server set up and the appropriate users and groups defined. To enable Web Server (trusted realm) authentication:

    1. Edit the `install.properties` file (located in the `PortalConfigure` directory of the installation) and specify the property values as follows:

        ```
        $USER_DOMAIN$=web
        $AUTH_MECHANISM$=trusted
        $SERVICES_OMI_DOMAIN$=DefaultAuth
        $IOM_DOMAIN$=DefaultAuth
        $DAV_DOMAIN$=DefaultAuth
        $PORTAL_AUTH_MODULE$=com.sas.portal.
                delegates.authentication.factory.BasicAuthentication
        $SERVICES_WEB_DOMAIN$=web
        ```

        In addition, change the following user ID values to specify non−domain qualified user IDs:

        ```
        $PORTAL_GUEST_ID$=sasguest
        $PORTAL_ADMIN_ID$=saswbadm
        $PORTAL_DEMO_ID$=sasdemo
        ```
    2. Run the `configure_wik.bat` utility (located in the `PortalConfigure` directory of the installation) to create new service deployment configurations and new `SASStoredProcess.war` and `Portal.war` files

        .
    3. Deploy the `Portal.war` and `SASStoredProcess.war` files to the servlet container on your *portal Web application's Web server machine*.
    4. Set up the Web server for trusted realm authentication.
    5. Ensure that the required users and groups are added to the SAS Metadata Server.
    6. For server access, add additional credentials.
- If you have used the basic install to install the portal Web application (and for authentication, you chose to use the Web server's authentication provider):

    1. Set up the Web server for trusted realm authentication.
    2. Add the required users to the host system.
    3. Set up the SAS Metadata Server.
    4. Ensure that the required users and groups are added to the SAS Metadata Server.
    5. For server access, add additional credentials

Step 1: Set Up the Web Server for Trusted Realm Authentication

To use Web server (trusted realm) authentication with the portal Web application, you must set up a Web server that will authenticate the user before the user accesses the portal Web application. For information about setting up authentication for users on a Web server, refer to the documentation for your web server product. For information about the Apache server authentication, see Apache HTTP Server 2.0 Authentication, Authorization and Access Control on the Apache Web site.

The administrator must add the following users to the Web server authentication provider:

- *SAS Demo User (Optional):* Add a person entry for the SAS Demo User, for example specifying the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program wizard.)

Step 2: Add the Required Users to the Host System

Add the following user account to the host operating system:

- *SAS (Required for Unix and z/OS only):* Add an individual account for the SAS user and a shared account for the SAS group. For example, specify the user ID `sas` and the password `Admin123`, and specify the shared ID `sas` (or `sasgrp` on z/Os) and the password `Admin123`.
- *SAS Administrator (Required):* Add a person entry for the SAS Administrator user, for example specifying the user ID `sasadm` and the password `Admin123`. (Note: You did not enter information for this user during the install program.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS Trusted User (Required):* Add a person entry for the SAS Trusted User, for example specifying the user ID `sastrust` and the password `Trust123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program wizard) For the following Windows systems, give this account the following user rights:
    - ♦ On Windows NT and 2000: Act as part of the Operating System.
    - ♦ On all Windows versions: Log on as a batch job.
- *SAS Web Administrator (Required):* Add a person entry for the SAS Web Administrator (portal administrator) user, for example specifying the user ID `saswbadm` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.
- *SAS Guest (Required):* Add a person entry for the SAS Guest user, for example specifying the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.

Step 3: Set up the SAS Metadata Server

To set up your SAS Metadata Server, see the setup instructions in the SAS 9.1 Metadata Server: Setup Guide. The

following list provides specific additions (for each step) for the portal Web application SAS Metadata Server set up.

1. Create directories for the metadata server, repository manager, and repositories as described in the *SAS 9.1 Metadata Server: Setup Guide*.
2. Set directory and file access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Give the SAS user permissions for this directory.
3. Set system access permissions as described in the *SAS 9.1 Metadata Server: Setup Guide*. Set server configuration options in an omaconfig.xml file as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note: Ensure that the omaconfig.xml file contains the security setting `<OMA AUTHCHCK="INHERIT"/>`. For example:

   ```
   <OMAconfig>
     <OMA AUTHCHCK="INHERIT"/>
   </OMAconfig>
   ```
4. Configure special users in adminUsers.txt and trustedUsers.txt files as described in the *SAS 9.1 Metadata Server: Setup Guide*.

   Note 1: In the adminUsers.txt file, add an entry for the SAS Administrator. For Windows systems, this entry must be fully qualified with the Windows domain or machine name. In addition, to grant unrestricted access to this user (so that the user can locate users to load metadata), place an asterisk in the first character position of the fully qualified user ID.

   Note 2: In the trustedUsers.txt file, add an entry for the SAS Trusted User. For Windows systems, this entry must be fully qualified with the Windows domain or machine name.

Step 4: Ensure That the Required Users and Groups Are Added to the SAS Metadata Server

You must ensure that the six initial portal Web application users, their logins, and the two initial groups are added to the SAS Metadata Server. To add new users and groups, follow these steps:

1. **Set up the SAS Management Console profile**. Start SAS Management Console, and create a new profile and metadata repository. Use the following values when answering prompts:

   - Assign the same machine that you specified when you ran the install program wizard. if you do not remember which value you specified, check the value of the `$SERVICES_OMI_HOST$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - Assign the same port that you specified when you ran the install program wizard. if you do not remember which value you specified, check the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
   - If you are creating a new repository, it must be a foundation repository.
   - Assign the same repository name that you specified when you ran the install program wizard. if you do not remember which value you specified, check the value of the `$SERVICES_OMI_REPOSITORY$` property in the `install.properties` file (found in the

`PortalConfigure` subdirectory of the setup directory).

2. **Add on the SAS Metadata Repository**.

For Web server authentication, each user must have access to login credentials for all the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

Special Note: If all of the following conditions are true, you may be able to set up all of your login credentials within the same authentication domain (i.e., the default authentication domain, DefaultAuth):

- All servers use the same credentials as the Web server's authentication provider.
- All of your users use the same credentials for other applications that use the servers.

To reconfigure your portal Web application to use only the DefaultAuth authentication domain, see reconfiguring for One Authentication Domain. For each initial user definition, you can then define only one login definition and specify the default authentication domain (e.g. DefaultAuth).

A user with administrative permissions can manually create user definitions in the metadata repository. Log in to SAS Management Console as the SAS Administrator and create the user definitions with the User Manager plug−in. If you have already created a user definition for one of these users as part of another install, do not create it again; instead, modify the login definitions as specified. For details about defining SAS users, see Defining a User in the *SAS Management Console: User's Guide*.

When you define or modify a user and login definition, the User Manager requires you to enter the following fields:

Name *(of the user definition)*
specifies the name of the user.

User ID *(of the login definition)*
specifies the user ID for the login credentials of the user. The user ID is specified differently depending on whether your web server passes the domain with the login credentials:

- If the web server passes the domain with the credentials, specify the **user ID** as `<domain>\user ID` (e.g. `<domain>\sasadm`)
- If the web server does not pass the domain with the credentials, specify the **user ID** as `user ID` (e.g. `sasadm`).

Password *(of the login definition)*
specifies the password for the user ID. The password is not required for Web server authentication. The password is required for IOM server access.

Authentication Domain *(of the login definition)*
specifies the logical grouping that associates logins and resources.

Add the following users:

- **SAS Administrator**: Add a new user definition for the SAS Administrator. You did not enter information for this user during the install program. For example, for the user definition:
  a. General tab.
  Name: `SAS Administrator`
  b. Logins tab. For the initial login definition, fill in the fields as follows:
    - **User ID**: `sasadm`
    - **Password**: `Admin123`

- **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Trusted User**: Add a new user definition for the SAS Trusted User using the information you provided in the install program wizard. You must use the exact user ID and name entered in the install program wizard and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Trusted User`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  - **User ID**: `sastrust`
  - **Password**: Do not specify a password.
  - **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Guest**. Add a new user definition for the SAS Guest using the information you provided in the install program wizard. You must use the exact user ID and password entered in the install program and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Guest`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  - **User ID**: `sasguest`
  - **Password**: `Guest123`
  - **Authentication Domain**: **`DefaultAuth`**

  Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Web Administrator**: Add a new user definition for the SAS Web Administrator (Portal Administrator) user using the information you provided in the install program wizard. You must use the exact user ID and name entered in the install program Wizard and in Step 1. For example, for the user definition:
  a. General tab.
  Name: `SAS Web Administrator`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  - **User ID**: `saswbadm`
  - **Password**: `Admin123`
  - **Authentication Domain**: **`DefaultAuth`**

Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- **SAS Demo User**: Add a new user definition for the SAS Demo User using the information you provided in the install program wizard. For example, for the user definition:

  a. General tab.
  Name: `SAS Demo User`
  b. Logins tab. For the initial login definition, fill in the fields as follows:

  - **User ID**: `sasdemo`
  - **Password**: `Demo123`
  - **Authentication Domain**: **`web`**

3. **Add the required and demo portal Web application groups to the repository and add the necessary users to those groups.** If you have already created a group definition for one of these groups as part of another install, do ***not*** create it again. However, you will need to make sure that all the specified users have been added to the group.
   - **SAS General Servers**: Add a new group definition for the SAS General Servers group, specifying the name `SAS General Servers`. Add a group login definition that specifies the login credentials for the SAS General Servers account that you defined on the host authentication provider. You must use the exact user ID and password entered in the install program and in Step 1. For example, for the group definition:

     a. General tab.
     Name: `SAS General Servers`
     b. Logins tab. For the initial login definition, fill in the fields as follows:

     - **User ID**: `sassrv`
     - **Password**: `Admin123`
     - **Authentication Domain**: **`DefaultAuth`**

     Note: Specify the default authentication domain that you specified when you ran the install program wizard. If you do not remember which value you specified, check the value of the `$SERVICES_OMI_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

     Add the SAS Trusted User to the SAS General Servers group.
   - **Portal Admins**:Add a new group definition for portal Web application administrators specifying the name `Portal Admins`. Add the SAS Web Administrator user as a group member.
   - **Portal Demos**: Add a new group definition for Portal Demos specifying the name `Portal Demos`. Add the SAS Demo User as a group member.

For details about defining users and groups, see the SAS Management Console User Manager Help, and refer to Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

The administrator only needs to create the user definitions for the user in the metadata repository. The first time the user logs in to the portal, the portal Web application automatically creates a profile definition in the metadata repository.

Step 4: For Server Access, Add Additional Credentials

If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account).

Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, the account must have the following user right:

- "Log on as a batch job" user right

If the server uses the same host or alternative authentication provider as the SAS Metadata Server, you must set up an additional user or group (shared) login definition (credentials) for the user on the SAS Metadata Server. For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains. To set up valid server credentials, for each server, do one of the following:

- **If the server uses the same authentication process as the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

  - **Set up an individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**.

    1. Ensure that the following users can authenticate against the authentication provider for the server:
       - *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`.
       - *SAS General Servers (Required):* Add a shared account for the SAS General Servers group (shared) login. A shared account is an account that maps to a login owned by a SAS group on the SAS Metadata Server. For example, specify the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program wizard)

         For the following Windows systems, give this account the specified user rights:

         - On Windows NT and 2000: Act as part of the Operating System.
         - On all Windows versions: Log on as a batch job.
       - *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.
       - *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.
    2. Set up an additional login definition for the SAS Demo User on the SAS Metadata Server.

       Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login

definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

- For example, for the SAS Demo User, define an additional login definition and fill in the fields as follows:
  - **User ID**: `RALEIGH\sasdemo`
  - **Password**: `Demo123`
  - **Authentication Domain**: **`DefaultAuth`**

♦ **Set up a shared account on the authentication provider and associated group (shared) login for a SAS group definition (that contains the SAS user) on the SAS Metadata Server**. For all servers, determine existing or set up a new set up a shared account on the server's authentication provider.

Use SAS Management Console to set up or add to a SAS group that contains

◊ the shared account as a group (shared) login of the SAS group. On the login definition, specify the default authentication domain, DefaultAuth.
◊ the user as a member of the SAS group. The user will then use the group (shared) login credentials to access the servers.

For details about defining SAS groups, see Defining a Group in the *SAS Management Console: User's Guide*.

For an example that details how to define user or group credentials for a new authentication domains, see Defining Logins for Multiple Authentication Domains.

- **If the server uses a different host or alternate authentication provider than the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

♦ **set up an individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**.

1. Ensure that the following users can authenticate against the authentication provider for the server:
   - *SAS (Required):* Add an individual account for the SAS user. For example, specify the user ID `sas` and the password `Admin123`.
   - *SAS General Servers (Required):* Add an individual account for the SAS General Servers group credentials, for example specifying the user ID `sassrv` and the password `Admin123`. (Note: You must use the exact user ID and password entered in the install program wizard.)

     For the following Windows systems, give this account the specified user rights:

     - On Windows NT and 2000: Act as part of the Operating System.
     - On all Windows versions: Log on as a batch job.
   - *SAS Guest (Required):* Add an individual account for the SAS Guest user. For example, specify the user ID `sasguest` and the password `Guest123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On Windows, give this user the "Log on as a batch job" user right.
   - *SAS Demo User (Optional):* Add an individual account for the SAS Demo User. For example, specify the user ID `sasdemo` and the password `Demo123`. (Note: You must use the exact user ID and password entered in the install program wizard.) On

Windows, give this user the "Log on as a batch job" user right.

2. Set up an additional login definition for the SAS General Servers group, SAS Guest, and SAS Demo User on the SAS Metadata Server.

   Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

   Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternate authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

   · For example, for the SAS General Servers group, define an additional login definition and fill in the fields as follows:
   - **User ID**: `RALEIGH\sassrv`
   - **Password**: `Admin123`
   - **Authentication Domain**: **`ServerAuth`**

     Note:

     ♦ If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the `$IOM_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).
     ♦ If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

   · For example, for the SAS Guest user, define an additional login definition and fill in the fields as follows:
   - **User ID**: `RALEIGH\sasguest`
   - **Password**: `Guest123`
   - **Authentication Domain**: **`ServerAuth`**

     Note:

     ♦ If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the `$IOM_DOMAIN$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

- If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

· For example, for the SAS Demo User, define an additional login definition and fill in the fields as follows:
  - **User ID**: `RALEIGH\sasdemo`
  - **Password**: `Demo123`
  - **Authentication Domain**: **`ServerAuth`**

  Note:

  - If you performed a basic install and defined your server in a separate authentication domain (than the default authentication domain), for the SAS Workspace and SAS Stored Process Server, use the value of the IOM_DOMAIN property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory)).
  - If you performed a basic or project install and did not define your server in a separate authentication domain (than the default authentication domain), you must reconfigure the server to specify a new authentication domain (and then specify that authentication domain in the login definition).

- **Set up a shared account on the authentication provider and associated group (shared) login for a SAS group definition (that contains the SAS user) on the SAS Metadata Server**. For all servers, determine existing or set up a new set up a shared account on the server's authentication provider.

  Use SAS Management Console to set up or add to a SAS group that contains

  ◊ the shared account as a group (shared) login of the SAS group.

  Note: If the SAS OLAP Server authenticates against an alternate provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

  ◊ the user as a member of the SAS group. The user will then use the group (shared) login credentials to access the servers.

  For details about defining SAS groups, see Defining a Group in the *SAS Management Console: User's Guide*.

To add additional users for Web Server authentication, see Adding Users (Web Server Authentication).

Reconfiguring the Installation for One Authentication Domain

To reconfigure your portal Web application to use only the DefaultAuth authentication domain, (instead of the web authentication domain for Web server authentication and the DefaultAuth authentication domain for server access), follow these steps:

1. Edit the `install.properties` file (found in the `PortalConfigure` subdirectory of the installation directory) in a text editor.

   Locate the following lines:

   ```
   $USER_DOMAIN$=web
   $SERVICES_WEB_DOMAIN$=web
   ```

   Change these lines to use the default authentication domain, e.g., DefaultAuth:

   ```
   $USER_DOMAIN$=DefaultAuth
   $SERVICES_WEB_DOMAIN$=DefaultAuth
   ```
2. Run the `configure_wik.bat` utility to create new service deployment configurations and new `SASStoredProcess.war` and `Portal.war` files.
3. Deploy the `Portal.war` and `SASStoredProcess.war` to the servlet container on your *portal Web application's web server machine*.

When you define your user and login definitions, define your initial login definition in the default authentication domain (e.g., DefaultAuth) instead of the web authentication domain (e.g., web).

Installation

Default Security Installation

Definitions for users of the portal Web application are stored by both the authentication provider (for authentication) and the SAS Metadata Repository (for authorization).

Initial Users: SAS Trusted User, SAS Administrator, SAS Web Administrator, SAS Guest, and SAS Demo User

When you install the portal Web application using the basic install or project install, you are prompted to enter user IDs and passwords for five specific users. The default user names and user IDs for the five initial users are SAS Trusted User (e.g., `sastrust`), SAS Administrator (e.g., `sasadm`), SAS Web Administrator (e.g. `saswbadm`), SAS Guest (e.g., `sasguest`), and SAS Demo User (e.g., `sasdemo`). Each of these users is listed by its default name and described below:

Note: When you installed the portal Web application, you might have specified different user names and user IDs for these users:

- **SAS Trusted User**: The default SAS Trusted User is `sastrust`. (The SAS Trusted User is set up as a *trusted user* by listing it in the `trustedUsers.txt` file). The servers that are deployed with the portal Web application use the SAS Trusted User account to connect to the SAS Metadata Server and retrieve configuration information. For Web server authentication, the SAS Trusted User enables mid−tier (Web−tier) users to be viewed as already−authenticated by the Web server and connect to the SAS Metadata Server for authorization purposes.

  For information about *trusted users*, see Trusted Users in the *SAS 9.1 Metadata Server: Setup Guide*.
- **SAS Administrator**: The default SAS Administrator is `sasadm`. The SAS Administrator is set up as an *unrestricted user* and has unrestricted access to the metadata. (The SAS Administrator is set up as an unrestricted user by listing this user in the `adminUsers.txt` file and preceding the user ID with an asterisk). You can use the SAS Administrator to log in to SAS Management Console and create the portal Web application's content, user, and authorization metadata on the SAS Metadata Server.

  For more information about the *unrestricted user*, see Server Administrative Privileges in the *SAS 9.1 Metadata Server: Setup Guide*.
- **SAS Web Administrator**: The default SAS Web Administrator is `saswbadm`. Because the SAS Web Administrator is a member of the Portal Admins group, the SAS Web Administrator has unrestricted access to view users' personal portal Web application content and share that content with a SAS group. The SAS Web Administrator can also modify users' personal portal Web application content.

  Note: Due to the permissions granted to the SAS Web Administrator, it is recommended that you do not use the SAS Web Administrator for general tasks.

  The portal Web application shell uses the SAS Web Administrator to perform specific tasks, such as deploying portlets and creating SAS group permission trees. The portal Web application installation also uses the SAS Web Administrator to load initial metadata.

  To further understand the role of the SAS Web Administrator, see Portal Admins group.
- **SAS Guest**: The default SAS Guest is `sasguest`. The SAS Guest is the administrator for the Public Kiosk. The Public Kiosk is displayed to users who have not yet logged in to the portal Web application. The SAS

Guest user can create and edit the Public Kiosk that is displayed.

Note: If you installed only the SAS Web Infrastructure Kit, to enable the SAS Guest to create and edit content for the Public Kiosk, you must configure the SAS Guest as a group content administrator. For details, see Configuring a Group Content Administrator.

Important Note: Because the SAS Guest user creates and edits the Public Kiosk that is displayed to all users, ensure that you only give these credentials to the administrator of the Public Kiosk.

Users who view the Public kiosk have access to content based on the authorization (access control) for the SAS Guest user.

The portal Web application installation also uses the SAS Guest to load initial metadata.

Note: If users authenticate using the Web server (trusted realm) authentication, no Public Kiosk is displayed; however, you still must define the SAS Guest account.

- **SAS Demo User**: The default SAS Demo User is `sasdemo`. The SAS Demo User is provided for demonstration purposes. If you loaded the initial demo data, this user allows users to test their portal Web application implementation and learn about the features.

  Note: If you installed only the SAS Web Infrastructure Kit, to enable the SAS Demo User to create and edit content, you must configure the SAS Demo User as a group content administrator. For details, see Configuring a Group Content Administrator.

The portal Web application installation configures the appropriate authorization (access control) for the initial users.

Note: If you need to change the password for the SAS Trusted User, SAS Guest, or SAS Web Administrator, see Changing the Password for the SAS Trusted User, SAS Guest, or SAS Web Administrator.

Initial Groups: SAS General Servers, Portal Admins and Portal Demos

In order to run, the portal Web application requires definitions for three groups at a minimum: `SAS General Servers`, `Portal Admins`, and `Portal Demos`. You create these group definitions during the installation process. Each of these groups is described as follows:

- **SAS General Servers**: The group `SAS General Servers` contains a group login that is used by the spawner to start the load−balancing SAS Stored Process Server(s).
- **Portal Admins**: The group `Portal Admins` contains users that are portal Web application administrators. The group initially contains the SAS Web Administrator (e.g., `saswbadmn`). Each member of the `Portal Admins` group has the following capabilities:

  - unrestricted access to view users' personal portal Web application content and share that content with a SAS group. Members of the Portal Admins group can also modify and delete users' personal portal Web application content.

    Note: Due to the permissions granted to members of the Portal Admins group, it is recommended that you do not use Portal Admins group members for general tasks.
  - the ability to bootstrap metadata for group−based content sharing in the portal Web application. If you create groups (on the SAS Metadata Server) after you start the servlet container for the portal Web

application, when a member of the Portal Admins group logs in to the portal Web application, the metadata for group−based content sharing (i.e. group permission trees) is updated. If there are a large number of groups, the log in time for a member of the Portal Admins group might be slower than the log in time for a typical user due to the bootstrap creation of metadata for group permission trees.

Within your installation, if you have any other users that are *unrestricted users*, add those users to the Portal Admins group.

- **Portal Demos**: The group `Portal Demos` is for the portal Web application's demo users. The group initially contains the SAS Demo User (e.g., `sasdemo`).

For Unix and z/OS Systems: SAS User and SAS Group

If you installed with the project install on Unix or z/OS, you created one additional user and one additional group on the operating system:

- **SAS** user: The default SAS user is `sas`. The SAS user should be used to start the following servers (if they are not started as a service) and spawners:
  - Start the spawner that starts the SAS Workspace Server(s) and SAS Stored Process Server(s).
  - If you are not starting the SAS Metadata Server as a service, start the SAS Metadata Server.
  - If you have installed a SAS OLAP Server and are not starting the OLAP server as a service, start the OLAP server.
- **SAS** group: The default SAS group is `sas` on Unix and `sasgrp` on z/OS. This group is used to control access to some directories and files.

For additional details about the SAS user and group, see "Pre−Installation Checklist for Unix" and "Pre−Installation Checklist for z/OS" in the SAS Intelligence Architecture: Planning and Administration Guide.

Initial User Accounts

If you deploy a distributed server configuration, or authenticate some users against an alternative authentication provider, the following table shows the required locations of the user accounts that you create before beginning your installation:

Summary of Required Accounts for Authentication of Initial Credentials				
User Name (User ID)	**SAS Metadata Server's authentication provider**	**SAS Workspace Server's host authentication provider**	**SAS Stored Process Server's host authentication provider**	**SAS OLAP Server's authentication provider**
SAS Administrator (e.g., sasadm)	Yes	No	No	Yes
SAS Trusted User (e.g., sastrust)	Yes	No	No	No
SAS Guest (e.g., sasguest)	Yes	Yes*	Yes	Yes

SAS Demo User (e.g., sasdemo)	Yes	Yes*	Yes	Yes
SAS General Server (e.g., sassrv)	Yes	Yes	Yes	No

Note: If the SAS Workspace Server is set up in a pooled configuration, you are not required to have an account for these user credentials on the host for the SAS Workspace Server.

Initial Metadata Identities on the SAS Metadata Server

The following table summarizes the user and group metadata identities that you have defined in the metadata in order for your servers and applications to work correctly. You can use the User Manager plug−in in SAS Management Console to verify that these objects have been created properly.

Summary of Metadata Identities

Metadata Identities	Logins			Group Membership Information
	User ID*	Password**	Authentication Domain	
User: SAS Administrator	sasadm			
User: SAS Trusted User	sastrust			**member of:** SAS General Servers group
User: SAS Guest	sasguest	********	DefaultAuth	
User: SAS Demo User	sasdemo	********	DefaultAuth	**member of:** Portal Demos
User: SAS Web Administrator	saswbadm	********	DefaultAuth	**member of:** Portal Admins group
Group: SAS General Servers	sassrv	********	DefaultAuth	**members:** SAS Trusted User
Group: Portal Admins				**members:** SAS Web Administrator
Group: Portal Demos				**members:** SAS Demo User

* These are the recommended IDs. They should correspond to accounts in your authentication provider. On Windows, the user ID in the login should be fully qualified with a host or domain name, for example, *host−name*\sasadm.

** If you are logged in to SAS Management Console as an unrestricted user, you will always see ******** in the password column, even if no password was specified.

Installation

Loading Initial Metadata

When you install the portal Web application, you can choose to run the `*.sas` files to load initial metadata for the portal Web application.

Two versions of every SAS program file are provided:

- The version that ends in `_utf8.sas` uses UTF−8 character encoding and should only be executed using SAS System Software that is Unicode enabled.
- The version that ends in `.sas` uses the character encoding of the machine where the `configure_wik` script is run and should only be executed using SAS System Software that is running the same character encoding.

If you do not load the initial demo data, when users start the portal Web application, the login screen is the first screen displayed. You can log in as the SAS Guest user (default, `sasguest`) and create the appropriate pages for the Public Kiosk. When users log in to the portal Web application, a message is displayed stating that no pages are defined. For a SAS Web Infrastructure Kit−only installation, common users will not have access to any portal Web application content until a content administrator creates or adds content to their portal Web application. For a SAS Information Delivery Portal installation, common users will not have access to any portal Web application content until they create or add content to their portal Web application. Common users might have access to content that is contained in the portal Web application's SAS Metadata Repository.

If you want to load the initial demo data and if the SAS Metadata Server runs on a different machine than the one where you installed the portal Web application , before you run the `*.sas` files to load the metadata on the SAS Metadata Server's machine, you must ensure that the encodings on the two machines are compatible. The `*.sas` files contain localized metadata that is created in the encoding of the machine where the portal Web application was installed:

- If the localized metadata cannot be represented in the default encoding of the SAS System on the SAS Metadata Server machine, in most cases, you should not transfer these files to that machine and submit them to the SAS System. However, you might be able to use the `−encoding` system option to change the encoding of the SAS Metadata Server machine's SAS System so that it successfully reads the `*.sas` files.
- If the localized metadata was successfully created in the encoding of the portal Web application's machine, you might be able to run the `*.sas` files using the SAS System of the portal Web application's machine in order to load the metadata to the SAS Metadata Server's machine. Before you submit the `*.sas` programs, use the SAS Program Editor to view the localized metadata and verify that it is correct.

Installation

Verifying Your Portal Installation

If you have completed all of the steps in the Project Install or the Basic Install, and if the demonstration portal Web application is operating successfully, then you can start customizing the portal Web application and adding your own content to meet the unique needs of your organization.

Before proceeding, you may wish to review the descriptive information in Understanding the Portal Environment. In addition, you may want to review the following tables to verify that you have completed all of the installation steps. For details on any of the items in the first table, refer to the appropriate section of the SAS Web Infrastructure Kit installation instructions (available with the installation and on the software media).

System Component	Verification Question	Yes/No	Installation Instructions Step
Java Environment	Have you installed the appropriate version of the Java 2 Software Development Kit (SDK)?		Step 1
	Is the Java executable present in your path?		Step 1
SAS Software	Have you installed all of the required SAS software (Version 9.1 of the SAS System, SAS Management Console, and SAS Foundation Services)?		Step 2
Servlet Container	Have you installed a servlet container that is supported for the SAS Web Infrastructure Kit?		Step 3
	Were you able to run the examples that were provided with the servlet container?		Step 3
	Is the servlet container installed in a path name that does ***not*** contain spaces?		Step 3
	Have you followed the installation tips that are provided for your servlet container software?		Step 3
WebDAV	Have you installed a WebDAV server (this step is optional)? Have you installed the Xythos WFS WebDAV server (this software is required only if you want to use the features of the SAS Web Infrastructure Kit that require this server)?		Step 4
Install Program	Did you run the install program for the SAS Web Infrastructure Kit?		Step 5
	Did you run the install program for the SAS Information Delivery Portal (if you purchased this product)?		Step 5
			Step 6.a

Configuration Script	If you chose not to install a WebDAV server, did you add the appropriate lines to the `install.properties` file?		
	Did you run the configuration script?		Step 6.c
SAS Metadata Server	If your metadata server is configured for host authentication, did you set up the necessary user accounts for the machine where the SAS Metadata Server is installed?		Step 7.a
	Has your SAS Metadata Server been set up?		Step 7.b
	Did you set the necessary system, directory, and file access permissions on the metadata server?		Step 7.b
	Did you set the appropriate configuration options in the `omaconfig.xml` file?		Step 7.b
	Did you configure the appropriate users in the `adminUsers.txt` and `trustedUsers.txt` files?		Step 7.b
	Does the script that is used to start the metadata server specify the correct port number and path?		Step 7.b
	Did you start the metadata server?		Step 7.b
	Did you use SAS Management Console to create a new profile and metadata repository?		Step 7.c
	Did you use SAS Management Console to add the required and demonstration users and their logins to the metadata repository?		Step 7.d
	Did you use SAS Management Console to add the initial groups to the metadata repository and to add the necessary users to those groups?		Step 7.d
	If you will be using stored processes to publish packages to WebDAV, did you create an entry for an HTTP server in your metadata repository?		Step 8.a
	Did you run the appropriate SAS programs in order to load the demonstration metadata into your metadata repository?		Step 8.b
SAS Object Spawner	Did you set up the SAS Object Spawner by using the appropriate instructions for your operating system?		Step 9
Servlet Container	Did you prepare your servlet container environment by using the appropriate procedures for your servlet container and		Step 10

	Java Virtual Machine (JVM)?		
	Did you manually deploy the `Portal.war`, `SASStoredProcess.war`, and `SASDoc.war` files to the servlet container by using the appropriate procedures for your software environment?		Step 11
SAS/GRAPH Applets	Did you take the necessary steps to make the graph applets available as `/sasweb/graph` from either the servlet container or the Web server that runs these applications?		Step 12
SAS Services application	Did you make the necessary modifications to the start script for the SAS Services application?		Step 13
Servers	Did you start the servers in the correct order?		Step 14
Servlet Container	Did you complete the recommended tuning steps in order to work around known servlet container issues and to improve performance?		Step 15

If you are using an LDAP or Microsoft Active Directory server to authenticate users, verify the following additional installation requirements:

Installation Component	Verification Question	Yes/No
SAS IT Administrator or Enterprise Console (LDAP only)	If you are using LDAP, have you installed SAS Integration Technologies Administrator, Version 1.6, or Enterprise Console in order to define person entries?	
	If you installed SAS Integration Technologies Administrator, do the `setServer` and `setBase` settings in the SAS Integration Technologies Administrator's configuration file (`site.cfg`) refer to the correct LDAP host and directory tree?	
LDAP or Microsoft Active Directory Software	Has the appropriate LDAP or Microsoft Active Directory software been installed?	
LDAP or Microsoft Active Directory Metadata	Have you set up the SAS and SAS General Servers credentials for host authentication? Have you set up the other 5 initial users (SAS Administrator, SAS Web Administrator, SAS Trusted User, SAS Demo User, and SAS Guest) for LDAP or Microsoft Active Directory authentication.	

If you are using a Web server to authenticate users, verify the following additional installation requirements:

Installation Component	Verification Question	Yes/No
Authentication Services	If you using a Web Server for authentication, have you set up the appropriate authentication services?	
	Have you set up authentication for the portal Web application shell's six initial users, `sasadm`, `sastrust`, `saswbadm`, `sasguest`, `sasdemo`, and `sassrv`?	

Note: To change the location in which logging information is recorded, you can modify the `logging_config_idp.xml` file. For details, see Modifying the Logging Output Information and Location.

Installation

Modifying the Logging Output Information and Location

You can modify the logging configurations for many SAS Web applications and for the SAS Services application by editing the logging configuration file that is associated with the application. You can change the log file name and location, the types of messages that are stored in the log, and the log message format.

To edit the logging configuration file for an application, you must first locate the file using the following table:

Application	Default Logging Configuration File	Location
SAS Services Application	`logging_config_svc.xml`	the **/web/Deployments/RemoteServices** subdirectory of the SAS configuration directory
Portal Web Application	`logging_config_idp.xml`	the **/web/Deployments/Portal** subdirectory of the SAS configuration directory
SAS Preferences Web Application	`logging_config_prefs.xml`	the **/web/Deployments/Portal** subdirectory of the SAS configuration directory
SAS Stored Processes Web Application	`logging_config_stp.xml`	the **/web/Deployments/Portal** subdirectory of the SAS configuration directory
SAS Web Report Studio	`DefaultLoggerProperties.xml`	the **/SASWebReportStudio/WEB−INF** subdirectory of the servlet container's **webapps** directory
SAS Web Report Viewer	`DefaultLoggerProperties.xml`	the **/SASWebReportViewer/WEB−INF** subdirectory of the servlet container's **webapps** directory

Note: Changes to the logging configuration files will be lost if you run the application's configuration script again.

Changing the Types of Messages That Are Stored in the Log

To change the types of messages that are stored in the log, specify the priority level attribute for the appropriate logging context. Specify one of the following values:

DEBUG displays the informational events that are most useful for debugging an application.

INFO displays informational messages that highlight the progress of the application.

WARN displays potentially harmful situations.

ERROR displays error events that might allow the application to continue to run.

FATAL displays very severe error events that will probably cause the application to abort.

For example, the following section from the portal logging configuration file shows the priority attributes in bold:

```
<RootLoggingContext priority="WARN">
  <OutputRef outputID="FILE"/>
  <OutputRef outputID="CONSOLE"/>
</RootLoggingContext>

<LoggingContext name="com.sas"
                priority="WARN"
```

```
                chained="false">
  <OutputRef outputID="FILE"/>
  <OutputRef outputID="CONSOLE"/>
</LoggingContext>

<LoggingContext name="com.sas.portal.container.deployment.PortletDeployer"
                priority="INFO"
                chained="false">
  <OutputRef outputID="CONSOLE_PortletDeployer"/>
</LoggingContext>

<LoggingContext name="com.sas.portal.container.PortalController"
                priority="INFO"
                chained="false">
  <OutputRef outputID="FILE"/>
</LoggingContext>
```

Changing the Log File Name and Location

To change the log file, modify the `File` parameter for the `<Output>` tag. The following example section shows the log file name in bold:

```
<Output id="FILE"
        type="File"
        layoutPattern = "%d [%p] %c – %m%n">
  <param name  = "File"
         value = "C:/SAS/cfg/Lev1/web/Deployments/Portal/log/portal.log">
</Output>
```

Note: In Windows, the path must use either backslash characters (/) or escaped forward slash characters (\\).

Changing the Log Message Format

To change the log format, modify the `layoutPattern` attribute for the `<Output>` tag. The following example shows the pattern in bold:

```
<Output id="FILE"
        type="File"
        layoutPattern = "%d [%p] %c – %m%n">
  <param name  = "File"
         value = "C:/SAS/cfg/Lev1/web/Deployments/Portal/log/portal.log">
</Output>
```

For more information about the pattern syntax, see Pattern Layout for easy formatting of output in the SAS Foundation Services class documentation.

Additional Information

For additional details about the elements in the logging configuration files, see the SAS Foundation Services class documentation for the com.sas.services.logging component.

Installation

Starting the Servers and Services

To ensure proper operation of your portal Web application implementation, if you are starting your servers and services manually, you must start your SAS Metadata Server, Xythos WFS WebDAV server, SAS Servers, remote services and servlet container in the appropriate order. The SAS servers have dependencies on the SAS Metadata Server and the servlet container has a dependency on the remote SAS Foundation Services. The following table shows the server and service dependencies:

Server	Dependency
LDAP Server	none
SAS Metadata Server	none
Xythos WebDAV Server	none
SAS Stored Process Server	SAS Metadata Server
SAS Workspace Server	SAS Metadata Server
SAS Services application	SAS Metadata Server
Servlet Container / Application Server	SAS Metadata Server, Xythos WebDAV Server, SAS Stored Process Server, SAS Workspace Server, SAS Services application

Ensure that the servers are started in the following order:

1. If you are authenticating against an LDAP or Microsoft Active Directory server, start the LDAP or Microsoft Active Directory server.
2. Start the SAS Metadata server first. (If you are using LDAP or Microsoft Active Directory server authentication, use the startup script that you created in Setting up LDAP Authentication and Setting up Microsoft Active Directory Authentication).
3. If you installed the Xythos WFS WebDAV server, start the WebDAV server.
4. Depending on how you configured your SAS Workspace Server and SAS Stored Process Server:
    - If you installed using the basic install, then one spawner starts both the SAS Workspace Server and SAS Stored Process Server. Use the spawner startup command to start both the SAS Stored Process Server and SAS Workspace Server.
    - If you set up different spawners for your SAS Workspace Server and SAS Stored Process Server, use each spawner's startup command to start the respective servers.
5. Start the SAS Services application (located in the `SASServices\WEB-INF` directory of your portal Web application installation). The SAS Services application must be started and initialized before you start the servlet container.
6. Start the servlet container. If the servlet container is already running, you must restart it before you access the portal Web application.

Installation

Administering the Portal Web Application

To understand and administer the portal Web application:

1. **Understand the SAS Web Infrastructure Kit and SAS Information Delivery Portal components**. For details, see the Portal Environment chapter.
2. **Understand the administration tools**. For details, see the Administration Tools chapter.
3. **Understand the server and SAS Foundation Services deployments and redistribute if necessary**. For details, see Foundation Service Deployment and SAS Server Deployment.
4. **Determine the content types that you want to add to the portal Web application**. For details, see the Content chapter.
5. **Understand security and plan which users and groups will access each type of portal Web application content**. For details, see the topic "Overview of Security Concepts" in the SAS Intelligence Architecture: Planning and Administration Guide and the Security chapter of this guide.
6. **Define users and groups.** For details, see Implementing Security in the Security chapter.
7. **Add content and implement authorization (access control) by following the appropriate instructions for the content type**. For details, see the appropriate section in the Content chapter.

Installation

Administering the Public Kiosk

The Public Kiosk can be used to display pages and portlets that you want all users to be able to view as follows:

- If you are not using the Web server's authentication provider for user authentication, when users access the portal Web application, you can display a Public Kiosk for users to view before they log in to the portal Web application.
- If you are using the Web server's authentication provider for user authentication, users directly access the portal Web application's login page, instead of the Public Kiosk.

Creating the Public Kiosk

The SAS Guest user is the administrator of the Public Kiosk. When you log in to the portal Web application as the SAS Guest user, you can create, edit, and display content for the Public Kiosk. (The SAS Guest user's personalized portal is the content that is displayed as the Public Kiosk).

Important Note: Because the SAS Guest user creates and edits the Public Kiosk that is displayed to all users, ensure that you only give these credentials to the administrator of the Public Kiosk.

To create or edit the Public Kiosk,

1. If you have only installed the SAS Web Infrastructure Kit, configure the SAS Guest user as a group content administrator so that the SAS Guest can create the Public Kiosk. For details, see Configuring a Group Content Administrator.
2. Log in to the portal Web application as the SAS Guest user. A collection of publicly−available pages (with the default as a single Public Kiosk page) are defined for the SAS Guest user.
3. Add the desired Public Kiosk content to the SAS Guest user's portal Web application. For details about adding content, refer to the appropriate section in the Content chapter.
4. Specify the appropriate access controls for the content that the SAS Guest user can view, and will display (via the Public Kiosk) to all users. When a user accesses the portal Web application's Public Kiosk, they can only retreive and view content that the SAS Guest user and the Public group are authorized to access. For details, see Authorizing Access to Content.

Removing the Public Kiosk

In some cases, you might not want to display a Public Kiosk to users. Depending on whether you have installed the initial demo data, you can eliminate a Public Kiosk display as follows::

- **If you have installed the initial demo data**, log in to the portal Web application as the SAS Guest user and delete all pages from the SAS Guest user's portal Web application.
- **If you have not installed the initial demo data**, do not define any pages for the SAS Guest user so that no Public Kiosk is available when users access the portal Web application.

Understanding the Portal Environment

Note: In this guide, "portal Web application" is a generic term that refers to either of the following:

- the SAS Portal Web Application Shell, which is a portal−like Web application shell that is included in the SAS Web Infrastructure Kit and is used by other SAS Web applications, or
- the SAS Information Delivery Portal, which (when installed with the SAS Web Infrastructure Kit) fully implements the capabilities of the SAS Portal Web Application Shell.

When you have completed the installation procedures, verified your installation, and ensured that your portal Web application is operating successfully, this means that all of the basic components of the portal Web application environment are in place. You can now begin the implementation tasks that are necessary to meet your organization's specific information delivery requirements.

Before you begin working with your portal Web application, it is useful to understand the how the portal Web application and associated products fit into the overall SAS Business Intelligence Architecture. For a description of this architecture, refer to the SAS Intelligence Architecture: Planning and Administration Guide.

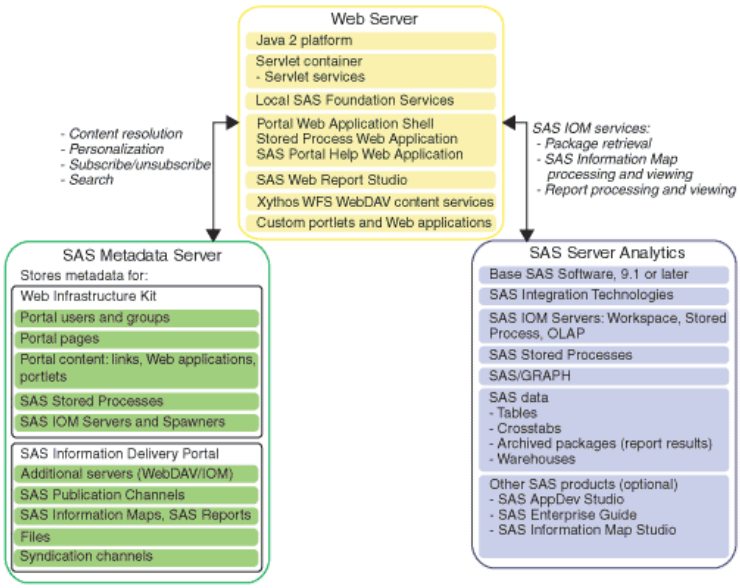
In addition, it is important to understand the features of the SAS Web Infrastructure Kit that are available to developers and to users, as well as the expanded features that are available if you have purchased the SAS Information Delivery Portal. Some of these features depend on other software, including the Xythos WFS WebDAV Server. For an explanation of these features and their software dependencies, refer to the Overview of the SAS Web Infrastructure Kit.

To understand the portal Web application components, see Understanding the Portal Web Application Components.

Portal Environment

Understanding the Portal Web Application Components

In addition to understanding how the SAS Web Infrastructure Kit and Information Delivery Portal fit into the SAS Business Intelligence Architecture, it is important to understand how the components of the portal Web application (as SAS Web Infrastructure Kit or SAS Information Delivery Portal) work together. The following diagram provides a high−level, conceptual view of the portal Web application's main components and how they interact with one another:



The architecture of the portal Web application gives you the flexibility to distribute these components as required. For small implementations, the Web server, SAS Metadata Server, and other SAS servers, such as the SAS Workspace Server and SAS Stored Process Server, can all run on the same machine. In contrast, a large enterprise might have multiple compute and data servers and a metadata repository that is distributed across multiple platforms. In addition, the components of the different tiers, such as Web applications on the Web server, might be distributed on separate machines.

The preceding diagram shows the following three components:

- **Web Server**:

  The Web server is the platform that supports the operation of the portal Web application. The portal Web application interacts with the SAS Metadata Repository (on the SAS Metadata Server) and Xythos WFS WebDAV repository (on the Xythos WFS WebDAV content server) to access or search content metadata. It also uses the back−end SAS analytic and reporting functions in order to surface information to the portal Web application. For more details, see Understanding the Web Server.
- **SAS Metadata Server**:

  The SAS Metadata Server provides access to a central repository (a SAS Metadata Repository) for the portal Web application's user, resource, and security information. The SAS Metadata Server stores metadata for the portal Web application's content and security and the portal Web application utilizes this metadata to authorize users for access to content. For user authentication, the SAS Metadata Server relies on one of the following authentication providers:

  - **host authentication**: Users are authenticated against the host system of the SAS Metadata Server's machine. For more details, see Understanding the SAS Metadata Server (Host Authentication).

- **LDAP or Microsoft Active Directory authentication**: Users are authenticated against an LDAP or Microsoft Active Directory server. For a diagram and understanding of the setup for the metadata servers when using the SAS Metadata Server with LDAP or Microsoft Active Directory Authentication, see Understanding the SAS Metadata Server (LDAP or Microsoft Active Directory Server Authentication).
- **Web Server (trusted realm) authentication**: Users are authenticated by the Web server's authentication provider; the portal Web application trusts the Web server's authentication mechanism. For a diagram and understanding of the setup for the metadata servers when using the SAS Metadata Server with Web server authentication, see Understanding the SAS Metadata Server (Web Server Authentication).

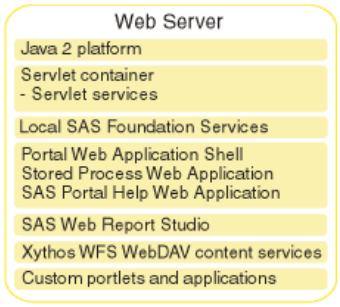
Note: You must define users on both the authentication provider and the SAS Metadata Server.

- **SAS Server Analytics**:

  The SAS server analytics allow the portal Web application to exploit SAS analytic and reporting functions in order to deliver information to the desktops of authorized portal Web application users. The back−end analytics of the SAS system provide the data for the portal Web application's content. For more details, see Understanding the SAS Server Analytics.

Portal Environment

Understanding the Web Server



The Web server is the platform that supports the operation of the portal Web application. You might distribute the components of this platform on a single Web server or on several Web servers. The Web server platform contains the following components:

Note: The SAS Services application usually runs on the same machine as one of the Web servers. The SAS Services application is a command−line application that deploys remote services to share with foundation service−enabled applications. Other applications can access the remote service deployment, thereby enabling integration with the portal Web application. The SAS Services application accesses an XML file to obtain the remote service deployment configuration. For details, see Service Deployment Configuration.

- **Java 2 platform**: The Java 2 Software Development kit (SDK), Standard Edition, provides the software development language and run−time environment for the portal Web application. For information, see the Products and APIs page on the Sun Microsystems Web site.
- **Servlet container**: The servlet container provides the platform, or engine, on which to run the portal Web application's servlets and JavaServer Pages (JSPs). For more information, see the Java Servlet Technology page on the Sun Microsystems Web site.
    - **Servlet container services**: The Servlet container provides a set of servlet services that provide life cycle and session management for all of the Web applications running on the Web server. These services enable the Web applications to receive and process HTTP requests and generate responses. The portal Web application uses the servlet container services as infrastructure for the Web applications.
    - **Local SAS Foundation Services**: SAS Foundation Services contains a set of common infrastructure components that enable the development of integrated, scalable, and secure applications. By default, the portal Web application deploys a local service deployment on the Web server where the portal Web application is installed. The portal Web application accesses an XML file to obtain the local service deployment configuration. For details, see Service Deployment Configuration. The SAS Services application deploys the remote foundation services.
- **Portal Web Application**: The portal Web application is a portal−like Web application shell that can be used by other SAS Web applications. The portal Web application has the following components:
    - **Portal Web Application Java classes**: The foundation of the portal Web application consists of Java classes contained in the Portal API. Refer to the Portal API class documentation for complete documentation of the Java classes included in these SDKs. If you want, you can use these classes to develop your own custom portlets and custom applications for deployment in the portal Web application. For details, see Using the Portlet API in the *SAS Web Infrastructure Kit Developer's Guide*.
    - **Portal Web Application Java Servlets, JSPs, JavaBeans**: The portal Web application servlets,

JSPs, and JavaBeans are the active components of the portal Web application. Using the portal Web application Java classes, these servlets, JSPs, and JavaBeans interact with the metadata server, SAS Stored Process Server, and the SAS Workspace Server to deliver portal Web application functionality and content to users.

- **Portal Web application themes**: The portal Web application themes control the appearance of the portal Web application's user interface. The themes consist of cascading style sheets (CSSs) and graphical elements, including the portal Web application's banner, background image, and logo. To modify the themes, refer to the *SAS Web Infrastructure Kit Developer's Guide*
- **Property files**: The `install.properties` file contains parameters that control the operation of the portal Web application. The `install.properties` file includes your installation directory locations, default locale setting, user ID and authentication domain information, and information about your SAS Metadata Server, Java RMI Server (for the SAS Services application), and WebDAV server.
- **Package Viewer**: The Package Viewer enables you to display packages in the portal Web application.
- **Web Report Viewer (available if you have installed the SAS Information Delivery Portal)**: The Web Report Viewer enables you to display SAS Reports in the portal Web application.
- **Information Map Viewer (available if you have installed the SAS Information Delivery Portal)**: The Information Map Viewer enables you to display SAS Information Maps in the portal Web application.

- **Stored Process Web Application**: The Stored Process Server Web application enables you to run stored processes. The Stored Process Web application can be run standalone or through the portal Web application. The Stored Process Web application uses the Stored Process Viewer to provide input to and display output from stored processes.
- **SAS Documentation Web Application**: The SAS Documentation Web application is a Web application that manages SAS documentation for the portal Web application and other Web applications.
- **Xythos WFS WebDAV Server Content Services**: The Web server also manages content that is accessible to HTTP clients. This content may be accessible through Uniform Resource Locators (URLs), or it may be accessible only through Web applications.

  Web Distributed Authoring And Versioning (DAV) provides services to help manage and locate content stored on the Web server. WebDAV enhancements to the HTTP protocol enable the Web to serve as a document database. Through this database, users in remote locations can collaborate in creating and editing documents (such as SAS Reports, word processing files, images, and SAS packages) that are stored in folders (called collections) within a hierarchical file system.

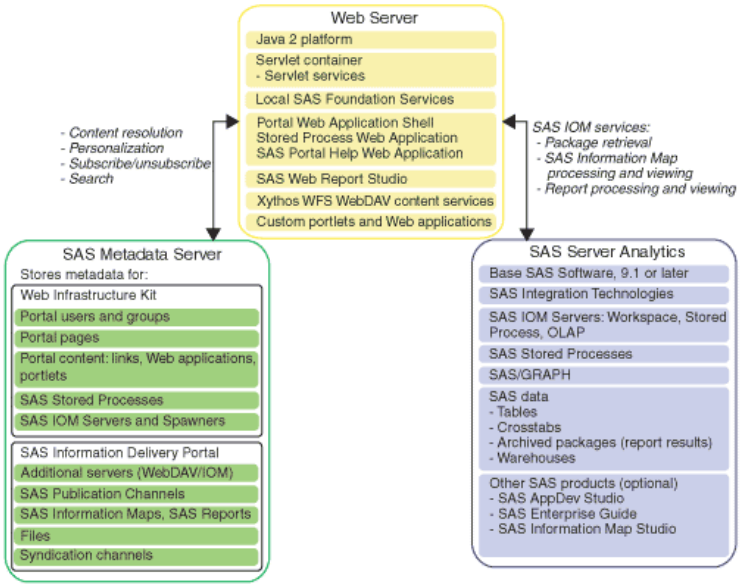
  The portal Web application requires the Xythos WFS WebDAV server to enable users to do the following:

  - run stored processes in the background
  - save stored process results to a WebDAV server
  - use the portal Web application alert features
  - use the WebDAV Navigator portlets
  - access files
  - access WebDAV−based publication channels
  - use WebDAV−based subscription management
  - publish content to WebDAV
- **SAS Web Report Studio (optional)**: SAS Web Report Studio is a Web application that enables you to create and view reports stored in the SAS Report Model format.
- **Custom Portlets (optional)**: You can develop your own custom portlets that take advantage of the portal Web application's content, metadata, and security services. For details about deploying portlets, see the *SAS Web Infrastructure Kit Developer's Guide*, Adding Custom−Developed Portlets, and Portlet Deployment.

- **Custom Applications (optional)**: You can develop your own custom Web applications using the SAS Foundation Services (and other Business Intelligence Services). When a foundation service−enabled Web application is invoked from the portal Web application, the portal Web application passes the application the session and application context which can then be used to obtain the authenticated user (and allow single signon). For more information, see the *SAS Web Infrastructure Kit Developer's Guide* and Adding Applications.
- **Other Solutions and Business Intelligence Web applications**: The Web server might also manage other Web applications, such as solutions or Business Intelligence Web applications that are built using the servlet container services and Business Intelligence Services.

Portal Environment

Understanding the SAS Metadata Server (Host Authentication)



The preceding diagram shows the portal Web application components with the host environment of the SAS Metadata Server's machine used for user authentication purposes. The SAS Metadata Server provides access to a central metadata repository, the SAS Metadata Repository, for the portal Web application's user, resource, and security information. The metadata repository does not contain actual content for the portal Web application; instead, it contains *metadata*, or data about the content.

- If you have only installed the SAS Web Infrastructure Kit, the SAS Metadata Server can contain metadata for SAS users and groups, portal Web application content, stored processes, and SAS servers and spawners (stored process server or workspace server).
- If you have installed the SAS Information Delivery Portal, the SAS Metadata Server might contain additional metadata for SAS publication channels, SAS Information Maps, SAS Reports, and additional SAS servers and spawners upon which these content types rely.

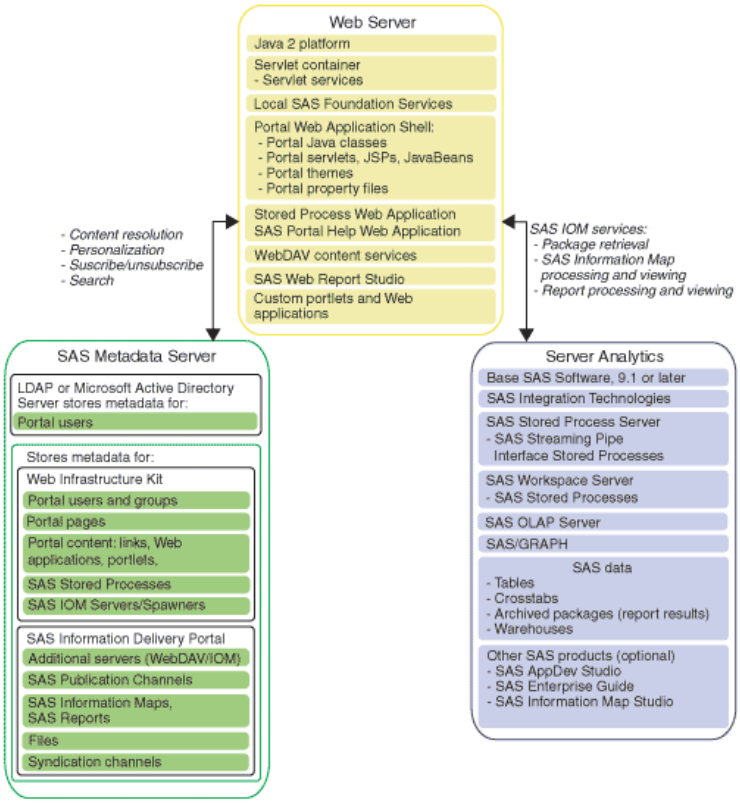
For additional information about the SAS Metadata Server and SAS Metadata Repository, see Getting Started with the SAS 9.1 Open Metadata Interface.

For information about metadata administration for the SAS Metadata Server metadata, see Understanding Metadata Server Administration.

For information about host authentication setup, see Setting up Host Authentication. For information about user administration for host authentication, see Defining Users (Host Authentication).

.Portal Environment

Understanding the Metadata Server (LDAP or Microsoft Active Directory Authentication)



The preceding diagram shows the portal Web application components with an LDAP or Microsoft Active Directory server used by the SAS Metadata Server for user authentication. For full details about SAS Metadata Server authentication, see the topic "Authentication" in the SAS Intelligence Architecture: Planning and Administration Guide.

The SAS Metadata Server provides access to a central metadata repository, the SAS Metadata Repository, for the portal Web application's user, resource, and security information. The metadata repository does not contain actual content for the portal Web application; instead, it contains *metadata*, or data about the content:

- If you have only installed the SAS Web Infrastructure Kit, the SAS Metadata Server can contain metadata for SAS users and groups, portal Web application content, stored processes, and SAS servers and spawners (stored process server or workspace server).
- If you have installed the SAS Information Delivery Portal, the SAS Metadata Server might contain additional metadata for SAS publication channels, SAS Information Maps, SAS Reports, and additional SAS servers and spawners upon which these content types rely.

For additional information about the metadata servers and metadata repositories:

- For the SAS Metadata Server and SAS Metadata Repository, see Getting Started with the SAS 9.1 Open Metadata Interface.
- For the LDAP server, (a server based on the Lightweight Directory Access Protocol), see Directory Services topic in the *SAS Integration Technologies Administrator's Guide (LDAP)*.

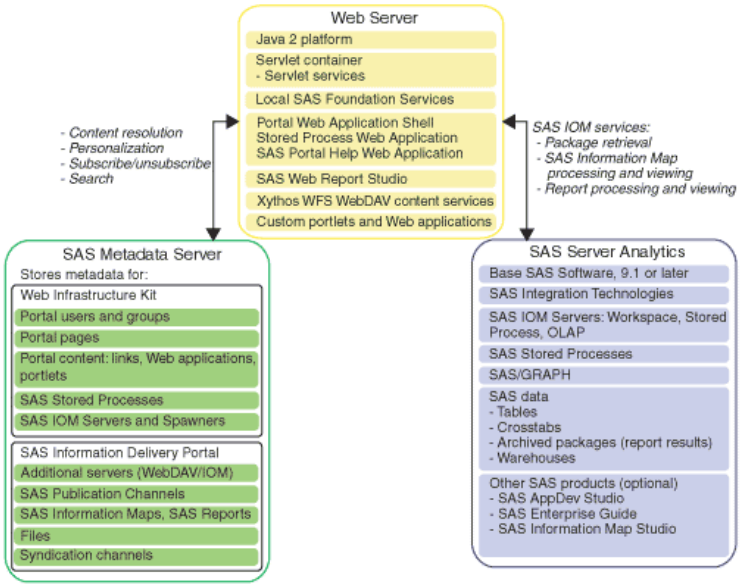
- For SAS Metadata Server administration, Understanding Metadata Server Administration.

To implement authentication against an LDAP or Microsoft Active Directory server, you must store user metadata on an LDAP or Microsoft Active Directory server. For information about metadata administration for the SAS Metadata Server metadata and LDAP or Microsoft Active Directory server user entries, see

- for LDAP authentication setup, see Setting up LDAP Server Authentication.
- for LDAP server user administration, see Defining Users (LDAP).
- for Microsoft Active Directory authentication setup, see Setting up Microsoft Active Directory Authentication.
- for Microsoft Active Directory server user administration, see Defining Users (Microsoft Active Directory).

Portal Environment

Understanding the Metadata Server (Web Server Authentication)



The preceding diagram shows the portal Web application components with a Web server used for authentication purposes. The SAS Metadata Server provides access to a central metadata repository, the SAS Metadata Repository, for the portal Web application's user, resource, and security information. The metadata repository does not contain actual content for the portal Web application; instead, it contains *metadata*, or data about the content.

- If you have only installed the SAS Web Infrastructure Kit, the SAS Metadata Server can contain metadata for SAS users and groups, portal Web application content, stored processes, and SAS servers and spawners (stored process server or workspace server).
- If you have installed the SAS Information Delivery Portal, the SAS Metadata Server might contain additional metadata for SAS publication channels, SAS Information Maps, SAS Reports, and additional SAS servers and spawners upon which these content types rely.

When you use the Web server to authenticate users, the SAS Metadata Server trusts that the mid−tier users have already been authenticated by the Web server. The portal Web application uses a *trusted user* to access the SAS Metadata Server and retrieve server credentials and authorization information for the mid−tier user.

To implement Web server authentication, the default portal Web application installation for Web server (trusted realm) authentication sets up a trusted user file (`trustedUser.txt`) for the user SAS Trusted User. You must then define the mid−tier users (and the appropriate login definitions) on the SAS Metadata Server. When the mid−tier user (who is already authenticated by a Web server) accesses the portal Web application, the *trusted user* acts on behalf of the mid−tier user to access the SAS Metadata Server, obtain the mid−tier user's SAS user identity, and retrieve credentials and authorization information for that user. If the user needs to access other IOM servers (workspace, stored process, or OLAP servers), the user definition (on the SAS Metadata Server) must contain login definitions with credentials for those servers. For full details about Web server authentication, see the topic "Authentication" in the SAS Intelligence Architecture: Planning and Administration Guide.

For additional information about the SAS Trusted User, SAS Metadata Servers, and SAS Metadata Repository:

- for details about *trusted users* and trusted user authentication, see Trusted User Authentication in the *SAS Integration Technologies Administrator's Guide*.
- for the SAS Metadata Server and SAS Metadata Repository, see Getting Started with the SAS 9.1 Open Metadata Interface.

For information about metadata administration for the SAS Metadata Server metadata and Web server user setup, see

- for SAS Metadata Server administration, Understanding Metadata Server Administration.
- for Web server (trusted realm) authentication setup, see Setting up Web Server Authentication.
- for Web server user administration, see Defining Users (Web Server (Trusted Realm)).

Portal Environment

Understanding Metadata Server Administration

If you installed the initial demo data, the portal Web application's installation process builds an initial set of metadata repository entries that form the basis for a demonstration portal Web application. Building on the base set of entries, you can add and change metadata as needed to implement a portal Web application that meets the needs of your organization. Procedures for updating the metadata are detailed throughout this guide. In these procedures, you will find that there are several ways to update the metadata:

- The **portal Web application shell Options menu** creates entries for portal Web application pages, portlets, and certain types of portal Web application content.
- The **SAS Management Console** application creates entries for the SAS users and groups, SAS Workspace Server configuration, SAS Stored Process Server and stored processes, SAS OLAP Server, and SAS publication channels.

In addition, the **SAS System** runs programs that load metadata for Web applications, page templates, and syndication channels.

For an overview of these administration tools, see the appropriate section under Understanding the Administration Tools.

How to Add Metadata

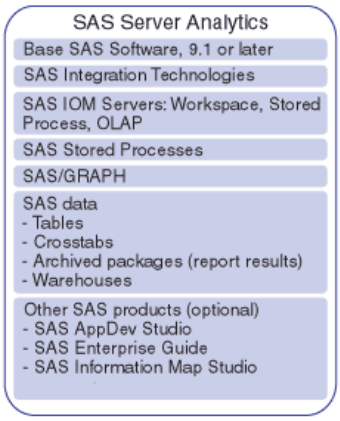
The following table provides a quick reference to the various categories of metadata that reside in the portal Web application's metadata repository. For each metadata category, the table shows the portal Web application component that the metadata describes, the initial metadata entries that are loaded during the initial demo data installation process (for components other than users and groups, which are defined during the install process), and the method that can be used to update the content metadata. For detailed documentation, click the entries in the "Component" column.

Metadata on the Portal Web Application's SAS Metadata Server			
Category	**Component**	**Initial Entries**	**How to Update**
Users and groups	**portal Web application users**	sasadm sastrust saswbadm sasdemo sasguest	for host authentication, host user tools and User Manager plug−in of SAS Management Console for LDAP authentication, LDAP tools and User Manager plug−in for Web server authentication, Web server user tools and User Manager plug−in
	Groups	Portal Admins Portal Demos SAS General Servers	SAS Management Console
SAS configuration	**SAS servers, spawners, users, and logins**	Main−Workspace Server	SAS Management Console

		Main−Stored Process Server localhost Spawner	
	Xythos WFS WebDAV configuration	none	SAS Management Console
Content	**Web Applications**	none	SAS
	Files (if you have installed SAS Information Delivery Portal and a Xythos WFS WebDAV server)	none	Xythos WFS WebDAV tools (used by the Xythos WFS WebDAV repository administrator)
	Links	SAS Home Page SAS Integration Technologies CNN CNNSI	portal Options menu
	SAS Information Maps (if you have installed SAS Information Delivery Portal)	none	SAS Information Map Studio (used by the information map administrator
	Custom−developed Portlets	Various	Hot−deploy mechanism
	Portlets	Various	portal Options menu
	SAS publication channels (if you have installed SAS Information Delivery Portal)	none	***Channels:*** Publishing Framework plug−in of SAS Management Console ***Subscribers:*** Publishing Framework plug−in ***Published packages:*** SAS Publishing Framework or Enterprise Guide
	SAS Reports(if you have installed SAS Information Delivery Portal)	none	SAS Web Report Studio (used by the report administrator)
	SAS Stored Processes	various	Stored Process Manager plug−in of SAS Management Console
	Syndication Channels (if you have installed SAS Information Delivery Portal)	none	SAS
User Interface	**Portal Web Application Pages**	Various	portal Options menu
	Portal Web Application Page Templates	none	SAS

Portal Environment

Understanding the SAS Server Analytics



The SAS server analytics environment contains:

- **Base SAS software**: Base SAS software performs the data access, management, analysis and presentation tasks that form the basis for all other SAS information delivery applications.
- **SAS Integration Technologies**: These components enable the operation of the SAS Integrated Object Model (IOM) server on the SAS Workspace Server, SAS Stored Process Server, and SAS OLAP Server machines. (For more information, refer to Integrated Object Model in the *SAS Integration Technologies Developer's Guide*.) The workspace server, stored process server, and OLAP server are three types of IOM servers that you can use to exploit SAS analytic and reporting functions in order to deliver information to the desktops of authorized users. For details about which content requires an IOM server, see Deploying Servers.

    - **SAS Workspace server**: The IOM server component of the SAS Workspace Server contains distributed object interfaces that allow programs (such as the portal Web application) on client machines to execute the Base SAS software features. An object spawner running on the server validates user and application requests for workspaces and instantiates workspaces as needed.

      The SAS Workspace Server is the platform that enables users to perform the following functions from client machines that have only a Web browser installed: run stored processes, run reports, view SAS Information Maps, subscribe to SAS publication channels, and view packages that are published to these channels.
    - **SAS Stored Process Server**: The IOM server component of the SAS Stored Process Server contains distributed object interfaces that allow programs (such as the portal Web application) on client machines to execute streaming stored processes and receive results by a streaming pipe interface.

      The SAS Stored Process Server is the platform that enables the portal Web application to receive streaming stored process results from client machines that only have a Web browser installed. Stored processes that stream results through a stored process pipe must execute on a SAS Stored Process Server.

      (The stored process server environment is compatible with the SAS/IntrNet Application Dispatcher. You can usually convert existing SAS/IntrNet Application Dispatcher programs to streaming stored processes with minimal or no modifications.)
    - **SAS OLAP Server**: The IOM server component of the SAS Stored Process Server contains distributed object interfaces that allow programs (such as the portal Web application) on client machines to execute the Base SAS software features.

The SAS OLAP Server is the platform that enables the portal Web application to view multi−dimensional data on client machines that only have a Web browser installed. Reports that surface multi−dimensional data execute on an OLAP server.

- **SAS data**: Your organization's SAS data can be stored either on the SAS server or on a machine that is accessible to the server.
- **SAS Stored Processes**: A stored process is a SAS program that resides on a SAS server and is available to be executed on a request basis. A stored process that returns output to the client in a results package runs on a SAS Workspace Server. A stored process that returns output to the client by a streaming pipe interface runs on a SAS Stored Process Server.

  For more information about running stored processes on stored process servers, see SAS Stored Processes in the *SAS Integration Technologies Developer's Guide* and see Adding Stored Processes in this guide.
- **SAS/GRAPH**: SAS/GRAPH software enables stored processes to generate graphs.
- **Other SAS products**: Other SAS products such as AppDev Studio, SAS Information Map Studio, and SAS Enterprise Guide can also be installed on the SAS server. By leveraging the capabilities of these products, you can provide enhanced information delivery capabilities to portal Web application users.

Understanding the Administration Tools

This chapter provides an overview of the administration tools used with the portal Web application. Administration tools allow the administrator to implement security, administer metadata, customize portal Web application content, re−create application WAR and configuration files, and remove portal−specific metadata.

The administrator can use administration tools for the following five types of tasks:

- **metadata administration**: You can administer metadata for SAS Metadata Servers or LDAP servers (user metadata for authentication only).
    - For SAS Metadata Servers, you can administer metadata with the User Manager, Server Manager, Stored Process Manager, and Publishing Framework plug−ins of SAS Management Console, and the portal Options menu.
    - For LDAP servers, you can administer user metadata (for authentication purposes) with the Enterprise Directory Console.
- **authorization (access control) metadata**: You can control access to content using the Authorization Manager plug−in of SAS Management Console or the portal Options menu.
- **personalization**: Content administrators, members of the Portal Admins group and common users that have the SAS Information Delivery Portal installed can use the portal Options menu to set up and display the portal Web application's content according to your implementation's requirements.
- **re−create WAR files**: You can use the Configure_wik Utility to re−create the WAR and configuration files for the portal Web application, SAS Stored Process Web Application and SAS Services application (remote services).
- **removal of portal−specific metadata**: You can use the SAS Portal Metadata Tool to remove the portal−specific metadata from the portal Web application's SAS Metadata Repository. The tool does not remove metadata that is managed by specific SAS Management Console plug−ins (such as Server Manager, Stored Process Manager, or Publishing Framework definitions).

Administration Tools

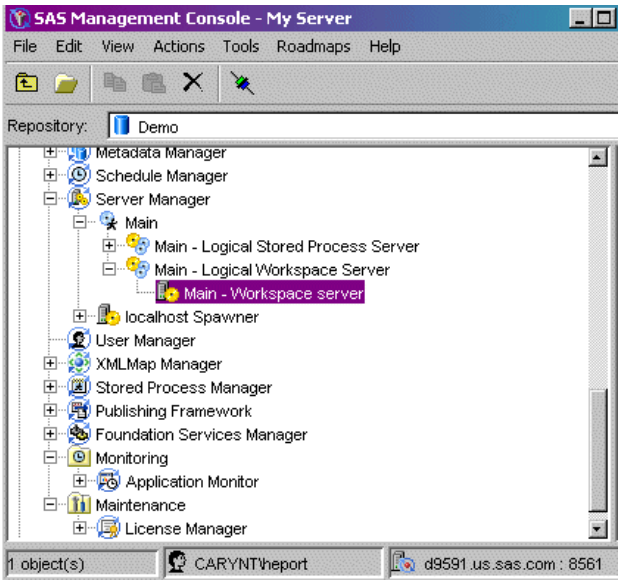
SAS Management Console

You can use SAS Management Console to manage SAS users, SAS groups, some content, and authorization metadata on a SAS Metadata Server. SAS Management Console is a Java application that provides a single point of control for SAS administrative tasks. The application provides a flexible administrative environment through the use of plug−ins. A plug−in is a Java file that is installed in the SAS Management Console directory to provide a specific administrative function. You can use the following plug−ins to manage metadata that is used by the portal Web application:

- **Authorization Manager**, which manages access control definitions for objects.
- **Data Library Manager**, which manages definitions for libraries and schemas.
- **Foundation Services Manager**, which manages SAS Foundation Services deployments.
- **Publishing Framework**, which manages publication channels and archives.
- **Server Manager**, which manages definitions for the servers and spawners.
- **Stored Process Manager**, which manages definitions for stored processes.
- **User Manager**, which manages definitions for the logins, users, and groups.

When you add objects using SAS Management Console, the application creates an object definition for each instance of an item and lists the object in the navigation tree under the plug−in used to create the object.

For example, if you use the Server Manager plug−in to define a SAS Workspace Server named "Main−Workspace Server", a server object called "Main−Workspace Server" is then listed in the navigation tree under the Server Manager. You can view and change the object's metadata by opening the object's properties and modifying the appropriate fields.



For more information about where to use SAS Management Console to add SAS Open Metadata Architecture content for the portal Web application, see Understanding the SAS Metadata Server and Understanding Metadata Server Administration.

Administration Tools

Portal Options Menu

The portal Web application is the collection of Java Servlets, JavaServer Pages, Java Beans, classes, and other resources that access information stored in metadata repositories and present a customizable interface to the user.

The user interacts with the portal Web application by navigating through a set of pages that consist of one or more portlets. The portal Options menu allows content administrators, members of the Portal Admins group, and common users that have the SAS Information Delivery Portal installed to perform several administration tasks:

- add, edit, share, remove, and delete pages in the portal Web application
- add, edit, remove, and delete portlets. In addition, when you add or edit collection portlets, you can add the following content to a collection:
    - ♦ applications
    - ♦ files (if you have installed the SAS Information Delivery Portal and a Xythos WFS WebDAV server)
    - ♦ links
    - ♦ packages
    - ♦ SAS Information Maps (if you have installed the SAS Information Delivery Portal)
    - ♦ SAS publication channels (if you have installed the SAS Information Delivery Portal)
    - ♦ SAS Reports (if you have installed the SAS Information Delivery Portal)
    - ♦ SAS Stored Processes
    - ♦ syndication channels (if you have installed the SAS Information Delivery Portal)
- manage publication channel subscriptions and subscriber profiles (if you have installed the SAS Information Delivery Portal).
- change personal preferences for country, language, and theme of the Web application
- clear user history in order to restore default pages that the user has removed.
- move the navigation bar to a different position (to the top or the side of the browser window).

The following diagram shows the portal Options menu and icons that allow you to perform the administration functions.

In addition, the portal Web application enables a user to perform several other tasks, which aid in administering the Web application:

- search the Web application for content.
- publish content (if you have installed the SAS Information Delivery Portal).
- use bookmarks to save markers to content. If you have installed the SAS Information Delivery Portal or are a group content administrator or member of the Portal Admins group, you can then create a collection portlet using the bookmarks.

Administration Tools

Configure_wik Utility

To create the WAR, deployment, and configuration files for the portal Web application, SAS Stored Process Web application, SAS Services application, and service deployments, you use the `configure_wik` configuration utility, which is located in the main installation directory for the portal Web application (`configure_wik.bat` for Windows, `configure_wik.sh` for Unix). You can use the `configure_wik` utility to

- **re−configure and re−deploy applications**: You can edit the values in the `install.properties` file and then use the `configure_WIK` to re−create the portal Web application, SAS Stored Process Web application, SAS Services application, and SAS Documentation Web application WAR files, and other deployment and configuration files.
- **create and deploy new themes**. You can create new themes and then use the `configure_wik` utility to re−create the portal Web application, SAS Stored Process Web application, SAS Services application, and SAS Documentation Web application WAR files and other deployment and configuration files.

When you run the `configure_wik` utility, it does the following:

1. Uses the `install.properties` to configure the portal Web application (`Portal.war`), the SAS Stored Process Web application (`SASStoredProcesses.war`), SAS Documentation Web application (`SASDoc.war`), SAS Services application, and associated deployment and configuration files.
2. Copies the local and remote service deployment files and configuration files to the appropriate directory.

Important Note: After you run the `configure_wik` utility, you must deploy the new `.war` files in the appropriate servlet container.

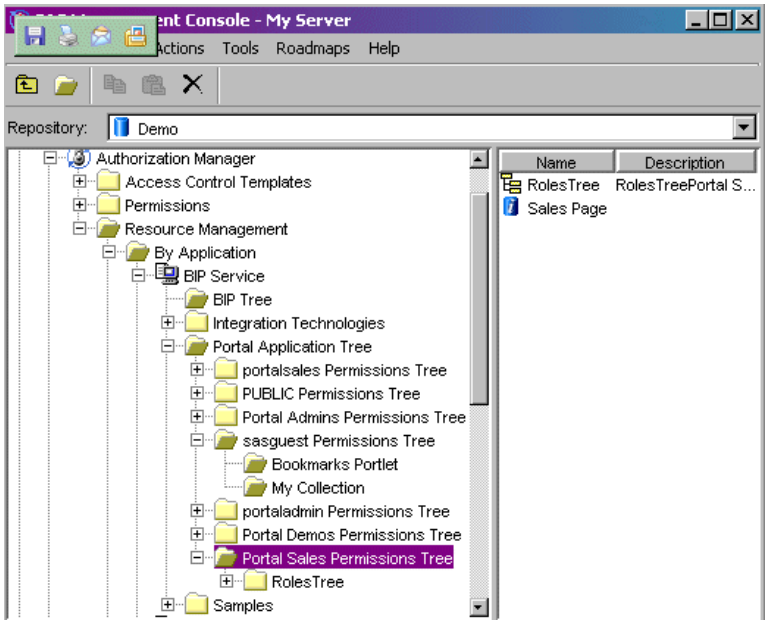
Administration Tools

SAS Portal Metadata Tool

The SAS Portal Metadata Tool removes portal−specific metadata from the SAS Metadata Repository. You might want to remove all the portal−specific metadata that you have created for either of the following reasons:

- a requirement to start with a clean SAS Metadata Repository
- a requirement to create a new set of portal−specific metadata

The portal−specific metadata is defined in the Portal Application Tree of the SAS Management Console navigation tree.

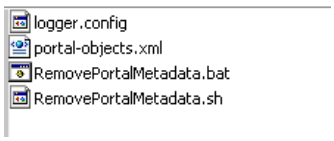


Portal−specific metadata includes:

- links
- pages and page templates
- portlets
- syndication channels
- user and group permission trees
- Web applications

The SAS Portal Metadata Tool only removes portal−specific metadata from the portal Web application's SAS Metadata Repository. The tool does not remove metadata that is managed by specific plug−ins (such as Server Manager, Stored Process Manager, or Publishing Framework plug−ins).

The SAS Portal Metadata Tool is installed in the `\Tools` directory of your portal Web application installation. The following display shows the initial files that are contained in this directory.



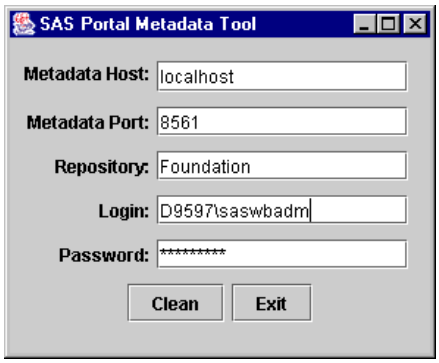
Note: Do not move or rename the `portal−objects.xml` file. This file contains the metadata information that the tool uses to remove the portal−specific metadata.

To run the SAS Portal Metadata Tool:

1. Back up your portal Web application metadata. You can back up the metadata server by using the `smsbakup.sas` autocall macro. For details, see Backing Up Metadata in the *SAS 9.1 Metadata Server: Setup Guide*.
2. Run the `RemovePortalMetadata` tool (`RemovePortalMetadata.bat` for Windows and `RemovePortalMetadata.sh` for Unix, located in the `Tools` directory of your portal Web application installation) to invoke the SAS Portal Metadata Tool. When you run the tool, you can specify the following options on the command line:

   - *−help* displays a list of options
   - *−nogui* does not display the GUI screen
   - *−noprompt* does not display the warning prompt
   - *logger=<logfilename>* outputs log4j messages to the specified file
   - *−host=<host name>* specifies the SAS Metadata Server machine ($SERVICES_OMI_HOST$ property in the install.properties)
   - *−port=<port>* specifies the SAS Metadata Server port ($SERVICES_OMI_PORT$ property in the install.properties file)
   - *repository=<Demo>* specifies the SAS Metadata Server repository ($SERVICES_OMI_REPOSITORY$ property in the install.properties file)
   - *user=<user ID>* specifies the fully qualified user ID for connection to the SAS Metadata Server
   - *pwd=<password>* specifies the password for connection to the SAS Metadata Server

   If you do not specify the `nogui` option, the SAS Portal Metadata Tool main screen appears.



3. Enter the following information for your SAS Metadata Server:
   - **Metadata Host**: Specify the machine name of the portal Web application's SAS Metadata Server.
   - **Metadata Port**: Specify the port of the portal Web application's SAS Metadata Server.
   - **Repository**: Specify the name of your portal Web application's SAS Metadata Repository.
   - **Login** and **Password**: Use the SAS Web Administrator's fully qualified user ID (e.g., `saswbadm`) and password. To use the SAS Portal Metadata Tool to delete the portal−specific metadata, the SAS Web Administrator's credentials (e.g. `saswbadm`) must have "Delete" permissions for the metadata.

   Click **Clean** to start the SAS Portal Metadata Tool.

   The tool runs and displays the logging messages to the screen, or writes the logging messages to a file as specified by the `logging.config` file.

   Note: The amount of metadata that is associated with the portal−specific metadata affects the time it takes to remove that metadata. For example, if 100 users are associated with a particular page of the portal Web application, the tool will take a longer time to remove that particular page of the portal Web application from the metadata.

To change the logging output for the SAS Portal Metadata Tool, you can edit the `logging.config` file and specify the desired logging output configuration. The `logging.config` file follows the Log4j standard. For details about the Log4j standard, see the information for the Log4j product on the Apache Jakarta Web site. The `logging.config` file specifies which messages are output to the following log files:

- error.log
- output.log
- xmlstatements.log

Administration Tools

Enterprise Directory Console

You can use the enterprise directory console to update user metadata in LDAP. You store user information in LDAP for authentication purposes only. For information about how the portal Web application can authenticate users in LDAP, see Understanding the Metadata Servers (LDAP Authentication).

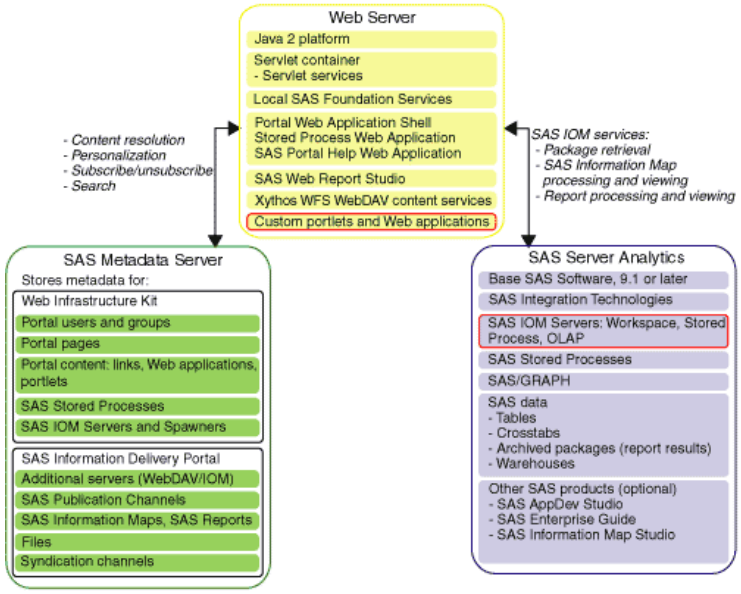
Services, Server, and Portlet Deployment

In order for the components of the portal Web application to work together and provide the desired content, the required services, servers, and portlets must be deployed. This chapter describes the portal Web application's server, service, and portlet deployment and how to redistribute Web applications and servers in order to meet the requirements of your enterprise. For a review of the portal Web application environment and where the servers, services, and portlets are located within the environment, see Understanding the Portal Web Application Components.

- **SAS Foundation Services Deployment**: Depending on your implementation and its integration with other applications, you might deploy the Business Intelligence remote SAS Foundation Services on the same machine as the portal Web application (default installation) or on a remote machine. For details, see Foundation Services Deployment.
- **SAS Server (SAS Workspace Servers, SAS Stored Process Servers, and SAS OLAP Servers) Deployment**: If you want to add certain types of content to the portal Web application, you must ensure that the appropriate SAS servers are configured and deployed (started). For details, see Server Deployment.
- **Portlet Deployment**: For your custom developed portlets to work correctly in the portal Web application, the portlets must be deployed. If you are deploying custom−developed portlets, for information about how to enable portlet deployment and an understanding about how the portal Web application deploys and executes portlets, see Portlet Deployment.

In addition, depending on your enterprise requirements, you might also want to redistribute the servers, services or Web applications that are deployed with the portal Web application. For details, see Redistributing Applications and Servers.

The following diagram shows the components of the portal Web application environment and the components which might be redistributed (in red).



Deployment

SAS Foundation Services Deployment for the Portal

SAS Foundation Services is a set of infrastructure and extension services which support the development of integrated, scalable, and secure applications based on Java. The portal Web application uses the following core foundation services for infrastructure:

- **Connection Service**, for IOM connection management.
- **Discovery Service**, for locating and binding to deployed services.
- **Event Services**, for event notification and information delivery.
- **Information Service**, for repository federation, searching repositories, a common entity interface, and creating personal repositories.
- **Logging Service**, for run−time execution tracing and error tracking.
- **Publish Service**, for access to the Publication Framework.
- **Security Service**, for user authentication, content authorization, action authorization, and task authorization.
- **Session Service**, for context management, resource management, and context passing.
- **Stored Process Service**, for access to stored process execution and result package navigation.
- **User and Authentication Service**, for access to authenticated user context, access to global, solution−wide, and application−specific profiles, and access to personal objects such as ad hoc results, bookmarks, documents, and alerts.

You can use the foundation services to develop custom applications and portlets that integrate with the portal Web application. For details, see Using SAS Foundation Services With the Portal in the *SAS Web Infrastructure Kit Developer's Guide*. For more information about the foundation services, refer to the SAS Foundation Services class documentation.

In order for the portal Web application to access the foundation services, they must be deployed. The default portal Web application installation deploys services using service deployment configurations accessed from XML files. The portal Web application deploys local foundation services; you must start the SAS Services Application to deploy remote foundation services. For details, see SAS Foundation Service Deployment Configuration.

Deployment

Service Deployment Configurations

In order for the portal Web application to access the SAS Foundation Services, the services must be deployed. A service deployment is a collection of foundation services that specifies the data necessary to deploy the services. A service deployment can be a local (accessible within a single Java Virtual Machine (JVM)) or remote service deployment (accessible within a single JVM, but available to other JVM processes). The portal Web application, SAS Services application, and other foundation service−enabled applications use the service deployments to deploy and access the foundation services. For details about service deployments, see Service Deployments in the *SAS Integration Technologies Administrator's Guide.*

You can store the metadata for local and remote service deployment configuration in an XML file or on the SAS Metadata Repository. The portal Web application currently uses XML files to access the service deployment configurations. The foundation services deployment configuration for the portal Web application includes both a local services deployment, `sas_services_idp_local_omr.xml`, and a remote services deployment, `sas_services_idp_remote_omr.xml`. These files contain the following service deployments and service deployment groups:

- **ID Portal Local Services (`sas_services_idp_local_omr.xml`)**.
  - **BI Local Services**: The portal Web application deploys the Authentication Service, Information Service, Logging Services, Session Service, and User Service as a local services deployment. The portal Web application has exclusive access to the locally−deployed services.
  - **BI Stored Process Service**: The SAS Stored Process Web application deploys the Stored Process Service as a local service deployment. The SAS Stored Process Web application has exclusive access to the locally−deployed Stored Process Service.
- **BI Remote Services (`sas_services_idp_remote_omr.xml`)**.
  - **BI Remote Services**: The SAS Services application deploys the Authentication Service, Discovery Service, Information Service, Logging Services, Session Service, and User Service as a remote service deployment and shares the services using a Java Remote Method Invocation (RMI) server. The remote service deployment enables other applications to access the services. To enable remote access to services, the remote services deployment registers the remote services with the Java Remote Method Invocation (RMI) service registry. The portal Web application, and other applications and portlets can then share session and user information by locating and accessing the remote services.

    The remote accessible Session Service enables single sign−on and communication between Web applications by allowing other Web applications, such as the SAS Stored Process Web application to access the remote Session Service.

For more information about how foundation services are deployed and located by the portal Web application and located, accessed, and used by applications and portlets, see SAS Foundation Service Deployment and Use.

Deployment

SAS Foundation Service Deployment and Use

Understanding how the portal Web application deploys and accesses the SAS Foundation Services can help you determine how to distribute your portal Web application implementation. Understanding how other Web applications and portlets use the foundation services can help you to understand how to integrate applications and portlets with the portal Web application. The following sections explain how the portal Web application deploys, distributes, locates and shares foundation services.

For information about developing foundation service−enabled applications and portlets that are integrated with the portal Web application, see Integrating Web Applications With the Portal in the *SAS Web Infrastructure Kit Developer's Guide.* .

How the Portal Web Application Deploys SAS Foundation Services

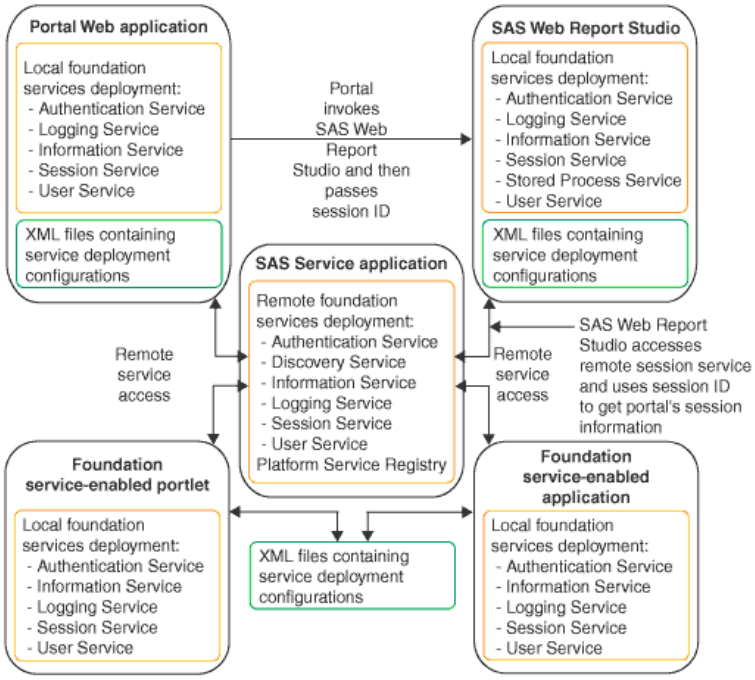
SAS Foundation Services are deployed as follows:

- **For local service deployment**, the portal Web application uses the `sas_metadata_source_client_omr.properties` properties file to locate the portal Web application local service deployment configuration (in the XML local service configuration file, `sas_services_idp_local_omr.xml`) and deploy the local services. The portal Web application has exclusive access to the locally−deployed services. The Stored Process Web application accesses the Stored Process Service local service deployment configuration (from the XML local service configuration file, `sas_services_idp_local_omr.xml`) and deploys the Stored Process Service as a local service.
- **For remote service deployment**, you must use the `StartRemoteServices.bat` utility to start the SAS Services application. (You must start the remote services before you start the servlet container). The SAS Services application uses the `sas_metadata_source_server_omr.properties` properties file to locate the remote service deployment configuration (in the XML remote service configuration file, `sas_services_idp_remote_omr.xml`) and deploy the remote services. All of the remote services are registered with a remote Discovery Service. The remote services registration enables the portal Web application, the SAS Stored Process Web application, and other applications and portlets to use the remote Discovery Service to locate and utilize the remotely−deployed services.

In addition, other applications and portlets might have their own local service deployment configurations in order to locally deploy certain SAS Foundation Services. The applications and portlets can access their local and remote service deployment configurations from an XML configuration file (for the portal Web application remote service deployment) or from the SAS Metadata Repository.

Note: The remote service deployment configurations, whether they reside in an XML file or in the metadata repository, must all contain the same remote service deployment configuration information.

The following diagram shows these components and how they work together.



In the previous diagram, your portal Web application, SAS Services application, SAS Web Report Studio application, and foundation service−enabled portlet and application all access their local and remote service deployment configurations from the SAS Metadata Server. All the applications share the same remote service deployment. In addition, each application has a local service deployment (for its own exclusive access). The SAS Stored Process Web Application (not shown) also accesses its local and remote service deployment configurations from the SAS Metadata Server, deploys its own set of local services, and share sthe same remote service deployment as the other applications.

How the Portal Web Application Components Are Distributed

The default installation deploys the SAS Stored Process Web application on the same machine as the portal Web application (the portal Web application installation machine). The default portal Web application installation also deploys both the local and remote services deployment (SAS Services application) on that same machine. You can move both the SAS Stored Process Web application and the SAS Services application (remote services) to separate machines.

For example, the different components in the previous diagram might exist on the same Web server or on different Web servers. In the diagram, the SAS Stored Process Web application might exist on the same machine as the portal Web application (default installation) or on a machine that can access the remotely−deployed services (SAS Services application). In addition, the remotely−deployed services (SAS Services application) might exist on the same machine as the portal Web application (default installation) or on a separate machine that is accessible to the applications and portlets that need to use the services.

To deploy the SAS Stored Process Web application or the SAS Services application (remote services) on a separate Web server machine, see Redistributing Applications.

How Applications Locate SAS Foundation Services

For information about how applications locate and bind to specific services, see How Applications Locate Foundation Services in the *SAS Integration Technologies Administrator's Guide*.

How the Portal Web Application Shares SAS Foundation Services

An application or portlet can use the foundation services to access the portal Web application's session context. For example, in the previous diagram, the SAS Web Report Studio and portal Web applications use the same remotely−deployed session service. When the portal Web application launches the SAS Web Report Studio application, it passes the portal Web application's session ID to the SAS Web Report Studio application. The SAS Web Report Studio application can then bind to the remote session service and obtain and use the portal Web application's session, user, and context information. This allows the user to seamlessly passthrough to the SAS Web Report Studio application without requiring a separate login.

Note: In order to seamlessly integrate with the portal Web application, SAS Web Report Studio must be able to access the remote service deployment on startup. Therefore, you must start the remote services (by starting the SAS Services application) before starting SAS Web Report Studio. If SAS Web Report Studio cannot access the remote services upon startup, when you start the portal Web application and try to view a report with SAS Web Report Studio, you will not be able to seamlessly access SAS Web Report Studio from the portal Web application; instead, you will need to login to SAS Web Report Studio.

Deployment

Server Deployment

The SAS Web Infrastructure Kit enables you to exploit the analytical and reporting powers of SAS by allowing you to deliver SAS data to the desktops of portal Web application users. From client machines that have only a Web browser installed, authorized portal Web application users can run SAS Stored Processes and return package or streaming results.

In addition, the SAS Information Delivery Portal builds on top of the SAS Web Infrastructure Kit. Through the SAS Information Delivery Portal, authorized users can perform the following functions from client machines that have only a Web browser installed:

- View SAS Information Maps
- Subscribe to SAS publication channels, and view packages that are published to these channels
- Run SAS reports

Before you can add SAS content to the portal Web application shell or SAS Information Delivery Portal, the appropriate servers and spawners must be deployed. In addition, the servers must be started in the appropriate order. (For details, see Starting the Servers). The following table shows the metadata definitions and server deployment that is required for each type of content.

Metadata on the SAS Metadata Server	
Content	**Required Server Definition**
SAS Information Maps	• for relational data, a SAS Workspace Server and Spawner • for multidimensional data, a SAS OLAP Server
Packages	• if published to an archive on a SAS Workspace Server, a SAS Workspace Server and spawner • if published to a Xythos WFS WebDAV server, a WebDAV server • if published to a file, no server definition is needed for the package
Publication Channels	• if publishing to an archive on a SAS Workspace Server, a SAS Workspace Server and spawner • if publishing to an archive on a Xythos WFS WebDAV server, a WebDAV server • if publishing to an archive in the file system, no server definition is needed for the publication channel **Note:** If you are publishing from the portal Web application to a WebDAV persistent store, you must have the Xythos WFS WebDAV server installed.
SAS Reports	

	• for relational data, SAS Workspace Server and spawner • for multidimensional data, a SAS OLAP Server • for storing reports in WebDAV, a WebDAV server
SAS Stored Processes − Package Results	• SAS Workspace Server and spawner • if outputting a package to a Xythos WFS WebDAV server, a WebDAV server
SAS Stored Processes − Streaming Results	SAS Stored Process Server and Multi−User Login

Note: A Xythos WFS WebDAV server is also required for storing files. To store file content for use in the portal Web application shell, you must ensure that a Xythos WFS WebDAV server is deployed. However, if you are only using the Xythos WFS WebDAV server to store files for the portal Web application, you are not required to have a Xythos WFS WebDAV server definition (content metadata) on the SAS Metadata Repository.

For details about SAS server deployment, see SAS Server Metadata. For details about WebDAV server requirements, see WebDAV Server Metadata.

Deployment

SAS Server Metadata

Before you can add SAS content to the portal Web application or SAS Information Delivery Portal, the appropriate servers and spawners must be deployed. In most cases, the appropriate servers and spawners should already have been administered and deployed by one of the following:

- the administrator of the producing application (for SAS Information Maps and SAS Reports)
- the portal Web application or SAS Information Delivery Portal post−installation setup (for SAS Publication Channels and SAS Stored Processes)
- the project install.

However, you should ensure that the metadata administration and deployment is correct. In the case where your initial servers are not defined and deployed, you can refer to the SAS Integration Technologies documentation to create the necessary metadata and startup scripts.

This section outlines the server configuration and startup that is required for each type of content, and provides links to the *SAS Integration Technologies Administrator's Guide* for server setup information.

To ensure that the appropriate servers are setup and started, follow these steps:

1. Verify or Add the Server Metadata.
2. Verify or Create a Spawner or Server Startup Script.

Step 1: Verify or Add the Server Metadata

For each type of content, the appropriate server metadata must be present in the metadata repository. Log in to SAS Management Console as the SAS Administrator and use the Server Manager plug−in to verify or modify the server metadata.

Load−Balancing SAS Stored Process Server

If you want to run stored processes that produce streaming results, the following metadata must be present on the metadata server:

- **SAS Stored Process Server definition**. The "Main − Stored Process Server" is automatically defined when you define a stored process server with the project install or load the portal Web application's initial metadata. The metadata for the load−balancing SAS Stored Process Server includes the following:
    - Server name
    - Host name
    - Connection information, including authentication domain, port number, and connection type
    - Multibridge connection information for load balancing
    - Multi−user login
    - Other information including encryption and server startup command, as required.
- **SAS spawner definition.** The IOM object spawner is a daemon that listens for incoming client requests for IOM services. When the daemon receives a request from a new client, it launches an instance of an IOM server to fulfill the request. A spawner is automatically defined when you define a workspace server with the project install or load the portal Web application's initial metadata. The spawner definition should include the

following:

- ♦ Spawner name
- ♦ Host name
- ♦ Authentication domain name (this must match the domain name of the associated server).

- **Multi−User Login and User definition**. SAS user and login definitions (user name, fully qualified user ID and password, and authentication domain) are a convenient method for providing the credentials necessary for a spawner to start a multi−user server. The SAS General Server group's login is automatically specified as the multi−user login on the Stored Process Server definition when you define a stored process server with the project install or load the portal Web application's initial metadata. The user and login definition for the multi−user login should include the following:

  - ♦ User name
  - ♦ Login information, consisting of the SAS user ID and password needed to access to the SAS server
  - ♦ Authentication domain name.

To add an initial load−balancing stored process server or to add a server to an existing load−balancing cluster, you must plan and setup the load−balancing server and spawner metadata. For details, see Load Balancing Metadata in the *SAS Integration Technologies Administrator's Guide* on the SAS Integration Technologies Web site.

Note: If you add new servers, you must add permission statements to your servlet container's policy file. For details, see Adding Permission Statements for Servers to Policy Files.

SAS Workspace Server

If you want to view SAS Information Maps or SAS reports that use relational data, SAS Publication Channels, or run SAS Stored Processes that produce package results, the following metadata must be present on the metadata server:

- **SAS server definition**. The "Main − Workspace Server" is automatically defined when you define a workspace server with the project install or load the portal Web application's initial metadata. The metadata for the SAS Workspace Server includes the following:

  - ♦ Server name
  - ♦ Host name
  - ♦ Connection information, including authentication domain, port number, and connection type
  - ♦ Other information including encryption, server startup command, and pooling, as required.
- **SAS spawner definition.** The IOM object spawner is a daemon that listens for incoming client requests for IOM services. When the daemon receives a request from a new client, it launches an instance of an IOM server to fulfill the request. A spawner is automatically defined when you define a workspace server with the project install or load the portal Web application's initial metadata. The spawner definition should include the following:

  - ♦ Spawner name
  - ♦ Host name
  - ♦ Authentication domain name (this must match the domain name of the associated server).

To add a new server to a spawner, or to add a new spawner and server, you must plan and setup the appropriate standard server and spawner metadata for your server connection type as follows:

- IOM Bridge connection. For details, see Standard Server Metadata in the *SAS Integration Technologies Administrator's Guide* on the SAS Integration Technologies Web site.
- COM connection. For details, see Standard Server Metadata in the *SAS Integration Technologies Administrator's Guide* on the SAS Integration Technologies Web site.

Note: If you add new servers, you must add permission statements to your servlet container's policy file. For details, see Add Permission Statements for Servers to Policy Files.

SAS OLAP Server

If you want to view SAS Information Maps or SAS reports that use multidimensional data, the following metadata must be present on the metadata server:

- **SAS server definition**. The "Main − OLAP server" is automatically defined when you define a SAS OLAP Server with the project install. The metadata for a SAS OLAP Server includes the following:
  - ♦ Server name
  - ♦ Host name
  - ♦ Connection information, authentication domain, port number, and connection type
  - ♦ Other information including encryption and server startup command, as required.

  To add a new SAS OLAP Server, you must plan for and setup the appropriate standard server metadata for your connection type as follows:
  - ♦ IOM Bridge connection. For details, see Standard Server Metadata in the *SAS Integration Technologies Administrator's Guide* on the SAS Integration Technologies Web site.
  - ♦ COM connection. For details, see Standard Server Metadata in the *SAS Integration Technologies Administrator's Guide* on the SAS Integration Technologies Web site.

Note: If you add a server to your initial server setup, you must add permission statements to your servlet container's policy file. For details, see Add Permission Statements for Servers to Policy Files.

Step 2: Verify or Create a Spawner or Server Startup Script

To access the server's content, the appropriate servers must be started. You can start the SAS Workspace Server and SAS Stored Process Server by administering and invoking an object spawner. You can start the SAS OLAP Server by invoking a SAS OLAP Server startup script.

Note: If you installed with the project install, you might have chosen to startup the spawner and server as services.

- For SAS Workspace and SAS Stored Process Servers, for details about administering and starting an object spawner, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.
- For SAS OLAP Servers, for details about starting the server as a service, see Starting the SAS OLAP Server as a Service in the *SAS OLAP Server 9.1 Administrator's Guide*.

SAS Workspace Server and SAS Stored Process Server

The IOM Object Spawner must be running on the machine where the SAS server runs. To locate the spawner startup script, check the value of the `$IOM_SERVERS_HOME$` property in the `install.properties` file (found in the

PortalConfigure subdirectory of the setup directory). Instructions for administering and starting an object spawner are available from Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*. The following is an example of a spawner command that works with SAS 9.1 and runs the on the Windows platform:

```
@echo off
cd /d "C:\Program Files\SAS\Servers\ObjectSpawner"
echo STARTING OBJECT SPAWNER ...
SET I=0
:LOOP
SET /A I=I+1
IF EXIST spawner_%I%.log GOTO LOOP

start/min "SAS Object Spawner" "C:\Program Files\SAS\SAS 9.1\objspawn"
                −sasSpawnercn "<machine name> Spawner"
                −xmlConfigFile OMRConfig.xml −slf spawner_%I%.log
```

where

"C:\Program Files\SAS\SAS 9.1\"
: specifies the SAS installation folder

OMRConfig.xml
: specifies the metadata configuration file that you created using the SAS METACONN utility. (For details about using the configuration program to create the metadata configuration file, see Creating a Metadata Configuration File in SAS in the *SAS Integration Technologies Administrator's Guide*). When you create the metadata configuration file, for the user ID and password, use the $SERVICES_OMI_USER_ID$ and $SERVICES_OMI_USER_PASSWORD$ properties from your install.properties file.

−sasSpawnercn
: specifies the name of the spawner definition in the metadata repository. For the basic install, this option should be set to the name of the SAS server machine (check the value of the STP_HOST property in the install.properties file found in the PortalConfigure subdirectory of the setup directory), followed by " Spawner" (e.g. localhost Spawner).

SAS OLAP Server

If you do not start the SAS OLAP Server as a service, you must run a startup script in order to start the SAS OLAP Server. To start a SAS OLAP Server, you must run a server startup script. For details about server startup scripts, see Starting a Server in the *SAS Integration Technologies Administrator's Guide* The following is an example of an OLAP startup script that works with SAS 9.1 and runs the SAS OLAP Server on the Windows platform at port number 5701:

```
@echo on
set olapport=5701
set scriptdir=c:\Program Files\SAS\Servers\olap%olapport%
cd /d "%scriptdir%"
"C:\Program Files\SAS\SAS 9.1\sas.exe" −log olap.log
−noterminal −nologo −objectserver
−objectserverparms "nosecurity protocol=bridge port=%stpport% multiuser
instantiate classfactory='15931E31−667F−11D5−8804−00C04F35AC8C'"
```

When the previously identified prerequisites are in place, you can proceed to add SAS content as described in the following topics:

- Adding SAS Information Maps
- Adding SAS Packages

- Adding SAS Publication Channels
- Adding SAS Reports
- Adding SAS Stored Processes

Deployment

SAS Server Metadata Table

When you set up the portal Web application using the basic or project install, you configure initial server configurations by loading the initial metadata or running the SAS Configuration Wizard.

The following table details the server configurations that might be set up.

Initial IOM Server Configurations					
Server	**Location and Type of Server Startup**	**Credentials Used for Server Startup and SAS Metadata Server Connection**	**Metadata**	**Credentials Used in Metadata Configuration**	**Modifying the Configuration**
SAS Workspace Server	**Spawner startup script**, located in the `ObjectSpawner` subdirectory of your install. See Spawner Overview and Invoking the Spawner.	**To start the server**, the spawner uses the client's credentials to launch the SAS Workspace Server. **To connect to the SAS Metadata Server**, the `ObjectSpawner` subdirectory also contains the spawner's metadata configuration file, `OMRConfig.xml`, which specifies the SAS Trusted User's user ID to connect to the SAS Metadata Server.	**Standard logical server definition** named Main−Logical Workspace Server.	N/A	Pooling. See Pooling Overview and Pooling Metadata. Adding a new server and spawner. See Standard Server Metadata.
			Server definition named Main − Workspace Server	N/A	
			Spawner definition	N/A	Adding a new server with a COM connection. See Standard Server Metadata.
SAS Stored Process Server	**Spawner startup script**, located in the `ObjectSpawner` subdirectory of your installation. Modifying the startup script. See Spawner Overview and Invoking the Spawner.	**To start the server**, the spawner uses the login credentials owned by the SAS General Servers group to launch the SAS Stored Process Server. **To connect to the SAS Metadata Server**, the `ObjectSpawner`	**Load−balancing logical server definition** named Main−Logical Stored Process Server	**Logical server credentials**, which are specified as the group login of the SAS General Servers group.	Load balancing. See Load Balancing Overview and Load Balancing Metadata. Adding a new server and spawner. See Standard Server Metadata.
			Load−balancing server definition named Main − Stored Process	Multi−user login, which is specified as the group login of the SAS	

		subdirectory also contains the spawner's metadata configuration file, OMRConfig.xml, which specifies the SAS Trusted User's user ID to connect to the SAS Metadata Server.	Server	General Servers group. This login is the user ID under which the SAS Stored Process Server runs.	
			Spawner definition	N/A	
SAS OLAP Server	**Startup script or service startup**, located in the `OLAPServer` subdirectory of your installation. Modifying the startup script or service configuration. See Creating and Modifying the SAS OLAP Server Script and Starting the SAS OLAP Server as a Service in the *SAS OLAP Server Administrator's Guide*.	**To start the server (if not started as a service)**, the SAS user credentials are used. **To connect to the SAS Metadata Server**, the SAS OLAP server uses the SAS Trusted User's user ID.	**Standard logical server definition** named Main−Logical OLAP Server	N/A	Adding a COM connection to the server. See Adding a COM Connection. Adding a New Server Definition. See Standard OLAP Server Metadata (IOM Bridge) and Standard Server Metadata (COM) . Also see the Server Manager Help in SAS Management Console.
			Server definition named Main − OLAP Server	N/A	

Deployment

WebDAV Server Metadata

To enable the portal Web application shell to search for files, packages, and reports in the Xythos WebFile Server (WFS) WebDAV server's repository, the portal Web application does not require a definition for the WebDAV server on the SAS Metadata Server. However, in the following cases, you must ensure that you have a WebDAV server definition (for the Xythos WFS WebDAV server) on the SAS Metadata Server:

- when you run SAS Stored Processes that publish to a Xythos WFS WebDAV server.
- when you configure WebDAV−based SAS publication channels or WebDAV package subscribers.
- when you run other applications (such as SAS Web Report Studio) that require a WebDAV server definition.

When you installed the Xythos WFS WebDAV Server, you specified an authentication domain for the WebDAV server. To check this value, look at the `$DAV_DOMAIN$` value in `install.properties` (located in the `PortalConfigure` directory of your install). When you define the WebDAV server definition on the metadata server, you should use this same authentication domain.

For information about using SAS Management Console to define WebDAV servers on the SAS Metadata Server, see Administering HTTP Servers and WebDAV in the *SAS Integration Technologies Administrator's Guide*

Important Note: With the exception of reports, which can be stored on any type of WebDAV server, the portal Web application can only access Xythos WFS WebDAV server content (for SAS publication channels, files, and SAS Stored Process package output).

Important Note: It is recommended that the base path for the Xythos WFS WebDAV server be a blank value. If you need to reconfigure the base path for the Xythos WFS WebDAV server, see Reconfiguring the Base Path for the Xythos WFS WebDAV Server.

Reconfiguring the Base Path for the Xythos WFS WebDAV Server

To reconfigure the base path for the Xythos WFS WebDAV Server as a blank value:

1. Edit the `install.properties` file (found in the `PortalConfigure` subdirectory of the installation directory) in a text editor.

   Locate the following line and specify the value as blank:

   ```
   $DAV_BASE$=
   ```
2. Run the `configure_wik.bat` utility to create and copy the new service deployment configurations.
3. If you configured the WebDAV server in the metadata, modify the base path in the WebDAV server definition. For details, see the SAS Management Console online Help for the Server Manager.

Deployment

Redistributing Applications and Servers

Depending on the performance considerations of your implementation, you might want to redistribute the application pieces of the portal Web application, or the servers upon which they rely.

The portal Web application installation deploys the following applications:

- portal Web application (which includes SAS Web Report Viewer)
- SAS Services application, which deploys remote services shared using a Java RMI server on the SAS Service application's host machine
- SAS Stored Process Web application
- SAS documentation Web application (always deployed on the portal Web application's machine)

In addition, you might have installed the SAS Web Report Studio Web application.

The portal Web application installation deploys one or more of the following SAS servers:

- SAS Metadata Server (required)
- SAS Stored Process Server (optional)
- SAS Workspace Server (optional)
- SAS OLAP Server (optional)

The following scenarios show two best practice cases for your server and service distribution:

- Best Practices: Scenario 1
- Best Practices: Scenario 2

Regardless of where they are located, you must ensure your servers and applications are started in the appropriate order. For details, see Starting the Servers.

You can redistribute applications and servers as follows:

- **Applications**. The default installation deploys the SAS Stored Process Web application and the SAS Services application on the same machine as the portal Web application (the portal Web application's installation machine). You can move both the Stored Process Web application and the SAS Services application (remote services and Java RMI server) to separate machines.

  Note: It is recommended that you leave the SAS Services application (remote services and Java RMI server) on the same machine as the portal Web application.

  For details about redistributing Web and other applications, see Redistributing Applications.
- **Servers**. When you installed the portal Web application and specified the configuration information, you specified the machine and port for the servers. However, after your initial installation, you might be required to move one or more of these servers to a different machine. Before you move servers to machines with different operating systems, be sure that you understand and have planned for your authentication domain(s). To understand authentication domains, see Planning for Authentication Domains. In addition, when you move servers to a new machine, you must update any permission statements for the servers. For details, see Adding Permissions for Servers to Policy Files.

Note: For performance reasons, it is recommended that you install the SAS Metadata Server on a separate machine.

For details about moving server locations, see the following sections:

- Moving the SAS Stored Process Server
- Moving the SAS Workspace Server
- Moving the SAS OLAP Server
- Moving the SAS Stored Process Server and SAS Workspace Server to the Same New Machine
- Moving the SAS Stored Process Server and SAS Workspace Server to Separate Machines

Deployment

Best Practices: Scenario 1

The default portal Web application installation installs all of the servers and Web application components on the same machine and Web server. If you used the project install, you might already have distributed servers and mid−tier components. However, to enable better performance, you can redistribute the server tier and mid−tier components. The following scenario shows a best practices implementation of your mid−tier and server tier for the portal Web application and its components.

Mid−tier

- ◊ **Web Server #1:**
  - · Portal Web application
  - · SAS Services Application.
- ◊ **Web Server #2:** SAS Stored Process Web application. For details about moving the SAS Stored Process Web application, see Redistributing the SAS Stored Process Web application.

Server tier

- ◊ **Machine #1:** SAS Metadata Server. For details about moving the SAS Metadata Server, see Moving the SAS Metadata Server.
- ◊ **Machine #2:**
  - · SAS Stored Process Server and SAS Workspace Server (optional). For details about moving both the SAS Stored Process and SAS Workspace Server to a new machine, see Moving Both the SAS Stored Process Server and SAS Workspace Server to the Same New Machine. If you have only installed the SAS Stored Process Server, see Moving the SAS Stored Process Server.
  - · SAS OLAP Server (optional). For details about moving the SAS OLAP Server to a new machine, see Moving the SAS OLAP Server.

Deployment

Best Practices: Scenario 2

The default portal Web application installation installs all of the servers and Web application components on the same machine and Web server. If you used the project install, you might already have distributed servers and mid−tier components. However, to enable better performance, you can redistribute the server and mid−tier components. The following scenario shows a best practices implementation of your mid−tier and server tier for the portal Web application and its components.

Mid−tier

- ◊ **Web Server #1:** Portal Web application.
- ◊ **Web Server #2:** SAS Stored Process Web application. For details about moving the SAS Stored Process Web application, see Redistributing the SAS Stored Process Web application.
- ◊ **Web Server #3:** SAS Services Application. For details about moving the SAS Services application (and associated Java RMI server), see Redistributing the SAS Services Application (and Java RMI Server).

Server tier

- ◊ **Machine #1:** SAS Metadata Server.
- ◊ **Machine #2:** SAS Stored Process Server. For details about moving both the SAS Stored Process Server and SAS Workspace Server to a new machine, see Moving the SAS Stored Process Server and SAS Workspace Server to Separate Machines. If you have only installed the SAS Stored Process Server, see Moving the SAS Stored Process Server.
- ◊ **Machine #3:**

  - · SAS Workspace Server (optional). For details about moving both the SAS Stored Process and Workspace Server to a new machine, see Moving the SAS Stored Process Server and SAS Workspace Server to Separate Machines.
  - · SAS OLAP Server (optional). For details about moving the SAS OLAP Server to a new machine, see Moving the SAS OLAP Server.

Deployment

Redistributing Applications

The portal Web application installation contains the following applications:

- **portal Web application** (which includes SAS Web Report Viewer if SAS Information Delivery Portal is installed), a portal−like Web application shell that is used by other SAS Web applications.
- **SAS Services application**, a command line application that manages services that are shared by SAS applications.
- **SAS Stored Process Web application**, a Web application that enables stored processes to be run from the Web.
- **SAS documentation Web application**, a Web application that manages SAS documentation (always deployed on the portal Web application's machine).

In addition, you might have installed the SAS Web Report Studio Web application.

You might want to move the SAS Stored Process Web application, SAS Services application, SAS Web Report Viewer, or SAS Web Report Studio Web application to separate machines or servlet containers. Where you deploy your applications depends on the size and organization of your implementation, and your performance considerations. For details about redistributing applications, see the following sections:

Redistributing the SAS Services Application (and Java RMI Server)

The SAS Services application deploys the remote services for access by the portal Web application, the SAS Stored Process application, remote portlets, and other applications such as SAS Web Report Studio. The SAS Services application uses a Java RMI server on its host machine to share the remote services with other applications. The remote services deployment configuration of the portal Web application gives you the flexibility to distribute the remote services as required. The recommended configuration (the default installation) is for both the local and remote foundation services to run on the same machine.

However, for some implementations, you might want to have the remote services (SAS Services application) deployed on a separate machine that the portlets and applications (portal Web application, SAS Stored Process Web application, and other portlets and applications (such as SAS Web Report Studio)) can access. To redistribute the SAS Services application to a new machine, follow these steps:

1. On the new machine, install the SAS Web Infrastructure Kit. In the RMI server host field of the install program, specify the new remote SAS Foundation Services host machine.
2. Perform the following post−installation instructions in the `wik_readme.html` file:

    a. Step 6: Run configuration scripts.
    b. Step 10: Prepare the servlet container environment.
    c. Step 13: Set up the SAS Services application.
    d. Step 15: Tune Web applications.
3. On the portal Web application and SAS Stored Process Web application's machine, follow these steps:

   a. Shut down the existing SAS Services application.
   b. Shut down the servlet container for the portal Web application and the SAS Stored Process Web application.
   c. Remove cached JSP and servlet files. Remove any expanded files (produced from the WAR file). Remove any deployed WAR files. For details, see Step 11 of the `wik_readme.html` file.
4. Use a text editor to edit the `install.properties` file (located in the `PortalConfigure` subdirectory of the installation directory).

   Locate the following lines:

   ```
   # RMI
   $SERVICES_RMI_PORT$=5099
   $SERVICES_RMI_HOST$=localhost
   ```

   The remote services deployment uses a Java RMI registry to register remote services. These lines specify the machine and port on which your Java RMI service registry runs. Replace the `$SERVICES_RMI_HOST$` entry value with the new machine name where the remote foundation services will be deployed (by the SAS Services application). For example, `$SERVICES_RMI_HOST$=a1234.us.abc.com`.
5. Run the `configure_wik.bat` utility to create new service deployment configurations and new `SASStoredProcess.war` and `Portal.war` files.
6. Deploy the `Portal.war` to the servlet container on your portal Web application's web server machine (for example, `c:\jakarta-tomcat-4.1.18\webapps`).
7. Ensure that other applications and portlets can access the remote service deployment configuration.

   You must enable the other applications and portlets to access the remote service deployment configuration from an XML file that contains the remote services deployment.

   To enable an application or portlet to access the remote service deployment XML file, copy the new remote services deployment configuration XML file (`sas_services_idp_remote_omr.xml`, found in the `SAS Foundation Services\Deployments\RemoteServices` subdirectory of the basic install directory and in the `Deployments\RemoteServices` directory of the project install directory) to a file with the file name of the remote services deployment configuration XML file for that application or portlet.

   For example, if you have installed the portal Web application using the basic or project install, and if you are integrating with SAS Web Report Studio, you must ensure that the service deployment XML file for SAS Web Report Studio contains (or points to) the remote service deployment configuration used by the SAS Services application (`sas_services_idp_remote_omr.xml`). SAS Web Report Studio uses the file name `sas_metadata_source_remote.xml` for its remote services deployment configuration. For SAS Web Report Studio to access the new remote services deployment configuration, you must copy the `sas_services_idp_remote_omr.xml` file to the `sas_metadata_source_remote.xml` file.
8. Ensure that other applications and portlets have the appropriate permissions in their policy files to enable access to the new machine for the SAS Services application. For details, see Adding Permission Statements to Policy Files.
9. On the SAS Service application's machine, run the `StartRemoteServices.bat` file to start the remote foundation services.
10. On the portal Web application's machine and the SAS Stored Process Web application's machine, restart the servlet container for the portal Web application and SAS Stored Process Web application.

Redistributing the SAS Stored Process Web Application

To redistribute the SAS Stored Process Web application to a new machine, follow these steps:

1. Uninstall the SAS Stored Process Web application from the servlet container for the portal Web application.
2. On the new machine, install the SAS Web Infrastructure Kit. In the install program, be sure to specify the appropriate RMI Server host and port where your SAS Services application will deploy the remote services. After installation, perform ONLY the following post−installation instructions:

    a. Step 6: Run configuration scripts.
    b. Step 10: Prepare the servlet container environment.
    c. Step 11: Deploy the Web application files into the servlet container. **Note:** Deploy ONLY the `SASStoredProcess.war` file into the servlet container.
    d. Step 15: Tune Web applications.
3. On your portal Web application machine, follow these steps:

    a. Edit the `InfrastructureContent.xml` file that is located in the `\Portal\WEB−INF\content` directory of your servlet container.

    Note: You could also edit this file directly in your servlet container. However, if you redeploy the `Portal.war` file, you will overwrite the changes in `InfrastructureContent.xml`.
    b. Add the URL for the host name (and if required, the port number) of the new machine for the SAS Stored Process Web application, as shown in the following example:

```
<Content
interface="com.sas.services.storedprocess.metadata.
   StoredProcessInterface"
category="storedprocess"
icon="StoredProcess.image"
viewer="http://host name:port number
/SASStoredProcess/do?_action=form,properties"
isViewerExternal="true"
appendSessionInfo="true"
passObjectInSession="false"
searchFilter="com.sas.services.storedprocess.metadata.
   StoredProcessFilter,com.sas.portal.
   filters.StoredProcessAttributeFilter"
searchRepositories="OMR"
version="2.0">
</Content>
```

    c. Run the `configure_wik.bat` utility to create a new `Portal.war` file
    d. Deploy the `Portal.war` to the servlet container on your portal Web application's web server machine (for example, `c:\jakarta−tomcat−4.1.18\webapps`).

Redistributing SAS Web Report Viewer

To redistribute SAS Web Report Viewer application to a new machine or servlet container, follow these steps:

1. Deploy the `sas.webreportviewer.war` file (from the servlet container on the portal Web application's machine) to the new servlet container.
2. On your portal Web application machine, follow these steps:

a. Edit the `PortalContent.xml` file that is located in the `\Portal\WEB-INF\content` directory of your servlet container.

   Note: You could also edit this file directly in your servlet container. However, if you redeploy the `Portal.war` file, you will overwrite the changes in `PortalContent.xml`.

b. Add the URL for the host name (and if required, the port number) of the new machine for the SAS Web Report Viewer application, as shown in the following example:

```
<Content interface="com.sas.report.repository.ReportEntryInterface"
 category="report"
 icon="Report.image"
 isViewerExternal="true"
 viewer="http://host name:port number
 /sas.webreportviewer/logonFromPortal.do"
 appendSessionInfo="true"
 newViewerWindow="true"
 passObjectInSession="false"
 searchFilter="com.sas.portal.filters.
 PortalReportFilter,com.sas.portal.filters.
 PortalReportAttributeFilter"
 searchRepositories="OMR"
 version="2.0">
 </Content>
```

c. Run the `configure_wik.bat` utility to create a new `Portal.war` file.

d. Copy the `Portal.war` to the servlet container on your portal Web application's web server machine (for example, `c:\jakarta-tomcat-4.1.18\webapps`).

Redistributing the SAS Web Report Studio Application

To redistribute the SAS Web Report Studio Web application to a new machine or servlet container, you must ensure that the application can access the remote service deployment that is deployed by the SAS Services application.

If you have installed the portal Web application using the basic or project install, and if you are integrating with the SAS Web Report Studio application, you must ensure that the service deployment XML file for the SAS Web Report Studio contains (or points to) the remote service deployment configuration used by the SAS Services application (`sas_services_idp_remote_omr.xml`, found in the `SAS Foundation Services\Deployments\RemoteServices` directory of the basic install and the `Deployments\RemoteServices` directory of the project install).

For example, the SAS Web Report Studio application uses the file name `sas_metadata_source_remote.xml` for its remote services deployment configuration. For the SAS Web Report Studio application to access the new remote services deployment configuration, you must copy the `sas_services_idp_remote_omr.xml` file to the `sas_metadata_source_remote.xml` file.

Note: In order to seamlessly integrate with the portal Web application, the SAS Web Report Studio must be able to access the remote service deployment on startup. Therefore, you must start the remote services (by starting the SAS Services application) before starting the SAS Web Report Studio application. If the SAS Web Report Studio application cannot access the remote services upon startup, when you start the portal Web application and try to view a report with the SAS Web Report Studio application, you will not be able to seamlessly access the SAS Web Report Studio from the portal Web application; instead, you will need to login to the SAS Web Report Studio application.

Deployment

Moving the SAS Metadata Server

Important Note: In addition to the configuration outlined in the following section, if you move the SAS Metadata Server to a machine with a different operating system, you might need to add or modify the login definition that is used to access the SAS Metadata Server. Use the User Manager plug−in to SAS Management Console to define the following new field values in a new login definition or to modify the following field values in an existing login definition:

- **new authentication domain for other IOM servers**. When you move the server, you might need to reconfigure other IOM servers for a new authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
- **user ID**. When you move a SAS Metadata Server, you might need to change the fully−qualified user ID that is used to access the server.
- **password**. If the user ID is only used to access the SAS Metadata Server, a password is not required. To access other servers, you must specify a password in the login credentials

To move the SAS Metadata Server to a different machine, follow these steps:

1. Shut down the servlet container for the portal Web application and the SAS Stored Process Web application.
2. Open the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory) in a text editor:

    a. Locate the following lines:

    ```
    $SERVICES_OMI_HOST$=localhost
    $SERVICES_OMI_PORT$=8561
    ```

    These lines specify the machine and port of your SAS Metadata Server.

    b. Replace the `$SERVICES_OMI_HOST$` entry value with the new machine name of your SAS Metadata Server. For example, `$SERVICES_OMI_HOST$=a1234.us.abc.com`.

    c. If you are changing the default port of the SAS Metadata Server, replace the `$SERVICES_OMI_PORT$` entry value with the new port of your SAS Metadata Server.

    d. Locate the following lines:

    ```
    $SERVICES_OMI_USER_ID$=sasadm
    $SERVICES_OMI_USER_PASSWORD$={sas001}QWRtaW4xMjM=
    $SERVICES_OMI_USER_NAME$=sasadm
    $PORTAL_GUEST_ID$=sasguest
    $PORTAL_GUEST_PASSWORD$={sas001}R3Vlc3QxMjM=
    $PORTAL_GUEST_NAME$=sasguest
    $PORTAL_ADMIN_ID$=saswbadm
    $PORTAL_ADMIN_PASSWORD$={sas001}QWRtaW4xMjM=
    $PORTAL_ADMIN_NAME$=SAS Web Administrator
    $PORTAL_DEMO_ID$=sasdemo
    $PORTAL_DEMO_PASSWORD$={sas001}RGVtbzEyMw==
    $PORTAL_DEMO_NAME$=SAS Demo
    ```

    The lines that are in bold type specify the user IDs for the initial portal Web application users.

    e. If necessary, change the user IDs to reflect the fully qualified user ID for the new operating system.
3. Run the `configure_wik.bat` utility to create new service deployment configurations and new `SASStoredProcess.war` and `Portal.war` files
4. Deploy the `Portal.war` to the servlet container on your portal Web application's machine.

5. Deploy the `SASStoredProcess.war` file to the servlet container on your Stored Process Web application's machine.
6. To set up the new SAS Metadata Server (including the user and group accounts for the appropriate authentication provider) on the new machine, ensure that you have performed the necessary setup for your authentication type:

    - **Host Authentication**. For details, see Setting up Host Authentication.
    - **LDAP Server Authentication**. For details, see Setting up LDAP Server Authentication.
    - **Microsoft Active Directory Server Authentication**. For details, see Setting up Microsoft Active Directory Server Authentication.
    - **Web Server (Trusted Realm) Authentication**. For details, see Setting up Web Server (Trusted Realm) Authentication.
7. Load the portal Web application's metadata to the SAS Metadata Repository in one of the following ways:

    - Load the initial metadata by following the instructions in Step 8 of the `wik_readme.html` file. For information about localization between machines, see the Installation chapter.
    - Use SAS Management Console to define the appropriate metadata. For details about defining the appropriate metadata, see Understanding Metadata Administration and the appropriate sections in the Deployment and Content chapters.
    - Move or copy the SAS Metadata Repository. For details, see Moving or Copying a Repository in the *SAS 9.1 Metadata Server: Setup Guide*.
    - If you are not starting the server as a service, ensure that the SAS user can authenticate against the host authentication provider for the machine.

Deployment

Moving the SAS Stored Process Server

If you have used the project install or basic install to install the SAS Stored Process Server on a separate machine from the SAS Workspace Server, you can use the instructions in this section to move the server to a new machine.

Important Note: In addition to changing the machine name (and optionally, port number), if you move a server to a machine with a different operating system or to a machine with an operating system other than Windows, you might need to reconfigure the following:

- **accounts for authentication**. You might need to define accounts on the authentication provider for the new server machine.
- **metadata on the SAS Metadata Server**. The following metadata definitions might require reconfiguration or additional configuration:
    - ♦ server definition. On the server definition, you might need to use the Server Manager plug−in to SAS Management Console to change the following parameters:
        - ◊ **SAS startup command.** You might need to change the startup command for the new operating system.
        - ◊ **authentication domain**. When you move a server, you might need to set up an additional authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
    - ♦ login definitions. For the login definitions that access the server and the login definitions that are used in the load−balancing configuration (e.g. the SAS Guest user's login), you might need to use the User Manager plug−in to SAS Management Console to do one or more of the following:
        - ◊ define a new login definition. When you move a server, you might need to create a new login definition for the new authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
        - ◊ define a new login definition for a different authentication process. When you move a server, you might need to create a new login definition with credentials to access a server in a different operating system within the default authentication domain.
        - ◊ change the format of the user ID in the login definition. When you move a server, you might need to change the fully−qualified user ID for any login credentials used to access that server.
    - ♦ stored process definitions. You might need to use the Stored Process Manager plug−in to SAS Management Console to specify a new location for your stored process repository.
- **spawner startup command**. If you change operating systems when you move machines, you might need to change the spawner startup command. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.

To move the SAS Stored Process Server to a different machine, follow these steps:

1. Use SAS Management Console to reconfigure the server definition for the new machine:

    a. Open SAS Management Console and connect to a metadata repository.
    b. In the SAS Management Console navigation tree, locate and select the server object (e.g., Main − Stored Process Server) that you want to modify.
    c. In the Display area, for each server connection, follow these steps:

        i. Select and right−click the connection definition, then select **Properties** from the pop−up menu.
        ii. Select the Options tab.
        iii. Change the **Host Name** to the host name of the new machine for your server.

iv. If you are changing the port, change the **Port** to the new port for your server.
v. If you need to change the authentication domain, click **New** and define the new **Authentication Domain** for your server.
vi. Click **OK**.

d. If you need to change the server startup command, select and right−click the server object, then select **Properties** from the pop−up menu. Select the Options tab and change the **Command** field.
e. Click **OK** to save the new configuration to the metadata repository.

2. Use SAS Management Console to reconfigure the spawner definition for the new machine:

   a. In the SAS Management Console navigation tree, locate the spawner object, then right−click the spawner definition, and select **Properties** from the pop−up menu.
   b. If your spawner name contains the machine name, change the **Name** field to specify the name of the new machine.
   c. Select the Options tab.
   d. Change the **Associated Machine** to the host name of the new machine for your server.
   e. If you have any other servers associated with the spawner, select the Servers tab. In the **Selected servers** list box, select the other servers and move them to the **Available servers** list box. Click **OK**. You must then define a new spawner for these servers.
   f. If you are changing the port of either the operator connection or load−balancing connection, in the Display area, select the connection, then right−click and select **Properties** from the pop−up menu. Select the Options tab and change the **Port** to the new port for your spawner connection.

      If you changed the server's authentication domain, select the same new **Authentication Domain** for your spawner.
   g. Click **OK** to save the new configuration to the metadata repository.

3. Edit the portal Web application and SAS Stored Process application's policy files to specify the location of the new server machine. For details, see Adding Permissions for Servers to Policy Files.
4. Install SAS 9.1 or higher and SAS Integration Technologies on the new machine.
5. Copy your metadata configuration file (XML file) and spawner startup script from your spawner configuration directory to the same directory on the new machine. If necessary, change the spawner startup script for the new machine. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.
6. Create a directory for stored process server log files. The recommended directory name is `STPDemo`, and the recommended location is the server home location that you specified when you ran the install program (for example, `C:\Program Files\SAS\Servers\STPDemo`.)

   If you do not remember the server home location, see the `$STP_HOME$` property in the `install.properties` file.
7. Ensure that the multi−user login (specified in the **Advanced Options** for the Stored Process Server definition as the login owned by the SAS General Server group) can authenticate against the host authentication provider for the SAS Stored Process Server's machine. On Windows NT and Windows 2000, give this account the Act as part of the Operating System user right.
8. Give the shared account for the SAS General Server group "Write" permission to the stored process log directory.
9. Ensure that the SAS user can authenticate against the host authentication provider for the machine.
10. Ensure that users who need to access the server are defined for the machine's host authentication provider.

When you are finished modifying the server and spawner definitions, do the following:

- if you have added a new authentication domain for the machine, do both of the following:

    - use the User Manager plug−in to SAS Management Console to add a login definition for access to the server. For details, see Defining Logins for Multiple Authentication Domains.
    - use the User Manager plug−in to SAS Management Console to modify the login definition for the SAS General Server group login. Modify the login definition to specify the new authentication, and, if required, the new user ID credentials.
- if you have changed operating systems and need to modify user credentials, use the User Manager plug−in to SAS Management Console to modify user and group login definition for the new user ID credentials of the new machine.
- if you need to move the stored process repositories to a different directory, use the Stored Process Manager plug−in to SAS Management Console to modify the stored process definition and change the **Source Repository** field on the Execution tab of the stored process definition.
- if your stored process definitions reference content on the old stored process or workspace server machine, you must add the content to the directory you defined in the stored process definition.

Deployment

Moving the SAS Workspace Server

If you have used the project intall or basic install to install the SAS Workspace server on a machine separate from the SAS Stored Process Server, you can use the instructions in this section to move the server to a new machine.

Important Note: In addition to changing the machine name (and optionally, port number), if you move a server to a machine with a different operating system or to a machine with an operating system other than Windows, you might need to reconfigure the following:

- **accounts for authentication**. You might need to define accounts on the authentication provider for the new server machine.
- **metadata on the SAS Metadata Server**. The following metadata definitions might require re−configuration or additional configuration:
    - ♦ server definition. On the server definition, you might need to use the Server Manager plug−in to SAS Management Console to change the following parameters:
        - ◊ **SAS startup command.** You might need to change the startup command for the new operating system.
        - ◊ **authentication domain**. When you move a server, you might need to set up an additional authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
    - ♦ login definitions. For the login definitions that access the server and the login definitions that are used in the load−balancing configuration (e.g. the SAS Guest user's login), you might need to use the User Manager plug−in to SAS Management Console to do one or more of the following:
        - ◊ define a new login definition. When you move a server, you might need to create a new login definition for the new authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
        - ◊ define a new login definition for a different authentication process. When you move a server, you might need to create a new login definition with credentials to access a server in a different operating system within the default authentication domain.
        - ◊ change the format of the user ID in the login definition. When you move a server, you might need to change the fully−qualified user ID for any login credentials used to access that server.
    - ♦ stored process definitions. You might need to use the Stored Process Manager plug−in to SAS Management Console to specify a new location for your stored process repository.
- **spawner startup command**. If you change operating systems when you move machines, you might need to change the spawner startup command. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.

To move the SAS Workspace server to a different machine, follow these steps:

1. Use SAS Management Console to reconfigure the SAS Workspace Server definition for the new machine:

    a. Open SAS Management Console and connect to a metadata repository.
    b. In the SAS Management Console navigation tree, locate and select the server object (e.g., Main − Workspace Server) that you want to modify.
    c. In the Display area, for each server connection, follow these steps:

        i. Select and right−click the connection definition, then select **Properties** from the pop−up menu.
        ii. Select the Options tab.
        iii. Change the **Host Name** to the host name of the new machine for your server.

iv. If you are changing the port, change the **Port** to the port of the new port for your server.
v. If you need to change the authentication domain, click **New** and define the new **Authentication Domain** for your server.
vi. Click **OK**.

d. If you need to change the server startup command, select and right−click the server object, then select **Properties** from the pop−up menu. Select the Options tab and change the **Command** field.
e. Click **OK** to save the new configuration to the metadata repository.

2. Use SAS Management Console to reconfigure the spawner definition for the new machine:

a. In the SAS Management Console navigation tree, locate and select the spawner definition, then right−click and select **Properties** from the pop−up menu.
b. If your spawner name contains the machine name, change the **Name** field to specify the name of the new machine.
c. Select the Options tab.
d. Change the **Host Name** to the host name of the new machine for your server.
e. Click **OK**.
f. If you have any other servers associated with the spawner, select the Servers tab. In the **Selected servers** list box, select the other servers and move them to the **Available servers** list box. Click **OK**. You must then define a new spawner for these servers.
g. If you are changing the port of either the operator connection or load−balancing connection, in the Display area, select the connection, then right−click and select **Properties** from the pop−up menu. Select the Options tab and change the **Port** to the new port for your spawner connection.

If you changed the server's authentication domain, select the same new **Authentication Domain** for your spawner.

h. Click **OK** to save the new configuration to the metadata repository.

3. Edit the portal Web application and SAS Stored Process application's policy files to specify the locations of the new server machine. For details, see Adding Permissions for Servers to Policy Files.
4. Install SAS 9.1 or higher and SAS Integration Technologies on the new machine.
5. Copy your metadata configuration file (XML file) and spawner startup script from your spawner configuration directory to the same directory on the new machine. If necessary, change the spawner startup script for the new machine. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.
6. Ensure that the SAS user can authenticate against the host authentication provider for the machine.
7. Ensure that users who need to access the server are defined for the machine's host authentication provider.

When you are finished modifying the server and spawner definitions:

- if you have added a new authentication domain for the machine, do both of the following:
  - use the User Manager plug−in to SAS Management Console to add a login definition for access to the server. For details, see Defining Logins for Multiple Authentication Domains.
  - use the User Manager plug−in to SAS Management Console to modify the login definition for the SAS General Server group login. Modify the login definition to specify the new authentication, and, if required, the new user ID credentials.
- if you have changed operating systems and need to modify user credentials, use the User Manager plug−in to SAS Management Console to modify user and group login definition for the new user ID credentials of the new machine.
- if you need to move the stored process repositories to a different directory, use the Stored Process Manager plug−in to SAS Management Console to modify the stored process definition and change the **Source Repository** field on the Execution tab of the stored process definition.

- if your stored process definitions reference content on the old stored process or workspace server machine, you must add the content to the directory you defined in the stored process definition.

Deployment

Moving the SAS OLAP Server

If you have used the project install or basic install to install the SAS OLAP Server, you can use the instructions in this section to move the server to a new machine.

Important Note: In addition to changing the machine name (and optionally, the port number), if you move a server to a machine with a different operating system or to a machine with an operating system other than Windows, you might need to reconfigure the following:

- **accounts for authentication**. You might need to define accounts on the authentication provider for the new server machine.
- **metadata on the SAS Metadata Server**. The following metadata definitions might require reconfiguration or additional configuration:
    - ♦ server definition. On the server definition, you might need to use the Server Manager plug−in to SAS Management Console to change the following parameters:
        - ◊ **SAS startup command.** You might need to change the startup command for the new operating system.
        - ◊ **authentication domain**. When you move a server, you might need to set up an additional authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
    - ♦ login definitions. For the login definitions that access the server and the login definitions that are used in the load−balancing configuration (e.g., the SAS Guest user's login), you might need to use the User Manager plug−in to SAS Management Console to do one or more of the following:
        - ◊ define a new login definition. When you move a server, you might need to create a new login definition for the new authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
        - ◊ define a new login definition for a different authentication process. When you move a server, you might need to create a new login definition with credentials to access a server in a different operating system within the default authentication domain.
        - ◊ change the format of the user ID in the login definition. When you move a server, you might need to change the fully−qualified user ID for any login credentials used to access that server.
- **server startup command**. You might need to change the server startup command depending on the operating system where you move the server configuration.

To move the SAS OLAP Server to a different machine, follow these steps:

1. Use SAS Management Console to reconfigure the SAS OLAP Server definition for the new machine:

    a. Open SAS Management Console and connect to a metadata repository.
    b. In the SAS Management Console navigation tree, locate and select the server object (Main − OLAP Server) that you want to modify.
    c. In the Display area, for each server connection, follow these steps:

        i. Select and right−click the connection definition, then select **Properties** from the pop−up menu.
        ii. Select the Options tab.
        iii. Change the **Host Name** to the host name of the new machine for your server.
        iv. If you are changing the port, change the **Port** to the port of the new port for your server.
        v. If you need to change the authentication domain, click **New** and define the new **Authentication Domain** for your server.

vi. Click **OK**.

d. If you need to change the server startup command, select and right−click the server object, then select **Properties** from the pop−up menu. Select the Options tab and change the **Command** field.

e. Click **OK** to save the new configuration to the metadata repository.

2. Edit the portal Web application and SAS Stored Process application's policy files to specify the locations of the new server machine. For details, see Adding Permissions for Servers to Policy Files.
3. On the new machine, install SAS 9.1 or higher and SAS Integration Technologies.
4. Depending on how your server startup is configured, do the following:

   - If you have a SAS OLAP Server startup script, copy your SAS OLAP Server startup script to the same directory on the new machine and modify as appropriate.
   - If the SAS OLAP Server is configured to start as a service, configure the new machine to start the SAS OLAP server as a service.
   - If you are not starting the server as a service, ensure that the SAS user can authenticate against the host authentication provider for each machine.
   - Ensure that users who need to access the server are defined for the appropriate authentication provider.

When you are finished modifying the server and spawner definitions, do the following:

- if you have added a new authentication domain for the machine, do both of the following:
  - use the User Manager plug−in to SAS Management Console to add a login definition for access to the server. For details, see Defining Logins for Multiple Authentication Domains.
  - use the User Manager plug−in to SAS Management Console to modify the login definition for the SAS General Server group login. Modify the login definition to specify the new authentication, and, if required, the new user ID credentials.
- if you have changed operating systems and need to modify user credentials, use the User Manager plug−in to SAS Management Console to modify user and group login definition for the new user ID credentials of the new machine.

Deployment

Moving Both the SAS Stored Process Server and SAS Workspace Server to the Same New Machine

Important Note: In addition to changing the machine name (and optionally, the port number), if you move a server to a machine with a different operating system or to a machine with an operating system other than Windows, you might need to reconfigure the following:

- **accounts for authentication**. You might need to define accounts on the authentication provider for the new server machine.
- **metadata on the SAS Metadata Server**. The following metadata definitions might require reconfiguration, or additional configuration:
    - ♦ server definition. On the server definition, you might need to use the Server Manager plug−in to SAS Management Console to change the following parameters:
        - ◊ **SAS startup command.** You might need to change the startup command for the new operating system.
        - ◊ **authentication domain**. When you move a server, you might need to set up an additional authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
    - ♦ login definitions. For the login definitions that access the server and the login definitions that are used in the load−balancing configuration (e.g., the SAS Guest user's login), you might need to use the User Manager plug−in of the SAS Management Console to do one or more of the following:
        - ◊ define a new login definition. When you move a server, you might need to create a new login definition for the new authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
        - ◊ define a new login definition for a different authentication process. When you move a server, you might need to create a new login definition with credentials to access a server in a different operating system within the default authentication domain.
        - ◊ change the format of the user ID in the login definition. When you move a server, you might need to change the fully−qualified user ID for any login credentials used to access that server.
    - ♦ stored process definitions. You might need to use the Stored Process Manager plug−in to SAS Management Console to specify a new location for your stored process repository.
- **spawner startup command**. If you change operating systems when you move machines, you might need to change the spawner startup command. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.

To move both the SAS Stored Process Server and SAS Workspace Server to a new machine, follow these steps:

1. Use SAS Management Console to reconfigure the SAS Workspace Server definition for the new machine:

    a. Open SAS Management Console and connect to a metadata repository.
    b. In the SAS Management Console navigation tree, locate and select the server object (e.g., Main − Workspace Server) that you want to modify.
    c. In the Display area, for each server connection, follow these steps:

        i. Select and right−click the connection definition, then select **Properties** from the pop−up menu.
        ii. Select the Options tab.
        iii. Change the **Host Name** to the host name of the new machine for your server.
        iv. If you are changing the port, change the **Port** to the port of the new port for your server.

v. If you need to change the authentication domain, click **New** and define the new **Authentication Domain** for your server.
vi. Click **OK**.

d. If you need to change the server startup command, select and right−click the server object, then select **Properties** from the pop−up menu. Select the Options tab and change the **Command** field.
e. Click **OK** to save the new configuration to the metadata repository.

2. Use SAS Management Console to reconfigure the SAS Stored Process Server definition for the new machine:

a. Open SAS Management Console and connect to a metadata repository.
b. In the SAS Management Console navigation tree, locate and select the server object (e.g., Main − Stored Process Server) that you want to modify.
c. In the Display area, for each server connection, follow these steps:

i. Select and right−click the connection definition, then select **Properties** from the pop−up menu.
ii. Select the Options tab.
iii. Change the **Host Name** to the host name of the new machine for your server.
iv. If you are changing the port, change the **Port** to the port of the new port for your server.
v. If you need to change the authentication domain, click **New** and define the new **Authentication Domain** for your server.
vi. Click **OK**.

d. If you need to change the server startup command, select and right−click the server object, then select **Properties** from the pop−up menu. Select the Options tab and change the **Command** field.
e. Click **OK** to save the new configuration to the metadata repository.

3. Use SAS Management Console to reconfigure the spawner definition for the new machine:

a. In the SAS Management Console navigation tree, locate and select the spawner definition, then right−click and select **Properties** from the pop−up menu.
b. If your spawner name contains the machine name, change the **Name** field to specify the name of the new machine.
c. Select the Options tab.
d. Click **OK**.
e. Change the **Associated Machine** to the host name of the new machine for your server.
f. Click **OK**.
g. If you have any other servers associated with the spawner, select the Servers tab. In the **Selected servers** list box, select the other servers and move them to the **Available servers** list box. Click **OK**. You must then define a new spawner for these servers.
h. If you are changing the port of either the operator connection or load−balancing connection, in the Display area, select the connection, then right−click and select **Properties** from the pop−up menu. Select the Options tab and change the **Port** to the new port for your spawner connection.

If you changed the server's authentication domain, select the same new **Authentication Domain** for your spawner.
i. Click **OK** to save the new configuration to the metadata repository.

4. Edit the portal Web application and SAS Stored Process application's policy files to specify the locations of the new server machines. For details, see Adding Permissions for Servers to Policy Files.
5. On the new machine, install SAS 9.1 or higher and SAS Integration Technologies
6. Copy your metadata configuration file (XML file) and spawner startup script from your spawner configuration directory to the same directory on the new machine. If necessary, change the spawner startup script for the new machine. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.

7. Create a directory for stored process server log files. The recommended directory name is `STPDemo`, and the recommended location is the server home location that you specified when you ran the install program (for example, `C:\Program Files\SAS\Servers\STPDemo`).

   If you do not remember the server home location, see the `$STP_HOME$` property in the `install.properties` file.
8. Ensure that the multi−user login (specified in the **Advanced Options** for the SAS Stored Process Server definition as the login owned by the SAS General Server group) can authenticate against the host authentication provider for the SAS Stored Process Server's machine. On Windows NT and Windows 2000, give this account the Act as part of the Operating System user right.
9. Give the shared account for the SAS General Server group "Write" permission to the stored process log directory.
10. Ensure that the SAS user can authenticate against the host authentication provider for each machine.
11. Ensure that users who need to access the server are defined for the machine's host authentication provider.

When you are finished modifying the server and spawner definitions:

- if you have added a new authentication domain for the machine, do both of the following:
  - use the User Manager plug−in to SAS Management Console to add a login definition for access to the server. For details, see Defining Logins for Multiple Authentication Domains.
  - use the User Manager plug−in to SAS Management Console to modify the login definition for the SAS General Server group login. Modify the login definition to specify the new authentication, and, if required, the new user ID credentials.
- if you have changed operating systems and need to modify user credentials, use the User Manager plug−in to SAS Management Console to modify user and group login definition for the new user ID credentials of the new machine.
- if you need to move the stored process repositories to a different directory, use the Stored Process Manager plug−in to SAS Management Console to modify the stored process definition and change the **Source Repository** field on the Execution tab of the stored process definition.
- if your stored process definitions reference content on the old stored process or workspace server machine, you must add the content to the directory you defined in the stored process definition.

Deployment

Moving the SAS Stored Process Server and SAS Workspace Server to Separate Machines

If you have used the project install or basic install to install the SAS Stored Process Server and SAS Workspace Server on the same machine, you can use the instructions in this section to move the servers to new (and separate) machines.

Important Note: In addition to changing the machine name (and optionally, the port number), if you move a server to a machine with a different operating system or to a machine with an operating system other than Windows, you might need to reconfigure the following:

- **accounts for authentication**. You might need to define accounts on the authentication provider for the new server machine.
- **metadata on the SAS Metadata Server**. The following metadata definitions might require reconfiguration or additional configuration:
    - ♦ server definition. On the server definition, you might need to use the Server Manager plug−in to SAS Management Console to change the following parameters:
        - ◊ **SAS startup command.** You might need to change the startup command for the new operating system.
        - ◊ **authentication domain**. When you move a server, you might need to set up an additional authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
    - ♦ login definitions. For the login definitions that access the server and the login definitions that are used in the load−balancing configuration (e.g., the SAS Guest user's login), you might need to use the User Manager plug−in to SAS Management Console to do one or more of the following:
        - ◊ define a new login definition. When you move a server, you might need to create a new login definition for the new authentication domain. To understand and plan for a new authentication domain, see Planning for Authentication Domains.
        - ◊ define a new login definition for a different authentication process. When you move a server, you might need to create a new login definition with credentials to access a server in a different operating system within the default authentication domain.
        - ◊ change the format of the user ID in the login definition. When you move a server, you might need to change the fully−qualified user ID for any login credentials used to access that server.
    - ♦ stored process definitions. You might need to use the Stored Process Manager plug−in of the SAS Management Console to specify a new location for your stored process repository.
- **spawner startup command**. If you change operating systems when you move machines, you might need to change the spawner startup command. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.

To move both the SAS Stored Process Server and the SAS Workspace Server to separate machines, follow these steps:

1. Use SAS Management Console to reconfigure the SAS Stored Process Server definition for the new machine:

    a. Open SAS Management Console and connect to a metadata repository.
    b. In the SAS Management Console navigation tree, locate and select the server object that you want to modify.
    c. In the Display area, for each server connection, follow these steps:

i. Select and right−click the connection definition, then select **Properties** from the pop−up menu.
ii. Select the Options tab.
iii. Change the **Host Name** to the host name of the new machine for your server.
iv. If you are changing the port, change the **Port** to the port of the new port for your server.
v. If you need to change the authentication domain, click **New** and define the new **Authentication Domain** for your server.
vi. Click **OK**.

d. If you need to change the server startup command, select and right−click the server object, then select **Properties** from the pop−up menu. Select the Options tab and change the **Command** field.
e. Click **OK** to save the new configuration to the metadata repository.

2. Use SAS Management Console to reconfigure the spawner definition for the new SAS Stored Process Server's machine:

a. Locate and select the spawner definition, then right−click and select **Properties** from the pop−up menu.
b. If your spawner name contains the machine name, change the **Name** field to specify the name of the new machine.
c. Select the Options tab.
d. Change the **Associated Machine** to the host name of the new machine for your server.
e. Click **OK**.
f. Select the Servers tab.
g. In the **Selected servers** list box, select the SAS Workspace Server named Main − Workspace server and move it the **Available servers** list box.

   If you have any other servers associated with the spawner, select the other servers and move them to the **Available servers** list box. You must then define a new spawner for these servers.
h. Click **OK**.
i. If you are changing the port of either the operator connection or load−balancing connection, in the Display area, select the connection, then right−click and select **Properties** from the pop−up menu. Select the Options tab and change the **Port** to the new port for your spawner connection.

   If you changed the server's authentication domain, select the same new **Authentication Domain** for your spawner.
j. Click **OK** to save the new configuration to the metadata repository.

3. Use SAS Management Console to reconfigure the SAS Workspace Server definition for the new machine:

a. Open SAS Management Console and connect to a metadata repository.
b. In the SAS Management Console navigation tree, locate and select the server object that you want to modify.
c. In the Display area, for each server connection, follow these steps:

i. Select and right−click the connection definition, then select **Properties** from the pop−up menu.
ii. Select the Options tab.
iii. Change the **Host Name** to the host name of the new machine for your server.
iv. If you are changing the port, change the **Port** to the port of the new port for your server.
v. If you need to change the authentication domain, click **New** and define the new **Authentication Domain** for your server.
vi. Click **OK**.

d. Click **OK** to save the new configuration to the metadata repository.

4. Use SAS Management Console to define a spawner definition for the SAS Workspace Server's new machine. See Using SAS Management Console to Define or Modify a Spawner in the *SAS Integration Technologies Administrator's Guide* and fill in the appropriate fields as follows:

    - **Name**. Specify the name of the spawner, e.g. <*machine_name*> Spawner.
    - **Selected servers**. Add the name of the SAS Workspace Server, i.e. Main − Workspace Server.
    - **Authentication Domain**. Specify the spawner domain (must be the same as the server's authentication domain).
    - **Host Name**. Specify the machine name of the SAS Workspace Server.
    - **Port Number**. Specify the spawner port, default is 8581.
5. On the new machine for the SAS Workspace Server, follow these steps:

    a. Install SAS 9.1 or higher and SAS Integration Technologies
    b. Copy your metadata configuration file (XML file) and spawner startup script from your spawner configuration directory to the same directory on the new machine. If necessary, change the spawner startup script for the new machine. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.
    c. Ensure that users who need to access the server are defined on the machine's host authentication provider.
    d. Change the spawner startup script to specify the new spawner name for the spawner, e.g., <*machine_name*> Spawner.
6. Edit the portal Web application and SAS Stored Process application's policy files to specify the locations of the new servers' machines. For details, see Adding Permissions for Servers to Policy Files.
7. On the new machine for the SAS Stored Process Server, follow these steps:

    a. Install SAS 9.1 or higher and SAS Integration Technologies.
    b. Copy your metadata configuration file (XML file) and spawner startup script from your spawner configuration directory to the same directory on the new machine. If necessary, change the spawner startup script for the new machine. For details, see Invoking (Starting) the Object Spawner in the *SAS Integration Technologies Administrator's Guide*.
    c. Create a directory for stored process server log files. The recommended directory name is `STPDemo`, and the recommended location is the server home location that you specified when you ran the install program (for example, `C:\Program Files\SAS\Servers\STPDemo`).

        If you do not remember the server home location, see the `$STP_HOME$` property in the `install.properties` file.
    d. Ensure that the multi−user login (specified in the **Advanced Options** for the SAS Stored Process Server definition as the login owned by the SAS General Server group) can authenticate against the host authentication provider for the SAS Stored Process Server's machine. On Windows NT and Windows 2000, give this account the Act as part of the Operating System user right.
    e. Give the shared account for the SAS General Server group "Write" permission to the stored process log directory.
    f. Ensure that users who need to access the server are defined for each machine's host authentication provider.
8. Ensure that the SAS user can authenticate against the host authentication provider for each machine.

When you are finished modifying the server and spawner definitions:

- if you have added a new authentication domain for the machine, do both of the following:
    - use the User Manager plug−in to SAS Management Console to add a login definition for access to the server. For details, see Defining Logins for Multiple Authentication Domains.

    - ♦ use the User Manager plug−in to SAS Management Console to modify the login definition for the SAS General Server group login. Modify the login definition to specify the new authentication, and, if required, the new user ID credentials.
- if you have changed operating systems and need to modify user credentials, use the User Manager plug−in to SAS Management Console to modify user and group login definition for the new user ID credentials of the new machine.
- if you need to move the stored process repositories to a different directory, use the Stored Process Manager plug−in to SAS Management Console to modify the stored process definition and change the **Source Repository** field on the Execution tab of the stored process definition.
- if your stored process definitions reference content on the old stored process or workspace server machine, you must add the content to the directory you defined in the stored process definition.

Deployment

Scaling SAS Workspace and SAS Stored Process Servers

For performance and security reasons, you might want to set up pooling or load−balancing for your SAS Workspace or SAS Stored Process Servers. For SAS Workspace Servers, you might want to configure your servers for pooling. For SAS Stored Process Servers, you might want to load balance across multiple machines:

- **Pooling SAS Workspace Servers**. The *SAS Integration Technologies Administrator's Guide* provides details about setting up your servers for pooling. For details, see Pooling Overview and Pooling Metadata in the *SAS Integration Technologies Administrator's Guide*.
- **Load balancing across multiple SAS Stored Process Server machines**. The *SAS Integration Technologies Administrator's Guide* provides details about setting up your servers for load balancing. For details, see Load Balancing Overview and Load Balancing Metadata in the *SAS Integration Technologies Administrator's Guide*.

Deployment

Portlet Deployment

To deploy your portlets, you must copy your PAR file into the appropriate portlet deployment directory. (If you are deploying a remote portlet, you must also deploy the WAR file to the servlet container). For details about creating the PAR file, see Creating a PAR File for Deployment in Your Application in the *SAS Web Infrastructure Kit Developer's Guide*. For complete instructions about adding custom−developed portlets to the portal Web application, see Adding Custom−Developed Portlets. The portal Web application then provides several functions with regard to portlets:

- Hot−deploy of portlets. After you copy your PAR file into the appropriate portlet deployment directory, the portal Web application automatically deploys the portlets via a hot−deploy mechanism that runs when the portal Web application's servlet container starts. For details, see Deploying Portlets.
- State management of portlets. The portal Web application manages portlet state and keeps track of the portlet context.
- Routing of user requests. The portal Web application routes user requests to the appropriate portlet. These portlets might be local portlets or remote portlets. For details about how local and remote portlets run in the portal Web application, see How Local and Remote Portlets Execute.

Deploying Portlets

To deploy portlets in the portal Web application, copy the `.par` file to the portlet deployment directory. To verify the location of your portlet deployment directory, see the `$PORTLET_DEPLOY_DIR$` value in the `install.properties` file. For example, copy `portlet.par` to the `C:\Program Files\SAS\Web\Portal2.0.1\DeployedPortlets` directory. (If you are deploying a remote portlet, you must also deploy the WAR file to the servlet container. When the servlet container starts, the portal Web application deploys the portlets through the portal Web application's hot−deploy mechanism. The portal Web application then handles portlets as follows:

- **Deploying Additional Portlets**. If you add a portlet and its resources to the servlet container while the portal Web application is running, the portal Web application automatically deploys the new portlet into the portal Web application.

  Important Note: The portal Web application shell makes one attempt to deploy the PAR file. If the hot−deploy is not successful, the portal Web application shell will not attempt to deploy the PAR file again.
- **Updating or Removing Portlets**. If you update or remove a portlet and its resources in the servlet container, the portal Web application does not automatically update or remove the portlet from the portal Web application.

  To update or remove a portlet, you must stop and restart the servlet container. The portal Web application will then check the portlet deployment directory and update or remove the appropriate portlets from the portal Web application.

How Portlet Hot−Deploy Works

Although the portal Web application automatically deploys portlets when the portal Web application's servlet container starts, it is helpful to understand how this deployment works.

To deploy the portlets, the portal Web application does the following:

1. Starts the PortletDeployer thread.
2. For each PAR file in the hot−deploy directory, the PortletDeployer thread
    a. opens the PAR file and locates the deployment descriptor file named `portlet.xml`.
    b. parses the `portlet.xml` file and determines the name of the portlet resource directory. The portlet resource directory is the portlet path followed by the portlet name.
    c. creates metadata entries if the portlet is being deployed for the first time. If a localized value for title and description are provided, the localized values are extracted from the appropriate `portletDisplayResources.properties` file.
    d. copies the portlet resources into the Web context under the `/portlet` folder. The portlet resources are JSPs, images, and other non−Java class files.
    e. registers the portlet actions with the PortletRegistry.

How Local and Remote Portlets Execute

From an administration and performance perspective, it is important to understand how portlets are executed. You can develop and deploy two types of portlets: local or remote. For details, see the *SAS Web Infrastructure Kit Developer's Guide*.

A **local portlet** is deployed inside the portal Web application and executes inside the portal's servlet container. Because a local portlet executes in the portal Web application's servlet container, it consumes the computing resources (for example, CPU, memory, and disk storage) of the server machine on which the portal Web application's servlet container runs. In addition, when local portlets are deployed, they might also include resources such as web pages, style sheets, images, resource bundles, and Java classes that are deployed inside the portal Web application.

A **remote portlet** might not execute within the same servlet container and Web application as the portal Web application. Remote portlets enable data from external applications to be incorporated into a Web application. Therefore, a remote portlet might consume computing resources (for example, CPU, memory, and disk storage) on a different machine than the server machine on which the portal Web application's servlet container runs.

For details about required development steps for remote portlets and a detailed sample of a remote portlet, see Creating a Remote Portlet and Sample: Remote Portlet (HelloUserRemotePortlet) in the *SAS Web Infrastructure Kit Developer's Guide*.

From a user's perspective, the local portlet and remote portlet look the same. When a user interacts with a remote portlet, the remote portlet looks like a local portlet.

Deployment

Adding Permissions to Policy Files

To enable Web applications (which run in a servlet container) to access resources (servers and services) on either their own machine or other machines, the appropriate security permissions must be specified in the policy file for the Web application's servlet container. In addition, to enable applications to share remote services, the appropriate security permissions must be specified in the policy file for the SAS Services application. The portal Web application installation provides two types of policy files:

- policy files with no security restrictions. The portal Web application provides three files that have no security restrictions:

  ```
  sas.wik.allpermissions.tomcat.policy
  sas.wik.allpermissions.weblogic.policy
  sas.wik.allpermissions.sasservices.policy
  ```

  The `sas.wik.allpermissions.tomcat.policy` and `sas.wik.allpermissions.weblogic.policy` files contain the permissions for the components of the portal Web application. To get your installation up and running in a non−production environment, add the contents of the sas.wik.allpermissions.tomcat.policy or `sas.wik.allpermissions.weblogic.policy` to the servlet container's policy file. In addition, use the policy file, `sas.wik.allpermissions.sasservices.policy`, for the SAS Services application.
- policy files with security restrictions. The portal Web application provides three files with security restrictions:

  ```
  sas.wi.tomcat.policy.orig
  sas.wik.weblogic.policy.orig
  sas.wik.sasservices.policy
  ```

  The `sas.wik.tomcat.policy` and `sas.wik.weblogic.policy` files contain the permissions for the components of the portal Web application. After you have your applications installed and working properly in a non−production environment, add the contents of the `sas.wik.tomcat.policy.orig` or `sas.wik.weblogic.policy.orig` to the servlet container's policy file. In addition, use the policy file, `sas.wik.sasservices.policy`, for the SAS Services application.

The security restrictions in the second type of policy file secure the appropriate resources for the components of the portal Web application infrastructure. To change the security for applications and resources, you can modify or add statements to your policy files. To secure resources within the portal Web application infrastructure, the appropriate permissions are required for the following applications:

- **portal Web application**. The portal Web application must be able to access the SAS Metadata Server, its local services, the Java remote method invocation (RMI) server for the SAS Services application's remote services, any other servers it needs to access, and any foundation service−enabled applications which it calls. The portal Web application also requires permission to listen for calls from foundation service−enabled applications.
- **SAS Stored Process Web application**. The SAS Stored Process application must have access to the SAS Metadata Server, its local services, the Java RMI server for the SAS Services application's remote services, and any other servers it needs to access. The SAS Stored Process application also requires permission to receive calls from any calling application, such as the portal Web application.
- **SAS Services application**. The SAS Services application must have access to the Java RMI server to register the remote services and must have permissions for all applications that participate in SAS Foundation Service

session sharing (access to remote−accessible services).

- **remote portlets or other foundation−service enabled Web applications**. Remote portlets or other foundation−service enabled Web applications must have access to the SAS Metadata Server, the Java RMI server for the SAS Services application's remote service. The remote portlet or Web application also requires permission to receive calls from any calling application.

To enable an application to access resources, you must add permission statements to the policy file for the application. When you add permission statements, if you use a value of localhost for the machine name, Java will resolve the localhost value to the IP address 127.0.0.1. Because the Java−resolved IP address is not the same as the machine's IP address, when you use the value localhost, you must specify two permissions statements— one statement for localhost and one for the fully qualified machine name. When you specify a permission statement with a fully qualified machine name, you only need to specify one statement— a statement for the fully qualified machine name. For example, to add a permission statement for the SAS Service application's machine, add the following two lines to the policy file:

```
permission java.net.SocketPermission "localhost:1024−",
        "listen, connect, accept, resolve";
permission java.net.SocketPermission
 <SAS Services application's machine name>:1024−",
        "listen, connect, accept, resolve";
```

The following resources require permissions in the application's policy file:

- **servers**. For each application (Web or stand−alone) that needs to communicate with a SAS server, the Java policy files for the calling application need to include a permission to communicate with the SAS Server. If you add a new portlet or Web application that communicates with servers, add new servers to your portal Web application's server deployment, or redistribute servers to other machines, you must update the appropriate policy file with permission statements for the new server machines. To add a permission statement for server access to a policy file, for each application's codebase, you must add a statement with the format:

  ```
  // SAS Stored Process, Workspace, or OLAP server − need one entry per machine
  permission java.net.SocketPermission "host:1024−", "connect, resolve";
  ```

  where *host* is the host name of your server.

  For example, in the Apache Tomcat's `catalina.policy` file, you must add a permission statement to each of the following codebases:

  ```
  grant codeBase "file:${catalina.home}/webapps/Portal/−" {

    // SAS Stored Process, Workspace, or OLAP server − need one entry per machine
    permission java.net.SocketPermission "host:1024−", "connect, resolve";
    // −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
  };
  grant codeBase "file:${catalina.home}/webapps/SASStoredProcess/−" {
    // SAS Stored Process or Workspace server − need one entry per machine
    permission java.net.SocketPermission "host:1024−", "connect, resolve";
  ```

- **services**. The SAS Services stand−alone application is used as a Java RMI server to enable access to remote services and session context sharing between applications. When an application (Web or stand−alone) must communicate with another application, it uses the SAS Services application to access a set of shared remote services; when the application and SAS Services application share remote services, the applications are both RMI endpoints. To enable RMI endpoints to communicate, the Java policy files for both applications must include a permission statement that enables communication with the other application end−point's machine. Add a permissions with the following format to both the policy file for the SAS Services applications and the

policy file for the foundation service−enabled remote portlet or Web application:

```
permission java.net.SocketPermission "machine:1024−", "listen, accept, connect, resolve";
```

To understand the required permissions for the SAS Services application and the foundation service−enabled remote portlet or Web application, see Permission Requirements for Remote Portlet or Web Applications.

- **content**, including syndication channels, URL Display portlets, and SAS publication channels. When you want to add the following content to the portal Web application, you must have been granted permissions for the content in the policy file for the portal Web application:
  - URL Display portlet. For details about adding the appropriate permissions for URl Display portlets, see Adding Template or Predefined Portlets.
  - Syndication channels. For details about adding the appropriate permissions for syndication channels, see Adding Syndication Channels.
  - SAS publication channels. For details about adding the appropriate permissions for SAS publication channels, see Adding SAS Publication Channels.

The portal Web application, SAS Stored Process Web application, and SAS Services application must each have specific permissions in order to access their required server and service resources. The following table shows the permission statements you must specify in each application to enable communication with its required servers and services.

Note: If some of the applications are located on the same machine, there might be duplicate permission statements.

Permission Requirements for the Portal Web Application, SAS Stored Process Web Application, and SAS Services Application

Codebase Name	Required Permissions
Portal	`// Access to the SAS Metadata server` `// When running on localhost, an entry is also required` `// containing the fully qualified host name.` `// permission java.net.SocketPermission "localhost:8561",` `//  "listen, connect, accept, resolve";` `permission java.net.SocketPermission` `"<SAS Metadata Server's machine>:8561",` `  "listen, connect, accept, resolve";`
	`// Access to the Java RMI server and remote` `// SAS Foundation Services` `// When running on localhost, an entry is also required` `// containing the fully qualified host name.` `// permission java.net.SocketPermission "localhost:1024−",` `//  "listen, connect, accept, resolve";` `permission java.net.SocketPermission` `"<SAS Services application's machine name>:1024−",` `  "listen, connect, accept, resolve";`
	`// Access to the portal Web application's` `// local SAS Foundation Services` `// Always need both the localhost and fully qualified host name.` `permission java.net.SocketPermission` `  "localhost:1024−", "listen, connect, accept, resolve";` `permission java.net.SocketPermission` `"<portal Web application's machine name>:1024−",`

	"listen, connect, accept, resolve";
	// **Access for foundation service−enabled applications** // **that are called by this application** // **to pass objects (via RMI) (e.g., remote portlets,** // **Web applications, and applications)** // Need one entry per machine. permission java.net.SocketPermission ***"<SAS Stored Process Web application's machine name>***:1024−", "listen, connect, accept, resolve";
	//**Access for foundation service−enabled** //**applications that call this application** //**to pass objects (via RMI) (to this application)** // Need one entry per machine allowing listen, // connect, accept, resolve for 1024:−. permission java.net.SocketPermission ***"<remote portlet or Web application's machine name>***:1024−", "listen, connect, accept, resolve";
	// **Access to a SAS Stored Process, Workspace, or OLAP server** // − Need one entry per machine. permission java.net.SocketPermission ***"<SAS Workspace Server's machine name>***:1024−", "connect, resolve"; permission java.net.SocketPermission ***"<SAS OLAP Server's machine name>***:1024−", "connect, resolve";
	// **Access to the WebDAV server** permission java.net.SocketPermission ***"<WebDAV server's machine name>***:8300", "connect, resolve";
SASStoredProcess	// **Access to the SAS Metadata server** // When running on localhost, an entry is also required // containing the fully qualified host name. // permission java.net.SocketPermission "localhost:8561", // "listen, connect, accept, resolve"; permission java.net.SocketPermission ***"<SAS Metadata Server's machine>***:8561", "listen, connect, accept, resolve";
	// **Access to the Java RMI server and remote SAS Foundation Services** // When running on localhost, an entry is also required // containing the fully qualified host name. // permission java.net.SocketPermission "localhost:1024−", "listen, connect, accept, resolve"; permission java.net.SocketPermission ***"<SAS Services application's machine name>***:1024−", "listen, connect, accept, resolve";
	// **Access to the SAS Stored Process Web** // **application's local SAS Foundation Services** // Always need both the localhost and fully qualified host name. permission java.net.SocketPermission "localhost:1024−", "listen, connect, accept, resolve"; permission java.net.SocketPermission ***"<SAS Stored Process Web application's machine name>***:1024−", "listen, connect, accept, resolve";

	//Access for foundation service−enabled **//applications that call this application** **//to pass objects (via RMI) (to this application)** // Need one entry per machine allowing // listen, connect, accept, resolve for 1024:−. permission java.net.SocketPermission ***"<portal Web application's machine name>***:1024−", "listen, connect, accept, resolve";
	// Access to a SAS Stored Process, Workspace, or OLAP server // − Need one entry per machine. permission java.net.SocketPermission ***"<SAS Stored Process Server's machine name>***:1024−", "connect, resolve";
	// Access to the WebDAV server permission java.net.SocketPermission ***<WebDAV"server's machine name>***:8300", "connect, resolve";
SASServices	**// Access to the Java RMI server and remote SAS Foundation Services** // When running on localhost, an entry is also required // containing the fully qualified host name. permission java.net.SocketPermission "localhost:1024−", "listen, connect, accept, resolve"; permission java.net.SocketPermission ***"<SAS Services application's machine name>***:1024−", "listen, connect, accept, resolve";
	// Connections with application(s) that utilize **// SAS Foundation Service session sharing** permission java.net.SocketPermission ***"<portal Web application's machine name>***:1024−", "listen, connect, accept, resolve"; permission java.net.SocketPermission ***"<SAS Stored Process Web application's machine name>***:1024−", "listen, connect, accept, resolve";

If you implement a remote portlet or foundation service−enabled Web application, you must add additional permissions to each portal Web application component's codebase and define a codebase and permissions for the remote portlet or foundation service−enabled Web application. The following table shows the permission statements you must specify in each application or portlet's policy file to enable communication with its required servers and services.

Permission Requirements for Remote Portlet or Web Application	
Codebase Name	**Required Permissions**
Codebase name for remote portlet or Web application	**// Access to the SAS Metadata server** // When running on localhost, an entry is also required containing the // fully qualified host name. // permission java.net.SocketPermission // "localhost:8561", "listen, connect, accept, resolve"; permission java.net.SocketPermission ***"<SAS Metadata Server's machine>***:8561", "listen, connect, accept, resolve";

	`// Access to the Java RMI server and remote SAS Foundation Services` `// When running on localhost, an entry is also required` `// containing the fully qualified host name.` `// permission java.net.SocketPermission` `//   "localhost:1024-", "listen, connect, accept, resolve";` `permission java.net.SocketPermission` `"<SAS Services application's machine name>:1024-",` `"listen, connect, accept, resolve";`
	`// Access to the remote portlet or Web application's` `// local SAS Foundation Services` `// Always need both the localhost and fully qualified host name.` `permission java.net.SocketPermission` `"localhost:1024-", "listen, connect, accept, resolve";` `permission java.net.SocketPermission` `"<remote portlet or Web application's machine name>:1024-",` `"listen, connect, accept, resolve";`
	`// Access for foundation service-enabled` `// applications that call this application` `// to pass objects (via RMI) (to this application)` `// Need one entry per machine allowing` `//  listen, connect, accept, resolve for 1024:-.` `permission java.net.SocketPermission` `"<portal Web application's machine name>:1024-",` `"listen, connect, accept, resolve";`
	`// Access to a SAS Stored Process, Workspace, or OLAP server -` `// Need one entry per machine.` `permission java.net.SocketPermission` `"<SAS Workspace Server's machine name>:1024-",` `"connect, resolve";` `permission java.net.SocketPermission` `"<SAS Stored Process Server's machine name>:1024-",` `"connect, resolve";` `permission java.net.SocketPermission` `"<SAS OLAP Server's machine name>:1024-",` `"connect, resolve";`
Portal	`// Access for foundation service-enabled` `// applications that are called by this application` `// to pass objects (via RMI) (e.g., remote portlets,` `// Web applications, and applications)` `// Need one entry per machine.` `permission java.net.SocketPermission` `"<remote portlet/Web application's machine name>:1024-",` `"listen, connect, accept, resolve";`
SASServices	`// Connections with application(s) that utilize` `// SAS Foundation Service session sharing` `permission java.net.SocketPermission` `"<remote portlet/Web application's machine name>:1024-",` `"listen, connect, accept, resolve";`

Security

To understand, plan for, and implement authentication and authorization for the Open Metadata Architecture, see "Understanding the Security Concepts in the SAS Intelligence Architecture" and its related security chapters in the SAS Intelligence Architecture: Planning and Administration Guide.

This chapter describes the portal Web application's security mechanisms and how you configure security for your implementation:

- **Overviews of Portal Web Application Security**.
  - **Administration, Authentication, and Authorization.** For an overview of administration, authentication, and authorization for the portal Web Application, see Administration, Authentication, and Authorization.
  - **Security Architecture**. For an overview of the server tier and mid−tier security structure of the portal Web application, see Security Architecture
  - **Security Implementation**. To understand the mechanisms by which you implement security for the portal Web application, see How You Implement Security.
- **Security Configuration**.
  - **Initial Security Definitions**. For an overview of the initial users and groups that are defined upon installation for the portal Web application, see Default Security Installation.
  - **Security Implementation.** For an overview of the steps to implement security, see Implementing Security. To implement security, this chapter provides the following sections:
    - **Planning for User and Groups.** To understand the planning of authentication domains for the portal, and how to plan for your groups, see Planning for Authentication Domains, and Planning for Users and Groups.
    - **Defining Users.** Depending on how you installed and set up authentication for your portal Web application, you can define additional users for host, LDAP, or Web server (trusted realm) authentication. For details, see Defining Users.
    - **Defining Groups**. After you define your users, you can define your groups. For details, see Defining Groups.
    - **Implementing Authorization**. After you have added your content, depending on the type of content, you can implement authorization (access control) by different authorization mechanisms. For details, see Authorizing Access to Content.

Security

Administration, Authentication, and Authorization

Each implementation of the portal Web application will have different security requirements. In determining how to implement portal Web application security, you should consider your organization's internal security policies, the security mechanisms that are in place in your environment, the types of users who will need to access the portal Web application, and the types of content that will be made available.

Understanding the Portal Web Application Administrators

To authenticate and authorize users in a security implementation, the portal Web Application uses up to four different types of administrators.

Note: When you installed the portal Web application, you might have specified different user names and user IDs for the first three administrators described as follows:

- **SAS** (Unix and z/OS only). The default SAS user is `sas`. The SAS user should be used to start the servers and spawners on Unix and z/OS.
- **SAS Administrator.** The default SAS Administrator is `sasadm`. The SAS Administrator is set up as an *unrestricted user* and has unrestricted access to the metadata. (The SAS Administrator is set up as an unrestricted user by listing it in the `adminUsers.txt` file and by preceding its user ID with an asterisk). You can use the SAS Administrator to log in to SAS Management Console and create the portal Web application's content, user, and authorization metadata on the SAS Metadata Server.

  For more information about the *unrestricted user*, see Server Administrative Privileges in the *SAS 9.1 Metadata Server: Setup Guide*.
- **SAS Web Administrator**. The default SAS Web Administrator is `saswbadm`. Because the SAS Web Administrator is a member of the Portal Admins group, the SAS Web Administrator is a group content administrator for all groups and has unrestricted access to view users' personal portal Web application content and share that content with a group. The SAS Web Administrator can also modify and delete users' personal portal Web application content and shared group content.

  Note: Due to the permissions granted to the SAS Web Administrator, it is recommended that you do not use the SAS Web Administrator for general tasks.

  The portal Web application shell also uses the SAS Web administrator to perform specific tasks, such as deploying portlets, creating group permission trees, and loading initial metadata.
- **Group Content Administrator**. To enable a user to share their personal content with a group, you can log in to SAS Management Console as the SAS Administrator and configure the user as a group content administrator for that group. A group content administrator for a particular group can share their personal content with that group. A group content administrator cannot modify or delete shared group content. For details, see Using the Portal Options Menu to Share Pages.

  Note: Members of the Portal Admins group (e.g. SAS Web Administrator) are already configured as group content administrators for all groups.

Understanding How The Portal Web Application Authenticates and Authorizes

Authentication. Depending on which method you chose for authentication, the portal Web application shell authenticates users as follows:

- **SAS Metadata Server authentication**. When a user first brings up the portal Web application, the public areas of the portal Web application become available for searching and viewing. To establish a specific user identity, the user chooses the **Log On** task from the toolbar. On the log−on page, the user enters their user ID and password. The portal Web application then uses the SAS Metadata Server's authentication provider to validate the user ID and password; the SAS Metadata Server's authentication provider can be the host authentication provider (default), or the LDAP server or Microsoft Active Directory alternate authentication providers. After authentication, the portal Web application uses the SAS Metadata Server to locate the user definition (metadata identity) that contains the user ID that was authenticated. The portal Web application then has the metadata identity of the user and displays the user's home page. The portal Web application can also retrieve additional login credentials (for access to servers in other authentication domains) from the user metadata identity. For full details about SAS Metadata Server authentication and additional server authentication, see the topics "Initial Authentication on a Metadata Server" and "Additional Authentication" in the SAS Intelligence Architecture: Planning and Administration Guide
- **Web Server authentication**. When a mid−tier user accesses the portal Web application, the portal Web application trusts that the mid−tier user has already been authenticated by the Web server. The SAS Metadata Server's Trusted User then connects to the SAS Metadata Server to locate the user definition (metadata identity) that contains the user ID of the mid−tier user. The portal Web application shell then has the metadata identity for the user and displays the user's home page. The portal Web application can also retrieve additional login credentials (for access to servers in other authentication domains) from the user metadata identity. For full details about Web server authentication and additional server authentication, see the topics "Initial Authentication on a Mid−Tier Server" and "Additional Authentication" in the SAS Intelligence Architecture: Planning and Administration Guide.

Authorization. To authorize users for content, the portal Web application uses the user metadata identity to determine which content the user is authorized to access. To determine whether the user metadata identity has access to particular content, the portal Web application checks the access control permissions set for that content in the SAS Metadata Repository. For full details about SAS Metadata Server authorization, see the topic "Authorization Layers in the SAS Intelligence Architecture" in the SAS Intelligence Architecture: Planning and Administration Guide.

The installation process for the portal Web application creates a default security structure in your SAS Metadata Repository that controls security on both the Web server (mid−tier) and SAS server (server tier):

- If users authenticate against the SAS Metadata Server, the authentication provider and SAS Metadata Server (server tier) enable this structure.
- If users authenticate against a Web server, the Web server's authentication services (mid−tier) and SAS Metadata Server (back tier) enable this structure.

The structure includes a default set of permissions that enable the portal Web application to operate on a demonstration basis. For a description of the structure see Security Architecture.

Security

Security Architecture

The installation process for the portal Web application shell creates a security structure that uses an authentication mechanism to authenticate users and a SAS Metadata Server to control access on both the mid−tier and the server tier. This structure provides a starting point that you can build upon as needed to meet your organization's specific security requirements.

Mid−Tier Security

The security structure for the mid−tier enables authorized access to system components that reside within the portal Web application shell, including the following:

- some types of portal Web application content, including Web applications, files, links, portlets, syndication channels, and packages that are stored on a Xythos WebFile (WFS) WebDAV server
- portal Web application pages and page templates

The security structure for the mid−tier includes the following levels of authorization:

- **Authorization for the SAS Trusted User**. The SAS Trusted User is used to perform specific tasks for the portal Web application. In the default portal Web application shell installation, the SAS Trusted User belongs to a user called `sastrust`. (If you want to use another name for the SAS Trusted User, you must change the `install.properties` file, the authentication provider accounts, the SAS Metadata Server users, and the `trustedusers.txt` file). For Web server authentication, this user also acts as the *trusted user*.
- **Authorization for the SAS Administrator**. The SAS Administrator is used to create metadata on the SAS Metadata Repository. In the default portal Web application shell installation, the SAS Administrator belongs to a user called `sasadm`. (If you want to use another name for the SAS Administrator, you must change the `install.properties` files, the authentication provider users, the SAS Metadata Server users, and the `adminusers.txt` file).
- **Authorization for the SAS Web Administrator**. The portal Web application shell uses a privileged identity to perform specific tasks on behalf of users who are logged on to the application. The portal Web application uses the SAS Web Administrator to perform tasks such as deploying portlets and creating group permission trees. In addition, as the SAS Web Administrator, you can access users' personal content and share that content with any group. In addition, the SAS Web Administrator can modify and delete the shared content.
- **Authorization for Public Access**. Certain content items in the default initial demo data installation of the portal Web application are set up to allow search and read access for all users. These include anonymous users who have not logged on to the portal Web application and have not been defined in the metadata repository. To add, modify, or delete public content, a member of the Portal Admins group (e.g., SAS Web Administrator), or Public group content administrator can log in as the public content administrator, and use the portal Options to add and share public content.
- **Authorization for Public Kiosk** . In the default initial demo data installation, pages are set up for the SAS Guest (e.g., sasguest) user. When a user (who is not using Web server authentication) accesses the portal Web application shell, these pages are displayed in the Public Kiosk. From the Public Kiosk, users can also search and display Public content. If you have installed the SAS Information Delivery Portal or if you configure the SAS Guest as a content administrator, the SAS Guest user can add, create, or modify pages to be displayed in the Public Kiosk.
- **Authorization for Group Members (Access by Members of a Group)**. When member of the Portal Admins group (e.g., SAS Web Administrator) or group content administrator shares group−specific content, the portal Web application automatically grants read access to all users who belong to the SAS group. The default initial demo data installation does not contain any content that is shared with a group. To share content with a group, a member of the Portal Admins group or a group content administrator can log on to the portal Web

application shell and choose the portal Options menu Share feature. Any member of the Portal Admins group or a group content administrator can edit or delete group content.

- **Authorization for Defined User**.

  Note: If you have installed the SAS Web Infrastructure Kit, only members of the Portal Admins group and group content administrators can add content to the portal Web application. If you have installed the SAS Information Delivery Portal, all users can add content to the portal Web application.

  When users add content (referred to as "personal content") to the portal Web application, the portal Web application shell automatically grants read and write access to the user who created the content. The default portal Web application installation includes personal content for a sample user called SAS Demo User. To add, modify, or delete personal content, the user can log on to the portal Web application and use the portal Options to add, modify or delete their own content.

  Note: If the user is a group content administrator, the user has read and write permissions and can share their personal content with a group. Members of the Portal Admins group can also share, edit, and delete the user's personal content.

If your portal Web application shell authenticates users against a Web server, the mid−tier also implements authentication services for the Web users.

Server Tier (Authentication Provider and SAS Metadata Server) Security

The security structure for the authentication provider and metadata servers (server tier) authenticates users and enables authorized access to metadata or the resources that it describes.

- **Authentication**. If your portal Web application shell does not use the Web server authentication, one of the following authentication providers authenticates users for the portal Web application:
  - ♦ host authentication
  - ♦ LDAP directory server
  - ♦ Microsoft Active Directory server
- **Authorization**. You can log in to SAS Management Console as the SAS Administrator to implement authorization (access control) for other SAS servers in the server tier.

The security structure for the SAS Metadata Server server tier includes the following levels of access:

- **Authorization for SAS Administrator**. The SAS Administrator uses SAS Management Console to create the metadata in the SAS Metadata Repository.
- **Authorization for SAS Web Administrator**. When a SAS Web Administrator logs in (or accesses the portal Web application from the mid−tier), a connection to the SAS Metadata Server is made. The SAS Web Administrator can then use the portal Web application to access metadata for users' personal content and share users' personal content with groups.
- **Authorization for Defined User**. When a user logs in (or accesses the portal Web application from a Web server), a connection to the SAS Metadata Server is made.

  Note: If you have installed the SAS Web Infrastructure Kit, only members of the Portal Admins group and group content administrators can add content to the portal Web application. If you have installed the SAS Information Delivery Portal, all users can add content to the portal Web application.

The user can use the portal Web application to create content and automatically update the metadata for certain content, including links, portlets, and pages.

Server Tier (SAS Server) Security

The security structure for the SAS server (server tier) authorizes access to SAS system components. User and group definitions (metadata identities) on the SAS Metadata Server are the primary mechanism for authorizing access to these objects. In addition, for server access, the user or group metadata identity must have a login with the same authentication domain as the server that the login must access.

The security structure for the SAS server tier includes the following levels of access:

- **Authorization for Defined Users**. When a user logs in (or accesses the portal Web application from a Web server), a connection to the SAS Metadata Server is made. The portal Web application uses the SAS Metadata Server to determine whether the requesting user's metadata identity is allowed access to particular content. If the user's metadata identity is allowed access, the portal Web application uses the SAS Metadata Server to retrieve the login credentials associated with the authentication domain of the SAS server. The portal Web application then uses the login credentials to obtain a connection the SAS server.

Implementing Security for Your Environment

Each implementation of the portal Web application will have different security requirements. In determining how to implement portal Web application security, you should consider your organization's internal security policies, the security mechanisms that are in place in your environment, the types of users who will need to access the portal Web application, and the type of content that will be made available. Then you can modify the default portal Web application security structure to meet your requirements.

Security

How You Implement Security

You can implement your security requirements using the following mechanisms:

- **User definitions**. The portal Web application requires that you define individual users for authentication and authorization:

    - **authentication**. For authentication purposes, you must define users on one of the following authentication providers:
        - host system
        - LDAP directory server
        - Microsoft Active Directory server
        - Web server's (trusted realm) authentication provider
    - **authorization**. You must define user, group, and login (credentials) definitions on the SAS Metadata Server.

  A user who has been defined in the SAS Metadata Repository and on a system used for authentication can personalize the portal Web application by adding or modifying his or her own pages, portlets, and content items as follows:

    - If you have installed the SAS Information Delivery Portal, all users can personalize the portal Web application.
    - If you have installed only the SAS Web Infrastructure Kit, members of the Portal Admins group and group content administrators can personalize the portal Web application.

  In addition, users can be granted access to specific portal Web application content. See Planning for Users and Groups and Defining Users for details about planning for setting up users for the appropriate authentication provider and on the SAS Metadata Server.
- **Group definitions**. For efficient management of portal Web application security, it is recommended that you organize users into groups on the metadata repository. You can then grant access to portal Web application content to the appropriate groups based on the sensitivity of the data and the users' needs for information. For details about setting up groups, see Planning for Users and Groups and Defining Groups.
- **Authorization mechanisms (access control)**. You can use several different methods to allow or restrict access to portal Web application content:

    - **Using the portal Options menu share feature**. The share feature of the portal Options menu enables users to create personal content and share it as group content.
        - **Personal content access.**

          Note: If you have installed the SAS Information Delivery Portal, all users can use the portal Options menu to create personal content. If you have installed only the SAS Web Infrastructure Kit, members of the Portal Admins group and group content administrators can use the portal Options menu to create personal content.

          Users can create pages, collection portlets (that contain content), and links. After creating these items, users can access them from the portal Web application, edit them, remove them from the portal Web application, use the Search tool to find them, or delete them permanently. Personal content is available only to the user who adds it to the portal Web application. The portal Web application uses access control rules to impose these restrictions.
        - **Group content access**. Group content is content that a particular group of users can access. Group content can be shared as follows:

- The SAS Web Administrator (or any member of the Portal Admins group) can share their personal content or other users' personal content with any group.
- A user who is designated as a group content administrator for a group can share their personal content with the group.

Group content can be edited by anyone who is a group content administrator for the group, or by anyone who is in the Portal Admins SAS group. Members of the Portal Admins group can also delete group content. The portal Web application uses access control rules to impose these restrictions.

Important Note: If specific content items within the shared personal content have access control permissions that do not allow the user or group members to access the content, this access control takes precedence and the user will not be able to access that particular content. For example, if a group content administrator, SAS Web Administrator, or member of the Portal Admins group shares a page with a portlet that contains two reports, and the user that receives shared access to the portlet does not have permissions to view the report, then the user will not be able to view the report in the portlet.

- **Specifying authorization (access control) metadata**. The portal Web application uses access control rules in the metadata repository to determine which portal Web application components or content can be accessed by the user. For a given object or group of objects, you can specify access control that explicitly allows or disallows specific types of access to individual users or groups of users. In addition, when you develop a portlet or load specific portal Web application content, such as Web applications, page templates, or syndication channels, you might specify authorization (access control) for the content. Depending on the type of content, there are several ways you can implement authorization (access control):
  - **Authorization (access control) for SAS content**. For SAS content, an authorized administrator can manually update the metadata repository with authorization metadata to control access to any resource in the metadata repository.

    Use of access control provides unlimited flexibility in controlling access to portal Web application content.
  - **Authorization (access control) for custom−developed portlets**. When custom portlets are developed, the developer can use the portlet deployment descriptor file to specify which user or group are authorized to access the portlet.
  - **Authorization (access control) for Web applications, page templates, and syndication channels**. When you run the `.sas` files to load the metadata for Web applications, page templates, and syndication channels, you can specify which user or group are authorized to access the portlet.
  - **Authorization (Access Control) for Xythos WFS WebDAV content**. An authorized administrator can specify access control rules on the Xythos WFS WebDAV server to authorize access to specific folders in the Xythos WFS WebDAV repository.

Understanding Which Content Requires You to Implement Authorization

Some content requires you to set up access control for authorization. Other content already has authorization (access control) in place.

- **For Web applications, files, links, SAS packages, pages, page templates, predefined portlets, SAS publication channels, syndication channels, and some SAS stored processes**, you must implement the appropriate authorization.

- **For custom−developed portlets**, some authorization is implemented by the developer and is part of the portlet deployment descriptor file.
- **For SAS information maps, SAS reports, and SAS Stored Processes that are produced by SAS Enterprise Guide**, the producing application and administrator implement the required authorization. This security allows authorized users to add the information maps, stored processes, and reports to the portal Web application.

For details about enabling authorized access for the portal Web application, see Authorizing Access to Content.

Security

Default Security Installation

Definitions for users of the portal Web application are stored by both the authentication provider (for authentication) and the SAS Metadata Repository (for authorization).

Initial Users: SAS Trusted User, SAS Administrator, SAS Web Administrator, SAS Guest, and SAS Demo User

When you install the portal Web application using the basic install or project install, you are prompted to enter user IDs and passwords for five specific users. The default user names and user IDs for the five initial users are SAS Trusted User (e.g., `sastrust`), SAS Administrator (e.g., `sasadm`), SAS Web Administrator (e.g. `saswbadm`), SAS Guest (e.g., `sasguest`), and SAS Demo User (e.g., `sasdemo`). Each of these users is listed by its default name and described below:

Note: When you installed the portal Web application, you might have specified different user names and user IDs for these users:

- **SAS Trusted User**: The default SAS Trusted User is `sastrust`. (The SAS Trusted User is set up as a *trusted user* by listing it in the `trustedUsers.txt` file). The servers that are deployed with the portal Web application use the SAS Trusted User account to connect to the SAS Metadata Server and retrieve configuration information. For Web server authentication, the SAS Trusted User enables mid−tier (Web−tier) users to be viewed as already−authenticated by the Web server and connect to the SAS Metadata Server for authorization purposes.

  For information about *trusted users*, see Trusted Users in the *SAS 9.1 Metadata Server: Setup Guide*.
- **SAS Administrator**: The default SAS Administrator is `sasadm`. The SAS Administrator is set up as an *unrestricted user* and has unrestricted access to the metadata. (The SAS Administrator is set up as an unrestricted user by listing this user in the `adminUsers.txt` file and preceding the user ID with an asterisk). You can use the SAS Administrator to log in to SAS Management Console and create the portal Web application's content, user, and authorization metadata on the SAS Metadata Server.

  For more information about the *unrestricted user*, see Server Administrative Privileges in the *SAS 9.1 Metadata Server: Setup Guide*.
- **SAS Web Administrator**: The default SAS Web Administrator is `saswbadm`. Because the SAS Web Administrator is a member of the Portal Admins group, the SAS Web Administrator has unrestricted access to view users' personal portal Web application content and share that content with a SAS group. The SAS Web Administrator can also modify users' personal portal Web application content.

  Note: Due to the permissions granted to the SAS Web Administrator, it is recommended that you do not use the SAS Web Administrator for general tasks.

  The portal Web application shell uses the SAS Web Administrator to perform specific tasks, such as deploying portlets and creating SAS group permission trees. The portal Web application installation also uses the SAS Web Administrator to load initial metadata.

  To further understand the role of the SAS Web Administrator, see Portal Admins group.
- **SAS Guest**: The default SAS Guest is `sasguest`. The SAS Guest is the administrator for the Public Kiosk. The Public Kiosk is displayed to users who have not yet logged in to the portal Web application. The SAS

Guest user can create and edit the Public Kiosk that is displayed.

Note: If you installed only the SAS Web Infrastructure Kit, to enable the SAS Guest to create and edit content for the Public Kiosk, you must configure the SAS Guest as a group content administrator. For details, see Configuring a Group Content Administrator.

Important Note: Because the SAS Guest user creates and edits the Public Kiosk that is displayed to all users, ensure that you only give these credentials to the administrator of the Public Kiosk.

Users who view the Public kiosk have access to content based on the authorization (access control) for the SAS Guest user.

The portal Web application installation also uses the SAS Guest to load initial metadata.

Note: If users authenticate using the Web server (trusted realm) authentication, no Public Kiosk is displayed; however, you still must define the SAS Guest account.

- **SAS Demo User**: The default SAS Demo User is `sasdemo`. The SAS Demo User is provided for demonstration purposes. If you loaded the initial demo data, this user allows users to test their portal Web application implementation and learn about the features.

  Note: If you installed only the SAS Web Infrastructure Kit, to enable the SAS Demo User to create and edit content, you must configure the SAS Demo User as a group content administrator. For details, see Configuring a Group Content Administrator.

The portal Web application installation configures the appropriate authorization (access control) for the initial users.

Note: If you need to change the password for the SAS Trusted User, SAS Guest, or SAS Web Administrator, see Changing the Password for the SAS Trusted User, SAS Guest, or SAS Web Administrator.

Initial Groups: SAS General Servers, Portal Admins and Portal Demos

In order to run, the portal Web application requires definitions for three groups at a minimum: `SAS General Servers`, `Portal Admins`, and `Portal Demos`. You create these group definitions during the installation process. Each of these groups is described as follows:

- **SAS General Servers**: The group `SAS General Servers` contains a group login that is used by the spawner to start the load−balancing SAS Stored Process Server(s).
- **Portal Admins**: The group `Portal Admins` contains users that are portal Web application administrators. The group initially contains the SAS Web Administrator (e.g., `saswbadmn`). Each member of the `Portal Admins` group has the following capabilities:

  - unrestricted access to view users' personal portal Web application content and share that content with a SAS group. Members of the Portal Admins group can also modify and delete users' personal portal Web application content.

    Note: Due to the permissions granted to members of the Portal Admins group, it is recommended that you do not use Portal Admins group members for general tasks.
  - the ability to bootstrap metadata for group−based content sharing in the portal Web application. If you create groups (on the SAS Metadata Server) after you start the servlet container for the portal Web

application, when a member of the Portal Admins group logs in to the portal Web application, the metadata for group−based content sharing (i.e. group permission trees) is updated. If there are a large number of groups, the log in time for a member of the Portal Admins group might be slower than the log in time for a typical user due to the bootstrap creation of metadata for group permission trees.

Within your installation, if you have any other users that are *unrestricted users*, add those users to the Portal Admins group.

- **Portal Demos**: The group `Portal Demos` is for the portal Web application's demo users. The group initially contains the SAS Demo User (e.g., `sasdemo`).

For Unix and z/OS Systems: SAS User and SAS Group

If you installed with the project install on Unix or z/OS, you created one additional user and one additional group on the operating system:

- **SAS** user: The default SAS user is `sas`. The SAS user should be used to start the following servers (if they are not started as a service) and spawners:
  - Start the spawner that starts the SAS Workspace Server(s) and SAS Stored Process Server(s).
  - If you are not starting the SAS Metadata Server as a service, start the SAS Metadata Server.
  - If you have installed a SAS OLAP Server and are not starting the OLAP server as a service, start the OLAP server.
- **SAS** group: The default SAS group is `sas` on Unix and `sasgrp` on z/OS. This group is used to control access to some directories and files.

For additional details about the SAS user and group, see "Pre−Installation Checklist for Unix" and "Pre−Installation Checklist for z/OS" in the SAS Intelligence Architecture: Planning and Administration Guide.

Initial User Accounts

If you deploy a distributed server configuration, or authenticate some users against an alternative authentication provider, the following table shows the required locations of the user accounts that you create before beginning your installation:

Summary of Required Accounts for Authentication of Initial Credentials				
User Name (User ID)	**SAS Metadata Server's authentication provider**	**SAS Workspace Server's host authentication provider**	**SAS Stored Process Server's host authentication provider**	**SAS OLAP Server's authentication provider**
SAS Administrator (e.g., sasadm)	Yes	No	No	Yes
SAS Trusted User (e.g., sastrust)	Yes	No	No	No
SAS Guest (e.g., sasguest)	Yes	Yes*	Yes	Yes

SAS Demo User (e.g., sasdemo)	Yes	Yes*	Yes	Yes
SAS General Server (e.g., sassrv)	Yes	Yes	Yes	No

Note: If the SAS Workspace Server is set up in a pooled configuration, you are not required to have an account for these user credentials on the host for the SAS Workspace Server.

Initial Metadata Identities on the SAS Metadata Server

The following table summarizes the user and group metadata identities that you have defined in the metadata in order for your servers and applications to work correctly. You can use the User Manager plug−in in SAS Management Console to verify that these objects have been created properly.

Summary of Metadata Identities

Metadata Identities	Logins			Group Membership Information
	User ID*	Password**	Authentication Domain	
User: SAS Administrator	sasadm			
User: SAS Trusted User	sastrust			**member of:** SAS General Servers group
User: SAS Guest	sasguest	********	DefaultAuth	
User: SAS Demo User	sasdemo	********	DefaultAuth	**member of:** Portal Demos
User: SAS Web Administrator	saswbadm	********	DefaultAuth	**member of:** Portal Admins group
Group: SAS General Servers	sassrv	********	DefaultAuth	**members:** SAS Trusted User
Group: Portal Admins				**members:** SAS Web Administrator
Group: Portal Demos				**members:** SAS Demo User

* These are the recommended IDs. They should correspond to accounts in your authentication provider. On Windows, the user ID in the login should be fully qualified with a host or domain name, for example, *host−name*\sasadm.

** If you are logged in to SAS Management Console as an unrestricted user, you will always see ******** in the password column, even if no password was specified.

Security

Implementing Security

To understand, plan for, and implement security within a basic or project install implementation, refer to "Understanding the Security Concepts in the SAS Intelligence Architecture," "Developing your Security Plan," and "Implementing Security" in the SAS Intelligence Architecture: Planning and Administration Guide.

To plan for and set up users and groups for your portal Web application implementation, you must follow these steps:

1. **Plan your users and groups** according to your security requirements. For an overview, see Planning for Users and Groups.
2. **Define users for authentication and authorization:**
    - For authentication, set up users on your authentication provider(s).
    - For authorization, set up users on the SAS Metadata Server.

   For details, see Defining Users.
3. **Define your groups**. For details, see Defining Groups.
4. **To enable the appropriate SAS group permission trees to be created on the SAS Metadata Server**, do one of the following:
    - re−start the servlet container
    - log in to the portal Web application as the SAS Web Administrator (or any member of the Portal Admins group)

When you add your portal Web application content, you must implement authorization (access control) for the content. Depending on your content type, you can implement authorization in one or more of the following ways:

- Use the portal Options menu to share pages that contain content.
- Depending on your content type, specify access controls in the metadata in one or more of the following ways:
    - Specify authorization metadata in the portlet deployment descriptor file.
    - Specify authorization metadata when you add the metadata for the content to the SAS Metadata Server.
    - Specify authorization metadata using SAS Management Console.
    - Specify authorization metadata using the Xythos WFS WebDAV server's access control.

To understand authorization mechanisms, see Authorizing Access to Content.*Security*

Planning for Authentication Domains

Authentication domains support additional authentication for IOM Servers (SAS Workspace, SAS Stored Process, and SAS OLAP) servers that are defined in a different authentication domain than the default or Web server (trusted realm) authentication domain. Authentication domains enable you to define logical groupings of computing resources and logins within a metadata repository. During additional authentication, an application searches the metadata for a login that is associated with the authentication domain in which the target IOM server is defined.

Within the portal Web application installation, there are several reasons you might have set up or might need to set up an authentication domain (in addition to the default authentication domain):

- If you have set up Web server authentication for the portal Web application, you have already set up separate authentication domains for your Web server authentication (web) and IOM server authentication (DefaultAuth).
- If you specified different authentication domains for your default authentication domain (e.g., DefaultAuth) and your IOM server authentication domain (e.g., ServerAuth), you have separate authentication domains.
- If you redistribute your servers to different machines with different operating systems (i.e. authentication processes), you might need to set up a new authentication domain.

To understand more about when you might need to define additional authentication domains for IOM servers, see "Authentication Domains" in the SAS Intelligence Architecture: Planning and Administration Guide.

Each user must have an initial login definition that is used to access the SAS Metadata Server; these user credentials must also be valid on the SAS Metadata Server's authentication provider. For each user who must access servers in a new authentication domain, you must ensure that users can authenticate against the authentication provider of the server's machine; in addition, you must define an additional user or group (shared) login on the SAS Metadata Server. Therefore, on the SAS Metadata Server, each portal Web application user that must access a SAS server in the new authentication domain must own or have access to at least two login definitions:

- a login definition to connect to the SAS Metadata Server. This login definition only requires a password if it is also used as an outbound login to connect to an IOM server.

  Note: If you are using Web server authentication, this login definition is defined in the Web server (trusted realm) authentication domain (i.e., web).
- a login definition for an IOM server's authentication domain (e.g., ServerAuth). This login definition is used as an outbound login and requires a password.

In addition, you might have additional login definitions to access IOM servers in other authentication domains. These login definitions are used as outbound logins and require a password.

Depending on your security requirements, you can set up the additional login definitions in either of the following ways:

- an individual account on the authentication provider for the server's machine and user login definition on the SAS Metadata Server
- a shared account on the authentication provider for the server's machine and a group (shared) login definition (owned by a group) on the SAS Metadata Server.

Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider.

The following table shows the required accounts for the host authentication provider of the SAS Metadata Server's machine and the IOM servers' machines, and the required user, group and login definitions on the SAS Metadata Server when you perform initial authentication against the SAS Metadata Server's host authentication provider, SAS Metadata Server's LDAP or Microsoft Active Directory server, or Web Server's authentication provider.

Host Authentication Provider Account and SAS Metadata Server Metadata Requirements When Using Different Primary Authentication Providers			
Type of Install	**Host Authentication**	**LDAP or Microsoft Active Directory Server Authentication**	**Web Server Authentication**
All servers run on the same operating system	**Host authentication provider for the SAS Metadata Server and IOM Servers' machine****. For each user, individual accounts. **SAS Metadata Server**. For each user, a user definition with one login definition that contains a user ID and password.	**Host authentication provider for the SAS Metadata Server and IOM Servers' machine****. For each user who needs to access an IOM server, an individual or shared account on the host authentication provider of the SAS Metadata Server and IOM servers' machine. The SAS General Servers group login credentials must be able to authenticate against the host authentication provider for the SAS Stored Process Server's machine. The SAS user credentials must be able to authenticate against the host authentication provider for each IOM server's machine. *** **SAS Metadata Server**. For each user, a user definition with access to two or more logins: • one login definition to connect to the SAS Metadata Server. • one or more user or group login definitions to connect to IOM servers.	**Host authentication provider for the SAS Metadata Server and IOM Servers' machine****. For each user who needs to access an IOM server, an individual or shared account on the host authentication provider of the SAS Metadata Server and IOM servers' machine. The SAS General Servers group login credentials must be able to authenticate against the host authentication provider for the SAS Stored Process Server's machine. The SAS user credentials must be able to authenticate against the host authentication provider for each IOM server's machine. ***

			SAS Metadata Server. For each user, a user definition with access to two or more logins: • one login definition to connect to the SAS Metadata Server. • one or more user or group login definitions to connect to IOM servers.
Distributed or redistributed install with servers that run on different operating systems	**Host authentication provider for the SAS Metadata Server's machine**. For each user, individual accounts on the host authentication provider of the SAS Metadata Server's machine. **Authentication provider for the IOM server's machines**. For each user who needs to access an IOM server, an individual or shared account on the authentication provider of the IOM server's machine. The SAS General Servers group login credentials must be able to authenticate against the host authentication provider for the SAS Stored Process Server's machine. The SAS user credentials must be able to authenticate against the host authentication provider for each IOM server's machine. *** **SAS Metadata Server**. For each user, a user definition with	**Host authentication provider for the SAS Metadata Server's machine**. No additional accounts required. **Authentication provider for the IOM server's machines**. For each user who needs to access an IOM server, an individual or shared account on the authentication provider of the IOM server's machine. The SAS General Servers group login credentials must be able to authenticate against the host authentication provider for the SAS Stored Process Server's machine. The SAS user credentials must be able to authenticate against the host authentication provider for each IOM server's machine. *** **SAS Metadata Server**. For each user, a user definition with access to two or more logins:	**Host authentication provider for the SAS Metadata Server's machine**. No additional accounts required. **Authentication provider for the IOM server's machines**. For each user who needs to access an IOM server, an individual or shared account on the authentication provider of the IOM server's machine. The SAS General Servers group login credentials must be able to authenticate against the host authentication provider for the

	access to two or more logins: • one login definition to connect to the SAS Metadata Server • one or more user or group login definitions to connect to IOM servers.	• one login definition to connect to the SAS Metadata Server • one or more user or group login definitions to connect to IOM servers.	SAS Stored Process Server's machine. The SAS user credentials must be able to authenticate against the host authentication provider for each IOM server's machine. *** **SAS Metadata Server**. For each user, a user definition with access to two or more logins: • one login definition to connect to the SAS Metadata Server • one or more user or group login definitions to connect to IOM servers.

- ** If the SAS OLAP Server authenticates against an alternate authentication provider, ensure that the individual or shared account can authenticate against the alternate authentication provider.
- *** If the SAS OLAP Server is started as a service, then the SAS user does not need to authenticate against the authentication provider for the SAS OLAP Server's machine.

For details about how to set up server, user, group, and login definitions for a new authentication domain, see Defining Logins for Multiple Authentication Domains.

Security

Defining Logins for Multiple Authentication Domains

If you add workspace, stored process or OLAP servers to a new authentication domain, for each user that must access the server, you must use the User Manager plug−in to SAS Management Console to define a new login definition for the user's metadata identity or add the user's metadata identity to a group metadata identity that owns a group (shared) login definition for the authentication domain. In addition, each user must be able to authenticate against the authentication provider for the server's machine. Workspace and stored process servers always authenticate against the host authentication provider; OLAP Servers can authenticate against the host, LDAP, or Microsoft Directory authentication provider.

Each user that must access a SAS server in the new authentication domain must own or have access to at least two login definitions:

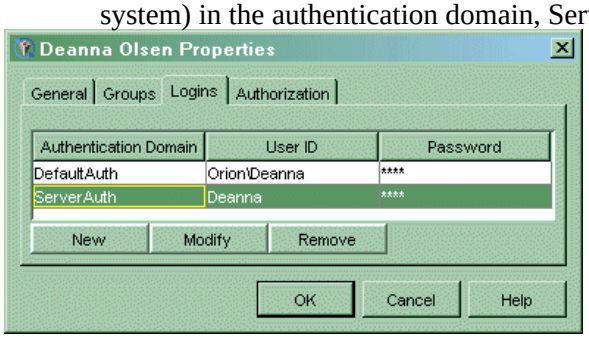
- a login definition that is used to connect to the SAS Metadata Server and any IOM servers that run in the default authentication domain.
    - ♦ If any of the IOM servers run in the default authentication domain and use the same authentication process as the SAS Metadata Server, specify a password. This login definition will be used as both an inbound login to connect to the SAS Metadata Server and an outbound login to connect to the IOM servers.
    - ♦ If all of the IOM servers do not run in the default authentication domain, do not specify a password. This login definition will only be used as the inbound login definition to connect to the SAS Metadata Server.
- a login definition that is used to connect to the servers in an additional authentication domain (e.g., ServerAuth). This login definition specifies the credentials for an out−bound login and requires a password.

You can set up additional login definitions in either of the following ways:

- **For each user, add a new login definition to the user's metadata identity** (in addition to the login used to connect to the SAS Metadata Server).

  For example, the following display shows the following login definitions for a user named Deanna:

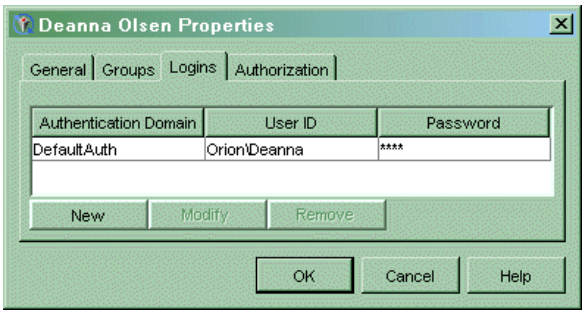
    - ♦ one login definition that is used to connect to the SAS Metadata Server and a SAS Workspace Server in the default authentication domain.
    - ♦ one login definition that is used to connect to a SAS OLAP Server (running on a UNIX operating system) in the authentication domain, ServerAuth.



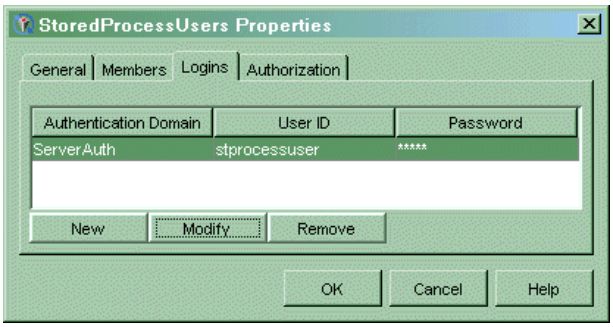
  Note: If you are creating the login definition for a SAS OLAP Server that authenticates against an alternate provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*

For workspace, stored process, and OLAP servers, ensure that the credentials in the new login definition can authenticate against the authentication provider for the server's machine.

- **For each user, add the user's metadata identity to a group metadata identity with a group (shared) login for the new authentication domain (e.g., ServerAuth)**. For the second login definition (used for server access), if you do not want to add a new login definition to each user's metadata identity, you can create a group with a group (shared) login; this group then contains the users (metadata identities) who need access to the servers in the new authentication domain. Each user in a group with a group (shared) login for the new authentication domain is not required to have a second login definition in his or her user definition. Create a group with a group (shared) login as follows:
    1. For each user, define a user metadata identity with a login definition to connect to the SAS Metadata Server. For example, the following display shows one login definition for a user named Deanna.



    2. Create a group and define a group login for the new authentication domain (e.g., ServerAuth). This login will be used to access the IOM servers in the new authentication domain (SAS Stored Process Server, SAS Workspace Server, SAS OLAP Server). For example, the following display shows a group login definition for the ServerAuth authentication domain for a group named StoredProcessUsers.



    Note: If you are creating the login definition for a SAS OLAP Server that authenticates against an alternate provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*
    3. Add each user (from step 1) to the group (from step 2) in order to enable each user to use the group login definition for the new authentication domain (e.g., ServerDomain). For example, the following display shows all of the users that are members of the group StoredProcessUsers and that can use the login definition to access servers in the ServerAuth authentication domain.

For workspace, stored process, and OLAP servers, ensure that the group (shared) login credentials can authenticate against the authentication provider of the server's machine.

Security

Planning for Users and Groups

When setting up user entries for the portal Web application, it is recommended that you organize the portal Web application users into groups. You can then grant access to content to the appropriate groups based on the sensitivity of the data and the users' needs for information. The use of groups is particularly important if the users have differing information needs and differing rights to view content.

The use of groups simplifies the process of administering and maintaining portal Web application security and reduces the chance for errors. For example,

- As new content is added to the Web application, you can make it available to the appropriate groups based on the type of information and its level of sensitivity. This process is much simpler than giving access to a long list of individual users. For details, see Authorizing Access to Content.
- As new users are added, you can assign them to the appropriate groups and they will automatically have access to the appropriate content. For details about adding users, see Defining Users.
- Users who are authorized as group content administrators can use the portal Options menu to share their pages with members of the group (s) for which they are a group content administrator.
- A member of the Portal Admins group (e.g., the `SAS Web Administrator`) can use the portal Options menu to share any user's content with any group.

For more information about group definitions, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

Guidelines for Dividing Users Into Groups

The project install documentation provides additional information about planning for your groups. For details, see topic "Planning Your User Groups" in the SAS Intelligence Architecture: Planning and Administration Guide. The following steps outline basic tasks for planning your user groups for portal Web application content.

Step 1: Analyze Content

The first step in setting up groups is to analyze the content that is planned for the portal Web application. For each category of content, determine whether authorization restrictions are needed. If restrictions are needed, identify the types of users that should and should not be authorized to access the content.

Step 2: Analyze and Group Users

After analyzing the content, you can identify groups of users. These user groups might be based on your organization's structure; however, it is more important to group users that have similar data access needs.

For the portal Web application, in order to implement the appropriate security, you must define groups for the following content:

- **Files**. If you are storing file content on a Xythos WFS WebDAV repository, you must set up groups for access to the appropriate group folders. (If you have installed the SAS Information Delivery Portal, you might already have group folders set up for SAS reports that are stored on the Xythos WFS WebDAV server). For details about adding file content, see Adding Files.
- **Packages published on a Xythos WFS WebDAV server**. If you have installed the SAS Information Delivery Portal and are publishing packages to a Xythos WFS WebDAV server, you must set up a group that

contains all the users who must publish to the Xythos WFS WebDAV server. For details about setting up users for publishing, refer to the Publishing to Secure Servers topic in the Publishing chapter of the *SAS Integration Technologies Administrator's Guide*. In addition, you should plan for the Xythos WFS WebDAV personal and group folders where you will publish and access the packages.
- **SAS publication channels on a Xythos WFS WebDAV server**. If you have installed the SAS Information Delivery Portal and are publishing packages to a SAS publication channel on a Xythos WFS WebDAV server, you must set up a group that contains all the users who must publish to the publication channel's Xythos WFS WebDAV server. For details about setting up users for publishing, see Publishing to Secure Servers in the *SAS Integration Technologies Administrator's Guide*. In addition, you should plan for the Xythos WFS WebDAV personal and group folders where you will publish and access the packages.

In addition, you might set up groups based on the following criteria:

- **Portal Web application content**. You might define groups based on the portal Web application content that members of the group need to access. Portal Web application content includes Web applications, links, page templates, portlets, and syndication channels (SAS Information Delivery Portal) only.
- **Access to content on IOM servers** (SAS Workspace Servers, SAS Stored Process Servers, SAS OLAP Servers). You might define groups based on which users need access to data on particular servers. In addition, you might set up a group definition for users to access a server in a different authentication domain than the SAS Metadata or Web server's authentication domain. To understand authentication domains and when you might want to set up a group definition for server access, see Planning for Authentication Domains.
- **Groups that have already been created for SAS Reports or SAS Information Maps**. Some of the groups that you need to define for portal Web application content might be the same groups that are already defined for SAS Reports, SAS Information Maps, or SAS Stored Processes.

The structure of group definitions within the Open Metadata Architecture allows you to do both of the following:

- **Add a user as a member of more than one group**. You might find that the authorization (access) requirements of a group of users are not necessarily identical. In these cases, you can assign a user to more than one group to accommodate unique needs.
- **Add a group as a member of another group**. You might find that a larger group might have smaller groups as members. For example, a group of worldwide sales users might contain a group of regional sales users.

You could start by identifying large groups of users. You can then subdivide those large groups into smaller groups if necessary. For example, you could create an Accounting user group that needs access to financial files through the portal Web application. Within that group, you could identify a subgroup of users who need access to salary information files that should not be accessed by the rest of the group.

The goal is to organize the user base in a way that reduces the number of cases in which specific users must be granted access to specific data. By keeping exception situations to a minimum, you will simplify maintenance tasks and reduce the chance for errors.

Step 3: Assign Group Content Administrators

After you set up a group, you can configure a user to be a group content administrator. The portal Web application gives the group content administrator authorization to share their personal pages so that they can be accessed by all members of that particular group. For each group that you plan to define, determine if you need to assign a group content administrator for that group.

Note: Members of the Portal Admins group (e.g., `SAS Web Administrator`) can also share any portal Web application user's content with any group.

To configure a user as a group content administrator, log in to SAS Management Console as the SAS Administrator and grant the user the `WriteMetadata` permission on the group's permission tree. (For details, see Configuring a Group Content Administrator.)

Security

Defining Users

In addition to the initial required users, you must define each portal Web application user. To add a portal Web application user, you must define users in two locations:

1. **Authentication provider**. You must define your user (or use a shared account) on the authentication provider that you are using to authenticate portal Web application users:

    - host authentication
    - LDAP authentication
    - Microsoft Active Directory authentication
    - Web server (trusted realm) authentication
2. **SAS Metadata Server**. You must define the user and its credentials on the SAS Metadata Server. To define a user on the SAS Metadata Server, you must log in to SAS Management Console as the SAS Administrator.

In addition, if you are using LDAP, Microsoft Active Directory, or Web server authentication, for any user that needs to access a SAS Stored Process, SAS Workspace, or SAS OLAP Server, you must ensure that the user can authenticate against the host authentication provider for the machine where that server runs.

To add users,

- For host authentication, see Adding Users.
- For LDAP authentication, see Adding Users (LDAP).
- For Microsoft Active Directory authentication, see Adding Users (Microsoft Active Directory).
- For Web server (trusted realm) authentication, see Adding Users (Web Server).

After the user's definition has been created, the following capabilities become available:

- **User personalization**. Group content administrators (and any member of the Portal Admins group) can add and organize portal Web application content for users. If the SAS Information Delivery Portal is installed, any user can also add and organize portal Web application content to meet that user's unique needs. For details, see the online Help for the portal Web application.
- **Group content access**. You can add the user to a group, giving the user access to shared content and other content that is restricted to particular groups. For details, see Planning for Users and Groups and Defining Groups.
- **User content access**. By specifying the user's metadata identity for access control, you can give the user access to portal Web application content other than that which is available publicly or to groups. For details, see Authorizing Access to Content.

After you define a user, if you need to change a password for credentials that access a server, see Changing Passwords for User or Group Credentials.

Security

Defining Users (Host Authentication)

If you authenticate users against a SAS Metadata Server using host authentication, each user must have an account on the operating system of the SAS Metadata Server. Each user must also have a user definition and login definition on the SAS Metadata Server.

In addition, for each user that needs to access IOM servers that run on a different machine than the SAS Metadata Server, you might need to add additional individual or shared accounts to the authentication provider for the server's machine and additional user or group login definitions (credentials) on the SAS Metadata Server.

For host authentication, each user must have access to login credentials for all the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

To add a new user for the portal Web application:

1. **Add the user to the host authentication provider for the SAS Metadata Server's machine.** Set up user accounts on the host authentication provider of the SAS Metadata Server's machine as follows:

   - **Define a valid user ID and password for the operating system account that provides access to the SAS Metadata Server's machine**. The procedure for adding host users varies depending on the operating system that you are using.
   - **For the Windows and Unix operating systems, set specific system permissions**. The *SAS 9.1 Metadata Server: Setup Guide* contains information about setting system permissions. For specific operating system instructions, see Setting System Access Permissions in the *SAS 9.1 Metadata Server: Setup Guide*.
2. **Add the user to the SAS Metadata Repository**. Log in to the SAS Management Console as the SAS Administrator and use the User Manager plug−in to create a user definition and initial login definition for the user. If you have already created a user definition for the user as part of another install, do not create it again. Instead, modify the login definition as specified.

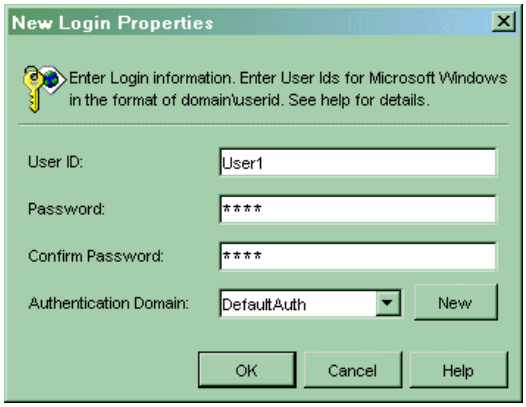
   From the User Manager, fill in the user and login definitions field as follows:

   a. General tab.
   Name
   specify the name of your user, e.g., `User1`
   b. Logins tab. For the initial login definition, fill in the fields as follows:

   Authentication Domain
   specify the default authentication domain (e.g., DefaultAuth).
   User ID
   specify the fully qualified user ID, e.g. `Sales\User1`
   Password
   - If any of the IOM servers run in the default authentication domain and use the same authentication process as the SAS Metadata Server, specify a password. This login definition will be used as both an inbound login to connect to the SAS Metadata Server and an outbound login to connect to the IOM servers.
   - If all of the IOM servers do not run in the default authentication domain, do not specify a password. This login definition will only be used as the inbound login

definition to connect to the SAS Metadata Server.

The following SAS Management Console display shows the initial login definition for the credentials that are used to access the SAS Metadata Server:



For details about defining users on the SAS Metadata Server, see Defining a User in the *SAS Management Console: User's Guide*.

3. **If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access**. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account). If the server uses a different authentication process than the SAS Metadata Server, you must setup an additional user or group (shared) login definition for the user on the SAS Metadata Server.

   Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, you must give the account the following user right:

   - "Log on as a batch job" user right.

   To set up valid server credentials, for each server, do one of the following:

   - **If the server runs on the same operating system and requires the same credentials as the SAS Metadata Server**, ensure that the user can authenticate against the authentication provider for the server's machine.

     If your server is defined in the default authentication domain, the portal Web application uses credential caching to retrieve the appropriate credentials for the server; you do not need to specify an additional login on the SAS Metadata Server. If another application that does not implement credential caching uses this user's initial login credentials to connect to the SAS Metadata Server and other IOM servers, you must specify the server's authentication domain in the **Authentication Domain** field of the initial login definition.

     Note: If your server is defined in an additional authentication domain but runs on the same operating system (and uses the same credentials) as the SAS Metadata Server, use SAS Management Console to reconfigure your server definition to specify the default authentication domain (DefaultAuth) for the authentication domain.
   - **If the server runs on a different operating system than the SAS Metadata Server**, set up credentials for the server in one of the following ways:

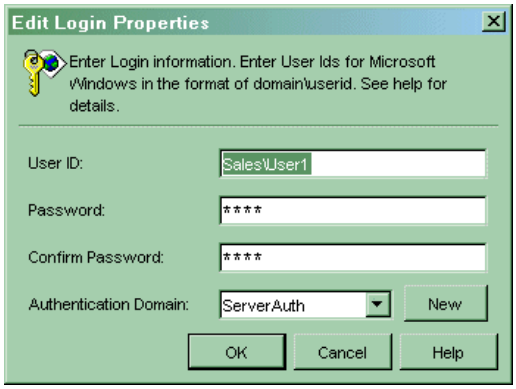
Set up an individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server. For all servers, ensure the user can authenticate against the authentication provider for the server's machine.

Use the User Manager plug−in to SAS Management Console to define a new login definition for the user.

Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

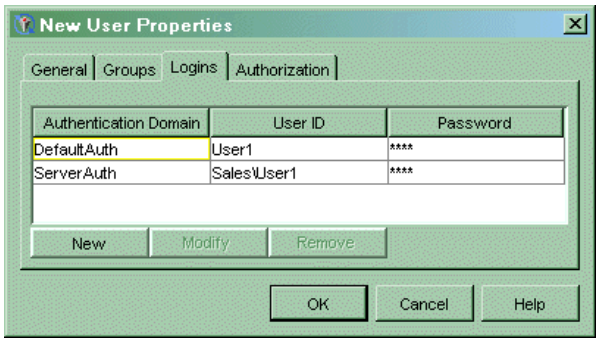
For an additional login definition, fill in the fields as follows:

Authentication Domain
specify the server's authentication domain (e.g., `ServerAuth`)
User ID
specify the fully qualified user ID, e.g. `Sales\User1`
Password
specify the password.
The following SAS Management Console display shows a user's additional login definition for accessing a server in the server's authentication domain, ServerAuth:



The following SAS Management Console screen shot shows a user with two logins:

- The first login is used to connect to the SAS Metadata Server and access a server in the default authentication domain, DefaultAuth.
- The second login is used to connect to a server in the authentication domain, ServerAuth:

◊ 

Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

◊ **Set up a shared account on the authentication provider and associated group (shared) login for a group definition (that contains the user metadata identity) on the SAS Metadata Server**. For all servers, determine an existing shared account or set up a new shared account on the server's authentication provider.

Use SAS Management Console to set up or add to a group that contains the following:

- the shared account as a group (shared) login of the group. For the group (shared) login definition, fill in the fields as follows:

  Authentication Domain
  specify the server's authentication domain.
  User ID
  specify the fully qualified user ID for the group credentials, e.g., `stprocessuser`
  Password
  specify the password.
  Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.
- the user as a member of the group. The user will then use the group (shared) login credentials to access the servers.

For details about defining groups on the SAS Metadata Server, see Defining a Group in the *SAS Management Console: User's Guide*.

For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains.

Security

Defining Users (LDAP Authentication)

If you authenticate users against a SAS Metadata Server using LDAP server authentication, each user must have an account on the LDAP Server. Each user must also have a user definition and login definition on the SAS Metadata Server.

In addition, for each user that needs to access IOM servers that run on a different machine than the SAS Metadata Server, you might need to add additional individual or shared accounts to the authentication provider for the server's machine and additional user or group login definitions (credentials) on the SAS Metadata Server.

For LDAP Server authentication, each user must have access to login credentials for all the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

To add a new user for the portal Web application, follow these steps:

1. **Add the user to an LDAP directory server**. The administrator only needs to create a person entry for the user.

   Each directory entry in the `ou=People` organizational unit should look like the following. The bold items are those that are different for each user.

   ```
   dn: cn=username,$PERSON_CONTEXT$
   cn: username
   description: user description
   mail: user email address
   objectclass: inetorgperson
   objectclass: person
   sn: short name of the user
   uid: user's portal login ID
   userpassword: login password
   ```

   Creating an entry in the directory manually for each portal Web application user can be time consuming. Creating and importing an LDIF file simplifies the process and also provides a backup file of portal Web application users.

   For further details about setting up person entries on an LDAP directory server, see Adding Person Entries to the Directory in the *SAS Integration Technologies Administrator's Guide (LDAP)*.
2. **Add the user to the SAS Metadata Repository**. Log in to SAS Management Console as the SAS Administrator and use the User Manager plug−in to create a user definition and initial login definition for the user. If you have already created a user definition for the user as part of another install, do not create it again. Instead, modify the login definition as specified.

   From the User Manager, fill in the user and login definitions field as follows:

   a. General tab
      Name
      specify the name of your user, e.g., `User1`
   b. Logins Tab. For the initial login definition, fill in the fields as follows:

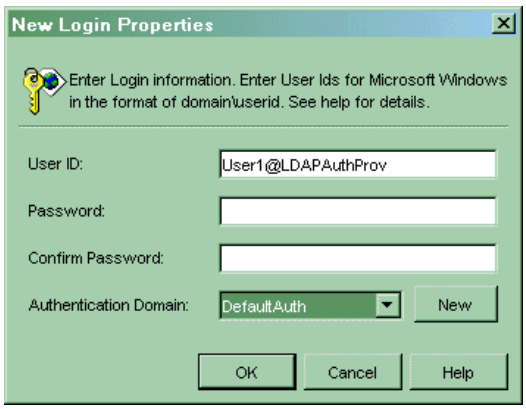
Authentication Domain
specify the default authentication domain, e.g., DefaultAuth

User ID
specify the fully qualified user ID, e.g., `User1@LDAPAuthProv`

Password
specify the password as follows:

- If any of the IOM servers run in the default authentication domain and use the same authentication process as the SAS Metadata Server, specify a password. This login definition will be used as both an inbound login to connect to the SAS Metadata Server and an outbound login to connect to the IOM servers.
- If all of the IOM servers do not run in the default authentication domain, do not specify a password. This login definition will only be used as the inbound login definition to connect to the SAS Metadata Server.

The following SAS Management Console display shows the initial login definition for the credentials that are used to access the SAS Metadata Server:



For details about defining users on the SAS Metadata Server, see Defining a User in the *SAS Management Console: User's Guide*.

3. **If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access**. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account). If the server uses a different authentication process than the SAS Metadata Server, you must setup an additional user or group (shared) login definition for the user on the SAS Metadata Server.

   Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, you must give the account the following user right:

   - "Log on as a batch job" user right.

   To set up valid server credentials, for each server, do one of the following:

   - **If the server uses the same authentication process (and requires the same credentials) as the SAS Metadata Server**, ensure the user can authenticate against the authentication provider for the server's machine.

     If your server is defined in the default authentication domain, the portal Web application uses credential caching to retrieve the appropriate credentials for the server; you do not need to specify an

additional login on the SAS Metadata Server. If another application that does not implement credential caching uses this user's initial login credentials to connect to the SAS Metadata Server and other IOM servers, you must specify the server's authentication domain in the **Authentication Domain** field of the initial login definition.

Note: If your server is defined in an additional authentication domain but runs on the same operating system (and uses the same credentials) as the SAS Metadata Server, use SAS Management Console to reconfigure your server definition to specify the default authentication domain (DefaultAuth) for the authentication domain.

- **If the server uses a different authentication process than the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

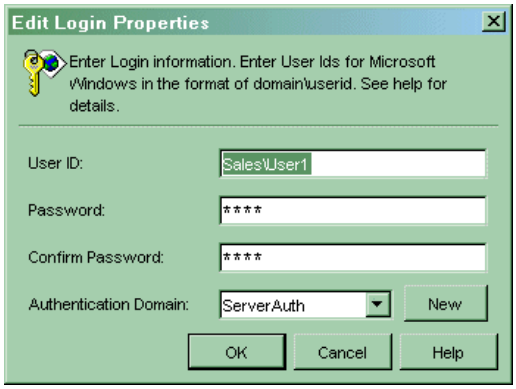
  - **Set up an individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**. For all servers, ensure the user can authenticate against the authentication provider for the server's machine.

    Use the User Manager plug−in to SAS Management Console to define a new login definition for the user.

    Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

    For an additional login definition, fill in the fields as follows:

    Authentication Domain
    specify the server's authentication domain.
    User ID
    specify the fully qualified user ID, e.g., `Sales\User1`
    Password
    specify the password.
    The following SAS Management Console display shows a user's additional login definition for accessing a server in the authentication domain, ServerAuth:

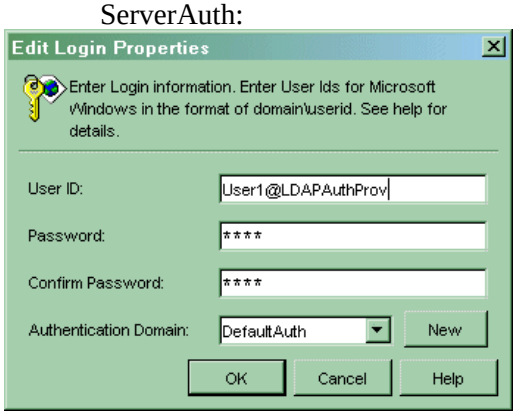


    Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required

format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

The following SAS Management Console display shows a user definition with two logins:

- The first login is used to connect to the SAS Metadata Server and authenticate against an LDAP server. If a password were specified for this login, it could also be used to connect to an OLAP server (in the default authentication domain) that authenticates against an LDAP server.
- The second login is used to connect to a server in the authentication domain, ServerAuth:



◊ **Set up a shared account on the authentication provider and login for a group definition (that contains the user) on the SAS Metadata Server**. For all servers, determine an existing shared account or set up a new shared account on the server's authentication provider.

Use SAS Management Console to set up or add to a group that contains the following:

- the shared account as a group (shared) login of the group. For the group (shared) login definition, fill in the fields as follows:

  Authentication Domain
  specify the server's authentication domain.
  User ID
  specify the fully qualified user ID for the group credentials, e.g., `stprocessuser`
  Password
  specify the password.
  Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.
- the user as a member of the group. The user will then use the group (shared) login credentials to access the servers.

For details about defining groups on the SAS Metadata Server, see Defining a Group in the *SAS Management Console: User's Guide*.

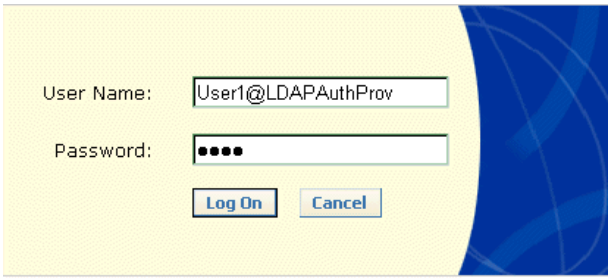
For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains.

Logging in to the Portal Web Application for LDAP Authentication

When a user logs in to the portal Web application, they must specify the LDAP domain that was configured in the SAS Metadata Server startup command and in the user definitions on the SAS Metadata Server. For example,

```
User Name: User1@LDAPAuthProv
Password:  User1
```

The following display shows the user's log in to the portal Web application:



Security

Defining Users (Microsoft Active Directory Authentication)

If you authenticate users against a SAS Metadata Server using Microsoft Active Directory Server authentication, each user must have an account on the Microsoft Active Directory Server. Each user must also have a user definition and login definition on the SAS Metadata Server.

In addition, for each user that needs to access IOM servers that run on a different machine than the SAS Metadata Server, you might need to add additional individual or shared accounts to the authentication provider for the server's machine and additional user or group login definitions (credentials) on the SAS Metadata Server.

For Microsoft Active Directory Server authentication, each user must have access to login credentials for all of the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

To add a new user for the portal Web application, follow these steps:

1. **Add the users to an Microsoft Active Directory Server.** The administrator only needs to create a person entry for the user.
2. **Add the user to the SAS Metadata Repository**. Log in to the SAS Management Console as the SAS Administrator and use the User Manager plug−in to create a user definition and initial login definition for the user. If you have already created a user definition for the user as part of another install, do not create it again. Instead, modify the login definition as specified.

   From the User Manager, fill in the user and login definitions field as follows:

   a. General tab.

   Name

   specify the name of your user, e.g., `User1`

   b. Logins tab. For the initial login definition, fill in the fields as follows:

   Authentication Domain

   specify the default authentication domain, e.g. DefaultAuth

   User ID

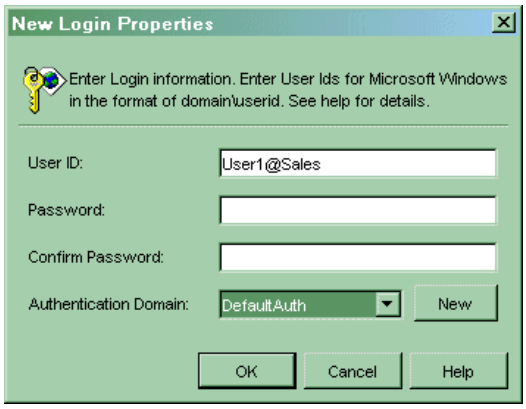
   specify the fully qualified user ID, e.g. `User1@Sales`

   Password

   specify the password as follows:

   - If any of the IOM servers run in the default authentication domain and use the same authentication process as the SAS Metadata Server, specify a password. This login definition will be used as both an inbound login to connect to the SAS Metadata Server and an outbound login to connect to the IOM servers.
   - If all of the IOM servers do not run in the default authentication domain, do not specify a password. This login definition will only be used as the inbound login definition to connect to the SAS Metadata Server.

   The following SAS Management Console display shows the initial login definition for the credentials that are used to access the SAS Metadata Server:



For details about defining users on the SAS Metadata Server, see Defining a User in the *SAS Management Console: User's Guide*.

3. **If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access**. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account). If the server uses a different authentication process than the SAS Metadata Server, you must setup an additional user or group (shared) login definition for the user on the SAS Metadata Server.

   Note: SAS Workspace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, you must give the account the following user right:

   - "Log on as a batch job" user right.

To set up valid server credentials, for each server, do one of the following:

- **If the server uses the same authentication process (and requires the same credentials) as the SAS Metadata Server**, ensure the user can authenticate against the authentication provider for the server's machine.

  If your server is defined in the default authentication domain, the portal Web application uses credential caching to retrieve the appropriate credentials for the server; you do not need to specify an additional login on the SAS Metadata Server. If another application that does not implement credential caching uses this user's initial login credentials to connect to the SAS Metadata Server and other IOM servers, you must specify the server's authentication domain in the **Authentication Domain** field of the initial login definition.

  Note: If your server is defined in an additional authentication domain but runs in the same operating system (and uses the same credentials) as the SAS Metadata Server, use SAS Management Console to reconfigure your server definition to specify the default authentication domain (DefaultAuth) for the authentication domain.
- **If the server uses a different authentication process than the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

  - **individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**. For all servers, ensure the user can authenticate against the authentication provider for the server's machine.

Use the User Manager plug−in to SAS Management Console to define a new login definition for the user.

Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

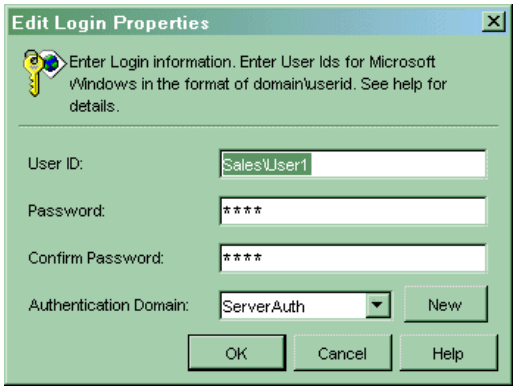
For an additional login definition, fill in the fields as follows:

Authentication Domain
: specify the server's authentication domain

User ID
: specify the fully qualified user ID, e.g., `Sales\User1`

Password
: specify the password.

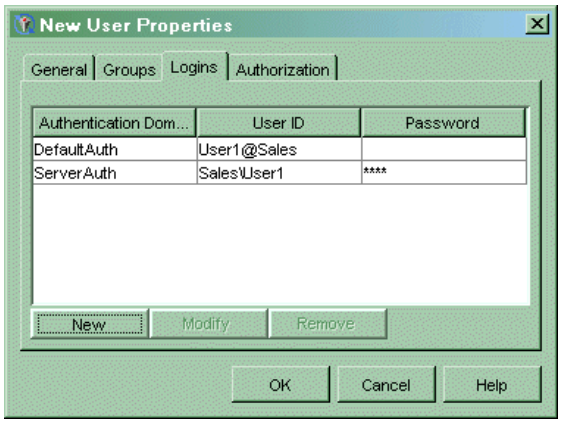
The following SAS Management Console display shows a user's additional login definition for accessing a server in the authentication domain, ServerAuth:



Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

The following SAS Management Console display shows a user definition with two logins:

- The first login is used to connect to the SAS Metadata Server and authenticate against an LDAP server. If a password were specified for this login, it could also be used to connect to an OLAP server (in the default authentication domain) that authenticates against an LDAP server.
- The second login is used to connect to a server in the authentication domain, ServerAuth:



◊ **shared account on the authentication provider and associated group (shared) login for a group definition (that contains the user metadata identity) on the SAS Metadata Server**. For all servers, determine an existing shared account or set up a new shared account on the server's authentication provider.

Use SAS Management Console to set up or add to a group that contains:

· the shared account as a group (shared) login of the group. For the group (shared) login definition, fill in the fields as follows:

Authentication Domain
specify the server's authentication domain

User ID
specify the fully qualified user ID for the group credentials, e.g., `stprocessuser`

Password
specify the password.

Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternate provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

· the user as a member of the group. The user will then use the group (shared) login credentials to access the servers.

For details about defining groups on the SAS Metadata Server, see Defining a Group in the *SAS Management Console: User's Guide*.

Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains.

Logging in to the Portal for Microsoft Active Directory Authentication

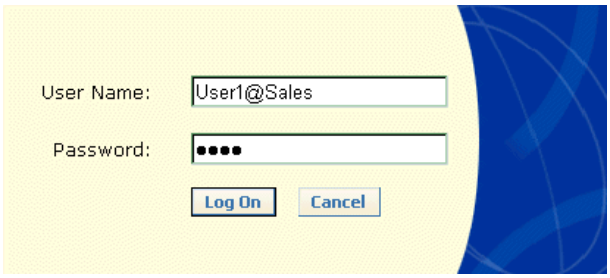
When a user logs in to the portal, they must specify the following user ID format:

```
userID@domain
domain\userID
```

where domain is the Windows network domain. For example,

```
User Name: User1@Windows network domain
Password:  User1
```

The following display shows the user's log in to the portal Web application:



Security

Defining Users (Web Server Authentication (Trusted Realm))

If you use a SAS Metadata Server's trusted user to trust users as already authenticated by the Web server's authentication provider, each user must have an account on the authentication provider for the Web server. Each user must also have a user definition and login definition on the SAS Metadata Server.

In addition, for each user that needs to access IOM servers that run on a different machine than the SAS Metadata Server, you might need to add additional individual or shared accounts to the authentication provider for the server's machine and additional user or group login definitions (credentials) on the SAS Metadata Server.

For Web server authentication, each user must have access to login credentials for all the authentication domains that contain resources that the user will access. Before you set up users, you should understand authentication domain and user credential requirements within the portal Web application installation. For details, see Planning for Authentication Domains.

To add a new user for the portal Web application, follow these steps:

1. **Ensure that the user can authenticate against the Web server's authentication provider.** For example, if your Web server authenticates users against an LDAP server, add a person entry for the user to the LDAP server.
2. **Add the user to the SAS Metadata Repository**. Log in to the SAS Management Console as the SAS Administrator and use the User Manager plug−in to create a user definition and initial login definition for the user. If you have already created a user definition for the user as part of another install, do not create it again. Instead, modify the login definition as specified.

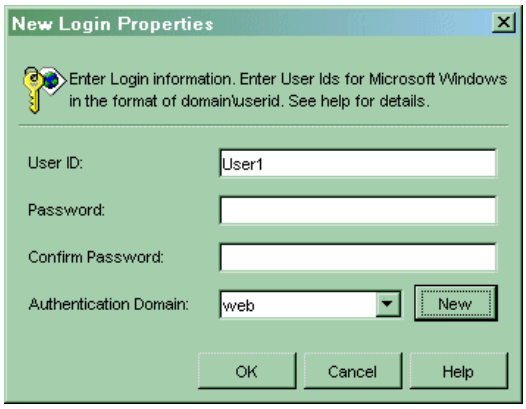
   From the User Manager, fill in the user and login definitions field as follows:

   a. General tab
   Name
   specify the name of your user, e.g., `User1`
   b. Logins tab. For the initial login definition, fill in the fields as follows:

   Authentication Domain
   specify the Web server authentication domain, e.g. web
   User ID
   specify the fullyqualified user ID as follows:
   - If the Web server passes the SAS Metadata Server user credentials that contain a domain, specify a domain. For example, `WINNT\User1`
   - If the Web Server does not pass the SAS Metadata Server user credentials that contain a domain, do not specify a domain. For example, `User1`

   Password
   do not specify a password.

   The following SAS Management Console display shows the initial login definition for the credentials that are used to access the SAS Metadata Server:



For details about defining users on the SAS Metadata Server, see Defining a User in the *SAS Management Console: User's Guide*.

3. **If the user needs to access a SAS Workspace, SAS Stored Process, or SAS OLAP Server, give the user the required operating system accounts and login definitions for server access**. For all servers, you must ensure that users can authenticate against the authentication provider of the machine (using an individual or shared account). If the server uses a different authentication process than the SAS Metadata Server, you must setup an additional user or group (shared) login definition for the user on the SAS Metadata Server.

   Note: SAS Workpace and SAS Stored Process Servers always authenticate against the host authentication provider; SAS OLAP Servers can authenticate against the host, LDAP, or Microsoft Active Directory authentication provider. If the server authenticates users against a host authentication provider on Windows, you must give the account the following user right:

   - "Log on as a batch job" user right.

To set up valid server credentials, for each server, do one of the following:

- **If the server uses the same authentication process (and requires the same credentials) as the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

  Note: If your server is defined in an additional authentication domain but runs in the same operating system (and uses the same credentials) as the SAS Metadata Server, use SAS Management Console to reconfigure your server definition to specify the default authentication domain (DefaultAuth) for the authentication domain.

  Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

  - **individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**. For all servers, ensure the user can authenticate against the authentication provider for the server's machine.

    Use the User Manager plug−in to SAS Management Console to define a new login definition for the user.

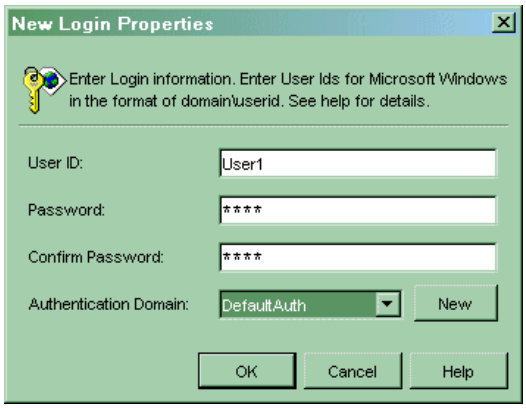
    For an additional login definition, fill in the fields as follows:

Authentication Domain
specify the default authentication domain, e.g., DefaultAuth

User ID
specify the fully qualified user ID, e.g., `Sales\User1`

Password
specify the password.

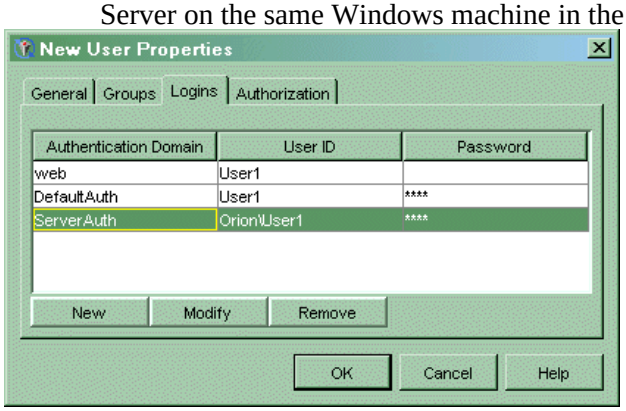
The following SAS Management Console display shows a user's additional login definition for accessing a server in the authentication domain, DefaultAuth:



Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

The following SAS Management Console display shows a user definition with three logins:

- The first login is used to connect to the SAS Metadata Server and authenticate against an Web server's authentication provider. If a password were specified for this login, it could also be used to connect to an OLAP server (in the default authentication domain) that authenticates against the same authentication provider.
- The second login is used to connect to a SAS OLAP Server on a Unix machine in the default authentication domain, DefaultAuth.
- The third login is used to connect to both a SAS Stored Process and SAS Workspace Server on the same Windows machine in the authentication domain, ServerAuth.



◊ **Set up a shared account on the authentication provider and login for a SAS group definition (that contains the user) on the SAS Metadata Server**. For all servers, determine an existing shared account or set up a new shared account on the server's authentication provider.

Use SAS Management Console to set up or add to a SAS group that contains

- the shared account as a group (shared) login of the SAS group. For the group (shared) login definition, fill in the fields as follows:

  Authentication Domain
  specify the server's authentication domain
  User ID
  specify the fully qualified user ID for the group credentials, e.g., `stprocessuser`
  Password
  specify the password.
  Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.
- the user as a member of the SAS group. The user will then use the group (shared) login credentials to access the servers.

For details about defining SAS groups, see Defining a Group in the *SAS Management Console: User's Guide*.

♦ **If the server uses a different authentication process than the SAS Metadata Server**, set up credentials for the servers in one of the following ways:

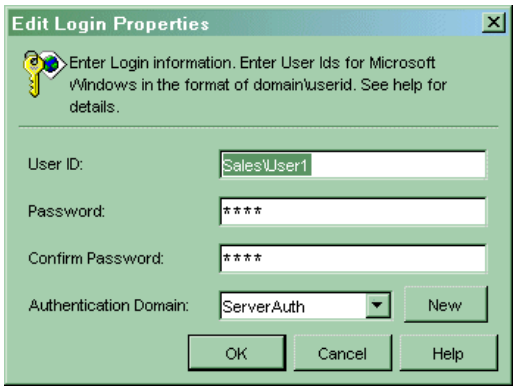
◊ **Set up an individual account on the server's authentication provider and an additional login definition for the user definition on the SAS Metadata Server**. For all servers, ensure the user can authenticate against the authentication provider for the server's machine.

Use the User Manager plug−in to SAS Management Console to define a new login definition for the user.

Note: If you already have a login definition defined for an authentication domain, and that login definition contains the required credentials for the server, do not define another login definition in that authentication domain. If the current login definition for your server's authentication domain does not contain the required credentials, you must reconfigure the server to use a new authentication domain and add a login definition that specifies the server's new authentication domain.

For an additional login definition, fill in the fields as follows:

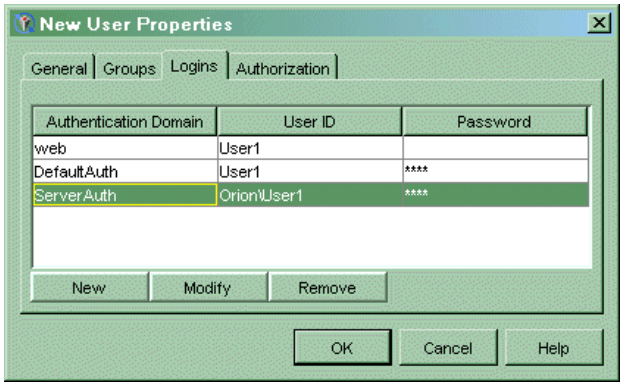
Authentication Domain
specify the server's authentication domain
User ID
specify the fully qualified user ID, e.g., `Sales\User1`
Password
specify the password.
The following SAS Management Console display shows a user's additional login definition for accessing a server in the authentication domain, ServerAuth:



Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

The following SAS Management Console display shows a user definition with three logins:

- The first login is used to connect to the SAS Metadata Server and authenticate against an Web server's authentication provider. If a password were specified for this login, it could also be used to connect to an OLAP server (in the default authentication domain) that authenticates against the same authentication provider.
- The second login is used to connect to a SAS OLAP Server on a Unix machine in the default authentication domain, DefaultAuth.
- The third login is used to connect to both a SAS Stored Process and SAS Workspace Server on the same Windows machine in the authentication domain, ServerAuth.



◊ **Set up a shared account on the authentication provider and associated group (shared) login for a SAS group definition (that contains the user) on the SAS Metadata Server**. For all servers, determine an existing shared account or set up a new shared account on the server's authentication provider.

Use SAS Management Console to set up or add to a group that contains

- the shared account as a group (shared) login of the group. For the group (shared) login definition, fill in the fields as follows:

Authentication Domain
specify the server's authentication domain
User ID

specify the fully qualified user ID for the group credentials, e.g.
`stprocessuser`

Password

specify the password.

Note: If you are defining a login definition that is used to access a SAS OLAP Server that authenticates against an alternative authentication provider, be sure to specify the required format for the user ID. For details, see Defining Users, Groups, and Logins in the *SAS Integration Technologies Administrator's Guide*.

- the user as a member of the group. The user will then use the group (shared) login credentials to access the servers.

For details about defining groups on the SAS Metadata Server, see Defining a Group in the *SAS Management Console: User's Guide*.

For an example that details how to define user or group credentials for a new authentication domain, see Defining Logins for Multiple Authentication Domains.

Security

Defining Groups

Group definitions are stored in the SAS Metadata Repository. You can log in to SAS Management Console as the SAS Administrator and use the User Manager plug−in to create group definitions.

For details about defining groups on the SAS Metadata Server, see the SAS Management Console User Manager Help and Defining a Group in the *SAS Management Console: User's Guide*.

Authorizing Groups to Access Content

Once your user groups have been defined, you can use various methods to give the groups access to portal Web application content. For details, see Authorizing Access to Content.

Security

Changing Passwords for User or Group Credentials

Note: If a user or group is defined as part of a project install installation, you might need to change the user's or group's password in other configuration locations. For details, see "Resetting Passwords" in the SAS Intelligence Architecture: Planning and Administration Guide.

You must keep the credentials that are stored in your users' or groups' login definitions in sync with your individual or shared accounts on the authentication provider. For example, if a user or group's password for an operating system account that provides access to a workspace server changes, the login definition (on the SAS Metadata Server) that contains credentials for that account must be updated to reflect the change.

Each user can reset his or her own passwords using either SAS Management Console or the personal login manager utility. An unrestricted user (e.g., the SAS Administrator) can use SAS Management Console to reset a password for any user.

Changing the Password for the SAS Trusted User, SAS Guest, or SAS Web Administrator

If you change the password for the SAS Trusted User, you must change the password in the `OMRConfig.xml` file located in the `ObjectSpawner` subdirectory. For details, see Verify or Create a Spawner or Server Startup Script.

If you change the password for the SAS Trusted User, SAS Guest, or SAS Web Administrator, you also need to complete the following steps:

1. Use PROC PWENCODE to encode the new password. For example, you would submit the following SAS statements to encode a password of "SAStrust1"

   ```
   proc pwencode in='SAStrust1';
   run;
   ```

   The encoded password is written to your SAS log.
2. Edit the `install.properties` files (located in the `PortalConfigure` directory of your installation). Locate the appropriate user's value for the current encoded password and replace it with the value for the newly encoded password as follows:

   SAS Trusted User
   Replace the value in the following line:

   ```
   $SERVICES_OMI_USER_PASSWORD$=
   ```

   SAS Guest
   Replace the value in the following line:

   ```
   $PORTAL_GUEST_PASSWORD$=
   ```

   SAS Web Administrator
   Replace the value in the following line:

   ```
   $PORTAL_ADMIN_PASSWORD$=
   ```
3. Run the configure_wik utility to create new service deployment configurations and new `SASStoredProcess.war` and `Portal.war` files.

4. Deploy the `Portal.war` and `SASStoredProcess.war` file to the servlet container on your portal Web application's Web server machine.

Security

Authorizing Access to Content

When administering the portal Web application, you must ensure that the appropriate authorization (to allow or restrict access) is implemented for the portal Web application content (portal Web application and SAS content). In addition, to run the portal Web application, each user (or a user group that the user belongs to) must have `ReadMetadata` and `WriteMetadata` permissions on the repository ACT. For details about ensuring that users have the correct permissions on the repository ACT, see the Authorization Manager online Help.

For the portal Web application, the methods for implementing authorization for content vary depending on the type of content. For each type of content, you can implement authorization in two basic ways:

- specify authorization (access control) metadata on the SAS Metadata Server. Depending on the content type, there are several ways that you can set up this access control.
- use the Share feature of the portal Options menu to share a page and allow group access to the page (and portlets and links on the page).

  Note: The portal Web application uses the authorization (access control) metadata on the SAS Metadata Server to determine who can view the content on a page and in a portlet; if a user is not authorized to view content on a page or portlet that has been shared, the content will not appear.

Before using any of these methods, it is generally helpful to first organize the potential users of the portal Web application into groups. Each group should contain users who have similar job functions and/or similar information needs. A user can be assigned to more than one group. For portal−specific details about planning for and creating groups, see Planning for Users and Groups and Defining Groups.

After organizing your users into groups, the level of additional access control you apply will depend on your user base and on the sensitivity of the content that you make available through the portal Web application. For details about planning your access controls, see "Planning your Access Controls" in the SAS Intelligence Architecture: Planning and Administration Guide.

The following table summarizes the available authorization options and their applicability to each content type:

Content Category	Content Type	How to Implement Authorization (Access Control)				
		Specify Authorization Metadata in the Portlet Descriptor File	Specify Authorization Metadata in the SAS Load Metadata File	Specify Authorization Metadata Using SAS Management Console	Specify Authorization Metadata Using the Xythos WFS WebDAV Server's Access Control	Use the Portal Options Menu to Share Pages
Portal Content	Web Application		**x**			**x**
	File				**x**	(if users have the appropriate authorization for the file)
	Link					**x**

	Portlet					**x**
	Custom−Developed Portlet	**x**				**x**
	Syndication Channel		**x**			**x**
Portal Component	Page					**x**
SAS	Publication Channel			**x**		(if users have the appropriate authorization for the SAS Publication Channel)
	Package Published to Xythos WFS WebDAV or a Xythos WFS WebDAV Publication Channel				**x**	(if users have the appropriate authorization for the SAS Package)
	Package Published to a File or Archive Publication Channel			**x**		(if users have the appropriate authorization for the SAS Package)
	Stored Process			**x** Could also be specified by SAS Enterprise Guide		(if users have the appropriate authorization for the SAS Stored Process)
	Package stored on Xythos WFS WebDAV				**x**	(if users have the appropriate authorization for the SAS Package)
	Information Map			Specified by SAS Information Map administrator		(if users have the appropriate authorization for the SAS Information Map)
	Report			Specified by SAS Report administrator		(if users have the appropriate

						authorization for the SAS Report)

Specify Authorization Metadata in the Portlet Descriptor File

When a portlet is developed, authorization metadata (for which user or group can access the portlet) can be specified in the descriptor file for the portlet. For information about using the portlet deployment descriptor file to specify which user or group is authorized to access the portlet, see Creating a Portlet Deployment Descriptor and the group DTD tag in the *SAS Web Infrastructure Kit Developer's Guide*.

Note: When you specify a user for portlet access, the user is granted `ReadMetadata` and `WriteMetadata` permissions to enable the user to view and edit the portlet. When you specify a group for portlet access the group is granted `ReadMetadata` permission to enable the group members to view the content.

Specify Authorization Metadata in the SAS Load Metadata File

When you add the metadata for Web applications, page templates, and syndication channels, you also add the authorization metadata by specifying the user or group who is authorized to access the content as follows:

- **Add the metadata to a user (Web applications and syndication channels)**. When you add the Web application or syndication channel metadata to a user, the user is granted `ReadMetadata` and `WriteMetadata` permissions to enable the user to view and edit the content. A user who is a group content administrator or member of the Portal Admins group can then use the portal Options menu to share content with a group.
- **Add the metadata to a group (Web applications, page templates, and syndication channels)**. When you add the Web application, page template, or syndication channel metadata to a group, the group is granted `ReadMetadata` permission to enable the group members to view the content.

Note: When you load the metadata for the content, the Public group is denied `ReadMetadata` and `WriteMetadata` permissions for the content.

For details about loading the authorization metadata for Web applications, page templates, and syndication channels, see Adding Applications, Adding Page Templates, and Adding Syndication Channels.

Specify Authorization Metadata (Access Control) Using SAS Management Console

You can log in to SAS Management Console as the SAS Administrator and specify which users or groups have access to the resource, and what type of access permissions they have for the resource. When specifying access control, you can choose to restrict access at one or both of the following locations:

- the server definition for the server that hosts the content
- the resource definition, which includes SAS Publication Channels and SAS Stored Processes definitions.

Note: In the portal Web application, subscriber profiles designate a set of personal preferences for subscribing to SAS publication channels. You can also specify authorization metadata for the subscriber profiles.

In SAS Management Console, you can configure access control through the Authorization Manager plug−in or on the resource's Authorization tab within the resource's plug−in. For details, see Using SAS Management Console to Set Up Authorization (Access Control).

Specify Authorization Metadata Using the Xythos WFS WebDAV Server's Access Control

The SAS User Management Customization provided with the Xythos WFS WebDAV server allows you to specify which users or groups are authorized to access specific folders in the Xythos WFS WebDAV repository, and what type of access permissions they have for the folders. Use the Xythos WFS WebDAV Administration GUI to associate access controls with the folders.

For more details about authentication and authorization with the Xythos WFS WebDAV server, see Implementing Authentication and Authorization for Xythos WFS WebDAV and Scenario: Using the Xythos Administration GUI and SAS User Management Customization with the Portal in the *SAS Integration Technologies Administrator's Guide*. For further details, refer to the product documentation.

Use the Portal Options Menu to Share Pages

Important Note: After you have set up your users and groups on the SAS Metadata Server, to enable the appropriate group permission trees (for sharing pages to groups) to be created on the SAS Metadata Server, you must do one of the following:

- Re−start the servlet container.
- Log in to the portal Web application as the SAS Web Administrator (or any member of the Portal Admins group).

If you installed the SAS Information Delivery Portal, all users can use the portal Options menu to create personal content. If you installed only the SAS Web Infrastructure Kit, members of the Portal Admins group and group content administrators can use the portal's Options menu to create personal content.

When users add personal content (including Web applications, files, links, SAS Information Maps, SAS packages, SAS publication channels, SAS Reports, SAS Stored Processes, and syndication channels) to a collection portlet on a page, only the user and members of the Portal Admins group (e.g., SAS Web Administrator) have authorization to view and edit the portlet, page, and any links (`ReadMetadata` and `WriteMetadata` permissions). The page can then be shared in either of the following ways:

- If you configure a user to be the group content administrator of a particular group, the user can share their content with that group. All users in the group have `ReadMetadata` permission for the page, and any portlets and links on the page. After a group content administrator shares a page, the group content administrator cannot delete the shared page.
- Any member of the Portal Admins group can also use the portal Options to share any page with a group of users (including the Public group of users). Members of the Portal Admins group have `ReadMetadata` and `WriteMetadata` permissions for the page, and any portlets and links on the page. Members of the Portal

Admins group can also delete shared pages.

When a user shares a page with a group, group members can only view the content on the page or portlet for which they have access (as determined by the access controls specified on the SAS Metadata Server). For details about personal, group, and public access, see Using the Portal Options to Create Personal and Share Group Content. For details about configuring users as group content administrators, see Configuring a Group Content Administrator.

Security

Using the Portal Options to Create and Share Personal Content

For portal Web application content other than SAS data and processes, the most efficient way to control access is to use the portal Options menu to

- **create personal content**. *Personal Content* is content that can only be edited, viewed, and deleted by the user who added it to the portal Web application. (The SAS Web Administrator (or any member of the Portal Admins group) can also edit, view, and delete a user's personal content).

  Note: If you have installed the SAS Web Infrastructure Kit, only members of the Portal Admins group and group content administrators can add personal content to the portal Web application. If you have installed the SAS Information Delivery Portal, all users can add personal content to the portal Web application.

  Through the portal Options menu, a user can create personal pages, and then add or create portlets, including Xythos WFS WebDAV portlets, and collection portlets that contain content (such as applications, files, SAS Information Maps, links, packages, SAS publication channels, SAS Reports, SAS Stored Processes, and syndication channels). When a user creates a collection portlet, they can also create personal links. Personal content can only be edited and deleted by the user who created it (or any member of the Portal Admins group).

  The user who creates the personal content (and any member of the Portal Admins group) is granted the `ReadMetadata` and `WriteMetadata` permissions on the content.
- **share content with a group**. *Group Content* is content that has been shared with a group of users so that all users in the group can view it. Content can be shared with a group as follows:
  - ♦ The SAS Web Administrator (or any member of the Portal Admins group) can share their own or other users' personal pages (that contain content) with any group.
  - ♦ A user who is designated as a group content administrator for a group can share their personal pages (that contain content) with the group. To configure a user as a group content administrator, see Configuring a Group Content Administrator.

  When the SAS Web Administrator, any member of the Portal Admins group, or a group content administrator uses the portal Options menu Share feature to share (to a particular group) personal pages with collection portlets that contain content, the content becomes shared as follows:

  - ♦ For Web applications, links, pages, portlets, and syndication channels, the content is group content that is viewable by all users in the group. The users in the group are granted the `ReadMetadata` permission on the content.
  - ♦ For files on a Xythos WFS WebDAV server, SAS Stored Process, SAS Publication Channels, SAS Packages, SAS Information Maps, and SAS Reports, the users in the group are granted the `ReadMetadata` permission on the content and content is viewable as follows:
    - ◊ if there are NO additional access control restrictions, the content is group content that is viewable by all users.
    - ◊ if there are additional access control restrictions, only authorized users in the group can view the content.

  A group content administrator or a member of the Portal Admins group can edit group content. (The group content administrator and members of the Portal Admins group have `ReadMetadata` and `WriteMetadata` permissions on the content). A member of the Portal Admins group can also delete group content.
- **add content to share as Public content**. *Public Content* is content that has been shared with the Public group

so that all users can view it. Content can be shared to all users (the Public group) as follows:

- The SAS Web Administrator (or any member of the Portal Admins group) can share their own or other users' personal pages (that contain content) with the Public group so that all users can view it.
- A user who is designated as a group content administrator for the Public group can share personal pages (that contain content) to the Public group so that all users can view it. To configure a user as a group content administrator, see Configuring a Group Content Administrator.

When the SAS Web Administrator, any member of the Portal Admins group, or a group content administrator uses the portal Options menu Share feature to share (to the Public group) personal pages with collection portlets that contain content, the content becomes shared as follows:

- For Web applications, links, pages, portlets, and syndication channels, the content is Public group content that is viewable to all users.
- For files on a Xythos WFS WebDAV server, SAS Stored Process, SAS Publication Channels, SAS Packages, SAS Information Maps, and SAS Reports, the users in the group are granted the `ReadMetadata` permission on the content and content is viewable as follows:
  - if there are NO additional access control restrictions, the content is Public group content that is viewable by all users.
  - if there are additional access control restrictions, only authorized users in the group can view the content.

Public content can be edited by the group content administrator for the Public group, or any member of the Portal Admins group. (The group content administrator and members of the Portal Admins group have `ReadMetadata` and `WriteMetadata` permissions on the content). Members of the Portal Admins group can also delete the Public content.

Important Note: Remember, when you share a page, the portlets on the page are shared as well. When other users view a page that you have shared, they will see only the content in the portlets that they are authorized to see. For example, suppose the page that you share contains two portlets, one with a SAS Report that contains salary information and one with a SAS Report that contains company news items. If a user who is not authorized to view the SAS Report with salary information accesses the page, only the SAS Report with the news items will be visible to that user.

For details about creating personal content and sharing personal content with a group, refer to the online Help.

Security

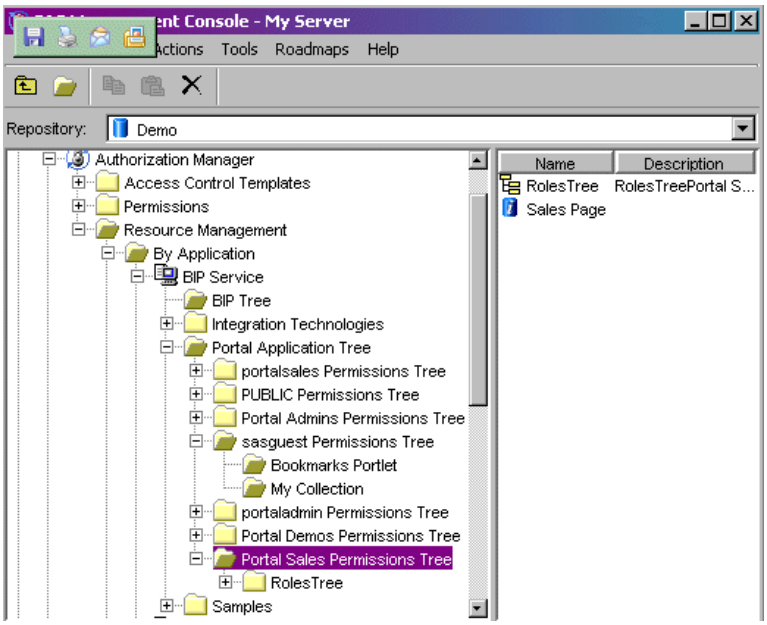
Configuring a Group Content Administrator

To share personal content with a group, a user must be a group content administrator of that particular group. After a group content administrator shares a page, they cannot delete that page. (Any member of the Portal Admins group can also share any user's content with any group. In addition, members of the Portal Admins group can delete shared pages).

Important Note: After you have set up your users and groups on the SAS Metadata Server, to enable the appropriate group permission trees to be created on the SAS Metadata Server, you must do one of the following:

- re−start the servlet container
- log in to the portal Web application as the SAS Web Administrator (or any member of the Portal Admins group)

To configure group content administrators, you must log in to the SAS Management Console as the SAS Administrator. To configure a user as the group content administrator for a particular group, in that group's permission tree of the Authorization Manager plug−in, you must directly assign the `WriteMetadata` permission to the user. (For details about directly assigned permissions, see the SAS Management Console Authorization Manager Help). The following screen shot shows a view of the Portal Application Tree in the SAS Management Console's Authorization Manager:



The Portal Application Tree contains permission trees for the individual users and groups that own content in the portal. To configure a user as a group content administrator, edit the Authorization tab of the appropriate group's permission tree, add the user, and directly assign the `WriteMetadata` permission to the user.

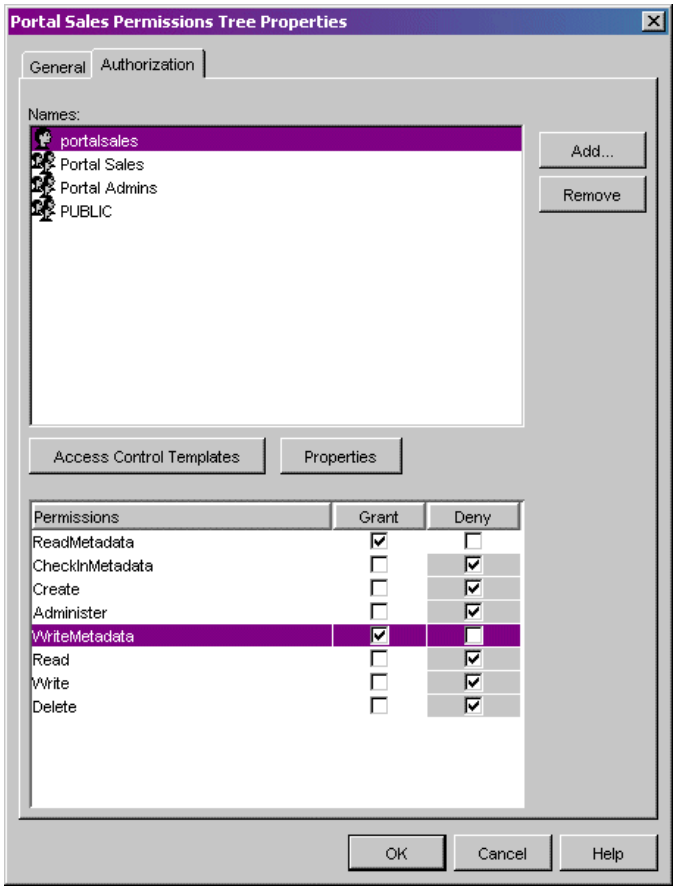
For example, the `Portal Sales` group and `portalsales` user were created for demonstration purposes. To configure a user (e.g. `portalsales`) as a group content administrator (e.g. `Portal Sales`), follow these steps:

1. Log in to SAS Management Console as the SAS Administrator.
2. In the navigation tree under the Authorization Manager, open the Resource Management folder, then open the BIP Service folder. Expand the Portal Application Tree folder.
3. In the Portal Application Tree folder, select the group for which you wish to assign a group content administrator.

4. From the main menu, select **File** ➧ **Properties**.
5. In the Properties dialog box, select the Authorization tab.
6. In the **Names** list box on the Authorization tab, select a user.

   Note: If a particular user or group is not listed, click **Add** and use the **Add Users and/or Groups** dialog box to add the user or group. When you return to the Authorization tab, make sure the appropriate user or group is selected in the **Names** list box.
7. To modify the permissions for the selected user, in the permissions list row for the `WriteMetadata` permission, select `Grant`.
   Note: The check box for a permission that comes from a directly assigned access control entry (ACE) has no added background color.

   The following screen shot of the Authorization tab shows the users and groups who have permissions set for the `Portal Sales` permission tree. The `portalsales` user has the `WriteMetadata` permission directly assigned.



   Important Note: If the check box for a permission has a background color, to remove the background color and designate the permission as a directly assigned permission, click the checkbox.
8. In the properties dialog box, click **OK** to save your changes.

The user that was configured as a group content administrator can now use the portal Options Share tool to share personal content with that group. For details, see Using Portal Options to Create Personal and Share Group Content.

Security

Using SAS Management Console to Set Up Authorization (Access Control)

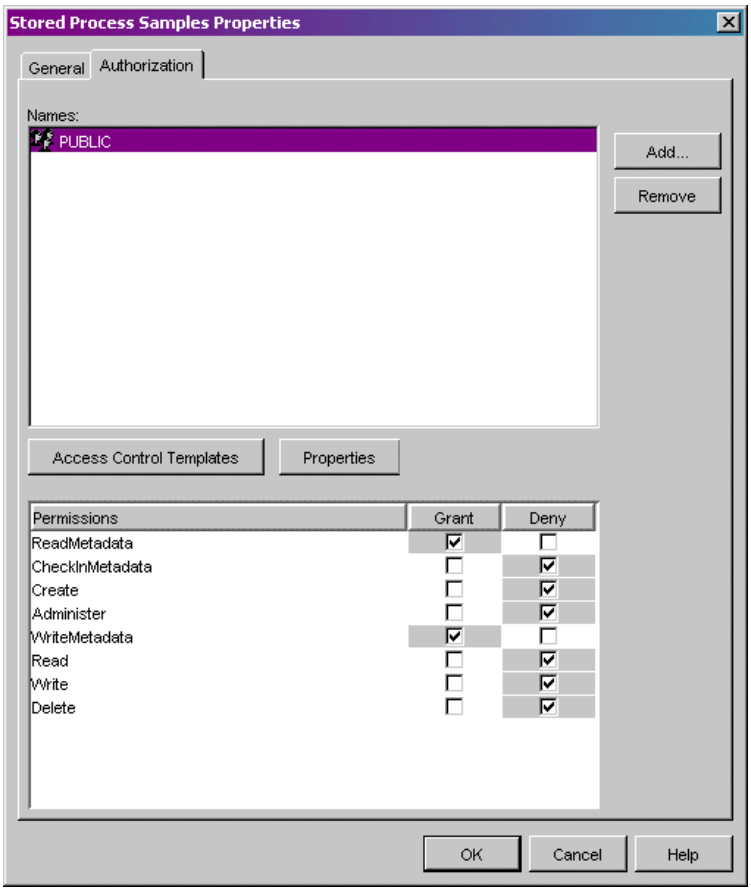
For certain content, such as SAS Stored Processes and SAS publication channels, you might need to implement authorization by manually assigning access controls for the content metadata on the SAS Metadata Server. You can also implement authorization for SAS Stored Processes and SAS publication channels by manually assigning access controls for the server−level metadata on the SAS Metadata Server. By granting or denying permissions in the metadata for the portal Web application's SAS Metadata Server, you can control security at virtually any level of granularity.

For general recommendations about planning for authorization (access control) and specific recommendations about planning for authorization for SAS Stored Processes, see "Planning your Access Controls" in the SAS Intelligence Architecture: Planning and Administration Guide.

To specify access control permissions, you can log in to SAS Management Console as a SAS Administrator and use the Authorization Manager plug−in to specify authorization metadata. SAS Management Console's Authorization Manager allows you to specify access control for SAS publication channels, SAS Stored Processes, servers, and their resources as follows:

- SAS Publishing Framework plug−in resources, including:
  - SAS publication channels. For users to self−subscribe to SAS publication channels, the user must have `ReadMetadata` access on the SAS Publication Channel.
  - SAS subscribers. In the portal Web application, subscriber profiles designate a set of personal preferences for subscribing to SAS publication channels. The SAS Administrator can also specify authorization metadata for the subscriber profiles.
- Server Manager plug−in resources, including:
  - SAS servers (SAS Workspace Server, SAS Stored Process Server, SAS OLAP Server)
- SAS Stored Processes Manager plug−in resources, including:
  - SAS Stored Processes
  - Paths in which stored processes reside

After you create a resource, you can use SAS Management Console to associate access controls with the resource. You associate access controls with a resource by modifying the resource's properties. The Authorization tab of a resource's Properties window maintains the authorization information:



Using SAS Management Console, you can open a resource's Properties window in either of the following ways:

- By using the plug−in in which the resource was created. You can use the Authorization Manager of SAS Management Console to access the Authorization tab for a resource and set permissions on the resource for the appropriate user or group. Directly assigned permissions always take precedence over any conflicting inherited or ACT−derived permissions.

  To directly assign permissions for a particular resource:

  1. In the appropriate plug−in, locate and select the resource.
  2. From the main menu, select **File** ➧ **Properties**.
  3. In the properties dialog box for the resource, select the Authorization tab.
  4. Use the Authorization tab to directly assign permissions.
- From the Resource Management folder of the Authorization Manager. The Resource Management folder of the Authorization Manager organizes the metadata stored in a repository by application, by physical location, and by type.

  1. Under the Authorization Manager's Resource Management folder, locate and select the resource.
  2. From the main menu, select **File** ➧ **Properties**.
  3. In the properties dialog box for the resource, select the Authorization tab.
  4. Use the Authorization tab to directly assign permissions.

For additional help on Authorization Manager and specifying access control, see the Authorization Manager help and Managing Authorizations in the *SAS Management Console: User's Guide*.

Content

This chapter provides information about adding content to the portal Web application. This content might require SAS servers as follows:

- To add portal Web application content, you are not required to have specific SAS servers defined and deployed.
- To add SAS content items, you must ensure that the appropriate servers for that content are already defined and deployed. For details, see Deploying Servers.

After you have ensured that the appropriate servers are deployed you can begin to add content to the portal Web application. All content requires the addition of metadata to the SAS Metadata Repository; this metadata consists of the following:

- content metadata, or metadata that describes the particular content
- authorization metadata, or metadata that specifies which SAS users and groups are authorized to access the content.

The portal Web application allows you to add the following types of content:

- **portal Web application content for which you administer the content and authorization metadata.** For some types of portal Web application content, you must perform some additional administration in order for that content item to be available for use in the portal Web Application. You must then ensure that the appropriate users are authorized to access the content.
- **portal Web application content for which the portal Web application administers content metadata and you administer authorization metadata.** For certain types of portal Web application content, you add the content item, and the portal Web application administers the metadata that allows the content to be available for use in the portal Web Application. You must then ensure that the appropriate users are authorized to access the content.
- **SAS content for which you administer content metadata and authorization metadata.** For some types of SAS content, you must perform additional administration in order for those content items to be available for use in the portal Web Application. You must then ensure that the appropriate users are authorized to access the content.
- **SAS content, such as SAS Information Maps and SAS reports, that has already had the administration performed by the SAS Information Map Studio or SAS Web Report Studio application.** For some types of SAS content, such as SAS Information Maps and SAS reports, the producing application and its administrator create the content and authorization metadata. The portal Web application allows a user to search the SAS Metadata Repository for this content and presents the search results as available content for users.

  In addition, content and authorization metadata for SAS Stored Processes might already have been administered by the SAS Enterprise Guide application.

The following table shows the content category, the content item, icon, description, and the administration tool used to add the portal Web application content to the SAS Metadata Repository or Xythos WFS WebDAV repository. You must then ensure that the appropriate users are authorized to access the content. Click on the content item to see detailed information about administering and adding the content to the portal Web application.

Metadata in the Portal Metadata Repository

Category	Content	Description	How to Add Content Metadata
Portal Web application Content	**Web Application** 	a Web−based computer program. An administrator must administer the content and authorization metadata for the application in order to add it to the portal Web application. Authorized users can then launch the application from the portal Web application shell. For information about developing applications, see the *SAS Web Infrastructure Kit Developer's Guide*.	SAS
	File (SAS Information Delivery Portal and Xythos WFS WebDAV server only) 	a file of any type. Files allow portal Web application users (who have access) to view a variety of document types in the portal Web application shell. An administrator must add files to the Xythos WFS WebDAV repository in order to make them available for access in the portal Web application. When the administrator adds the file to the Xythos WFS WebDAV server, the content metadata is available to the portal Web application. The administrator must add the authorization metadata. If you have installed the SAS Information Delivery Portal with a Xythos WFS WebDAV server, authorized users can add files to the portal Web application.	Xythos WFS WebDAV server tools
	Link 	content that is addressable using a universal resource locator (URL). Users can create links to sites on the Web or on a local intranet. When users add a link to the portal Web application, the appropriate content and authorization metadata is updated. Authorized users can then display these Web or intranet links.	Portal
	Page Template	a Web page in the portal Web application shell that is a template Page which contains portlets. An administrator must administer the content and authorization metadata for the page template in order to add it to the portal Web application of a specific user or group. Authorized users can then edit the portlets on the page template.	SAS
	Portal Web Application Shell Page 	a Web page in the portal Web application shell that contains portlets. When users create, add, edit, rearrange, and remove pages in your personal portal Web application view,	Portal Options

		the appropriate content and authorization metadata is updated. To specify group content administrators for the page, you must log in to SAS Management Console as the SAS Administrator and configure the appropriate group content administrator. The group content administrator (or a member of the Portal Admins group) can then share that page with a group of users.	
	Custom−Developed Portlet 	a rectangular display component of the portal Web application shell in which content and links to content are displayed. Administrators can add custom−developed local or remote portlets to the portal Web application. When the administrator adds the portlet, the hot−deploy mechanism updates the content and authorization metadata. Users can then add these portlets to a page.	Portlet Hot−Deploy Mechanism
	Portlet 	a rectangular display component of the portal Web application shell in which content and links to content are displayed. Users can create portlets from template portlets or add predefined portlets to a page in the portal Web application. The portal Web application administers the content and authorization metadata for these portlets. Users who are group content administrators (or any member of the Portal Admins group) can then share that page with a group of users.	Portal Options
	Syndication Channel (SAS Information Delivery Portal only) 	a channel that provides syndicated, continuously updated Web content. If you have installed the SAS Information Delivery Portal, users can add syndication channels to the portal Web application. An administrator must administer the content and authorization metadata for the syndication channel in order to add it to the portal Web application. Authorized users can then view the syndication channel from the portal Web application.	SAS
SAS Content	**SAS Publication Channel (SAS Information Delivery Portal only)** 	a channel created by the SAS Publishing Framework. Publication channels can be used to provide access to archived content published through the SAS Publication Framework. To enable users to add SAS publication channels to the portal Web application, you must log in to SAS Management Console as the SAS	***Channels:*** Publishing Framework plug−in ***Subscribers:*** Publishing Framework plug−in ***Published packages:*** Publishing Framework plug−in

	Administrator and define publication channel content and authorization metadata. If you have installed the SAS Information Delivery Portal, authorized users can then subscribe to, view the contents of, and publish content to SAS publication channels.	
Package (SAS Information Delivery Portal only) 	a collection of structured and unstructured content that has been published using the SAS Publishing Framework. The content and authorization metadata is part of the metadata for the SAS publication channel or Xythos WFS WebDAV repository. If you have installed the SAS Information Delivery Portal, authorized users can add packages to the portal Web application if they have been published to a SAS publication channel or to a Xythos WFS WebDAV repository.	The applications that use SAS Publishing Framework to create the package metadata and the physical archives. When the packages or archive expires, the portal Web application shell manages cleanup of the metadata and physical archives.
SAS Stored Process 	a SAS program that is stored in a central location and is available to be executed on a request basis. To enable users to add stored processes to the portal Web application, you might need to log in to SAS Management Console as the SAS Administrator to define stored process content and authorization metadata. However, in some cases, the metadata might have been administered by the producing application (e.g., SAS Enterprise Guide). Authorized users can then run stored processes from the portal Web application.	Stored Process Manager plug−in and SAS Enterprise Guide
SAS Information Map (SAS Information Delivery Portal only) 	business−oriented view of multi−dimensional and relational data, which can be used to easily develop ad hoc reports. SAS Information Maps are available in the portal Web application shell if your organization has installed SAS Information Map Studio. The information map metadata is administered by SAS Information Map Studio and the information map administrator.	SAS Information Map Studio
SAS Report (SAS Information Delivery Portal only) 	a visual representation of data models and the results of analysis and summarization of the data from SAS procedural output. A SAS report is stored in the SAS Report Model format. Reports are available in the portal Web application if your organization has	SAS Web Report Studio

		installed SAS Web Report Studio. The report metadata is administered by the reporting applications and the report administrator.	

Content

Content Table

Based on the software that your organization has installed, you can use the following table to determine the availability of features:

Feature	Software Installed			
	SAS Web Infrastructure Kit		SAS Information Delivery Portal	
	Without Xythos WFS WebDAV Server	With Xythos WFS WebDAV Server	Without Xythos WFS WebDAV Server	With Xythos WFS WebDAV Server
Launch applications	Yes	Yes	Yes	Yes
View links	Yes	Yes	Yes	Yes
Use personalization features	Yes (content administrators only)	Yes (content administrators only)	Yes (all users)	Yes (all users)
Execute dynamic SAS Stored Processes	Yes	Yes	Yes	Yes
Execute SAS Stored Processes running in the background and view results stored in WebDAV	No	Yes	No	Yes
View files stored in WebDAV	No	Yes	No	Yes
Manage subscriptions to publication channels	No	No	Yes	Yes
Publish portal content to publication channels	No	No	Yes	Yes
Publish portal content to WebDAV	No	No	No	Yes
View published packages stored on a server	No	No	Yes	Yes
View published packages stored in WebDAV	No	No	No	Yes
View syndication channel content	No	No	Yes	Yes
View SAS reports (Preproduction Feature) **Note:** SAS Web Report Viewer must be installed.	No	No	Yes	Yes

View SAS information maps (Preproduction Feature) **Note:** SAS Information Map Studio must be installed.	No	No	Yes	Yes

Content

Adding Portal Content

For portal Web application content, the appropriate metadata is added to the SAS Metadata Repository or the WebDAV repository in one of the following ways:

- When you add content to a portlet in the Web application, the portal Web application updates the metadata repository.
- When you want to add portal Web application content to the portal Web application, you must first administer the content metadata using the appropriate administration tools for the metadata repository. (For an overview of the metadata administration tools, see Understanding the Administration Tools.)
- When you want to add WebDAV content to the portal Web application, you must first add the WebDAV content to the WebDAV server using the appropriate administration or publishing tools.

In any of these cases, you might want to implement authorization (access controls) for the content so that only the appropriate users can access that content. For an overview of access control for content, see Authorizing Access to Content.*Content*

Adding Web Applications

To design and develop a custom Web application for access from the portal, you should have a working knowledge of JavaServer Pages (JSPs), Java servlets, and the Java programming language. A Web application can be either a standard Web application or a foundation services−enabled Web application. In addition, a Web application can be accessed both from within the portal Web application and from outside the portal Web application. To implement a Web application in the portal Web application, you can

- **implement a remote portlet and a corresponding Web application**. A remote portlet looks like any other portlet, but it calls a remote Web application. The remote Web application returns an HTML fragment to the portal Web application to be displayed within the portlet's borders. This approach is useful when you want to incorporate a portion of the output from your application into the portal. To add a remote portlet and corresponding Web application to the portal Web application, see Adding Custom−Developed Portlets.
- **implement a stand−alone application that is invoked from the portal Web application but executed remotely**. The Web application returns a complete HTML page, which is displayed in a separate browser window. This approach is useful when you want to enable portal Web application users to invoke your application from the portal, but the application output needs to appear separately. To add a stand−alone Web application, follow the instructions on this page.

Follow these steps to develop a custom Web application and add it to the portal Web application:

1. Design and code the Web application.
2. Deploy the Web application's WAR file in the servlet container.
3. Ensure that the appropriate user or group permission tree is created in the SAS Metadata Repository.
4. Add the Web application's metadata to the SAS Metadata Repository.
5. Ensure that the appropriate resource metadata is added to the SAS Metadata Repository.
6. Add the permission statements for the Web application to the required policy files.
7. Implement authorization (access control) for the Web application.
8. Add the Web application to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal Web application users.

Step 1: Design and Code the Web Application

Design and code your Web application.

For information about developing and integrating Web application with the portal Web application, see Integrating Web Applications With the Portal in the *SAS Web Infrastructure Kit Developer's Guide*. For a detailed example of a Web application that uses the SAS Foundation Services, see Sample: Web Application (HelloUserWikExample) in the *SAS Web Infrastructure Kit Developer's Guide*.

When you have finished coding the Web application, proceed to Step 2.

Step 2: Deploy the Web Application's WAR file in the Servlet Container

After you code the Web application, you must create a WAR file for the Web application. You must then deploy your Web application into the servlet container.

In addition, if the Web application is a foundation service−enabled Web application, you must add permissions to the SAS Services application's policy file. For details, see Adding Permission Statements for Services to Policy File.

Step 3: Ensure that the appropriate User or Group Permission Tree Is Created in the SAS Metadata Repository

When you add the Web application metadata (content metadata) in Step 4, you also add the authorization metadata. To authorize the appropriate user or group metadata identity for access from within the portal Web application, you can load the metadata and add and share the Web application in one of the following ways:

- **Add the Web application metadata to a user**. When you add the metadata to a user, the user is granted `ReadMetadata` and `WriteMetadata` permissions to enable the user to view and edit the content. The Web application can then be shared to a group as follows:
    1. If required, you can log in to SAS Management Console as the SAS Administrator and configure the appropriate group content administrator (Step 7).
    2. A user adds the Web application to a collection portlet on a page in the portal Web application (Step 8).

       Note: If the SAS Information Delivery Portal is installed, all users can add content to the portal Web application. If only the SAS Web Infrastructure Kit is installed, only members of the Portal Admins group and content administrators can add content to the portal Web application.
    3. A user who is a group content administrator or member of the Portal Admins group (e.g., SAS Web Administrator) shares the page with a group so that the Web application is accessible to members of the group (Step 8).
- **Add the Web application metadata to a group**. When you add the Web application metadata to a group, the group is granted `ReadMetadata` permission to enable the group members to view the content.

Note: When you load the metadata for the content, the Public group is denied `ReadMetadata` and `WriteMetadata` permissions for the content.

Before you can add the Web application authorization metadata in Step 4, the appropriate user or group permission tree must be created. To ensure that the user or group permission tree is created:

1. Ensure that you have defined the appropriate user or group (on the SAS Metadata Server) that you will add the metadata to in Step 4.
2. Enable the permission tree to be created as follows:
    - **If you are adding the metadata to a group**, and you added the group to the SAS Metadata Server after starting the servlet container, to enable the portal Web application to create the appropriate group permission tree, do either of the following:
        - Log in to the portal Web application as a member of the Portal Admins group (e.g. SAS Web Administrator).
        - Restart the servlet container.
    - **If you are adding the metadata to a user**, to create the user permission tree, log in to the portal Web application as that user.

Step 4: Add the Web Application's Metadata to the SAS Metadata Repository

To define the Web application in the SAS Metadata Repository, you must modify and run the `LoadWebApplicationExample.sas` SAS program (located in the `OMR` directory of your installation) to load the Web application's metadata into the SAS Metadata Repository.

Edit the `LoadWebApplicationExample.sas` SAS program and specify the appropriate variables for your Web application:

options metaserver="<host>"
: Specify the host name of the SAS Metadata Server. Use the value of the `$SERVICES_OMI_HOST$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory). For example:

```
localhost
machine
machine.mycompany.com
```

metaport=<port>
: Specify the port number of the SAS Metadata Server. This value is a number between 0 and 65536. Use the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

metauser="<user ID>"
: Specify the user ID to use to connect to the SAS Metadata Server; this user ID is typically the SAS Administrator (default, sasadm). For Windows users, the user ID is domain or machine name qualified. For example,

```
machine\saswbadm  where machine is the local machine
NTDOMAIN\saswbadm where NTDOMAIN is the Windows authentication domain
```

metapass="<password>"
: Specify the password for the metauser.

metarepository="<repository>";
: Specify the name of the SAS Metadata Repository where your portal Web application metadata is stored, followed by a ";". Use the value of the `$SERVICES_OMI_REPOSITORY$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

%let groupOrUserName=<SAS User or Group>;
: Specify the SAS group or user that you want to add the data to, followed by a ";".

%let webappName=<Web application name>;
: Specify the name of the Web application that you want to create, followed by a ";".

%let webappDescription=<Web application description>;
: Specify the description of the Web application that you want to create, followed by a ";".

%let webappURI=<Web application URI>;
: Specify a valid URL for the Web application, followed by a ";"

Step 5: Ensure That the Appropriate Resource Metadata Is Added to the SAS Metadata Repository

If your data resources have already been defined in the metadata repository, you can skip this step.

To enable the Web application to leverage SAS content and security features, you must ensure that the appropriate metadata for each resource has been added to the portal Web application's SAS Metadata Repository. Resources might include SAS Stored Processes, SAS Information Maps, SAS packages, SAS publication channels, and SAS Reports. The SAS servers, spawners, and logins associated with the resources must also be defined.

For an overview of metadata requirements, see the following:

- for server metadata, refer to Deploying SAS Servers
- for content metadata, refer to the metadata addition steps in the appropriate content section of the Content chapter.

In addition, when you add SAS publication channels, syndication channels, and servers, you must enable your Web application to access the content by specifying the appropriate permissions in your servlet container's policy file.

Note: Although the metadata for Web application sources must be added to the SAS Metadata Repository, it is not necessary for these data sources to be surfaced in Web applications.

Step 6: Add the Permission Statements for the Web Application to the Required Policy Files

Add the Web application's codebase and permissions, and any additional permissions for the Portal, and SAS Services codebases to the required policy file. For details, see Adding Permissions to Policy Files.

Step 7: Implement Authorization (Access Control) for the Web Application

Take any additional necessary steps to control access to the Web application.

Note: When you implement authorization (access control), access to content is only controlled from within the portal Web application. Users outside of the portal Web application will be able to use the Web application's URL to access the Web application.

For general information about access control, see Authorizing Access to Content.

Step 8: Add the Web Application to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) With Other Portal Users.

Depending on who has access permission to the Web application, users can use one of several methods to make it appear in the portal Web application:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a Web application to a collection portlet on a page. The SAS Web Administrator can then use the portal Options menu to share the page (that contains the portlet) with the following:
    - ♦ any SAS group defined in the portal Web application's SAS Metadata Repository
    - ♦ the Public group (accessible to all users).
- A group content administrator can edit a portlet to add a Web application to a collection portlet on a page. The group content administrator can then share the page as follows:
    - ♦ If the user is the group content administrator for the Public group, the user can use the portal Options menu to share the page with the Public group (all users).
    - ♦ If the user is the group content administrator for a particular group, the user can use the portal Options menu to share the page (that contains the portlet) with that group.

- If you have installed the SAS Information Delivery Portal, all users can also edit a portlet to add a Web application to a collection portlet on a page.

Once the page (that contains the portlet with the Web application) is shared with a group, all members of that group can access the Web application as group content. If the page is not shared to a group, it is only accessible to the user who created the page.

For more information about using the portal Options menu, refer to the online Help.

Content

Adding Files

Note: If you have installed the SAS Information Delivery Portal and your organization's portal installation includes Xythos WebFile (WFS) WebDAV support, users can add files to the portal Web application.

A file can be a file of any type. You must add files to the Xythos WFS WebDAV repository in order to make them available in the portal Web application. Files allow portal users (who have access) to view a variety of document types in the portal Web application shell. When a user selects a file for viewing, the browser displays it using the appropriate software based on the MIME type that is assigned to the file.

To add a file to the portal:

1. Add the file to a Xythos WebFile Server (WFS) WebDAV server.
2. Implement authorization (access control) for the file.
3. Add the file to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal users.

Step 1: Add the File to the Xythos WebFile Server (WFS) WebDAV Server

Note: If you have installed the SAS Information Delivery Portal, you might already have group folders set up for SAS Reports that are stored on the Xythos WFS WebDAV server.

Note: It is recommended that the base path for the Xythos WFS WebDAV server be a blank value. If you need to reconfigure the base path for the Xythos WFS WebDAV server, see Reconfiguring the Base Path for the Xythos WFS WebDAV Server.

You can add the file to a personal folder for personal access or to a group folder for group access as follows:

- To add the file to the Xythos WFS WebDAV repository for a user's personal access:

    1. Login (to the portal Web application) as the user in order to create the user's personal repository directory on the Xythos WFS WebDAV server.
    2. Use the administration tool provided with the Xythos WFS WebDAV server to locate the appropriate user folder (located under the root Xythos WFS WebDAV installation directory) for the content.
    3. Use an administration tool (such as Microsoft Web Folders) to add content to the appropriate folder(s).
- To add the file to the Xythos WFS WebDAV repository for group access:

    1. Determine which SAS group(s) will access the content.
    2. Use the administration tool provided with the Xythos WFS WebDAV server to create the appropriate group folder(s) for the content.
    3. Use an administration tool (such as Microsoft Web Folders) to add content to the appropriate folder(s).

Microsoft Web Folders

Microsoft Web folders provide an easy way for you to manage files and folders on Web servers. You can use Microsoft Web folders to manage files and folders on a Web server just as you would perform the same actions in

Windows Explorer. When you view the contents of a Web folder, a list of files and folders and their associated Internet addresses is displayed.

To access Microsoft Web Folders on Windows 2000, NT, or XP,

1. From your Windows desktop, double−click **My Network Places**. The **My Network Places** folder opens.
2. From your My Network Places folder, double−click **Add Network Place**. The **Welcome to the Add Network Place Wizard** appears.
3. Follow the wizard screens and fill in the fields with the required values.

When you are finished, a Microsoft Web Folder appears which contains your WebDAV server files.

See Microsoft Windows online help for information about using **My Network Places** and the **Add Network Place Wizard**.

Step 2: Implement Authorization (Access Control) for the File

Take any necessary steps to control access to the file. For a Xythos WFS WebDAV server, use the access control tools provided with the Xythos WFS WebDAV server. For general information about access control, see Authorizing Access to Content.

Step 3: Add the File to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) with Other Portal Users.

Depending on who has access permission to the file, you can use one of several methods to make it appear in the portal Web application:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a file to a collection portlet on a page. The SAS Web Administrator can then use the portal Options menu to share the page (that contains the portlet) with the following:
  - any SAS group that is authorized to access the file's folder on the Xythos WFS WebDAV repository
  - the Public group (accessible to all users), if the Public group has access to the file's folder on the Xythos WFS WebDAV repository.
- A group content administrator can edit a portlet to add a file to a collection portlet on a page. The group content administrator can then share the page as follows:
  - If the user is the group content administrator for the Public group, if the Public group is authorized to access the file's folder on the Xythos WFS WebDAV repository, the user can use the portal Options menu to share the page with the Public group (all users).
  - If the user is the group content administrator for a particular group, if that group is authorized to access the file's folder on the Xythos WFS WebDAV repository, the user can use the portal Options menu to share the page (that contains the portlet) with that group.
- All users can also edit a portlet to add a file to a collection portlet on a page.

Users can also publish the file to a SAS Publication Channel and then either add the SAS Publication Channel or SAS Package to a collection portlet or add the Publication Channel Subscriptions Portlet to their portal Web application. For details, see Adding SAS Packages and Adding SAS Publication Channels.

For more information, refer to the online Help.

Content

Adding Links

A link is content that is addressable using a universal resource locator (URL). Users can create links to sites on the Web or on a local intranet. When a user add a link, the appropriate metadata is updated. Users (who have access) can then include the links in collection portlets and display them on pages in the portal Web application.

Note: Since the document can be accessed through a URL that is independent of the portal Web application, the portal Web application does not secure the physical document. However, you can secure the document through Web server security.

To add a new link to the portal Web application:

1. Add a link to the portal Web application and the SAS Metadata Repository.
2. Implement authorization (access control) for the link.
3. Add the link to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal Web application users.

Step 1: Use the Portal Options Menu to Add the Link to the Portal Web Application and the SAS Metadata Repository

Note: If you installed the SAS Information Delivery Portal, all users can use the portal Options menu to create personal content. If you installed only the SAS Web Infrastructure Kit, members of the Portal Admins group and group content administrators can use the portal Options menu to create personal content.

A user can add a new link to the portal Web Application's SAS Metadata Server by either of the following two ways:

- Add a collection portlet and edit the collection portlet to add a new link item to the collection portlet.
- Edit an existing collection portlet and add a new link item to the collection portlet.

When a user adds a new link, the Web application provides a graphical user interface for adding the name, description, and URL address for the link. (When a user adds a new link to a new collection portlet, the portal Web application also adds the appropriate content metadata to the SAS Metadata Server.)

Step 2: Implement Authorization (Access Control) for the Link

Take any necessary steps to control access to the link. For general information about access control, see Authorizing Access to Content.

Step 3: Add the Link to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) with Other Portal Users.

Depending on who has access permission to the link, you can use one of several methods to make it appear in the portal Web application:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a link to a collection portlet on a page. The SAS Web Administrator can then use the portal Options menu to share the

page (that contains the portlet) with the following:
    - any SAS group defined in the portal Web application's SAS Metadata Repository
    - the Public group (accessible to all users).
- A group content administrator can edit a portlet to add a link to a collection portlet on a page. The group content administrator can then share the page as follows:
    - If the user is the group content administrator for the Public group, the user can use the portal Options menu to share the page with the Public group (all users).
    - If the user is the group content administrator for a particular group, the user can use the portal Options menu to share the page (that contains the portlet) with that group.
- If you have installed the SAS Information Delivery Portal, all users can also edit a portlet to add a link to a collection portlet on a page.

Once the page (that contains the portlet with the link) is shared with a group, all members of that group can access the link as group content.

Users can also add the file to a SAS publication channel and then either add the SAS publication channel or SAS package to a collection portlet or add the Publication Channel Subscriptions Portlet to their portal Web application. For details, see Adding SAS Packages and Adding SAS Publication Channels.

For more information about using the portal Options menu, refer to the online Help.

Content

Adding Pages

A page is a Web page in the portal Web application shell that contains portlets.

To add a page to the portal Web application:

1. Use the portal Options menu to add a page.
2. Implement authorization (access control) for the page.
3. Use the portal Options menu to share the page.

Step 1: Use the Portal Options Menu to Add a Page

Note: If you have installed the SAS Web Infrastructure Kit, only members of the Portal Admins group and group content administrators can add pages to the portal Web application. If you have installed the SAS Information Delivery Portal, all users can add pages to the portal Web application.

Use the portal Options menu to add a page to the portal Web application. The page will then appear as a tab on the portal Web application. For details about adding a page, refer to the online Help. When you have finished adding the page, proceed to Step 2.

Step 2: Implement Authorization (Access Control) for the Page

Take any necessary steps to control access to the page. For general information about access control, see Authorizing Access to Content.

Step 3: Use the Portal Options Menu to Share the Page

Depending on who is authorized to share the page, users can share the page with a group to make the page appear on the group member's portal Web application as one of the following types:

- **Available**. Available public pages are pages that all users can find using the search tool. Any user can add these pages to their personal portal Web application.
- **Default**. Default public pages are automatically added to the portal Web application of all users. Users can then remove the page if they do not need it.
- **Sticky**. Sticky public pages are automatically added to the portal Web application of all users, and users cannot remove them.

Users can share the page with a SAS group as follows:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can use the portal Options menu to share the page with the following:
  - ♦ any SAS group defined in the portal Web application's SAS Metadata Repository
  - ♦ the Public group (accessible to all users)
- If a user is the group content administrator for the Public group, the user can use the portal Options menu to share the page with the Public group (all users).
- If a user is the group content administrator for a particular group, the user can use the portal Options menu to share the page with that group.

For more information about using the portal Options menu, refer to the online Help.

Content

Adding Page Templates

A page template is a specific implementation of a Page definition. Page templates allow an administrator to define which pages a new user will see the first time they log in to the portal Web application.

Important Note: In most cases, if you have not installed the SAS Information Delivery Portal, all users (i.e. users who are not group content administrators or members of the Portal Admins group) cannot personalize their portal. However, for a SAS Web Infrastructure Kit−only installation, if you add a page template to a user's portal Web application, then all of the users can use the portal Options menu to edit the collection portlets on that page template.

To add a page template to the portal Web application:

1. Ensure that the appropriate group permission tree is created in the SAS Metadata Repository.
2. Add the page template's metadata to the SAS Metadata Repository.

Step 1: Ensure That the Appropriate Group Permission Tree Is Created in the SAS Metadata Repository

Before you can add the page template authorization metadata in Step 2, the appropriate group permission tree must be created. To ensure that the group permission tree is created:

1. Ensure that you have defined the appropriate group (on the SAS Metadata Server) that you will add the metadata to in Step 2. When you add the metadata to a group, the group is granted `ReadMetadata` permission to enable the group members to view the content.
2. If you added the group to the SAS Metadata Server after starting the servlet container, to enable the portal Web application to create the appropriate group permission tree, do either of the following:
    - Log in to the portal Web application as a member of the Portal Admins group (e.g. SAS Web Administrator).
    - Restart the servlet container.

Step 2: Add the Page Template's Metadata to the SAS Metadata Repository

To define the page template in the metadata repository, you must modify and run the `LoadPageTemplateExample.sas` SAS program (located in the `OMR` directory of your installation) to load the Web application's metadata into the SAS Metadata Repository.

Edit the `LoadPageTemplateExample.sas` SAS program and specify the appropriate variables for your Web application:

options metaserver="<host>"
: Specify the host name of the SAS Metadata Server. Use the value of the `$SERVICES_OMI_HOST$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory). For example:

```
localhost
machine
machine.mycompany.com
```

metaport=<port>

Specify the port number of the SAS Metadata Server. This value is a number between 0 and 65536. Use the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

metauser="<user ID>"

Specify the user ID to use to connect to the SAS Metadata Server; this user ID is typically the SAS Administrator (default, `sasadm`). For Windows users, the user ID is domain or machine name qualified. For example,

```
machine\saswbadm  where machine is the local machine
NTDOMAIN\saswbadm where NTDOMAIN is the Windows authentication domain
```

metapass="<password>"

Specify the password for the metauser.

metarepository="<repository>";

Specify the name of the SAS Metadata Repository where your portal Web application metadata is stored, followed by a ";". Use the value of the `$SERVICES_OMI_REPOSITORY$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

%let groupOrUserName=<SAS User or Group>;

Specify the SAS group or user that you want to add the data to, followed by a ";".

%let pageName<Page Template Name>;

Specify the name of the page template that you want to create, followed by a ";".

%let pageDescription=<page template description>;

Specify the description of the page template that you want to create, followed by a ";".

%let shareType<Sticky or Default>;

Specify whether the page is Sticky or Default, followed by a ";".

Default.

Default user or group pages are automatically added to the portal Web application of the user, or all users in a group. The users can then remove the page if they do not need it.

Sticky

Sticky group pages are automatically added to the portal Web application of the user, or all users in the group and the users cannot remove them.

%let profile=DESKTOP_PROFILE;

DO NOT change this value.

%let role=DefaultRole;

DO NOT change this value.

data pageTemplate;

Specifies the SAS dataset that defines the data values for the page template contents. DO NOT modify the section between the "data pageTemplate" line and the "cards4" line, which describes the data in the dataset.

The data between the "cards4" line and the ";;;;" line describes each portlet (1 / line) that you want to place on the page template. The line is formatted as a csv (comma separated values) line and each column denotes a different value for the portlet.) For example, the following lines create four portlets, two in each page column:

```
1,1,Bookmarks,Bookmarks portlet Description,Bookmarks template
1,2,Alerts,Alerts portlet Description,Alerts template
2,1,My collection Portlet,Description of collection portlet,Collection template
2,2,Welcome,Welcome portlet Description,Welcome template
;;;;
```

columnNum

specifies the column number on the page in which to place the portlet. Each page in the portal Web application can have multiple columns (maximum of three columns).

portletPos

specifies the order of the portlets within the column; the portlets are ordered from lowest number to highest number.

portletName

specifies the name of the portlet to add. If a portlet already exists with the same portletName, the existing portlet is used and a new portlet will not be created. This field cannot contain a comma.

portletDescription

Specifies the description of the portlet to add. This field cannot contain a comma.

prototypeName

specifies the name of the prototype that was created when the portlet was deployed. This field cannot contain a comma.

After you run the SAS program to load the page template to a SAS user or SAS group, that page template will appear in the navigation bar of the user's or group's portal Web application. Users can then add portlets to the page. For details, see the online Help.

Content

Adding Custom−Developed Portlets

A portlet is a rectangular display component of the portal Web application shell in which content and links to content are displayed. You can develop a custom portlet and add it to the portal Web application. Your custom−developed portlet can be either a local portlet (contained in a PAR file) or a remote portlet (contained in a PAR file and a WAR file).

To design and develop a custom local or remote portlet for deployment in the Web application, you should have a working knowledge of JavaServer Pages (JSPs), Java servlets, and the Java programming language. Once you have developed a portlet, you can add it to the portal. The *SAS Web Infrastructure Kit Developer's Guide* provides guidance for developing custom portlets. To develop a custom portlet and add it to the Web application, follow these steps:

1. Design and code the portlet.
2. Deploy the portlet in the portal Web application.
3. Ensure that the appropriate resource metadata is added to the SAS Metadata Repository.
4. For remote portlets only, add the permission statements for the portlet to the required policy files.
5. Add the portlet to the portal Web application.

Step 1: Design and Code the Portlet

For details about designing and coding the portlet, see the *SAS Web Infrastructure Kit Developer's Guide*. When you have finished coding the portlet, proceed to Step 2.

Step 2: Deploy the Portlet in the Portal Web Application

To enable deployment of the portlet in the portal Web application, move or copy the PAR file to the portlet deployment directory. To verify the location of your portlet deployment directory, see the `$PORTLET_DEPLOY_DIR$` value in the `install.properties` file. The portal Web application automatically adds the portlet to the SAS Metadata Repository. For details about how the portal Web application deploys the portlets into the Web application and adds the portlet metadata to the Web application's metadata repository, see Portlet Deployment.

If the portlet is a remote portlet, you must also do the following:

1. Deploy the WAR file in the servlet container.
2. Add permissions to the SAS Services application's policy files. For details, see Adding Permission Statements for Services to Policy File.

Step 3: Ensure That the Appropriate Resource Metadata Is Added to the SAS Metadata Repository

If your data resources have already been defined in the metadata repository, you can skip this step.

To enable the portlet to leverage the portal Web applications content and security features, you must ensure that the appropriate metadata for each resource has been added to the portal Web application's SAS Metadata Repository. Resources might include SAS Stored Processes, SAS Information Maps, SAS packages, SAS publication channels, and SAS Reports. The SAS servers, spawners, and logins associated with the resources must also be defined. For an overview of metadata requirements, see the following:

- for server metadata, refer to Deploying SAS Servers.
- for content metadata, refer to the appropriate content section of the Content chapter.

In addition, when you add SAS publication channels, syndication channels, and servers, you must enable your portlet to access the content by specifying the appropriate permissions in your servlet container's policy file.

Note: Although the metadata for portlet data resources must be added to the SAS Metadata Repository, it is not necessary for these data resources to be surfaced in portlets.

Step 4: For Remote Portlets Only, Add the Permission Statements for the Portlet to the Required Policy Files

Add the remote portlet's codebase and permissions, and any additional permissions for the portal Web application and SAS Services application codebases to the required policy file. For details, see Adding Permissions to Policy Files.

Step 5: Add the Portlet to the Portal Web Application

To add your custom−developed portlet to the portal Web application, see Adding Portlets.

Content

Adding Portlets

A portlet is a rectangular display component of the portal Web application shell in which content and links to content are displayed.

Note: If you have installed the SAS Web Infrastructure Kit, only members of the Portal Admins group and group content administrators can add portlets to the portal Web application. If you have installed the SAS Information Delivery Portal, all users can add portlets to the portal Web application.

Users can do either of the following:

- **Create their own portlets from portlet templates**. Portlet templates are available for users to use as a basis for creating their own portlets, which the user can then edit. The following portlet templates are delivered with the portal Web application:
    - ♦ collection portlets
    - ♦ WebDAV navigator portlets (if you have installed the Xythos WFS WebDAV server)

      Note: When a user adds a WebDAV navigator portlet, they can only view the Xythos WFS WebDAV content that they are authorized to access.
    - ♦ URL display portlet

      Note: In order for users to add specific URLs to a URL display portlet that is not displayed in an inline frame (IFRAME), the administrator must have already added the appropriate access permissions in the policy file. Therefore, only administrators should add a URL display portlet that does not display in an IFRAME.

  Your organization can develop and deploy additional portlet templates for users to use as a basis for creating their own portlets. For details, see the *SAS Web Infrastructure Kit Developer's Guide*.
- **Add predefined portlets**. The portal Web application also contains predefined portlets which users can add to their personal pages. These portlets, which generally cannot be edited, could include the following:
    - ♦ collection portlets or WebDAV navigator portlets, which users have created using the portlet templates
    - ♦ portlets that are shipped with the portal (e.g., Bookmark, Publication Channel Subscriptions, and Welcome portlets)
    - ♦ custom portlets that your organization has developed and deployed.

Users can use the portlet templates to create their own editable portlets, or they can add predefined portlets to a page in the portal Web application. The portal Web application administers the content metadata for these portlets. Users who are group content administrators (or a member of the Portal Admins group (e.g., the SAS Web Administrator)) can then share the page (using the portal Options menu) with a group of users.

To add a portlet:

1. For URL display portlets that are not displayed in an inline frame (IFRAME), add the permission statements for the portlet to the required policy file.
2. Implement authorization (access control) for the portlet.
3. Add the portlet to a page. Content administrators can then share the page with other portal users.

Step 1 (optional): For URL Display Portlets That Are Not Displayed In An Inline Frame (IFRAME), Add the Permission Statements for the Portlet to the Required Policy File

A URL specifies the protocol and address of the HTML file to display. The Java permissions that are needed to access the HTML depend on whether the URL protocol is for a file system or an HTTP server. To enable the portal Web application to connect to the file system or HTTP server and access a URL, you must add a permission statement to the Java policy file for the portal Web application's servlet container. To add a permission statement to the policy file, depending on the URL type, do one of the following:

- For the file protocol, add a `java.io.FilePermission` that grants access to all of the files that make up the HTML fragment; these files include the HTML file and any resources it uses (such as images, CSS, JavaScript). The following permission grants access to the entire C drive and all subdirectories:

  ```
  permission java.io.FilePermission "C:\\-", "read";
  ```
- For the HTTP protocol, add a `java.net.SocketPermission` that grants access to the host and port of the machine serving up the HTML fragment. The following permission grants access to the Web server running on host.domain:

  ```
  permission java.net.SocketPermission "host.domain:80", "connect, resolve";
  ```

Step 2: Implement Authorization (Access Control) for the Page (that Contains the Portlet)

Take any necessary steps to implement authorization for the page (that will contain the portlet). For general information about access control, see Authorizing Access to Content

Step 3: Add the Portlet to a Page. Content Administrators Can Then Share the Page With Other Portal Users.

Depending on who is authorized to access the portlet, you can use one of several methods to make the portlet appear in the portal Web application:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can add the portlet on a page. The SAS Web Administrator can then use the portal Options menu to share the page (that contains the portlet) with the following:
  - ♦ any SAS group defined in the portal Web application's SAS Metadata Repository
  - ♦ the Public group (accessible to all users).
- A group content administrator can add a portlet on a page. The group content administrator can then share the page as follows:
  - ♦ If the user is the group content administrator for the Public group, the user can use the portal Options menu to share the page with the Public group (all users).
  - ♦ If the user is the group content administrator for a particular group, the user can use the portal Options menu to share the page (that contains the portlet) with that group.
- If you have installed the SAS Information Delivery Portal, all users can also add a portlet on a page.

Once the page (that contains the portlet) is shared with a group, all members of that group can access the portlet as group content.

For more information about using the portal Options menu, refer to the online Help.

Content

Adding Syndication Channels

Note: If you have installed the SAS Information Delivery Portal, users can add syndication channels to the portal Web application.

A syndication channel is a channel that provides syndicated, continuously updated Web content. The portal Web application provides support for the emerging RSS (Rich Site Summary) standard, a lightweight XML format designed for sharing news headlines and other syndicated Web content. By incorporating RSS content into the Web application, you can give users access to high−quality, continually updated news that is relevant to their roles in the organization. The BBC, CNET, CNN, Disney, Forbes, Motley Fool, Wired, Red Herring, Salon, Slashdot, and ZDNet channels are just a few examples of RSS channels that are available publicly.

RSS documents contain metadata, or summary information, about content that is available on the provider's Web site. Each content item consists of a title, a link, and a brief description. By clicking on a link, the user can display the full text for a content item.

The steps for adding a syndication channel are as follows:

1. Add the syndication channel's permission statement to the appropriate policy file.
2. Ensure that the appropriate user or group permission tree is created in the SAS Metadata Repository.
3. Add the syndication channels's metadata to the SAS Metadata Repository.
4. Implement authorization (access control) for the syndication channel.
5. Add the syndication channel to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal Web application users.

Step 1: Add the Syndication Channel's Permission Statement to the Appropriate Policy File

To connect to the site that is syndicating content for the syndication channel, you must add a permission statement to the policy file that grants the portal Web application permission to connect to the site.

To add a permission statement to the policy file, add a statement with the following format:

```
permission java.net.SocketPermission "machine.domain:80", "connect, resolve";
```

where `machine.domain` is the domain−qualified host where the XML file for the syndicated content is located.

Note: When the portal Web application's machine (that hosts the portal's servlet container) is running IPv6, the *machine.domain:80* host address format might not be valid for the permission statement. In these cases, you must either enable all socket permissions or determine the appropriate host address format to use in the policy file.

For example, if you are running an Apache Tomcat server and want to add a syndication channel from rssnews.acme.com, add the following statements:

```
grant codeBase "file:${catalina.home}/webapps/Portal/−" {
  ...
  permission java.net.SocketPermission "rssnews.acme.com:80", "connect, resolve";
  ...
};
```

where `...` are other permission statements in the policy file.

Step 2: Ensure That the appropriate User or Group Permission Tree Is Created in the SAS Metadata Repository

When you add the syndication channel metadata (content metadata) in Step 3, you also add the authorization metadata. To authorize the appropriate SAS users and groups for access, you can load the metadata and add and share the syndication channel in one of the following ways:

- **Add the syndication channel metadata to a user**. When you add the metadata to a user, the user is granted `ReadMetadata` and `WriteMetadata` permissions to enable the user to view and edit the content. The syndication channel can then be shared to a SAS group as follows:
    1. If required, you can log in to SAS Management Console as the SAS Administrator and configure the appropriate group content administrator (Step 4).
    2. A user adds the syndication channel to a collection portlet on a page in the portal Web application (Step 5).
    3. A user who is a group content administrator or member of the Portal Admins group (e.g., SAS Web Administrator) shares the page with a group so that the syndication channel is accessible to members of the group (Step 5).
- **Add the syndication channel metadata to a group**. When you add the metadata to a group, the group is granted `ReadMetadata` permission to enable the group members to view the content.

Before you can add the syndication channel authorization metadata in Step 3, the appropriate user or group permission tree must be created. To ensure that the user or group permission tree is created:

1. Ensure that you have defined the appropriate user or group (on the SAS Metadata Server) that you will add the metadata to in Step 3.
2. Enable the permission tree to be created as follows:
    - **If you are adding the metadata to a group**, and you added the group to the SAS Metadata Server after starting the servlet container, to enable the portal Web application to create the appropriate group permission tree, do either of the following:
        - Log in to the portal Web application as a member of the Portal Admins group (e.g. SAS Web Administrator).
        - Restart the servlet container.
    - **If you are adding the metadata to a user**, to create the user permission tree, log in to the portal Web application as that user.

Step 3: Add the Syndication Channel's Metadata to the SAS Metadata Repository

To define the syndication channel in the metadata repository, you must modify and run the `LoadSyndicationChannelExample.sas` SAS program (located in the `OMR` directory of your installation) to load the syndication channel's metadata into the SAS Metadata Repository.

Edit the `LoadSyndicationChannelExample.sas` SAS program and specify the appropriate variables for your syndication channel:

options metaserver="<host>"

Specify the host name of the SAS Metadata Server. Use the value of the `$SERVICES_OMI_HOST$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory). For example,

```
localhost
machine
machine.mycompany.com
```

metaport=<port>

Specify the port number of the SAS Metadata Server. This value is a number between 0 and 65536. Use the value of the `$SERVICES_OMI_PORT$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

metauser="<user ID>"

Specify the user ID to use to connect to the SAS Metadata Server; this user ID is typically the SAS Administrator (default, `sasadm`). For Windows users, the user ID is domain or machine name qualified. For example,

```
machine\saswbadm  where machine is the local machine
NTDOMAIN\saswbadm where NTDOMAIN is the Windows authentication domain
```

metapass="<password>"

Specify the password for the metauser.

metarepository="<repository>";

Specify the name of the SAS Metadata Repository where your portal Web application metadata is stored, followed by a ";". Use the value of the `$SERVICES_OMI_REPOSITORY$` property in the `install.properties` file (found in the `PortalConfigure` subdirectory of the setup directory).

%let groupOrUserName=<SAS User or Group>;

Specify the SAS group or user that you want to add the data to, followed by a ";".

%let channelName=<syndication channel name>;

Specify the name of the syndication channel that you want to create, followed by a ";".

%let channelDescriptio=<syndication channel description>;

Specify the description of the syndication channel that you want to create, followed by a ";".

%let channelURI=<syndication channel URI>;

Specify a valid URL for the syndication channel followed by a ";" For example:

```
%let channelURI=http://csociety.purdue.org/~jacoby/XML/CNN_US.xml.;
```

Step 4: Implement Authorization (Access Control) for the Syndication Channel

Take any additional necessary steps to control access to the syndication channel. For general information about access control, see Authorizing Access to Content.

Step 5: Add the Syndication Channel to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) with Other Portal Users.

Depending on who is authorized to access the syndication channel, users can use one of several methods to make it appear in the portal Web application:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a syndication channel to a collection portlet on a page. The SAS Web administrator can then use the portal Options menu to share the page (that contains the portlet) with the following:
    - any SAS group defined in the portal Web application's SAS Metadata Repository
    - the Public group (accessible to all users).
- A group content administrator can edit a portlet to add a syndication channel to a collection portlet on a page. The group content administrator can then share the page as follows:
    - If the user is the group content administrator for the Public group, the user can use the portal Options menu to share the page with the Public group (all users).
    - If the user is the group content administrator for a particular group, the user can use the portal Options menu to share the page (that contains the portlet) with that group.
- All users can also edit a portlet to add a syndication channel to a collection portlet on a page.

After the page (that contains the portlet with the syndication channel) is shared with a group, all members of that group can access the syndication channel as group content.

For more information about using the portal Options menu, refer to the online Help.

Content

Adding SAS Content

The portal Web application enables you to view the following SAS content:

- SAS Stored Processes
- SAS packages
- SAS publication channels
- SAS Information Maps
- SAS reports

For SAS publication channels, SAS packages, and SAS Stored Processes, the appropriate content and authorization metadata must be added to the SAS Metadata Repository or Xythos WebFile (WFS) WebDAV repository as follows:

- **Content metadata**. The content metadata is added in one of the following ways:
  - For SAS packages published from the portal, the SAS Publishing Framework updates the metadata repository with the content metadata.
  - For SAS packages produced from SAS Stored Processes, the SAS Publishing Framework updates the metadata repository with the content metadata.
  - For SAS publication channels, you must add the content metadata using the appropriate administration tool and metadata repository. (For an overview of the metadata administration tools, see Understanding the Administration Tools).
  - for SAS Stored Processes produced from an application such as SAS Enterprise Guide, the producing application updates the metadata repository with the content metadata.
  - for SAS Stored Processes that you create, you must add the content metadata using the appropriate administration tool and metadata repository. (For an overview of the metadata administration tools, see Understanding the Administration Tools).
- **Authorization metadata**. For SAS publication channels, SAS packages, and SAS Stored Processes, you might want to implement authorization (access controls) for the content so that only the appropriate users can access that content. For an overview of access control, see Authorizing Access to Content.

For SAS Information Maps and SAS Reports, the producing application adds the content metadata and the information map or report administrator adds the authorization metadata as follows:

- **For SAS Reports,** the SAS Web Report Studio application allows the report administrator to create reports in the SAS Report model format. The SAS Web Report Studio application then updates the metadata repository with the metadata for the report.
- **For SAS Information Maps,** the SAS Information Map Studio application allows the information map administrator to create SAS Information Maps. The SAS Information Map Studio application then updates the metadata repository with the metadata for the information map.

Content

Adding SAS Packages

Note: If you have installed the SAS Information Delivery Portal, users can view SAS packages from the portal Web application.

A package is a collection of structured and unstructured content that has been published using the SAS Publishing Framework, or created or published by running a SAS Stored Process on a SAS Workspace Server.

Packages are used to deliver the following:

- the content of publication channels, which publish information using the SAS Publishing Framework. If you publish a package from the SAS Information Delivery Portal, the package might include any of the following archived content types:
    - files (if you have installed the SAS Information Delivery Portal with the Xythos WFS WebDAV server)
    - links
    - SAS Information Maps (which are published as a link (reference) that will display the SAS Information Map in the Information Map Viewer of the portal)
    - SAS reports (which are published as a link (reference) that will display the SAS Report in the SAS Web Report Viewer of the portal)
- SAS Stored Process output, which can be published to a WebDAV server or a SAS publication channel.

Users can view packages from the portal Web application if the packages have been published to a SAS Publication Channel (SAS Information Delivery Portal only) or if the packages have been created or published to a Xythos WFS WebDAV repository. The portal Web application enables users to view packages by using the package viewer to display the contents.

To add a package to the portal Web application, follow these steps:

1. If the package is not already created, create the package.
2. Implement authorization (access control) for the package.
3. Make the package appear on the portal Web application.

Step 1: If the Package Is Not Created, Create the Package

If the package is not already created, create and publish the package to one of the following locations:

- SAS publication channel (if you have installed the SAS Information Delivery Portal)
- Xythos WFS WebDAV repository.

There are several ways that a package might be created and published:

- **SAS Stored Process**. You can develop a SAS Stored Process that runs on a SAS Workspace Server and produces result packages. These result packages can be stored on a Xythos WFS WebDAV server or published to a SAS publication channel. For details, see SAS Stored Processes in the *SAS Integration Technologies Developer's Guide*.
- **portal Options menu**. If you have installed the SAS Information Delivery Portal, users can use the portal Options menu to publish a package and add the package (content) metadata to the SAS Metadata Repository. For details about using the portal Web application to publish a package, refer to the online Help. When users

publish the package to a SAS publication channel or Xythos WFS WebDAV repository, the Web application adds the metadata for the package to the SAS Metadata or WebDAV Repository.
- **SAS Publishing Framework**. You can use SAS Publishing Framework to publish a package. For details, see Publishing Framework in the *SAS Integration Technologies Developer's Guide*.

Step 2: Implement Authorization (Access Control) for the Package

Take any necessary steps to control access to the package. For general information about access control, see Authorizing Access to Content.

Step 3: Make the Package Appear on the Portal Web Application

You can make the package appear on the portal Web application in any of the following ways:

- Add a SAS publication channel and view the package from the SAS publication channel (if you have installed the SAS Information Delivery Portal). For details about adding and viewing SAS publication channels, see Adding SAS Publication Channels and the online Help.
- Add a WebDAV navigator portlet and view the package from a WebDAV navigator portlet (if you have installed the Xythos WFS WebDAV server). For details, see the online Help.
- Edit a collection portlet and add the package to the collection portlet.

  Note: If you have installed the SAS Web Infrastructure Kit, only members of the Portal Admins group and group content administrators can edit collection portlets in the portal Web application. If you have installed the SAS Information Delivery Portal, all users can edit collection portlets in the portal Web application.

  You can then share the content using the portal Options menu. For details, see Using the Portal Options to Create and Share Personal Content.

Content

Adding SAS Publication Channels

Note: If you have installed the SAS Information Delivery Portal, users can access SAS publication channels from the portal Web application.

A SAS publication channel is a channel created by SAS Publishing Framework. Publication channels can be used to provide access to archived content published through SAS Publishing Framework. This feature relies on the SAS Publishing Framework software, which is part of SAS Integration Technologies. For detailed documentation of this software, see Publishing Framework in the *SAS Integration Technologies Developer's Guide*. In addition, the portal Web application allows you to publish files, links, SAS Information Maps, and SAS Reports to a publication channel; however, if you do not have the Xythos WFS WebDAV server installed, you cannot publish to a channel defined as a WebDAV persistent store.

From the portal Web application, you can publish a package that might include any of the following archived content types:

- files (if you have installed the SAS Information Delivery Portal with the Xythos WFS WebDAV server)
- links
- SAS Information Maps (which are published as a link (reference) that will display the SAS Information Map in the Information Map Viewer of the portal)
- SAS Reports (which are published as a link (reference) that will display the SAS Report in the SAS Web Report Viewer of the portal)

The portal provides an interface through which users can subscribe to SAS publication channels. After subscribing to a channel, users can use the portal to view archived content that is published through the channel. When a user subscribes to a channel, a subscriber profile is used. This profile contains information on how the information that is published to the channels is to be delivered.

To set up a channel in the portal, follow these steps:

1. (Optional): If publishing to an archive, add the SAS publication channel's archive permission statement to the appropriate policy file
2. Add the Publication Channel to the SAS Metadata Repository.
3. Implement authorization (access control) for the SAS publication channel.
4. Add the SAS publication channel to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal users.

After the publication channel is created, users can publish information to the channel and its subscribers.

WebDAV−based Publication Channel Considerations

If you are setting up a WebDAV−based publication channel, be aware of the following considerations:

- You must set up the appropriate SAS users and groups to enable users to publish to the Xythos WFS WebDAV server. For details, see Planning for Users and Groups.
- It is recommended that the base path for the Xythos WFS WebDAV server be a blank value. If you need to reconfigure the base path for the Xythos WFS WebDAV server, see Reconfiguring the Base Path for the Xythos WFS WebDAV Server.

Step 1 (optional): If Publishing to an Archive, Add the SAS Publication Channel's Archive Permission Statement to the Appropriate Policy File

To enable the portal Web application to connect to the file system in order to publish to an archive path, you must add a permission statement to the policy file that grants read and write access to the path.

To add a permission statement to the policy file, add a statement with one of the following formats:

- To grant read and write access to a specific directory:

  ```
  permission java.io.FilePermission "path", "read,write";
  ```
- To grant read and write access to all the files in a path:

  ```
  permission java.io.FilePermission "path/*", "read,write";
  ```
- To grant read and write access to all the files and subdirectories (recursively) in a path:

  ```
  permission java.io.FilePermission "path/-", "read,write";
  ```

For example, if you are running an Apache Tomcat server, to grant read and write access to all the files and subdirectories in the path `/sas/PubSub/`, add the following statement:

```
grant codeBase "file:${catalina.home}/webapps/Portal/-" {
  ...
permission java.io.FilePermission "/sas/PubSub/-", "read,write";

  ...
};
```

where `...` are other permission statements in the policy file.

Step 2: Add the Publication Channel to the SAS Metadata Repository

To add a publication channel to the SAS Metadata Repository, follow these steps:

1. Before you add the publication channel to the SAS Metadata Repository, ensure that you have the appropriate servers defined in the SAS Metadata Repository. Depending on the delivery method for your publication channel, you must have certain servers defined in your SAS Metadata Repository:

   - if you are publishing to an archive on a SAS Workspace Server, you must define a SAS Workspace Server and Spawner.
   - if you are publishing to an archive on a Xythos WFS WebDAV server, you must define a Xythos WFS WebDAV server.
   - if you are publishing to an archive in the file system, no server definition is needed for the publication channel.

   For details about verifying or adding server definitions, see Deploying Servers.
2. Log in to SAS Management Console as the SAS Administrator and use the Publishing Framework plug−in to define the channel in the metadata repository. For detailed instructions about defining channels, refer to the Publishing Framework Help and Creating Channels and Example: Creating a Channel in the publishing

chapter of the *SAS Integration Technologies Administrator's Guide*.

3. Use either the portal Options menu or the Publishing Framework plug−in to define one or more subscribers for the channel in the metadata repository. For detailed instructions about defining subscribers, refer to the Publishing Framework Help and the Managing Subscribers and Example: Creating a Subscriber topics in the Publishing chapter of the *SAS Integration Technologies Administrator's Guide*.

Step 3: Implement Authorization (Access Control) for the SAS Publication Channel

Take any necessary steps to control access to the Publication Channel. For general information about access control, see Authorizing Access to Content.

Step 4: Add the SAS Publication Channel to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) with Other Portal Users.

Depending on who has access permission to the publication channel, users can use one of several methods to make it appear in the portal Web application:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a publication channel to a collection portlet on a page. The SAS Web Administrator can then use the portal Options menu to share the page (that contains the portlet) with the following:
    - ♦ any SAS group defined in the portal's metadata repository
    - ♦ the Public group (accessible to all users).
- A group content administrator can edit a portlet to add a SAS publication channel to a collection portlet on a page. The group content administrator can then share the page as follows:
    - ♦ If the user is the group content administrator for the Public group, the user can use the portal Options menu to share the page with the Public group (all users).
    - ♦ If the user is the group content administrator for a particular group, the user can use the portal Options menu to share the page (that contains the portlet) with that group.
- All users can also edit a portlet to add a SAS publication channel to a collection portlet on a page.
- All users can use the Publication Channel Subscriptions portlet to display the SAS publications channels that they are subscribed to, providing a convenient way to view content published to the channels. Users can add this portlet to multiple pages.

For more information about using the portal Options menu, refer to the online Help.

Content

Adding SAS Stored Processes

SAS Stored Processes give users of the SAS Information Delivery Portal the ability to run SAS reports dynamically using current data residing on enterprise databases.

A SAS Stored Process is a SAS program that resides on a server and is available to be executed on a request basis. The benefits of stored processes include centralized code management, increased security, and ad hoc reporting capabilities. For more information, see SAS Stored Processes in the *SAS Integration Technologies Developer's Guide*.

When a user runs a stored process from the portal Web application, the Stored Process Viewer displays the associated input form, allowing the user to filter the output contents. The user can have the stored process viewer display the stored process results immediately (by running the stored process interactively), or the results can be stored for later viewing by the requesting user (by running the stored process in batch mode). (Batch mode is only available if you have installed the Xythos WFS WebDAV server.)

To set up a stored process in the portal Web application:

1. Develop and test the SAS code.
2. Place the code and data on a SAS Stored Process or SAS Workspace Server.
3. Ensure that the server metadata is added to the SAS Metadata Repository.
4. If not already defined, add the stored process and its application parameters to the SAS Metadata Repository.
5. Implement authorization (access control) for the stored process.
6. Add the SAS Stored Process to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal Web application users.

If you run a SAS Stored Process that produces package results or publishes a package to a SAS publication channel, if you have installed the SAS Information Delivery Portal, you might want to add the package or SAS publication channel to the portal Web application. For details, see Adding Packages and Adding SAS Publication Channels.

Step 1: Develop and Test the SAS Code

First, determine what type of stored process you would like to make available. Then, either locate an existing SAS program that produces the report or develop the program from scratch. Test the program on a stand−alone basis to be sure that it operates without errors and that it produces the desired output. For more information about developing stored processes for the portal Web application, see SAS Stored Processes in the *SAS Integration Technologies Developer's Guide*.

Step 2: Place the Code and Data on a SAS Stored Process or SAS Workspace Server

Depending on which type of output your stored process produces, you must place the stored process on one of the following servers:

- **If the stored process produces package results**, place the stored process on a SAS Workspace Server that the portal Web application can access.
- **If the stored process produces streaming results**, place the stored process on a SAS Stored Process Server that the portal Web application can access.

Step 3: Ensure That the Server Metadata Is Added to the SAS Metadata Repository

You must ensure that the following server metadata is in the SAS Metadata Repository.

- The SAS Stored Process Server or SAS Workspace Server on which you placed your stored process code must be defined in the SAS Metadata Repository.
- If the results of your stored process are stored in an archive on a SAS Workspace Server or Xythos WFS WebDAV server, the SAS Workspace Server or Xythos WFS WebDAV server must be defined in the SAS Metadata Repository.

For information about defining the stored process, workspace server, and Xythos WFS WebDAV servers, see Deploying Servers.

Step 4: If Not Already Defined, Add the Stored Process and Its Application Parameters to the SAS Metadata Repository

If the stored process is not already defined in the metadata, use the Stored Process Manager plug−in to SAS Management Console to update your metadata repository with metadata about the stored process and its execution parameters. For details, see the Stored Process Manager Help.

To define a stored process in the metadata repository, log in to the SAS Management Console as the SAS Administrator and register a stored process. Refer to the example stored process definition for an annotated illustration of these tasks. The links below point to specific portions of the example. The stored process definition includes the following:

- A Name, which will appear on lists in the portal Web application.
- The SAS server on which you have placed the stored process.
- The source repository, which specifies the path of the repository that contains the stored process.
- The source file, which specifies the file within the repository.
- The output type, which specifies the type of results produced by the stored process. If you choose package results, you must specify additional output details, such as archive or Xythos WFS WebDAV information, for the package.
- The parameters that are passed to the SAS program upon execution. These are the same parameters that you defined in the prologue section of the SAS program.

  For each parameter, you must define the following:

  - a name, which is a label (to appear on the user input form)
  - the SAS macro variable, which is the name of the SAS macro
  - constraints, which enable you to specify any constraints on the values for the parameter
  - attributes, which enable you to specify the status for the parameter. You can specify any or all of the following attributes: Required, Modifiable, Visible, Expert.

  When the portal Web application displays the default input form in the Stored Process window, it will render the possible values in list boxes. You can also provide a description and a default value.

To define a new stored process:

1. Select a folder or define a new folder in the navigation tree under the Stored Process Manager.

2. Right−click and select **File ➧ New Stored Process** from the pop−up menu. The Create Stored Process wizard appears.
3. Fill in the appropriate fields. For details about defining stored processes, click **Help** from the SAS Management Console Create Stored Process wizard. You can also refer to Administering Stored Processes in the *SAS Integration Technologies Administrator's Guide*.

Step 5: Implement Authorization (Access Control) for the Stored Process

Take any necessary steps to control access to the stored process. For general information about access control, see Authorizing Access to Content.

Step 6: Add the SAS Stored Process to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) With Other Portal Users.

Depending on who has access permission to the stored process, users can use one of several methods to make it appear in the portal Web application:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a SAS Stored Process to a collection portlet on a page. The SAS Web administrator can then use the portal Options menu to share the page (that contains the portlet) with the following:
  - ♦ any SAS group defined in the portal Web application's metadata repository
  - ♦ the Public group (accessible to all users).
- A group content administrator can edit a portlet to add a SAS Stored Process to a collection portlet on a page. The group content administrator can then share the page as follows:
  - ♦ If the user is the group content administrator for the Public group, the user can use the portal Options menu to share the page with the Public group (all users).
  - ♦ If the user is the group content administrator for a particular group, the user can use the portal Options menu to share the page (that contains the portlet) with that group.
- All users can also edit a portlet to add a SAS Stored Process to a collection portlet on a page.

For more information about using the portal Options menu, refer to the online Help.

If you run a SAS Stored Process that produces package results or publishes a package to a SAS publication channel, if you have installed the SAS Information Delivery Portal, you might want to add the package or SAS publication channel to the portal Web application. For details, see Adding Packages and Adding SAS Publication Channels.

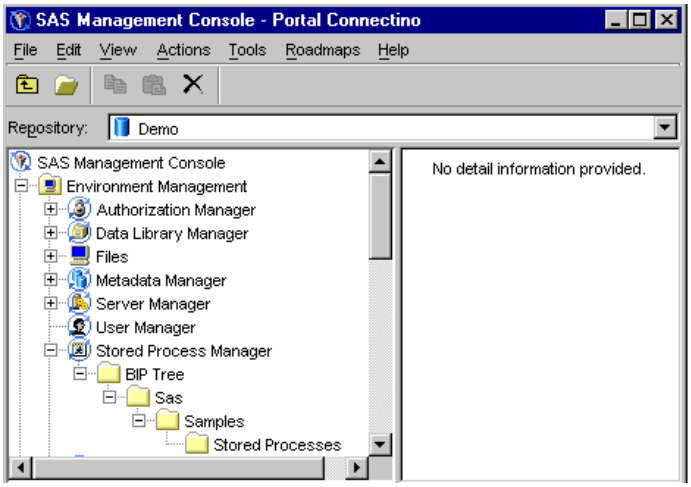
Content

SAS Stored Process Metadata Example

This page provides examples of metadata for stored processes. The examples are based on the stored process Hello World, which is installed automatically if you install the initial demo data for the portal Web application. When you log on to the portal Web application with the SAS Demo User, the stored process is returned when you search for SAS stored processes.

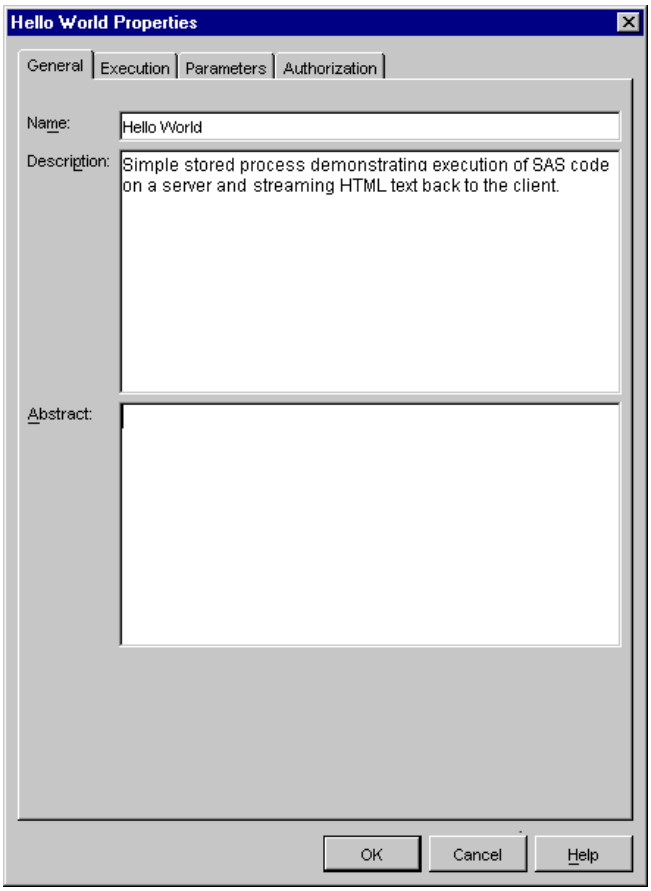
You can find the stored process sample code in the stored process sample path of the SAS installation. To check this value, see the `$STP_SAMPLE_PATH$` parameter of the `install.properties` file.

To view the metadata for the stored process, open the SAS Management Console interface, expand the **Stored Process Manager**, then expand the **BIP Tree** folder, **SAS** folder, and **Samples** folder to locate the Stored Process samples directory, as shown in this display:

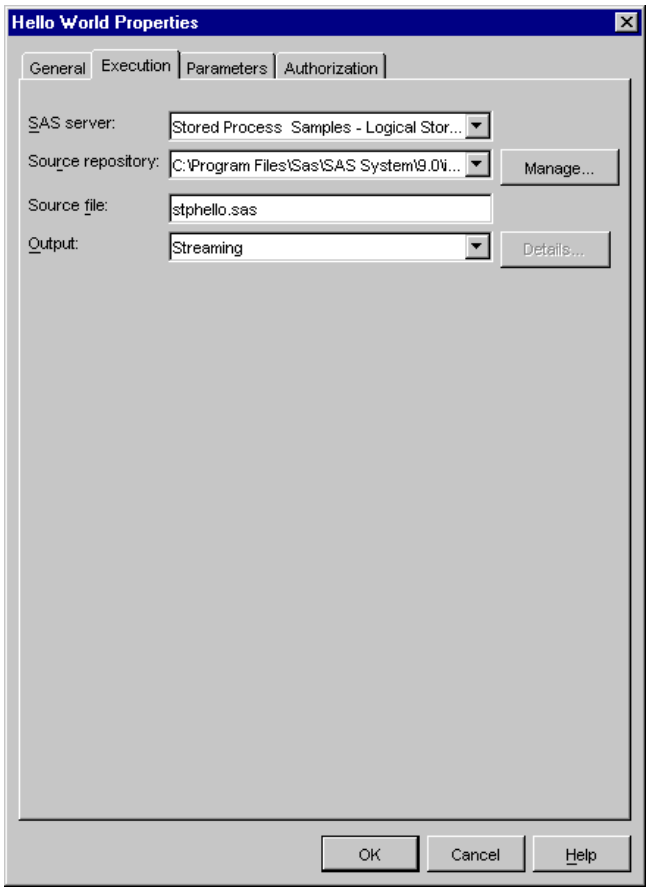


To view the stored process definition, in the SAS Management Console display area, right−click on the name of the stored process, and then select **Properties** from the pop−up menu. Select the General, Execution, or Parameters tab to view the fields for a stored process definition.

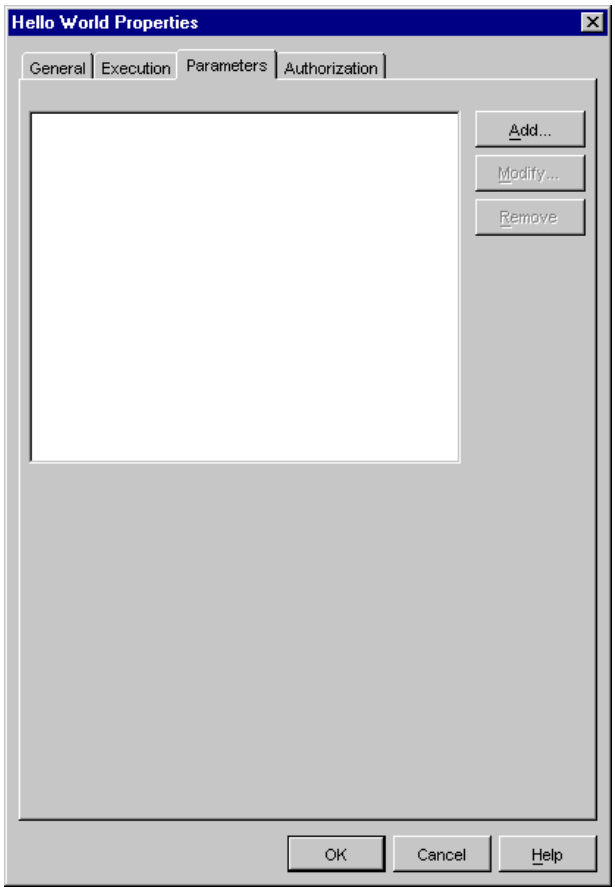
- **General tab.** The General tab displays the fields for name, description, and abstract, as shown in this display:



- **Execution tab.** The Execution tab displays the fields for SAS server, source repository, source file, and output, as shown in this display:



- **Parameters tab.** The Parameters tab displays a list of parameters. To view a parameter's fields, select the parameter, then click **Modify**. The Parameters tab is shown in this display:


Hello World Properties
General
Execution
Parameters
Authorization
Add...
Modify...
Remove
OK
Cancel
Help

Content

Adding SAS Information Maps

Note: If you have installed the appropriate software, you can view SAS Information Maps in the SAS Information Delivery Portal.

SAS Information Maps are user−friendly metadata definitions of physical data sources that enable your business users to query a data warehouse to meet specific business needs. The Information Delivery Portal allows authorized users to search for and view SAS Information Maps that exist in the SAS Metadata Repository. When users view a SAS Information Map Viewer in the portal, the portal uses the SAS Information Map Viewer to display the data associated with the information map. (The SAS Information Map Viewer is provided with the portal.)

SAS Information Maps that exist in the SAS Metadata Repository have already been created and administered by an information map administrator.

To add a SAS Information Map:

1. Determine who is authorized to access the SAS Information Map.
2. Add the SAS Information Map (or a SAS publication channel that contains a SAS Information Map) to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal users.

Step 1: Determine Who Is Authorized to Access the SAS Information Map

Determine who is authorized to access the SAS Information Map in order to determine which SAS users or groups will be allowed to view the SAS Information Map from the portal Web application. Take any necessary steps to implement additional authorization for the page (that will contain the portlet with the SAS Information Map). For general information about access control, see Authorizing Access to Content.

Step 2: Add the SAS Information Map (or a SAS Publication Channel that Contains a SAS Information Map) to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) With Other Portal Users.

Depending on who has access permission to the SAS Information Map, you can use one of several methods to make it appear in the portal Web application.

Add the SAS Information Map to a Collection Portlet

To make a SAS Information Map appear in a collection portlet, do one of the following:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a SAS Information Map to a collection portlet on a page. The SAS Web administrator can then use the portal Options menu to share the page (that contains the portlet) with the following:
    - ♦ SAS groups that are authorized to access the SAS Information Map.
    - ♦ the Public group (accessible to all users), if it is authorized to access the SAS Information Map

- A group content administrator can edit a portlet to add a SAS Information Map to a collection portlet on a page. The group content administrator can then share the page as follows:
    - ♦ If the user is the group content administrator for the Public group and the Public group is authorized to access the SAS Information Map, the user can use the portal Options menu to share the page with the Public group (all users).
    - ♦ If the user is the group content administrator for a particular group and that group is authorized to access the SAS Information Map, the user can use the portal Options menu to share the page with that group.
- All users can edit a portlet to add a SAS Information Map to a collection portlet on a page.

Publish the SAS Information Map to a SAS Publication Channel, Subscribe to the Publication Channel, and Add a Publication Channel Subscriptions Portlet

To make a SAS Information Map appear in the portal Web application, users can use the portal Web application or SAS Publishing Framework to publish a SAS Information Map to a SAS publication channel. Authorized users can then use the portal Options menu to subscribe to the SAS publication channel and then add the Publication Channel Subscriptions portlet to their portal Web application. For details, see the online Help.

Publish the SAS Information Map to a SAS Publication Channel and Add the SAS Publication Channel to a Portlet

To make a SAS Information Map appear in the portal Web application, users can use the portal Web application or SAS Publishing Framework to publish a SAS Information Map to a SAS publication channel and then add the SAS publication channel to a portlet in the portal Web application as follows:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add the appropriate SAS Publication Channel to a collection portlet on a page. The SAS Web administrator can then use the portal Options menu to share the page (that contains the SAS Publication channel's portlet) with the following:
    - ♦ SAS groups that are authorized to access the SAS Information Map.
    - ♦ the Public group (accessible to all users), if it is authorized to access the SAS Information Map
- A group content administrator can edit a portlet to add the appropriate SAS publication channel to a collection portlet on a page. The group content administrator can then share the page (that contains the SAS publication channel's portlet) as follows:
    - ♦ If the user is the group content administrator for the Public group and the Public group is authorized to access the SAS Information Map, the user can use the portal Options menu to share the page with the Public group (all users).
    - ♦ If the user is the group content administrator for a particular group and that group is authorized to access the SAS Information Map, the user can use the portal Options menu to share the page with that group.
- All users can edit a portlet to add the appropriate SAS publication channel to a collection portlet on a page.

For more information about using the portal Options menu, refer to the online Help.

Content

Adding SAS Reports

Note: If you have installed the appropriate software, you can view SAS Reports in the SAS Information Delivery Portal.

A SAS Report is a visual representation of data models and the results of analysis and summarization of the data from SAS procedural output. A SAS report is stored in the SAS Report Model format. The SAS Information Delivery Portal allows authorized users to search for and view SAS Reports that exist in the SAS Metadata Repository. When users view a report in the portal, the portal uses the SAS Web Report Viewer to display the report. (The SAS Web Report Viewer must be installed separately from the portal).

Reports that exist in the SAS Metadata Repository have already been created and administered by a report administrator.

To add a SAS Report:

1. Determine who is authorized to access the SAS Report.
2. Add the SAS Report (or a SAS publication channel that contains a SAS Report) to a collection portlet. Content administrators can then share the page (that contains the portlet) with other portal users.

Step 1: Determine Who Is Authorized to Access the SAS Report and Implement Authorization (Access Control)

Determine who is authorized to access the SAS Report in order to determine which SAS users or groups will be allowed to view the SAS report from the portal Web application. Take any necessary steps to implement additional authorization (access control) for the page (that will contain the portlet with the SAS Report). For general information about access control, see Authorizing Access to Content.

Step 2: Add the SAS Report (or a SAS publication channel That Contains a SAS Report) to a Collection Portlet. Content Administrators Can Then Share the Page (That Contains the Portlet) with Other Portal Users.

Depending on who has access permission to the SAS Report, you can use one of several methods to make it appear in the portal Web application:

Add the SAS Report to a Collection Portlet

To make a SAS Report appear as a selection on the portal Web application, do one of the following:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can edit a portlet to add a SAS Report to a collection portlet on a page. The SAS Web administrator can then use the portal Options to share the page (that contains the portlet) with the following:
    - ♦ SAS groups that are authorized to access the SAS Report
    - ♦ the Public group (accessible to all users), if it is authorized to access the SAS Report.
- A group content administrator can edit a portlet to add a SAS Report to a collection portlet on a page. The group content administrator can then share the page as follows:

    - If the user is the group content administrator for the Public group and the Public group is authorized to access the SAS Report, the user can use the portal Options menu to share the page with the Public group (all users).
    - If the user is the group content administrator for a particular group and that group is authorized to access the SAS Report, the user can use the portal Options menu to share the page with that group.
- If you have installed the SAS Information Delivery Portal, individual users can also edit a portlet to add a SAS Report to a collection portlet on a page.

Publish the SAS Report to a SAS publication channel, Subscribe to the Publication Channel, and Add a Publication Channel Subscriptions Portlet

To make a SAS Report appear in the portal Web application, users can use the portal Web application or SAS Publishing Framework to publish a SAS Information Map to a SAS publication channel. Authorized users can then use the portal Options menu to subscribe to the SAS publication channel and then add the Publication Channel Subscriptions Portlet to their portal Web application. For details, see the online Help.

Publish the SAS Report to a SAS Publication Channel and Add the SAS Publication Channel to a Portlet

To make a SAS Report appear in the portal Web application. users can use the portal Web application or SAS Publishing Framework to publish a SAS Report to a SAS publication channel and then add the SAS Publication channel to a portlet in the portal Web application as follows:

- A member of the Portal Admins group (e.g., the SAS Web Administrator) can use the portal Options menu to add the appropriate SAS publication channel to a collection portlet on a page. The SAS Web administrator can then use the portal Options to share the page (that contains the SAS Publication channel's portlet) with the following:
    - SAS groups that are authorized to access the SAS Report
    - the Public group (accessible to all users), if it is authorized to access the SAS Report.
- A group content administrator can edit a portlet to add the appropriate SAS publication channel to a collection portlet on a page. The group content administrator can then share the page (that contains the SAS publication channel's portlet) as follows:
    - If the user is the group content administrator for the Public group and the Public group is authorized to access the SAS Report, the user can use the portal Options menu to share the page with the Public group (all users).
    - If the user is the group content administrator for a particular group and that group is authorized to access the SAS Report, the user can use the portal Options menu to share the page with that group.
- If you have installed the SAS Information Delivery Portal, individual users can also edit a portlet to add the appropriate SAS publication channel to a collection portlet on a page.

For more information about using the portal Options menu, refer to the online Help.