Enabling Unchallenged Access in the SAS Information Delivery Portal

Overview

Unchallenged access to the 4.2 SAS Information Delivery Portal, via a 9.1.3 style Public Kiosk, provides a user access to the SAS Information Delivery Portal and thus to SAS content without receiving an authentication challenge. The user can access the SAS Information Delivery Portal in this way by going to a special URL, such as http://host/SASPortal/public. When the SAS Information Delivery Portal receives this request, it creates a real user session and allows the unchallenged user to see SAS content as if they had logged onto the system.

Several changes were made to the SAS Information Delivery Portal user interface to accommodate unchallenged access. These changes are only visible to when the unchallenged user accesses the SAS Information Delivery Portal. The Options dropdown menu will not be displayed on the title bar. The Search menu item will be displayed on the title bar by default. It can be removed by setting a configuration property. The Log Off *user* menu item will be displayed on the title bar by default. It can optionally be removed or replaced with a Log On menu item by setting a configuration property.

When the unchallenged user is finished interacting with the SAS Information Delivery Portal, they can choose to log out, log into the SAS Information Delivery Portal as an existing user, let the session timeout, or close the browser. Selecting the log on menu item will take the user to the SAS Logon Manager. If a user has an account in the deployment, they can skip the public content and directly log on to the SAS Information Delivery Portal by going to another URL; for example, http://host/SASPortal. This will utilize the standard log on process.

This document outlines the steps required to convert a 4.2 SAS Information Delivery Portal deployment to support unchallenged access. Unchallenged access is delivered as part of 9.2, maintenance 2. See the *Out-of-the-Box Deployment* section for the process of converting a new 9.2 deployment to support unchallenged access. See the *Migration Deployment* section for the process of converting a 9.2 deployment, migrated from an existing 9.1.3 Public Kiosk deployment, to support unchallenged access.

Security Considerations

In the SAS 9.2 release, all Web applications use a common security architecture provided by the SAS Web Infrastructure Platform. Two cornerstones of this architecture are prompting a user for credentials and routing requests through Web application filters to validate a user's security token before allowing access to content. Enabling unchallenged access to the SAS Information Delivery Portal removes one of these cornerstones, so it should only be enabled when other strategies do not work. When enabled, a greater share of the security burden falls on the site administrator to thoroughly review the content surfaced to unchallenged users, to understand how the content surfaced utilizes SAS backend servers, and to make sure the content and its behavior are appropriate.

Unchallenged access is a product-specific capability in the SAS Information Delivery Portal. As with previous implementations, the unchallenged user cannot be differentiated from a challenged user, one who logged in using the SAS Logon Manager, by other Web applications in the SAS suite of Web applications. It is important to apply this knowledge when determining what type of content to surface through the unchallenged user. There are a number of potential security concerns that can be addressed by limiting the content displayed during unchallenged access. Two examples from a SAS Enterprise BI Server deployment are listed below.

Any application or portlet that allows a user to save data should not be surfaced to unchallenged users unless the unchallenged user base is known. Some applications may support configuration options to disable the ability to save data. When unchallenged access is configured, the SAS Information Delivery Portal does not allow the unchallenged user to modify pages or edit portlets. The following SAS content types may launch applications that allow a user to save data and thus the security ramifications of doing this should be considered.

> BI Dashboard – The default application configured for viewing dashboards, SAS BI Dashboard, can be configured to allow users to administer dashboards. By default, the unchallenged user is not an administrator; this behavior should be maintained. See the instructions in the *Configure the Unchallenged User* section for details.
>
> Information Maps and Data Exploration – The default application configured for viewing information maps and data explorations, the Visual Data Explorer, allows the unchallenged user to create new data explorations and save them to the unchallenged user's My Folder and any other Folders they have been granted permission to in the SAS Metadata Server.
>
> Report – The default application configured for viewing reports, SAS Web Report Studio, allows the unchallenged user to save reports to the unchallenged user's My Folder and any other Folders they have been granted permission to in the SAS Metadata Server. SAS Web Report Studio can be configured to prevent a user from saving reports. See the instructions in the *Configure the Unchallenged User* section for details.

Any content, application, or portlet that allows a user to interact with the SAS server tier should be reviewed before it is surfaced to unchallenged users, unless the unchallenged user base is known. This includes accessing data, especially with unbounded queries, or submitting code for processing. Dashboards, information maps, data explorations, reports, and stored processes are examples of content that utilize the SAS Server tier. They may also be configured to launch applications that allow a user to interact with the SAS Server tier.

The security considerations that apply to the SAS Enterprise BI Server also apply to SAS Solutions that enhance the SAS Information Delivery Portal with portlets and content.

In the 9.2 release of SAS software, WebDAV services are provided by the SAS Content Server. The mechanisms for securing content in the SAS Content Server are different than those in the Xythos WebDAV server used by the 9.1.3 release. The unchallenged user is treated as a normal user by the SAS Content Server. This means that any content that jcr:authenticated allows READ access to will be visible to the unchallenged user. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on implementing authorization in the SAS Content Server.

Out-of-the-Box Deployment

The following process outlines the steps required to convert a new 9.2 deployment to support unchallenged access. These instructions assume:

- The deployment uses host authentication. Unchallenged access will work with other authentication schemes, but that process is not documented.
- The unchallenged access content will be managed by the SAS Guest User using the sasguest login. Unchallenged access will work for other users, but that process is not documented.
- The instructions are based on, but not limited to, a Windows deployment.

Install SAS 9.2, maintenance 2

1. Install SAS 9.2 maintenance 2.
2. Validate the new deployment.
3. Stop the Web application server, Remote Services application, and SAS servers.
4. Backup the deployment.

Configure the Unchallenged User

1. Create the operating system user account for the SAS Guest User, for example sasguest, if it does not exist. See the SAS® 9.2 Intelligence Platform: Installation and Configuration Guide for details.
2. Start the SAS servers and Remote Services application. **Important Note:** Do ***not*** start the Web application server.
3. Use the SAS Management Console to create the SAS Guest User.
   3.1. Log on as the administrative user, for example sasadm@saspw.
   3.2. On the **Plug-ins** tab, right-click on the **User manager** and then select the **New → User** menu item.
   3.3. On the **General** tab, set the **Name** to sasguest and the **Display Name** to SAS Guest User.
   3.4. Select the **Accounts** tab and then select the **New** button to create the primary login. The **User ID** should be the operating system account created in the first step. For example, sasguest. The **Password** should be left blank. The **Authentication Domain** should be the default domain used by other portal users. For example, DefaultAuth. Select the **New** button to create a second login. The **User ID** should be the same as the first login. For example, sasguest. The **Password** should be left blank. Create a new, unique **Authentication Domain** that will only be used by this login. For example, IDPUnchallengedAccess.
4. If dashboards are available for unchallenged access, make sure the SAS Guest User and the PUBLIC and SASUSERS groups are **not** members of the BI Dashboard Administrators group. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on administering security for SAS BI Dashboard.
5. If reports are available for unchallenged access, make sure the SAS Guest User and the PUBLIC and SASUSERS groups are **not** members of either the Web Report Studio: Report Creation or Web Report Studio: Advanced roles. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on roles in SAS Web Report Studio.
6. **Important Note:** Do ***not*** log on to the Information Delivery Portal using the SAS Guest User at this time. Doing so will create group shared pages and page from page templates. If pages are created with a persistent store, it is difficult to remove them from the SAS Guest User's page list.

Configure the SAS Information Delivery Portal Web Application for Unchallenged Access

1. Edit SASHOME\SASInformationDeliveryPortal\4.2\Configurable\wars\sas.portal\WEB-INF\web.xml.orig.
   1.1. Locate the following filter-mapping entry in the web.xml.orig file:

```
<!-- Uncomment to enable Unchallenged Access -->
<!--
<filter-mapping>
    <filter-name>UnchallengedAccessFilter</filter-name>
    <url-pattern>/public</url-pattern>
</filter-mapping>
-->
```

and uncomment the filter-mapping entry so it looks like:

```
<!-- Uncomment to enable Unchallenged Access -->
<filter-mapping>
    <filter-name>UnchallengedAccessFilter</filter-name>
    <url-pattern>/public</url-pattern>
</filter-mapping>
```

1.2. Locate the following servlet-mapping entry in the web.xml.orig file:

```
<!-- Uncomment to enable Unchallenged Access -->
<!--
<servlet-mapping>
    <servlet-name>public</servlet-name>
    <url-pattern>/public</url-pattern>
</servlet-mapping>
-->
```

and uncomment the servlet-mapping entry so it looks like:

```
<!-- Uncomment to enable Unchallenged Access -->
<servlet-mapping>
    <servlet-name>public</servlet-name>
    <url-pattern>/public</url-pattern>
</servlet-mapping>
```

1.3. To reduce the amount of memory consumed by unchallenged users who are no longer using the Information Delivery Portal, the servlet timeout should be reduced. Locate the following session-config entry in the web.xml.orig file:

```
<session-config>
   <session-timeout>30</session-timeout>
</session-config>
```

and change the session-timeout entry to reduce the number of minutes it takes for an unused session to time out, for example 10.

1.4. Save the web.xml.orig file when finished.

Rebuild and Redeploy the SAS Information Delivery Portal EAR File

In the previous section, changes were made to the web.xml.orig file in the SAS installation directory. In order to make these changes available, the SAS Information Delivery Portal Web application must be rebuilt and redeployed.

1. Stop the Web application server if it is running.
2. Rebuild the Information Delivery Portal Web application using the SAS Deployment Manager. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on rebuilding Web applications.
   2.1. Run the SAS Deployment Manager, for example C:\Program Files\SAS\SASDeploymentManager\9.2\config.exe.
   2.2. After choosing the runtime language, select the **Rebuild Web Applications** radio button.
   2.3. Select or enter your **Configuration Directory**.
   2.4. Enter the unrestricted user ID and password, for example sasadm@saspw.
   2.5. Check the Information Delivery Portal.
3. Redeploy the Information Delivery Portal Web application using the instructions documented in the SAS® 9.2 Intelligence Platform: Web Application Administration Guide.
4. **Important Note:** Do ***not*** log on to the Information Delivery Portal using the SAS Guest User at this time. Doing so will create group shared pages and page from page templates. If pages are created with a persistent store, it is difficult to remove them from the SAS Guest User's page list.

Configure SAS Information Delivery Portal Metadata for Unchallenged Access

To simplify management of unchallenged access, most configuration properties are stored in the SAS Metadata Server. These properties can be changed at any time after unchallenged access is enabled, but the SAS Information Delivery Portal Web application must be stopped and restarted in order for the changes to take effect.

1. Stop the Web application server if it is running. The metadata created in this section is loaded into the SAS Information Delivery Portal Web application at startup time.
2. Use the SAS Management Console to add unchallenged access configuration properties to the SAS Metadata Server.
   2.1. Log on as the administrative user, for example sasadm@saspw.
   2.2. On the **Plug-ins** tab, expand **Application Management**, and then expand **Configuration Manager**.
   2.3. Right-click on **Information Delivery Portal 4.2** and then select the **Properties** menu item.
   2.4. Select the **Advanced** tab and add the following name / value pairs:

Property Name	Value	Description
`Unchallenged.Access.Enabled`	`true`	`true` to enable unchallenged access, `false` to disable
`Unchallenged.Access.UserID`	*`see description`*	The SAS Guest User ID created in an earlier step for the IDPUnchallengedAccess authentication domain, for example sasguest
`Unchallenged.Access.Logoff.Behavior`	`logoff`	`logoff` to display the log off menu item, `logon` to display the log on menu item (takes the user to the SAS Logon manager), `hide` to display no menu item
`Unchallenged.Access.Show.Search.Menu`	`true`	`true` to display the search menu item, `false` to hide it

Important Note: If the SAS Information Delivery Portal configuration is removed for any reason, the unchallenged access configuration properties will also be removed. After the SAS Deployment Wizard has reconfigured the SAS Information Delivery Portal, follow the instructions in this section to reset them.

Create Content for Unchallenged Access

When an unchallenged user accesses the Information Delivery Portal using the public URL, the will see all of the pages in the unchallenged user's page list.

1. Start the Web application server.
2. Log on to the Information Delivery Portal as the SAS Guest User, for example sasguest.
3. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on adding content to the Information Delivery Portal.
4. Review the SAS Guest User's pages and make sure the content displayed is appropriate for public access.
5. Log off the SAS Guest User.

Validate Unchallenged Access

1. Navigate to the public URL to make sure the Information Delivery Portal is configured properly and content is displayed appropriately. The default URL will be in the format of http://<machine:port>/SASPortal/public.
2. Unchallenged access allows users to view SAS content without authenticating. It is the SAS administrator's responsibility to make sure any content that needs to be secured is not accessible via unchallenged access. It is also the SAS administrator's responsibility to make sure the unchallenged content cannot be modified.

Migration Deployment

The following process outlines the steps required to convert a 9.2 deployment, migrated from an existing 9.1.3 Public Kiosk deployment, to support unchallenged access. These instructions assume:

- Migration is from a 9.1.3 SP4 SAS Information Delivery Portal deployment where content is made available to users without challenging them for credentials using the 9.1.3 Public Kiosk capability.
- The deployment uses host authentication. Unchallenged access will work with other authentication schemes, but that process is not documented.
- The 9.1.3 Public Kiosk content was managed by the SAS Guest person using the sasguest login. The unchallenged user content will be managed by the same user in the 9.2 deployment. Unchallenged access will work for other users, but that process is not documented.
- The instructions are based on, but not limited to, a Windows deployment.

Install SAS 9.2, maintenance 2

1. Run the SAS Migration Utility on the 9.1.3 SP4 deployment to create a migration package.
2. Install SAS 9.2 maintenance 2 using the migration path.
3. Validate the new deployment. **Important Note:** Do ***not*** log on to the Information Delivery Portal using the SAS Guest User at this time. Doing so will create group shared pages and page from page templates. If pages are created with a persistent store, it is difficult to remove them from the SAS Guest User's page list.
4. Stop the Web application server, Remote Services application, and SAS servers.
5. Backup the deployment.

Configure the Unchallenged User

1. Create the operating system user account for the SAS Guest User, for example sasguest, if it does not exist. See the SAS® 9.2 Intelligence Platform: Installation and Configuration Guide for details.
2. Start the SAS servers and Remote Services application. **Important Note:** Do ***not*** start the Web application server.
3. Since this is a migrated system, the SAS Guest person and sasguest login should already be defined.
4. Use the SAS Management Console to modify the SAS Guest user. Since this is a migrated system, the SAS Guest user and its sasguest login should already be defined.
   4.1. Log on as the administrative user, for example sasadm.
   4.2. If the sasguest host account or password is different from the 9.1.3 deployment, update the sasguest login.
   4.3. On the **Plug-ins** tab, select **User manager**.
   4.4. Right-click on the SAS Guest user and then select the **Properties** menu item.
   4.5. Select the **Accounts** tab and then select the **New** button to create a second login. The **User ID** should be the same as the first login. For example, sasguest. The **Password** should be left blank. Create a new, unique **Authentication Domain** that will only be used by this login. For example, IDPUnchallengedAccess.
5. If dashboards are available for unchallenged access, make sure the SAS Guest User and the PUBLIC and SASUSERS groups are **not** members of the BI Dashboard Administrators group. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on administering security for SAS BI Dashboard.
6. If reports are available for unchallenged access, make sure the SAS Guest User and the PUBLIC and SASUSERS groups are **not** members of either the Web Report Studio: Report Creation or Web Report Studio: Advanced roles. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on roles in SAS Web Report Studio.
7. Temporarily configure the SAS Guest User as the PUBLIC content administrator so migrated content can be converted for unchallenged access. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details.

Configure the SAS Information Delivery Portal Web Application for Unchallenged Access

1. Edit SASHOME\SASInformationDeliveryPortal\4.2\Configurable\wars\sas.portal\WEB-INF\web.xml.orig.
   1.1. Locate the following filter-mapping entry in the web.xml.orig file:

```
<!-- Uncomment to enable Unchallenged Access -->
<!--
<filter-mapping>
    <filter-name>UnchallengedAccessFilter</filter-name>
    <url-pattern>/public</url-pattern>
</filter-mapping>
-->
```

and uncomment the filter-mapping entry so it looks like:

```
<!-- Uncomment to enable Unchallenged Access -->
<filter-mapping>
    <filter-name>UnchallengedAccessFilter</filter-name>
    <url-pattern>/public</url-pattern>
</filter-mapping>
```

1.2. Locate the following servlet-mapping entry in the web.xml.orig file:

```
<!-- Uncomment to enable Unchallenged Access -->
<!--
<servlet-mapping>
    <servlet-name>public</servlet-name>
    <url-pattern>/public</url-pattern>
</servlet-mapping>
-->
```

and uncomment the servlet-mapping entry so it looks like:

```
<!-- Uncomment to enable Unchallenged Access -->
<servlet-mapping>
    <servlet-name>public</servlet-name>
    <url-pattern>/public</url-pattern>
</servlet-mapping>
```

1.3. To reduce the amount of memory consumed by unchallenged users who are no longer using the Information Delivery Portal, the servlet timeout should be reduced. Locate the following session-config entry in the web.xml.orig file:

```
<session-config>
   <session-timeout>30</session-timeout>
</session-config>
```

and change the session-timeout entry to reduce the number of minutes it takes for an unused session to time out, for example 10.

1.4. Save the web.xml.orig file when finished.

Rebuild and Redeploy the SAS Information Delivery Portal EAR File

In the previous section, changes were made to the web.xml.orig file in the SAS installation directory. In order to make these changes available, the SAS Information Delivery Portal Web application must be rebuilt and redeployed.

5. Stop the Web application server if it is running.
6. Rebuild the Information Delivery Portal Web application using the SAS Deployment Manager. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details on rebuilding Web applications.

6.1. Run the SAS Deployment Manager, for example C:\Program Files\SAS\SASDeploymentManager\9.2\config.exe.

6.2. After choosing the runtime language, select the **Rebuild Web Applications** radio button.

6.3. Select or enter your **Configuration Directory**.

6.4. Enter the unrestricted user ID and password, for example sasadm@saspw.

6.5. Check the Information Delivery Portal.

7. Redeploy the Information Delivery Portal Web application using the instructions documented in the SAS® 9.2 Intelligence Platform: Web Application Administration Guide.
8. **Important Note:** Do ***not*** log on to the Information Delivery Portal using the SAS Guest User at this time. Doing so will create group shared pages and page from page templates. If pages are created with a persistent store, it is difficult to remove them from the SAS Guest User's page list.

Configure SAS Information Delivery Portal Metadata for Unchallenged Access

To simplify management of unchallenged access, most configuration properties are stored in the SAS Metadata Server. These properties can be changed at any time after unchallenged access is enabled, but the SAS Information Delivery Portal Web application must be stopped and restarted in order for the changes to take effect.

1. Stop the Web application server if it is running. The metadata created in this section is loaded into the SAS Information Delivery Portal Web application at startup time.
2. Use the SAS Management Console to add unchallenged access configuration properties to the SAS Metadata Server.
   2.1. Log on as the administrative user, for example sasadm.
   2.2. On the **Plug-ins** tab, expand **Application Management**, and then expand **Configuration Manager**.
   2.3. Right-click on **Information Delivery Portal 4.2** and then select the **Properties** menu item.
   2.4. Select the **Advanced** tab and add the following name / value pairs:

Property Name	Value	Description
`Unchallenged.Access.Enabled`	`true`	`true` to enable unchallenged access, `false` to disable
`Unchallenged.Access.UserID`	*`see description`*	The SAS Guest User ID created in an earlier step for the IDPUnchallengedAccess authentication domain, for example sasguest
`Unchallenged.Access.Logoff.Behavior`	`logoff`	`logoff` to display the log off menu item, `logon` to display the log on menu item (takes the user to the SAS Logon manager), `hide` to display no menu item
`Unchallenged.Access.Show.Search.Menu`	`true`	`true` to display the search menu item, `false` to hide it

Important Note: If the SAS Information Delivery Portal configuration is removed for any reason, the unchallenged access configuration properties will also be removed. After the SAS Deployment Wizard has reconfigured the SAS Information Delivery Portal, follow the instructions in this section to reset them.

Create Content for Unchallenged Access

When an unchallenged user accesses the Information Delivery Portal using the public URL, the will see all of the pages in the unchallenged user's page list. This section describes how to convert the 9.1.3 Public Kiosk pages that were migrated to 9.2 PUBLIC shared pages to the unchallenged user's page list.

1. Start the Web application server.
2. Log on to the Information Delivery Portal as the SAS Guest user, for example sasguest.
3. The pages in the 9.1.3 Public Kiosk should be the only pages in the SAS Guest user's page list. Navigate to each page, select the **Options** menu and then select the **Edit Page Properties** menu item. On the **Edit Page Properties** screen change **Location** from **PUBLIC** to **not shared** to make the page private to the SAS Guest user. In most cases, select the **Move the following items to the specified share location** checkbox to make the page's content private.
4. Optionally reorder pages, added pages, or update existing page content.
5. Review the SAS Guest user's pages and make sure the content displayed is appropriate for public access.
6. Log off the SAS Guest user.
7. **Important Note:** Remove the SAS Guest user from the list of PUBLIC content administrators. See the SAS® 9.2 Intelligence Platform: Web Application Administration Guide for details.

Validate Unchallenged Access

1. Navigate to the public URL to make sure the Information Delivery Portal is configured properly and content is displayed appropriately. The default URL will be in the format of http://<machine:port>/SASPortal/public.
2. Unchallenged access allows users to view SAS content without authenticating. It is the SAS administrator's responsibility to make sure any content that needs to be secured is not accessible via unchallenged access. It is also the SAS administrator's responsibility to make sure the unchallenged content cannot be modified.

Maintenance Considerations

After Applying Maintenance or Hot Fixes

Configuring unchallenged access to the Information Delivery Portal requires manual changes to the web.xml.orig file in the SAS installation directory. These changes may be lost when maintenance or hot fixes are applied, so it is important to document them. Always review the web.xml.orig file after maintenance or hot fixes are installed and reapply unchallenged access modifications as needed. If modification must be reapplied, the sas.portal4.2.ear file will need to be rebuild and redeployed. To do this, follow the instructions in the *Rebuild the SAS Information Delivery Portal EAR file* and Configure *SAS Information Delivery Portal Metadata for Unchallenged Access* sections.

After Removing the SAS Information Delivery Portal Configuration

If the SAS Information Delivery Portal configuration is removed for any reason, the unchallenged access configuration properties will also be removed. After the SAS Deployment Wizard has reconfigured the SAS Information Delivery Portal, follow the instructions in the *Configure SAS Information Delivery Portal Metadata for Unchallenged Access* section.

SAS Logon Manager Configuration

When the unchallenged user logs off the SAS Information Delivery Portal or their session times out, they will be routed to the SAS Logon Manager. A site should not configure the SAS Logon Manager to display the Log On button unless they want the user to be able to log on to the SAS Information Delivery Portal. Selecting the Log On button will prompt the user for a user ID and password.

When the session times out, the user will be taken to the session timeout page of the SAS Logon Manager. The SAS Logon Manager supports customization of both the timeout and log off pages in two ways. A custom message can be displayed and/or Log on buttons can be displayed. There may be some opportunities to enhance the unchallenged user's experience by modifying the timeout and log off messages. The default message states:

> *Note: The information that you have just viewed will remain in your browser's memory until the window is closed. Therefore, for added security, please close your browser as soon as you are finished with your session.*