SUSTAINMENT MANAGEMENT SYSTEM™

U.S. ARMY CORPS OF ENGINEERS

ENGINEER RESEARCH AND DEVELOPMENT CENTER

System Administration Guide

Version 3.5 DoD

Authors:
Matthew E. Richards
Andrew J. Valentine
Mark E. Fisher
Brody H. Finney

Editor:
Audrey J. Fisher

Revised October 2019

Contents

Part I

Introduction to the Sustainment Management System

Chapter 1

Documentation Status

1.1 Document History

Revision	Date	Description
3.5	October 2019	(1) New feature: reCAPTCHA option for SMS on the web. (2) Existing feature documented: pass-through signin. (3) Reorganized section on web configuration (section 5.4.1).
3.3.12	April 2017	(1) Timeout in web.session.config changed from 20 minutes to 10 minutes; (2) http vs. https configuration; (3) changes to database upgrade procedure.
3.3.7	April 2016	Deleted Scenario database upgrade.
3.3	March 2016	Added Silverlight requirement.
3.2	March 2015	Revised commands and improved documentation.
0.2	September 2014	Separated ”Administration” and ”Installation” guides. Restructured and added content.
0.1	August 2014	Created Document.

Table 1.1: Document History

1.2 New in the October 2019 Documentation

1.2.1 New Feature: reCAPTCHA Option for SMS on the Web

reCAPTCHA verification has been added to the web login page for the Sustainment Management System (SMS). This feature is disabled by default to accommodate customers who do not have Internet access. Where the SMS is hosted on the web, a system administrator has the option to enable reCAPTCHA.

See section 6.4 on page 33 for how to activate reCAPTCHA for web logins.

1.2.2 Pass-Through Signin

Instructions for enabling pass-through signin have been added to the documentation. See section 6.5 on page 34.

Chapter 2

Getting Started

2.1 About this Guide

This guide is written to provide basic information and procedures for deploying and configuring the Sustainment Management System™ (SMS).

For information about installing this product, see the *Sustainment Management System Installation Guide*.

2.2 Using this Guide

A System Configuration Worksheet listing variables used in the guide may be found in Appendix C.

> **IMPORTANT:** The System Configuration Worksheet should have been completed prior to or during installation of this product. You may be able to find the needed variable values in a filled-out copy of the Appendix to the *Sustainment Management System Installation Guide*.

Variable names are presented in angle brackets (for example, <VAR_APP_POOL>, <WEB_APP_ROOT>) and are used to record and reference installation parameters. Where these variables appear in the instructions, the corresponding value from the System Configuration Worksheet should be substituted.

Chapter 3

System Requirements

3.1 Enterprise Configuration

3.1.1 SQL Server

- Windows Server 2012R2 Standard
- SQL Server 2014 Service Pack 2 (12.0.5000.0)
- 400 MB free storage per million square feet of managed inventory
- 2.0 GHz or faster processor, 64-bit, 4+ cores
- 8 GB RAM

Note: *Support for SQL Server 2008 R2 and SQL Server 2008 Express ended December 2016.*

3.1.2 Application Server

- Windows Server 2012R2 Standard
- Internet Information Services 8 (8.5.9600.16384)
- PowerShell 4.0. Note that Windows 2012R2 comes with PowerShell 4.0 If using Windows 2008, PowerShell Version 3 is sufficient.
- 4 GB of free storage plus desired image storage
- 2.0 GHz or faster processor, 64-bit, 4+ cores
- 8 GB RAM with an additional 100 MB per concurrent user

Note: *Support for Windows Server 2008 R2 ended December 2016.*

3.2 Single Server Configuration

- Windows Server 2012R2 Standard
- SQL Server 2014 Service Pack 2 (12.0.5000.0)
- Internet Information Services 8 (8.5.9600.16384)
- PowerShell 4.0. Note that Windows 2012R2 comes with PowerShell 4.0 If using Windows 2008, PowerShell Version 3 is sufficient.

- 4 GB of free storage plus desired image storage and 400 MB free storage per million square feet of managed inventory
- 2.0 GHz or faster processor, 64-bit, 4+ cores
- 8 GB RAM with an additional 100 MB per concurrent user

Note: *Support for Windows Server 2008 R2, SQL Server 2008 R2, and SQL Server 2008 Express ended December 2016.*

Chapter 4

Client Requirements

4.1 Supported Web Browser

Internet Explorer versions 10 and above are supported. It is recommended to add the URL of the SMS application to your list of trusted sites.

4.2 Microsoft Silverlight

Microsoft Silverlight 5 is a client-side system requirement for running BUILDER's Functionality and Scenario Visualization features.

Chapter 5

Architecture

5.1 Files and Permissions

5.1.1 Default Program Files Install Path

By default, files used in the installation are placed in **%SYSTEM DRIVE%\Program Files\ERDC-CERL\SMS**.

5.1.2 Program Files Folder Descriptions

5.1.2.1 Database

This folder contains scripts for creating and updating the databases.

5.1.2.2 SMS Config

This folder contains an SMS Application Configuration tool for modifying the web application's database connection configuration.

5.1.2.3 SMS Service

This folder contains SMS service executables and configuration files. The SMS service manages scenarios and performs database maintenance and nightly roll-ups.

5.1.2.4 SMSPowershell

This folder contains the PowerShell module for maintaining and administering the SMS web application.

5.1.2.5 Web Root

This folder contains the source files for building a web application. Web applications will not reference this directory; when a web application is created, these files are copied into a new directory and configured by IIS as a web application.

5.1.3 Web Application Root

When the SMS web application is added to a website, files are copied from the **%SYSTEM DRIVE%\Program Files\ERDC-CERL\SMS\Web Root** directory to a location that will be referenced by the website as a virtual directory. In this documentation, that location is referenced by the variable <WEB_APP_ROOT>.

After the files are copied, the following folder permissions are changed:

Folder	Permissions Change
<WEB_APP_ROOT>	Recursively Allow **Read & execute** for the <POOL_IDENTITY>
<WEB_APP_ROOT>\Files	Allow **Modify** for the <POOL_IDENTITY>
<WEB_APP_ROOT>\Exports	Allow **Modify** for the <POOL_IDENTITY>

Table 5.1: Folder permission changes when copied from Web Root to Web Application Root

5.1.4 Creating the Web Application Root Example

5.1.4.1 Creating the Application Folder and Copying Files

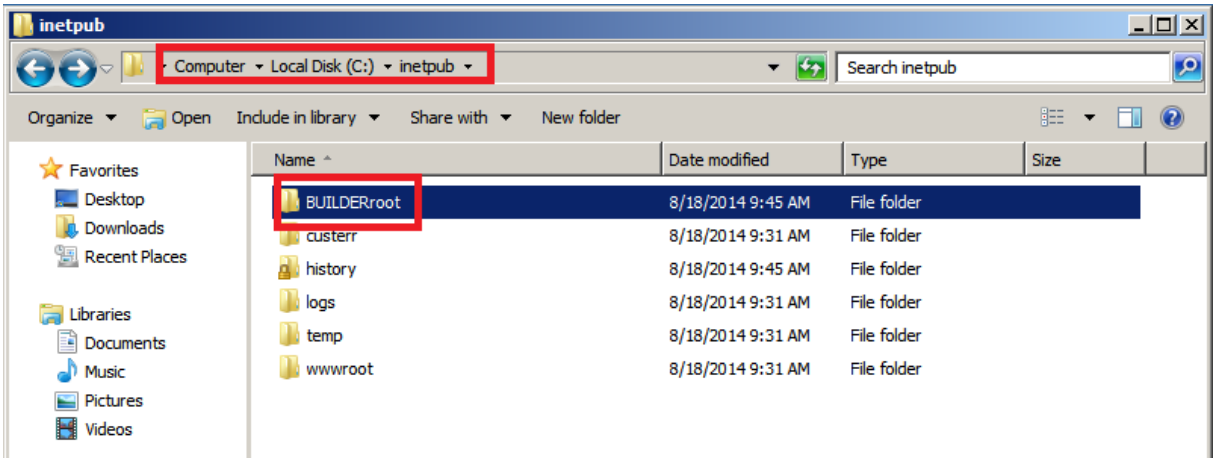


Figure 5.1: File Explorer

1. Determine a location for the web application, for example **C:\inetpub\BUILDERroot**.
2. Create the directory in Windows Explorer (*See Figure 5.1*).
3. Copy the contents of **Program Files/ERDC-CERL/SMS/Web Root** into the newly created web application folder.

5.1.4.2 Setting Application Folder Permissions

1. Right-click on the application folder and select **Properties**.
2. Select the **Security** tab (*See Figure 5.2*).
3. Click **Edit**.
4. Click **Add** (*See Figure 5.3*).
5. Type `IIS_IUSRS` in the text area.
6. Click **OK**.
7. Select **NETWORK**.
8. Click **OK**.

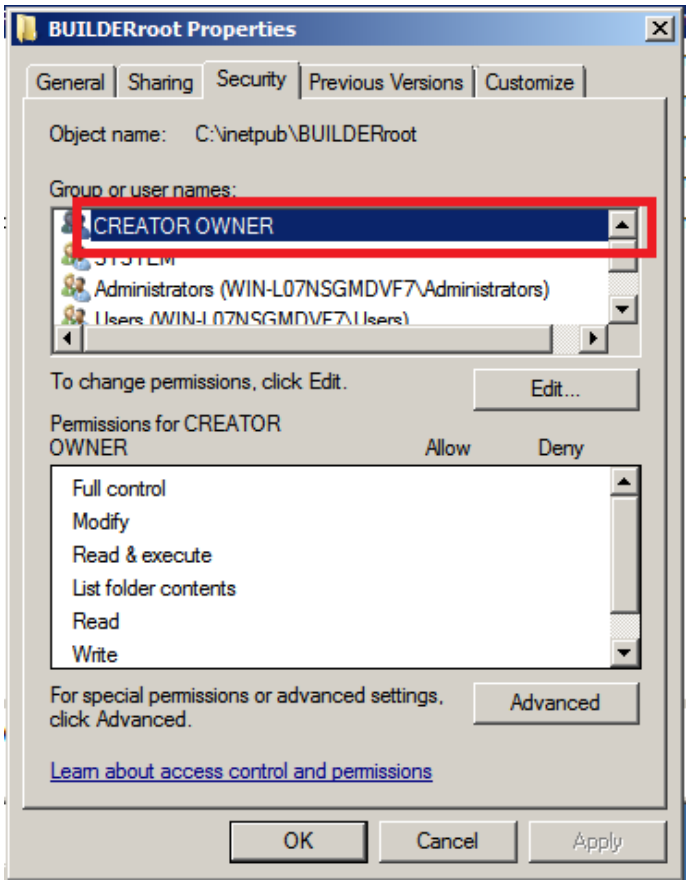


Figure 5.2: Application Folder Properties

5.2 Database Information

5.2.1 TCP Ports

If you are installing SQL Server on a separate machine from the IIS Server, port 1433 must be opened on the SQL Server.

5.2.2 Authentication and Permissions

5.2.2.1 Integrated Security

SQL Server Windows authentication is recommended. To configure integrated security, create a Domain or Local user as the <POOL_IDENTITY>; In IIS set the **Application Pool Identity** as <POOL_IDENTITY>; grant <POOL_IDENTITY> **db_owner** roles with the default schema **dbo** on both databases.

> ***Note:*** *Local users can only be used if SQL Server is installed on the same machine as the IIS Server.*

5.2.2.2 SQL Server Authentication

The PowerShell commands and the graphical configuration tools will encrypt the connection strings in the configuration files. If using this authentication method, the SQL Server user must be granted **db_owner** roles with the default schema **dbo** on both databases. The configuration is stored in the <WEB_APP_ROOT>\web.connections.config file.

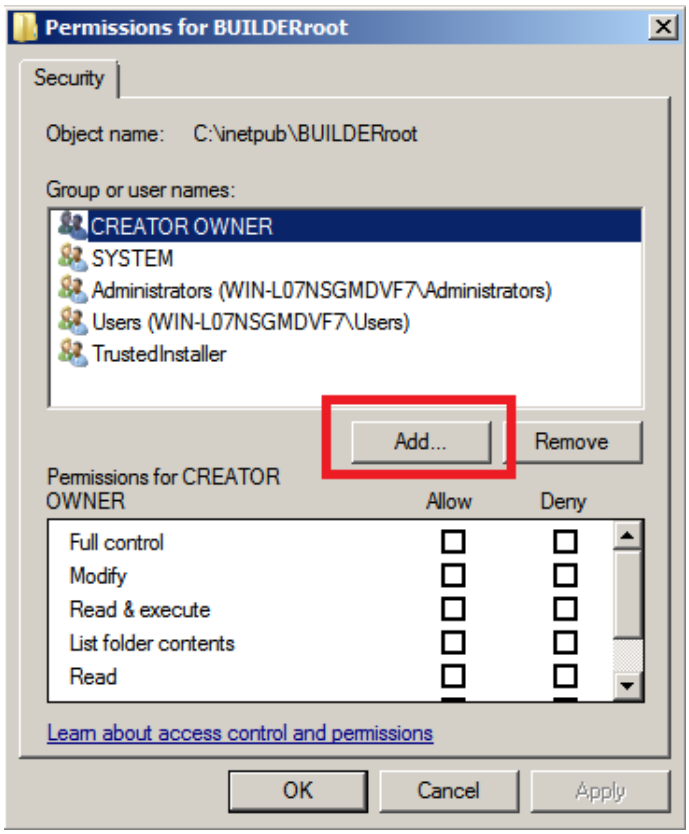


Figure 5.3: Add Application Folder Permission

5.3 Server Roles and Features

5.3.1 IIS Server

The **Web Server (IIS)** Role must be added in **Server Manager**. Additionally, the following features must be enabled:

- Common HTTP Features\Static Content
- Application Development\ASP.NET
- Application Development\.NET Extensibility
- Application Development\ISAPI Extensions
- Application Development\ISAPI Filters
- Management Tools\IIS Management Console

5.3.1.1 Add Roles and Features Example

1. Open the Server Manager Snap-in.
2. Select **Features** in the left pane.
3. Click the **Add Features** link in the right pane.
4. Select **.NET Framework 3.5.1 Features**.

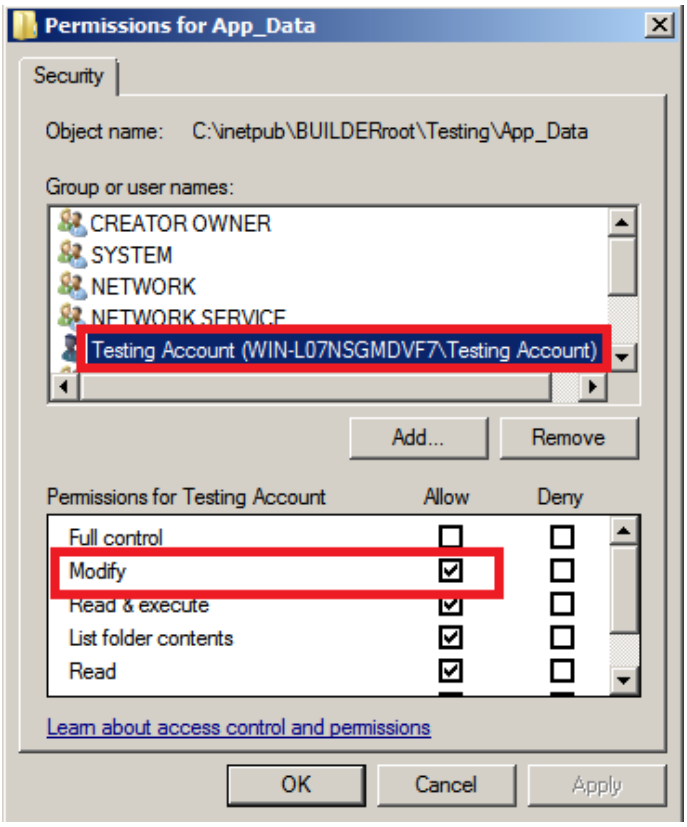


Figure 5.4: Change Application Folder Permission

5. A dialog box may open; if so, click **Add Required Role Services**.
6. Click **Next**.
7. Click **Next**.
8. Select **Application Development****ASP.NET** (See Figure 5.5).
9. A dialog box may open; if so, click **Add Required Role Services**.
10. Select **Common HTTP Features****Static Content**.
11. Select **Management Tools****IIS Management Console**.
12. Click **Next**.
13. Click **Install**.
14. After the installation has completed, click the **Close** button.

5.3.2 Database Server

The database server does not need any additional roles. SQL Server 2014 Service Pack 2 (12.0.5000.0) needs to be installed.

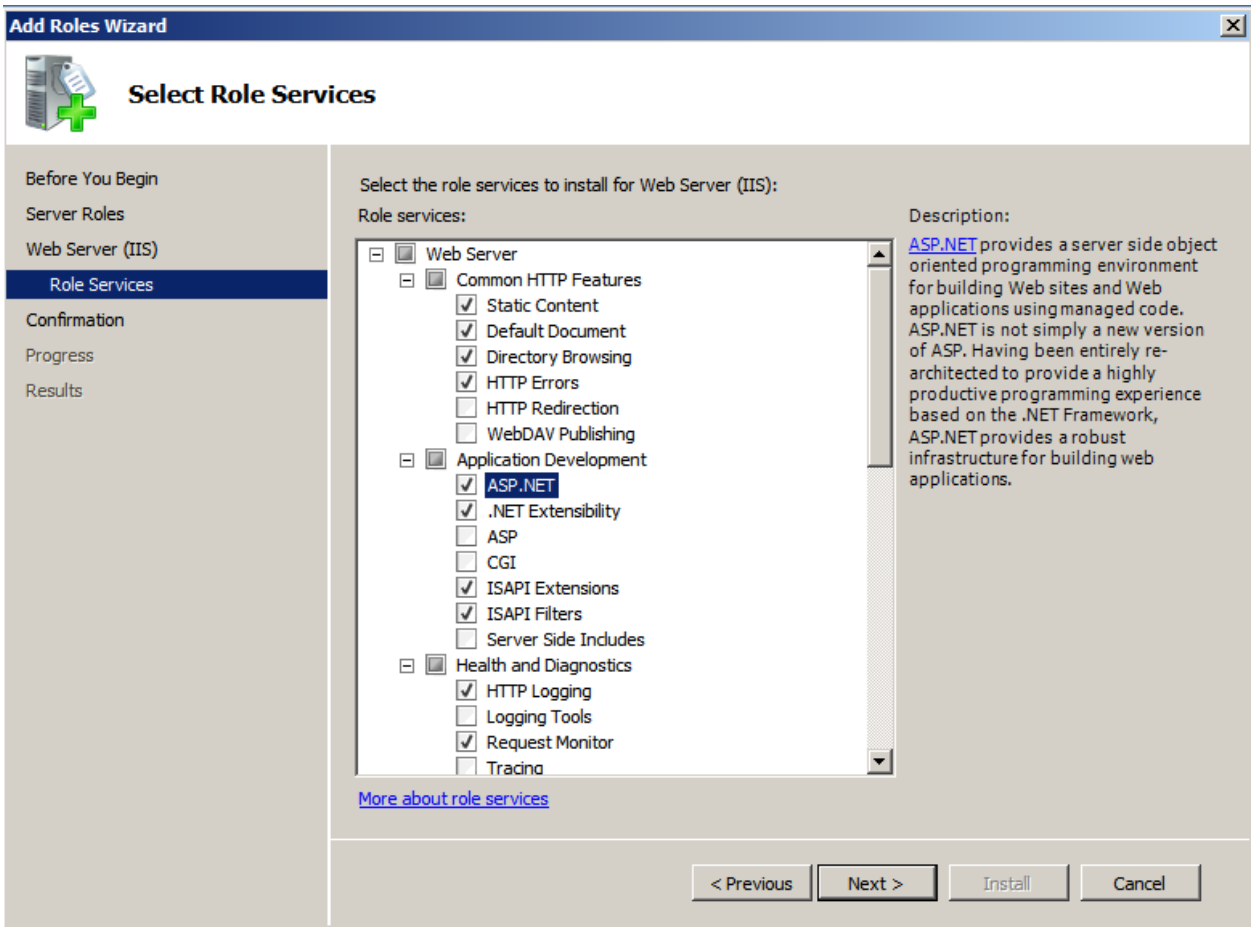


Figure 5.5: Role Services

5.3.3 Reports Server

The **Web Server (IIS)** Role must be added in **Server Manager** and the same features enabled as the IIS Server. SQL Server Reporting Service (SSRS) must be installed on the Reports server to run the SSRS standard and custom reports. This service may be installed on (a) a separate machine, (b) the SQL Server machine, or (c) the IIS Server machine.

5.4 SMS Web Application

5.4.1 Configuration Files

Location and other information about configuration files that affect the SMS web application is listed in the table below. Refer to the filled out System Configuration Worksheet (Appendix C) to see which directory corresponds to <WEB_APP_ROOT>. Each configuration file is discussed in more detail at the following headings.

5.4.1.1 Web.config

This file contains configurations and references. It is recommended that this file *not* be modified.

Doc Section	Configuration File	Directory	Replaced at Upgrade?	Separate Secure Version?
5.4.1.1	Web.config	<WEB_APP_ROOT>	Yes	No
5.4.1.2	Web.behaviors.config	<WEB_APP_ROOT>\Configs	No	Yes
5.4.1.3	Web.bindings.config	<WEB_APP_ROOT>\Configs	No	Yes
5.4.1.4	Web.connections.config	<WEB_APP_ROOT>\Configs	No	No
5.4.1.5	Web.debug.config	<WEB_APP_ROOT>\Configs	No	No
5.4.1.6	Web.services.config	<WEB_APP_ROOT>\Configs	No	Yes
5.4.1.7	Web.session.config	<WEB_APP_ROOT>\Configs	No	No

Table 5.2: SMS Configuration Files. Refer to the filled out System Configuration Worksheet (Appendix C) to see which directory corresponds to <WEB_APP_ROOT>.

5.4.1.2 Web.behaviors.config

Caution: *The only changes that should be necessary to this file are to support an https application environment if desired. It is recommended that this file only be modified with a full understanding of the configuration information.*

This file contains configuration information for the web service behaviors of the BUILDER web application. These behaviors are used by the build web services definitions, which are in turn used in the Silverlight portions of the application. .

This is one of three configuration files (web.behaviors.config, web.bindings.config, and web.services.config) that are available in both default and secure versions. Both (1) web.behaviors.config and (2) web.behaviors.secure.config will be available in the <WEB_APP_ROOT>\Configs directory. If running the application in IIS with https enabled, do the following:

1. Rename web.behaviors.config to another name, such as web.behaviors.default.config to preserve the file.
2. Rename web.behaviors.secure.config to web.behaviors.config

5.4.1.3 Web.bindings.config

Caution: *It is recommended that this file only be modified with a full understanding of the configuration information.*

This file contains configuration information for the web service and web application. It can be used to increase timeouts or modify the binding protocols.

This is one of three configuration files (web.behaviors.config, web.bindings.config, and web.services.config) that are available in both default and secure versions. Both (1) web.bindings.config and (2) web.bindings.secure.config files will be available in the <WEB_APP_ROOT>\Configs directory. If running the application in IIS with https enabled, do the following:

1. Rename web.bindings.config to another name, such as web.bindings.default.config to preserve the file.
2. Rename web.bindings.secure.config to web.bindings.config

5.4.1.4 Web.connections.config

Caution: *It is recommended that this file only be modified with a full understanding of the configuration information.*

This file contains the database connection configurations for the web application. It can be used to increase timeouts or modify the binding information.

5.4.1.5 Web.debug.config

WARNING: *If debugging is enabled, sensitive information about the application and configuration could be exposed to users.*

Note: *It is recommended that this file only be used to diagnose issues with possible software defects.*

This file can be used to configure additional error and process information for debugging.

5.4.1.6 Web.services.config

Caution: *The only changes that should be necessary to this file are to support an https application environment if desired. It is recommended that this file only be modified with a full understanding of the configuration information.*

This file contains configuration information for the web services of the BUILDER web application. These services are used by the Silverlight portions of the applications.

This is one of three configuration files (web.behaviors.config, web.bindings.config, and web.services.config) that are available in both default and secure versions. Both (1) web.services.config and (2) web.services.secure.config files will be available in the <WEB_APP_ROOT>\Configs directory. If running the application in IIS with https enabled, do the following:

1. Rename web.services.config to another name, such as web.services.default.config to preserve the file.
2. Rename web.services.secure.config to web.services.config

5.4.1.7 Web.session.config

This file contains configuration information for the web service and web application sessions. It can be used to change cookie and session timeout settings. Starting with Version 3.3.12, the default SMS session timeout is 10 minutes.

To alter the default 10-minute setting, change ”10” in the line <sessionState mode=”InProc” cookieless=”false” timeout=”10” >

Note: *BUILDER does not support separate timeout settings for administrator and non-administrator accounts.*

DoD users should consult Rules SV-83865r1_rule and SV-83867r1_rule from the Application Security and Development STIG before reconfiguring this value.

5.4.2 Logging

5.4.2.1 Event Viewer

By default, IIS writes logs to the **%SystemDrive%\inetpub\logs\LogFiles** directory. Information written in these logs includes page errors, client IP addresses, page requests, and information about client browsers. This file can be examined with standard web log parsers. The location of this file can be modified in the IIS Manager under **Logging**.

5.4.2.2 Web Logs

Handled web application exceptions, process messages, and debugging information is written to the Event Viewer in the **Application and Services Logs\BUILDER Log**. Any un-handled application exception can be found in the **Windows Logs\Application log**.

5.5 SMS Service

5.5.1 Configuration Files

5.5.1.1 ImpactConfiguration.xml

This file is located in the **%SYSTEM DRIVE%\Program Files\ERDC-CERL\SMS\SMS Service** directory. It contains the connection and configuration settings for the SMS Service. This file is *not* replaced with upgrades.

5.5.2 Logging

Handled service exceptions, process messages, rollup status, scenario status, and debugging information is written to the Event Viewer in the **Application and Services Logs\BUILDER Log**. Any un-handled service exceptions can be found in the **Windows Logs\Application log**.

5.6 TCP Ports

The TCP ports can be modified for security.

5.6.1 SQL Server

By default, SQL Server uses TCP Port 1433. This port can be modified within SQL Server. If this port is modified, the connection string located in the web.connections.config file must be updated with a text editor to reflect the change. The SMS Application Configuration tool cannot modify the ports.

5.6.2 IIS Server

The IIS server typically uses TCP Port 80 for http access and TCP Port 443 for https access. These ports can be modified within IIS Manager.

5.6.3 Reports Server

The SSRS reports server typically uses TCP Port 80 for http access and TCP Port 443 for https access. These ports can be modified within IIS Manager. The management URL is typically http:\\localhost\reports.

Part II

System Administration

Chapter 6

Security

6.1 FIPS Compliance

The SMS application has been compiled for Federal Information Processing Standard (FIPS) 140 compliance. The FIPS compliance policy setting is used to block applications that are using unapproved cryptography from Federal information systems. The SMS application will continue to operate with FIPS Compliance enabled. For more information see `https://technet.microsoft.com/en-us/library/jj852197(v=ws.10).aspx`

6.2 Configuring CAC Authentication

Update the SmartCardName setting in the inventory configuration table with any value to enable CAC authentication. The following is an example SQL script. Execute this on the inventory database in SQL Management Studio.

```
UPDATE dbo.Configuration
   SET ConfigValue = 'CAC'           -- name of smart card
 WHERE ConfigName = 'SmartCardName';
```

6.3 Configuring the SMS Web Service with `https`

If you want to configure the SMS web service with `https`, it is necessary that you have a certificate for IIS. After this certificate is in place, perform the following tasks:

6.3.1 Add the Certificates Snap-in

To add the **Certificates** Snap-in,

1. Open the Microsoft Management Console by typing `mmc` at a Run prompt.
2. In the "Console Root" box, open the **File** menu.
3. Select **Add/Remove Snap-in...** (*See Figure 6.1*).
4. In the "Add or Remove Snap-ins" popup box, select the **Certificates** Snap-in in the left panel.
5. Click the **Add** > button between the two panels. (*See Figure 6.2*)
6. In the "Certificates snap-in" popup box, click the **Computer Account** radio button.

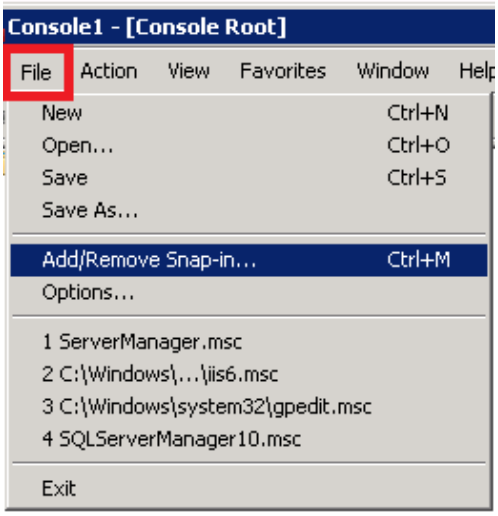


Figure 6.1: Console Root

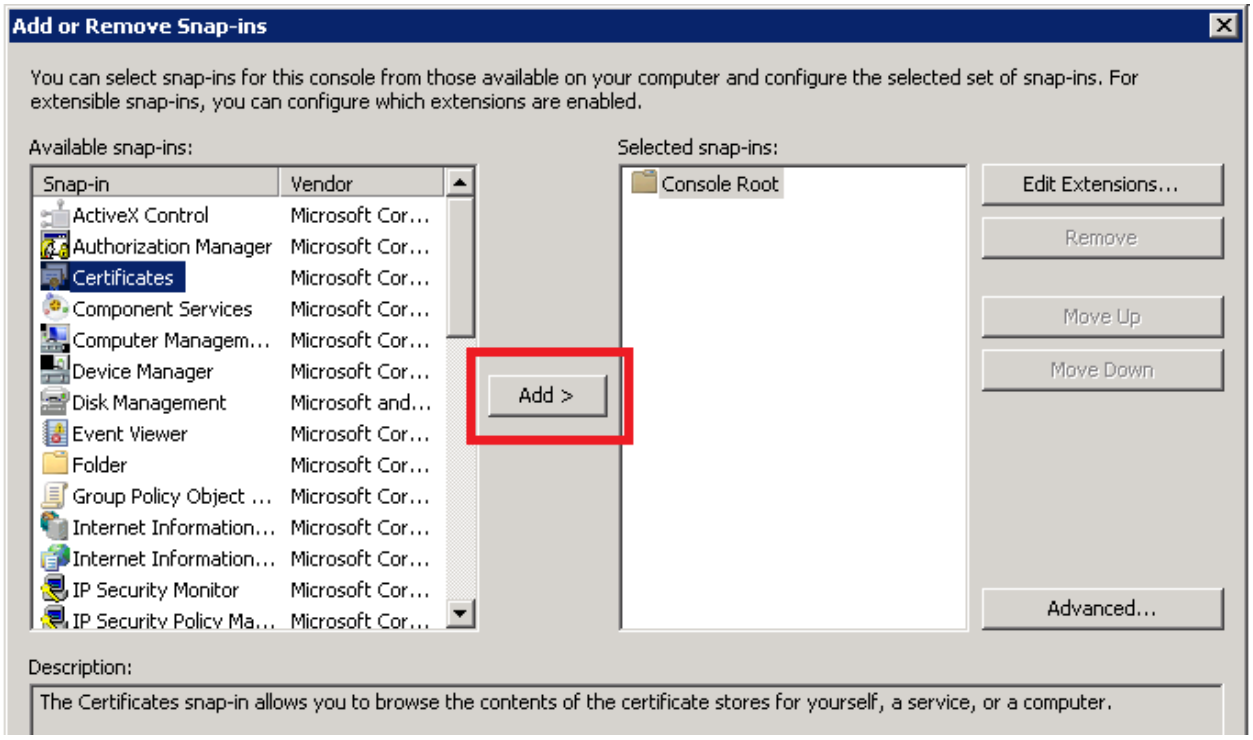


Figure 6.2: Add Snap-in

7. Click **Next**.
8. In the "Select Computer" popup box, click the **Local computer:** radio button, (*See Figure 6.3*)
9. Click **Finish**. You will be returned to the "Add or Remove Snap-ins" window.
10. Back at the "Add or Remove Snap-ins" window, you should now see **Certificates (Local Computer)** listed under the **Console Root** folder. (*See Figure 6.4*)
11. Click **OK**.

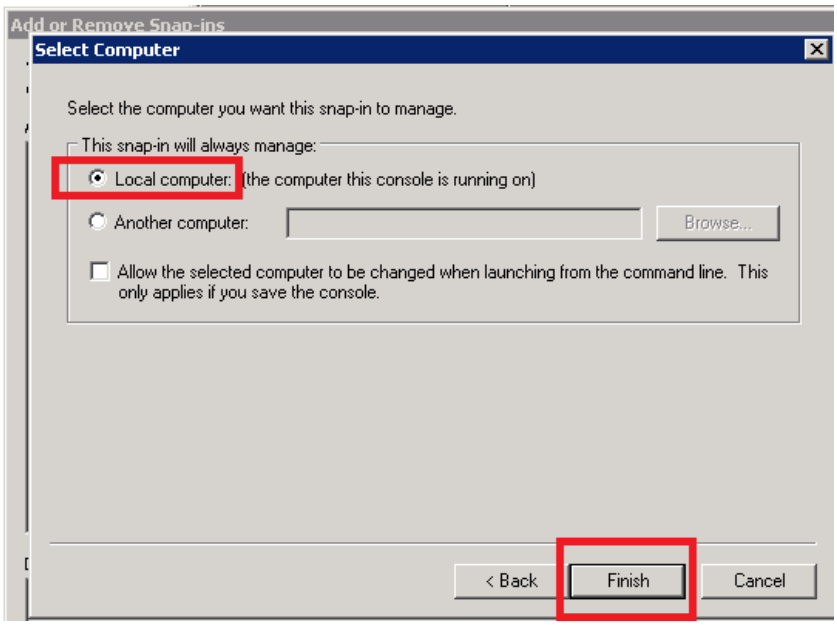


Figure 6.3: Select Computer

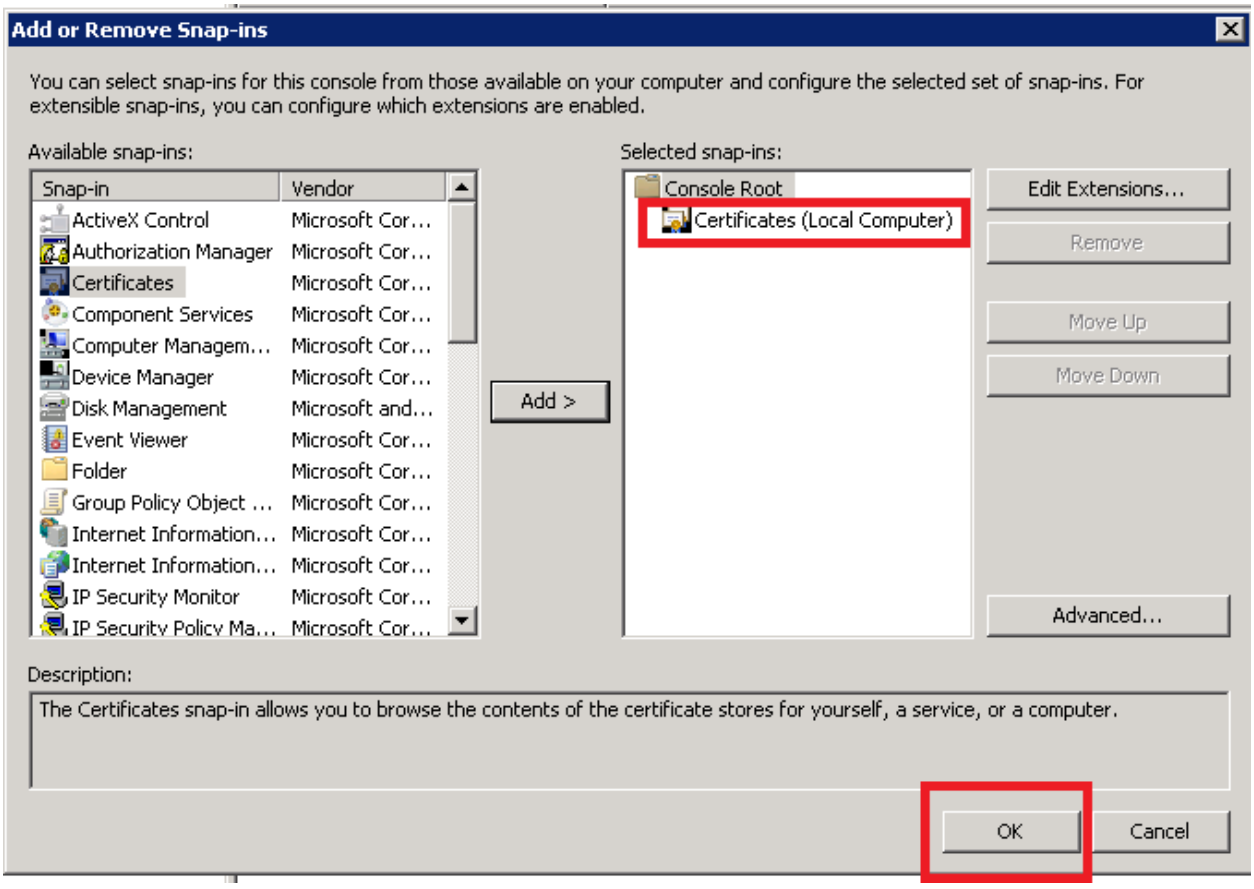


Figure 6.4: Certificate Snap-in Added

6.3.2 Apply Certificate and Set Permissions

1. In the **Certificates (Local Computer)** folder under **Console Root**, select the **Personal** folder, then the **Certificates** folder. (*See Figure 6.5*)
2. In the list of certificates provided, right-click the certificate used by the SMS site.
3. In the right-click menu, select **All Tasks**.
4. Under **All Tasks**, select **Manage Private Keys**. (*See Figure 6.5*)
5. In the "Permissions" popup box, Allow the user or group **Read** permission.
6. Click **OK**. (*See Figure 6.6*) The "Permissions" popup box should disappear.

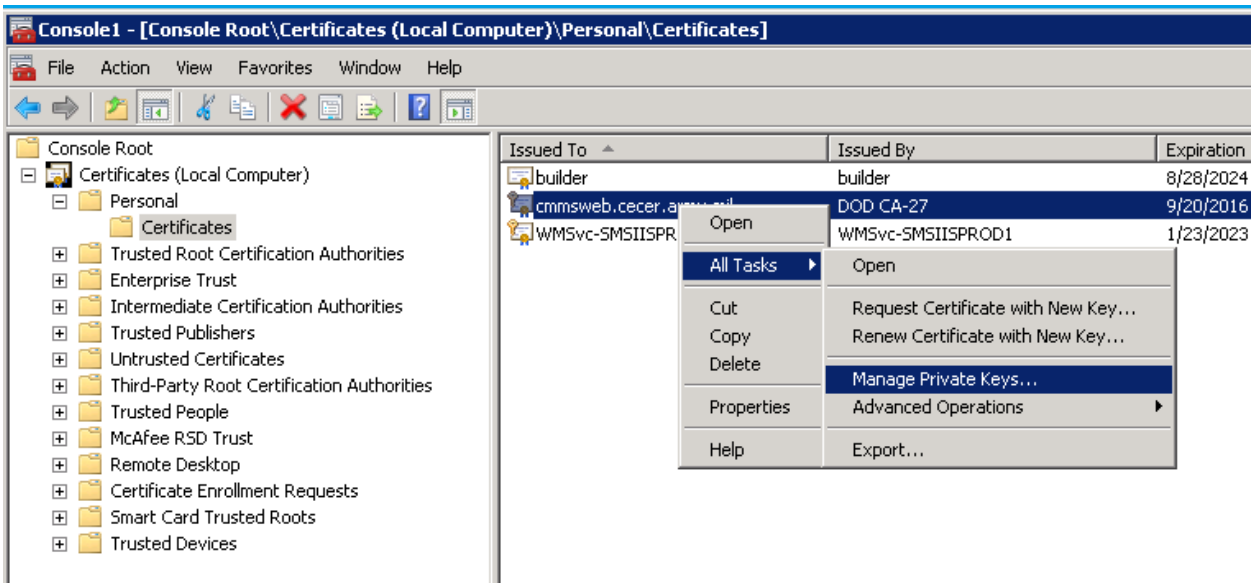


Figure 6.5: Navigate to Manage Private Keys

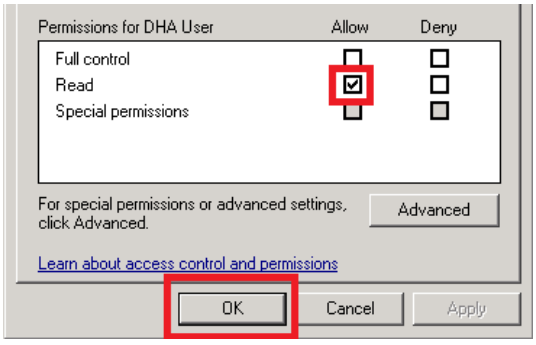


Figure 6.6: Navigate to Manage Private Keys

7. Close the console window, saving changes.

<APP_POOL_USER> now has read permissions on the certificate's private key.

6.4 reCAPTCHA Login Verification

Beginning with SMS Version 3.5.3, reCAPTCHA verification has been added to the web login page for the SMS. However, this feature is disabled by default to accommodate customers who do not have Internet access. The following subsections describe how to activate reCAPTCHA verification for the web login page.

6.4.1 Prerequisites for Enabling reCAPTCHA when Self-Hosting

If you are not self-hosting, proceed to section 6.4.2.

If self-hosting, you need to (1) apply for a reCAPTCHA key and (2) edit configuration before activating reCAPTCHA. Those steps are described in sections 6.4.1.1 and 6.4.1.2 immediately below.

6.4.1.1 Apply for reCAPTCHA key

1. Apply for a reCAPTCHA key at https://www.google.com/recaptcha/admin/create.

   IMPORTANT: The key must be for reCAPTCHA v2.

2. In the application process, you must choose between (a) restricted access and (b) allowing access from all domains/sites.

3. If you select restricted access, you will need to list the sites from which the key will be valid.

4. If you allow access to all domains, the level of security will be a bit lower.

5. At the end of the application process, you should receive a private key and a public key.

6.4.1.2 Edit Configuration File

The configuration file Web.recaptchaKey.config, in the <WEB_APP_ROOT>\Configs directory, should contain starter content. To prepare for using reCAPTCHA, you need to insert into the file the private key and the public key obtained above, as shown in the example below:

```
<?xml version="1.0" encoding="utf-8" ?>
<appSettings>
     <add key="recaptchaPrivatekey" value="--insert reCAPTCHA private key here--"/>
     <add key="recaptchaPublickey" value="--insert reCAPTCHA public key here--"/>
</appSettings>
```

Once you have the public and private reCAPTCHA keys and have entered them into the Web.recaptchaKey.config file, proceed to the activation instructions in the next subsection, 6.4.2.

6.4.2 Activating reCAPTCHA

To activate reCAPTCHA on the web login page for the SMS, run the following SQL query against your database:

```
INSERT INTO dbo.Configuration (ConfigName, ConfigValue)
VALUES ('ReCaptchaAPI', 'True')
```

This will ensure that the table contains an active entry where ConfigName="ReCaptchaAPI" and ConfigValue="True"

6.5 Pass-Through Signin

To establish pass-through signin, the user's certificate information (coded in binary) needs to be passed from the two-factor authentication program to SMS BUILDER via an HTTP header. To enable this,

1. In the two-factor authentication program, determine the name of the HTTP header where the user certificate is stored.
2. In the SMS configuration table, find the ConfigName "CertHeaderKey"
3. Set the ConfigValue of CertHeaderKey to the header name from step 1.

Chapter 7

Server Administration

7.1 Displaying User Notification Banners

It is possible to display a message to all clients' login pages. This is typically used to notify clients of scheduled downtime or other system messages. This is accomplished using the SMS PowerShell module commands.

7.1.1 Set-SMSMessage -Message <String> [-Name <String>] [-Site <String>]

This command displays a message on one or more SMS application login pages. If neither the **[-Name]** nor **[-Site]** parameter is specified, the default is the login page of all SMS applications in all sites.

7.1.1.1 -Message <String>

REQUIRED: The first <String> you provide is the message string. This needs to be a "quoted" string (enclosed in quotation marks).

7.1.1.2 [-Name <String>]

Optional: Specifies which SMS application. If omitted, the default is all SMS applications. If both the **[-Name]** and **[-Site]** parameters are omitted, the message will be displayed on the login page of all SMS applications on all sites.

7.1.1.3 [-Site <String>]

Optional: The <String> following the **[-Site]** parameter is the name of the designated site. If the **[-Site]** parameter is omitted, the default is all sites. If both the **[-Name]** and **[-Site]** parameters are omitted, the message will be displayed on the login page of all SMS applications on all sites.

> ***Note:*** *This parameter may be abbreviated to <String> only if the* ***[-Name]*** *parameter has been included before it.*

7.1.2 Reset-SMSMessage [-Name <String>] [-Site <String>]

This command removes the message from one or more SMS application login pages. If neither the **[-Name]** nor **[-Site]** parameter is specified, it removes any messages from the login page of all SMS applications in all sites.

7.1.2.1 [-Name<String>]

Optional: Specifies which SMS application. If omitted, the default is all SMS applications. If both the **[-Name]** and **[-Site]** parameters are omitted, all messages will be removed from the login pages of all SMS applications on all sites.

7.1.2.2 [-Site <String>]

Optional: The <String> following the **[-Site]** parameter is the name of the designated site. If this parameter is omitted, the default is all sites. If both the **[-Name]** and **[-Site]** parameters are omitted, all messages will be removed from the login pages of all SMS applications on all sites.

> ***Note:*** *This parameter may be abbreviated to <String> only if the* ***[-Name]*** *parameter has been included before it.*

7.2 Managing SMS Applications with PowerShell

7.2.1 Configuring the PowerShell Execution Policy

PowerShell needs to be enabled to manage the SMS application. By default, the execution policy is set to **Restricted**. This blocks all PowerShell scripts from being executed. The module included with this install is signed with a DoD certificate. If the DoD root certificates are installed on the IIS server, the execution policy can be set to **AllSigned**. If the DoD root certificates are *not* installed on the IIS server, the execution policy should be set to **Unrestricted**.

7.2.1.1 Example Instructions to Change Execution Policy

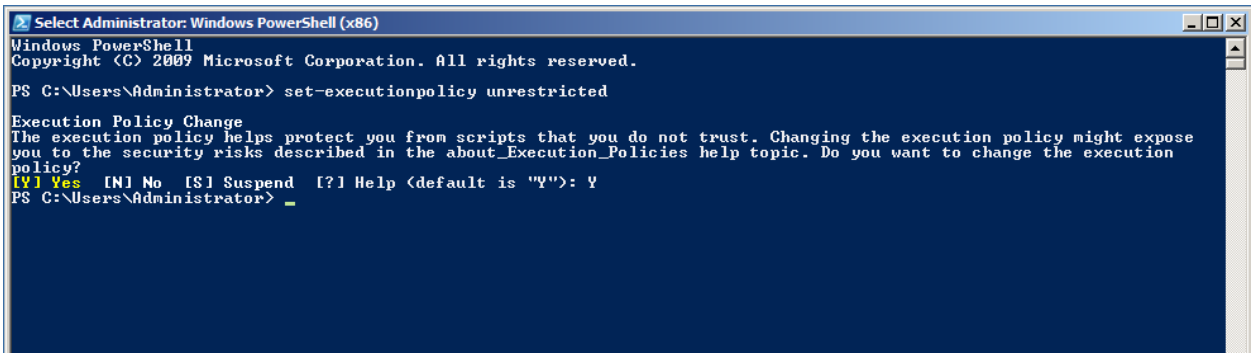


Figure 7.1: SMS Powershell

1. Click **Start**.
2. Click **All Programs**.
3. Click **ERDC-CERL**.
4. Click **Sustainment Management System**.
5. Click **SMS PowerShell**.
6. Type `Set-ExecutionPolicy AllSigned` and press **Enter**.

7. When prompted, type `Y` and press **Enter** (Figure 7.1)
8. Type `Import-module SMS-module` and press **Enter**.

7.3 Backing Up and Restoring

Backups need to be accomplished in two places. The SMS application stores user files in the <WEB_APP_ROOT>**files** directory. Additionally there are configuration files that are stored in the <WEB_APP_ROOT>directory. All files in <WEB_APP_ROOT>should be backed up. The second place backups need to occur is on the SQL Server, either scheduled through a maintenance plan or with a third party utility.

7.3.1 Backup-SMSApplication -BackupPath <String> [-Name <String>] [-Site <String>]

The SMS PowerShell module includes a backup utility that archives the application, configuration, and user files. It does *not* backup the databases; this will need to be configured and scheduled with a SQL Server Management Studio maintenance plan or with a third party backup application.

7.3.1.1 -BackupPath <String>

REQUIRED: Designates the path and filename that the archive will be stored to. This string should be enclosed in quotation marks if there are spaces in the path. The filename should have the .zip extension appended.

7.3.1.2 [-Name <String>]

Optional: Specifies the SMS application to be backed up. If omitted, the default is all SMS applications. If both the **[-Name]** and **[-Site]** parameters are omitted, all SMS applications for all sites will be backed up.

7.3.1.3 [-Site <String>]

Optional: Designates the site for which the SMS application(s) will be backed up. If omitted, the default is all sites. If both the **[-Name]** and **[-Site]** parameters are omitted, all SMS applications on all sites will be backed up.

> ***Note:*** *This parameter may be abbreviated to <String> only if the* ***[-Name]*** *parameter has been included before it.*

7.4 Managing and Configuring Logs

7.4.1 Log Locations

The logs are located in the Event Viewer and in the IIS logging path.

7.4.1.1 Application Event Log

By default, IIS writes logs to the **%SystemDrive%\inetpub\logs\LogFiles** directory. Information written in these logs includes page errors, client IP addresses, page requests, and information about client browsers. This file can be examined with standard web log parsers. The location of this file can be modified in the IIS Manager under **Logging**.

7.4.1.2 Application Web Log

Handled web application exceptions, process messages, and debugging information is written to the Event Viewer in the **Application and Services Logs\BUILDER Log**. Any un-handled application exception can be found in the **Windows Logs\Application log**.

7.4.1.3 Service Event Log

Handled service exceptions, process messages, rollup status, scenario status, and debugging information is written to the Event Viewer in the **Application and Services Logs****BUILDER Log**. Any un-handled service exceptions can be found in the **Windows Logs****Application log**.

7.4.2 Modifying Event Log Rights

The SMS Application and SMS Service must be granted rights to modify the Event Log. These programs will add custom event logs after starting for the first time. After the application and service start, the permissions on the Event Log can be changed to allow write only to the Impact Log and the BUILDER Log. To modify the permissions, add **Read** for the **IIS_IUSRS** group and the user the service is running under, typically <POOL_IDENTITY>.

7.4.2.1 Steps to modify the Event Log permissions:

1. Type `Regedit` in the Windows Search box, and then select the program and open it.
2. Navigate to **HKEY_Local_Machine/System/Current Control Set/Services/Event Log**.
3. Right-click the folder **Event log**, and select permissions from the options given.
4. Select **Add** and then type `IIS_IUSRS` in the **Enter the object name to select** box and click **OK**.
5. Check the **Read** permission with the **IIS_IUSERS** group highlighted, and then **Apply** (*See Figure 7.2*).

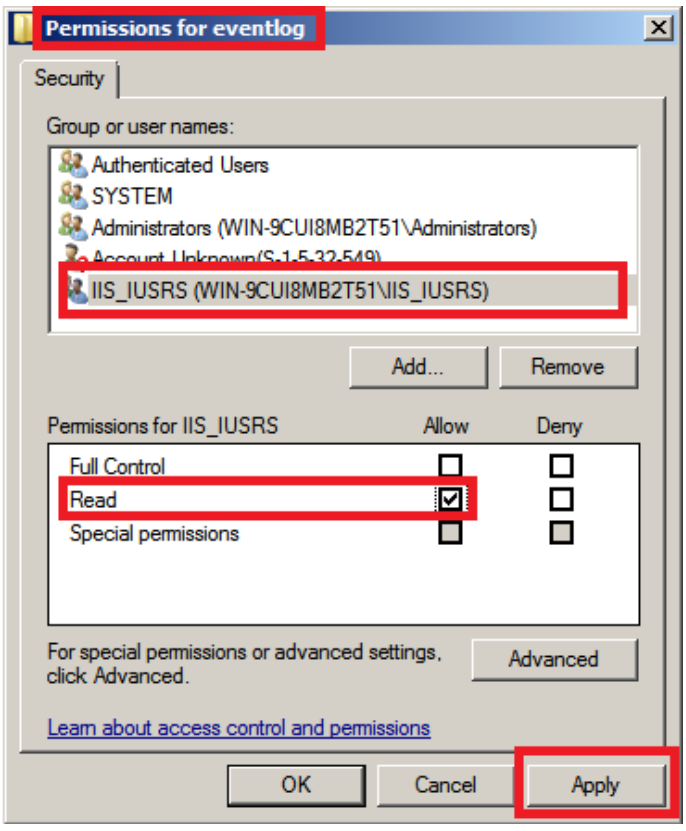


Figure 7.2: Modify Event Log Permissions

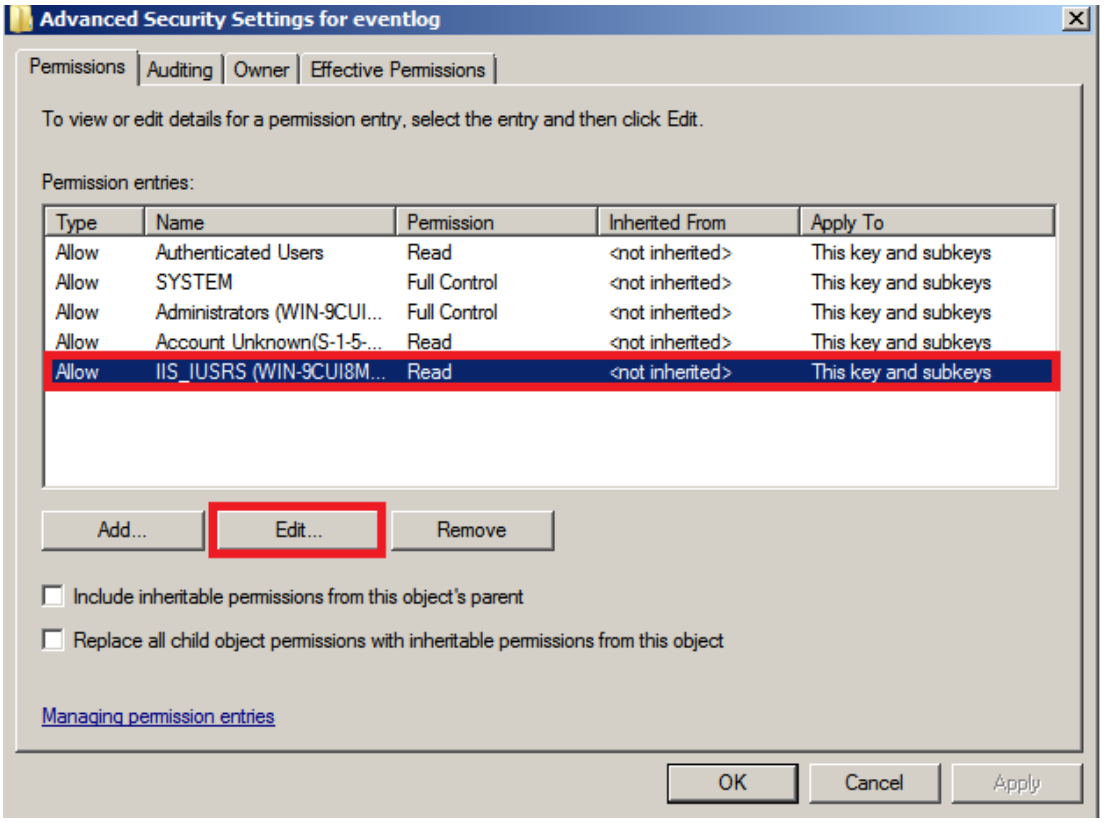


Figure 7.3: Modify Event Log Permissions

6. With **IIS_IUSRS** still selected, click the **Advanced** button, select **IIS_IUSRS** from the dialog box, and click **Edit** (*Figure 7.3*).

7. Ensure that checkboxes are checked for **Set Value** and **Create Subkey** to allow and then click **OK** (*See Figure 7.4*).

8. Select **Apply**, and then **OK**.

9. Select **Apply** and **OK** one more time.

10. Right-click the **Security** folder under **eventlog**, and select **Permissions** (*See Figure 7.5*).

11. Select **Add** at the dialogue box type `IIS_IUSRS` in the **Enter the object names to select** box. With IIS_IUSRS highlighted, click the Allow **Read** check box. Select **Apply** and then **OK**. You can now close the **Registry Editor** (*See Figure 7.5*).

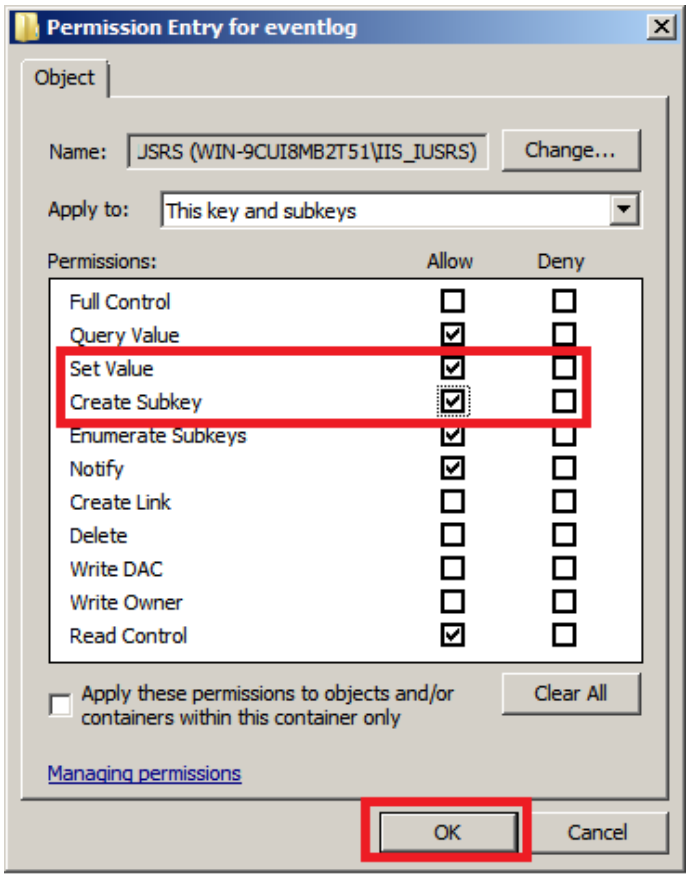


Figure 7.4: Modify Event Log Permissions

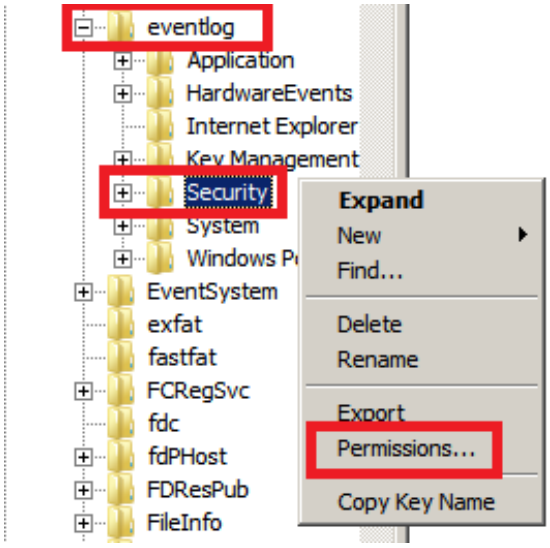


Figure 7.5: Modify Event Log Permissions

7.5 Installing Updates

7.5.1 Checking for Updates

There is an application in the Windows Start Menu that connects to the update server and checks for the latest version of SMS. This only updates the program files, scripts, tools, and SMS service. To update the web applications and databases, see the following sections. An update will not overwrite configuration settings or user files.

7.5.2 Updating SMS Applications

After checking for updates and installing the update, open the SMS PowerShell prompt and execute the following command:

Update-SMSApplication [-Name <String>] [-Site <String> [-BackupPath <String>] [-All] [-NoBackup] [-NoDatabaseUpdate]

This command updates one or more SMS applications. By default this command will backup the application, configuration, and user files to the **C:\Temp** directory.

7.5.2.1 [-Name] <String>

Optional: Specifies the SMS application to be updated. The **[-All]** switch may be used instead.

7.5.2.2 [-Site <String>]

Optional: Designates the site on which the SMS application(s) will be updated.

> ***Note:*** *This parameter may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

7.5.2.3 [-BackupPath <String>]

Optional: Designates the path that the backup archive will be stored to. The <String>should be enclosed in quotation marks if there are spaces in the path. The default path is **C:\Temp**.

7.5.2.4 [-All]

Optional: Update all SMS applications.

Unlike many other commands, omitting **[-Name] <String>]** and **[[-Site] <String>** will *not* perform the command on all SMS applications by default.

7.5.2.5 [-NoBackup]

Optional: Forces an update without backing up files.

7.5.2.6 [-NoDatabaseUpdate]

Optional: Forces an update without upgrading the database. Database upgrade must then be added manually (*see section 7.5.3*).

> ***Note:*** *This command will not overwrite configuration settings or user files.*

7.5.3 Updating the SMS Database

The **Update-SMSApplication** command will update the database by default. However, updating the database can also be done as a standalone operation as described below. Some application updates will require a database update.

7.5.3.1 Updating the SMS Database from Version 3.3.7 or Later

To perform the database update,

First copy the following file from the application server to the database server:

%ProgramFiles%\ERDC-CERL\Database\Update Scripts\InventoryDB_upgrade.sql

Next, open SQL Management Studio on the SQL Server and perform the following steps:

1. Open InventoryDB_upgrade.sql
2. Use Find and Replace to replace $SMSINVENTORYDB$ with the name of the SMS inventory database. There should be only one occurrence.
3. Execute the InventoryDB_upgrade.sql script.
4. If there are no errors, replace the line that reads, "@RUNTYPE = 'TEST' " with "@RUNTYPE = 'FINAL' "
5. Execute the InventoryDB_upgrade.sql script.

7.5.3.2 Updating the SMS Database from Version 3.3.6 or Earlier to Version 3.3.7 or later

Certain types of invalid data will cause updating the database from Version 3.3.6 to fail: for example, IDs of less than 36 characters that are used in lieu of GUIDs. In some cases, the update script will be able to identify problem data and either make an automatic fix or recommend what you can do to correct it.

The instructions for performing the database update from SMS Version 3.3.6 or are the same as above, except for this recommendation: The quantity of schema change between Version 3.3.6 and 3.3.7 is so great that it could result in Step 3 ("Execute the InventoryDB_upgrade.sql script") taking a very large amount of time. Because of this, you may want to check the length of the update time in advance by making a copy of the database and testing the database upgrade on a backup server first, where it will not create any service interruption. Armed with this information, you can then make plans to minimize database downtime during the actual database upgrade.

For database versions 3.3.7 or later, the database update should not take an unusually long time.

7.6 Adding Web Application

The procedure for installing an SMS web Application differs slightly between an installation using Windows Authentication and one using SQL Authentication. Each procedure is described separately below.

7.6.1 Install-SMSApplication (using Windows Authentication)

Install-SMSApplication -Site <**String**> **-Name** <**String**> **-DatabaseServer** <**String**> **-ApplicationPoolUser** <**String**> **-winAuthentication**

This command installs an SMS application to the IIS Server as a web application. The required parameters are listed below; refer to the System Configuration Worksheet (Appendix C on page 77) for values to be entered.

Important: Before running this script, please ensure that:

1. A web site exists, such as "Default Web Site". It can be named differently, but you must know the name of the site this application should install to;
2. The Application Pool user exists and you know the password;
3. If using Windows Authentication to your database, you are logged-in as a user with permissions to connect to the SMS application's database;
4. Your database has already been created AND data has been bulk copied. If not, please refer to the **Export-SMSDatabaseScripts (Using Windows Authentication)** command on page 82. Depending on your environment, you may need to run the resulting scripts on your database server.

7.6.1.1 -Site <String>

REQUIRED: Designates the site where the SMS application will be installed. Type `-Site` and enter the value of <DEFAULT_WEBSITE> from the System Configuration Worksheet. Alternatively, just enter the value of <DEFAULT_WEBSITE>.

7.6.1.2 -Name <String>

REQUIRED: Specifies which SMS application is to be installed. Type `-Name` and enter the value of <WEB_APP_NAME> from the System Configuration Worksheet. Alternatively, just enter the value of <WEB_APP_NAME>.

7.6.1.3 -DatabaseServer <String>

REQUIRED: This is the same as the **-databaseServer** parameter used with `Export-SMSDatabaseScripts`. Type `-databaseServer` and enter the value of <SQL_SERVER_NAME> from the System Configuration Worksheet.

7.6.1.4 -ApplicationPoolUser <Value>

Type `-ApplicationPoolUser` and enter the value of <POOL_IDENTITY> from the System Configuration Worksheet. When prompted, enter the associated password.

7.6.1.5 -winAuthentication

REQUIRED: Type `-winAuthentication` if you are using Windows Authentication for your database.

Visit Get-Help Install-SMSApplication to see optional parameters for this command.

7.6.2 Install-SMSApplication (using SQL Authentication)

Install-SMSApplication -Site <String> -Name <String> -DatabaseServer <String> -ApplicationPoolUser <String> -sqlAuthentication -DatabaseUser <String>

This command installs an SMS application to the IIS Server as a web application. The required parameters are listed below; refer to the System Configuration Worksheet (Appendix C) for values to be entered.

Important: Before running this script, please ensure that:

1. A website exists, such as "Default Web Site". It can be named differently, but you must know the name of the site this application should install to;
2. The Application Pool (AppPool) user exists and you know the password;

3. If using SQL Authentication to your database, you know the username and password of the user that will connect to the database on behalf of the SMS application, because you will be prompted for this information;
4. Your database has already been created AND data has been bulk copied. If not, please refer to the **Export-SMSDatabaseScripts (Using SQL Authentication)** command on page 83. Depending on your environment, you may need to run the resulting scripts on your database server.

7.6.2.1 -Site <Value>

REQUIRED: Designates the site for installing the SMS application. Type `-Site` and enter <DEFAULT_WEBSITE> from the System Configuration Worksheet. Alternatively, just enter <DEFAULT_WEBSITE>.

7.6.2.2 -Name <Value>

REQUIRED: Specifies which SMS application is to be installed. Type `-Name` and enter <WEB_APP_NAME> from the System Configuration Worksheet. Alternatively, just enter <WEB_APP_NAME>.

7.6.2.3 -DatabaseServer <Value>

REQUIRED: Type `-DatabaseServer` and enter the value of <SQL_SERVER_NAME> from the System Configuration Worksheet.

7.6.2.4 -ApplicationPoolUser <Value>

REQUIRED: Type `-ApplicationPoolUser` and enter the value of <POOL_IDENTITY> from the System Configuration Worksheet. When prompted, enter the associated password.

7.6.2.5 -sqlAuthentication

REQUIRED: Type `-sqlAuthentication` if you are using SQL Authentication for your database.

7.6.2.6 -DatabaseUser <String>

REQUIRED: This value is required only when SQL Authentication is being used. Type `-DatabaseUser` and enter the SQL Authentication username. (In the System Configuration Worksheet, this is the value for <SQL_AUTH_USERNAME>.) When prompted, enter the associated password.

Visit Get-Help Install-SMSApplication to see optional parameters for this command.

Chapter 8

SQL Server Reporting Services Administration

After the installation and configurations specified in the Installation chapter of the *Installation Guide* (Section 5.8, *Configure Custom Reports*), you can follow the appropriate set of instructions below either to (1) create and publish a BUILDER custom report or (2) load an existing custom report.

8.1 How to Create a Custom Report

This section outlines how to create and publish a custom BUILDER report using Visual Studio SQL Server Reporting Services (SSRS), one of Microsoft's Business Intelligence (BI) tools for Visual Studio. Microsoft SQL Server Report Builder may be used as an alternative if the user is familiar with it.

The output from either of these report building tools is an .RDL (Report Definition Language). These .RDL files can then be accessed and read using BUILDER's Custom Reports interface.

8.1.1 Background Information

Reports are created using a *data source* that points to the SQL Server database that underlies BUILDER. The BUILDER database is stored in SQL Server and is comprised of (1) a number of *tables*, as well as (2) stored data queries called *(data) views*.

On USA-CERL's server, a BUILDER database is named using the following convention:

ClientName_ModuleAbbreviations_BUILDERversion

where appropriate names will be substituted for the variables in italics, separated by underscores. For example, the database **USMC_Inv_31** stores the data for the U.S. Marine Corps' BUILDER implementation, INVENTORY module, BUILDER version number 3.1.

8.1.2 Major Steps in Creating and Publishing a Custom Report

The major steps in creating a custom report are:

1. In SQL Server Management Studio either (a) Locate and choose a view or (b) Create a view.
2. Create the report source file using Visual Studio SQL Server Reporting Services (SSRS). (Microsoft SQL Server Report Builder may also be used.)
3. Configure parameters and data sources.

8.1.3 Choose or Create a View

The first step in creating a custom report is either (a) choosing or (b) creating a view in SQL Server Management Studio. Often, a view will be created specifically for a single report. Note however, that there exist a great number of views already created in SQL Server that you might be able to use to feed a report. So the first step is to decide whether to create a new view or adapt an existing one.

If you want to create a custom view, then you need to have READ/WRITE/CREATE access to the BUILDER SQL Server database. You also need a basic understanding of the BUILDER table structure and of the relationship between the tables.

The purpose of the view is to collect and preprocess the data columns that will be used in your report.

8.1.4 Create a Report Source file

The second step in creating a custom report is creating a report source file. Note that when creating a report source file, it may be simplest to start by opening and immediately renaming an existing BUILDER custom report source file (RDL). This helps ensure stylistic consistency, keeping the "look and feel" the same across all of your custom reports. It is preferable to use as your model a report with sufficient detail in it to set formatting standards, but also without a great deal of content to be deleted.

To create a report source file from scratch, use either (a) Visual Studio SQL Server Reporting Services (SSRS), one of Microsoft's Business Intelligence (BI) tools for Visual Studio, or (b) Microsoft SQL Server Report Builder.

> **NOTE:** These instructions do not cover how to use these report writing tools. There are a number of tutorials online to help the user get started.

8.1.5 Configure Parameters and Data Sources

1. A Data Source will need to be created that will point to the SQL Server BUILDER database. A Data-Set (or sets) will then be created that uses the Data Source and points to the particular tables or views with the BUILDER database. Each data set is comprised of a SQL SELECT STATEMENT that pulls the data for the report. Each report must have one data-set, but it may have multiple sets that feed different regions of the report.

2. Another component of the report that needs to be understood by the user is the concept of input parameters for the report. Since Custom BUILDER reports can reside at different levels with BUILDER (i.e., Organization-Level, Site-Level, Complex-Level, Building-Level) the user must create a report *parameter* to match up with the level from which the report will be run. For example, if this is a Site-Level report, a report parameter must be set up within the report to receive the SITE_ID which BUILDER will pass to the report at run-time. The SITE_ID then behaves as a filter to confine the data-set records to the one particular site. The parameter should be named: BUILDERID, though SITE and COMPLEX are also valid parameter names.

3. The report is constructed and previewed using the Data Source defined within the report until a completed report is attained. Later the Data Source will be changed to point to the shared data source on the report server. (More on this later.)

4. Configure the report parameters using these four dialog boxes and settings:

Parameter Visibility: HIDDEN
Advanced: Always Refresh
Default Values: No Default Values
Available Values: NONE

Finally, save the report and exit the report writing tool, making a note of the .RDL filename.

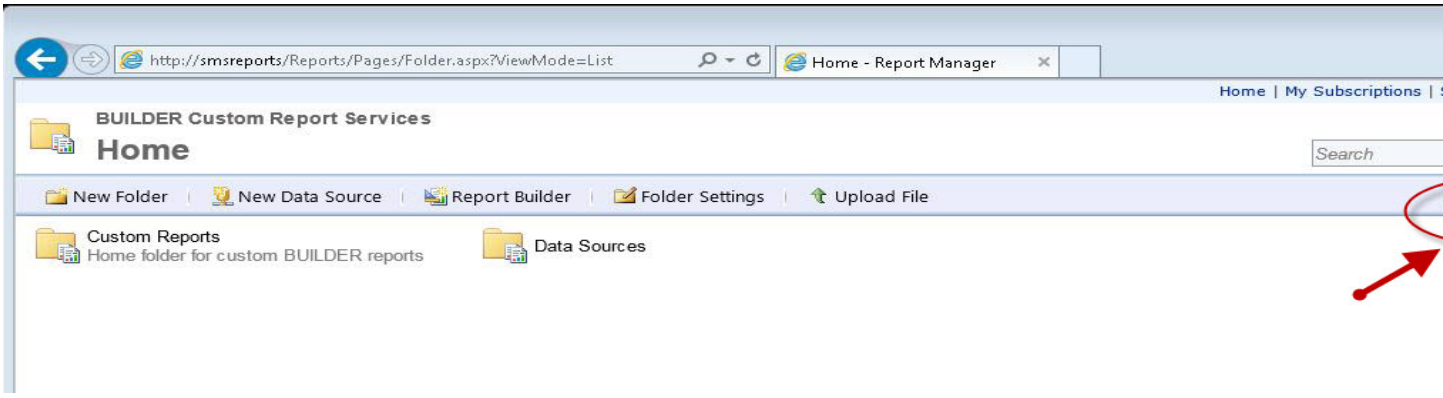
8.2 Upload the Report

Upload the .RDL Report File into the Report Server and set the Data Source

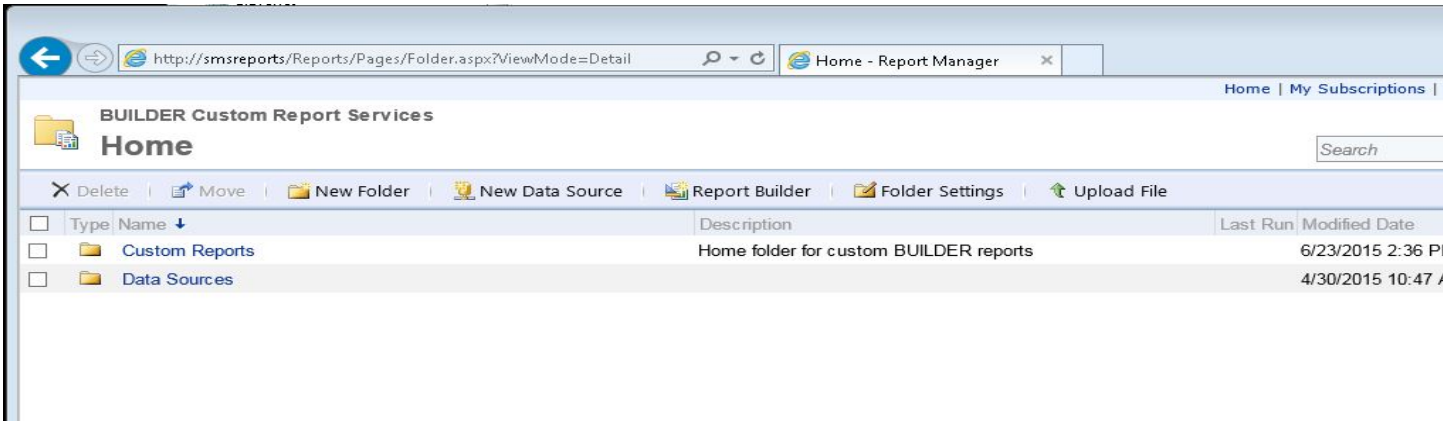
Publish the report by uploading the .RDL report file into the report server and setting the data source.

1. First the USER must login to the BUILDER report server. The user will need appropriate credentials to be able to do so. The screen-shot shows CERL's REPORT SERVER main screen. Use the **Details View** Option . . . it makes it easier to drill down through the reports menus.

Tile View:

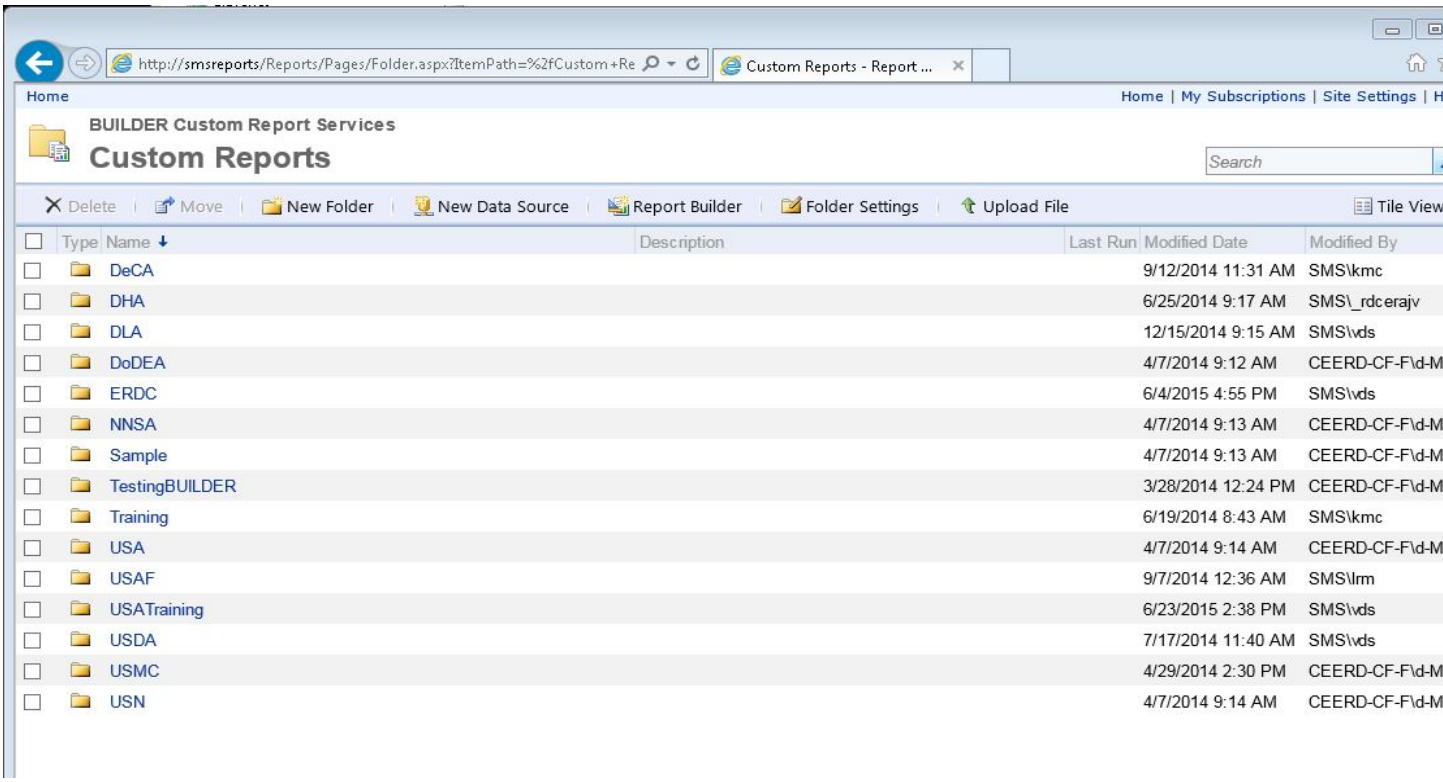


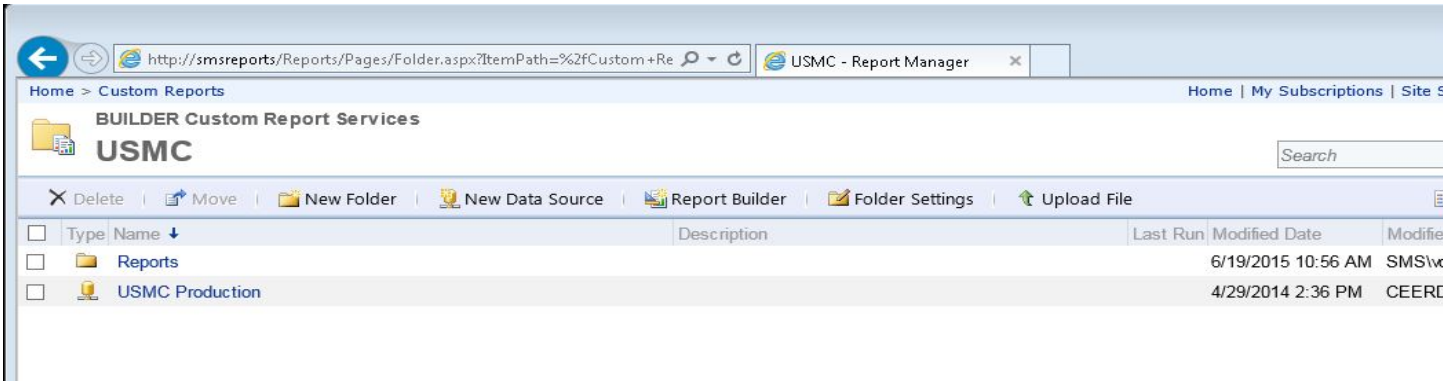
Details View:



In CERL's REPORT SERVER setup, there will be a folder for each BUILDER client implementation. Therefore clicking on the "Custom Reports" folder above will yield this screen where the client folders are clearly visible. We would assume that on the USMC local server, there will be just the one USMC folder and no others.

Clicking on the USMC folder opens this screen:





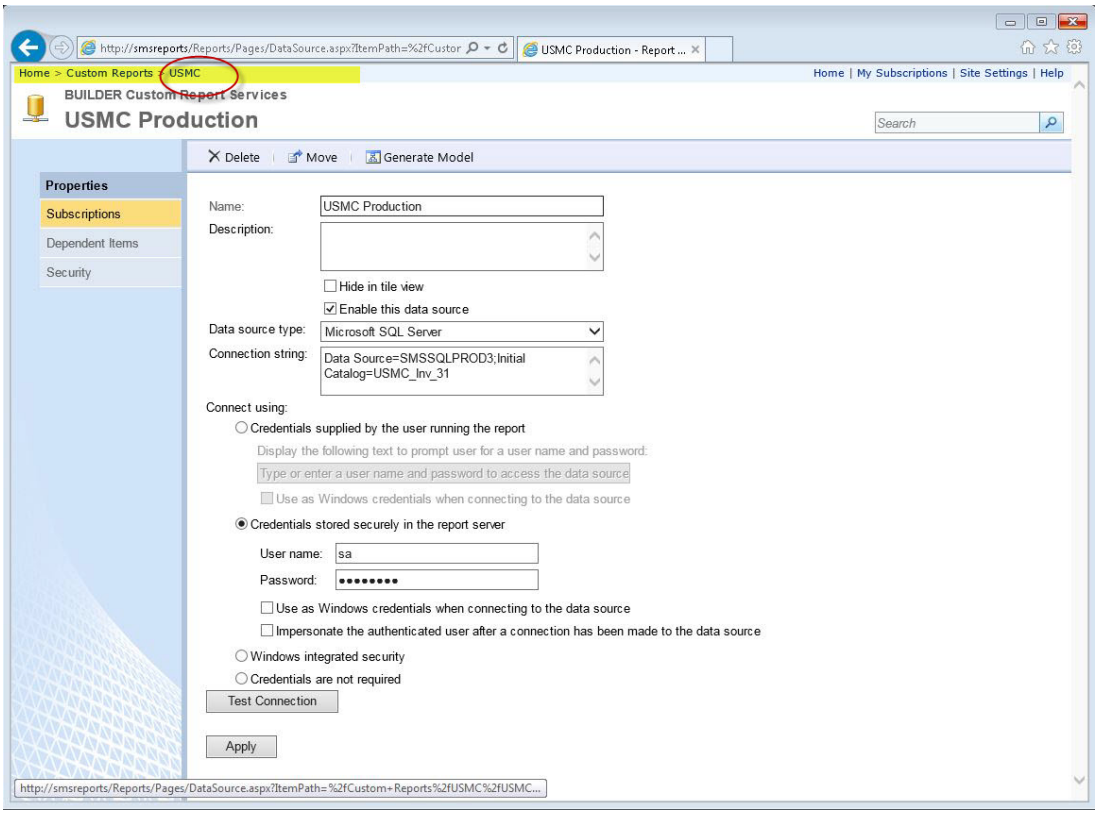
At CERL, the Shared Data Source for USMC reports has been configured in this folder. It is called "USMC Production."

If I double-click on the "USMC Production" Data Source, this screen is displayed which shows how the data source was configured to point to the report to the Sql Server USMC data.

To configure a new data source, fill out the screen and click the "Apply" button. To exit from this dialog box and return to the REPORT SERVER tree, use the bread-crumb trail hyperlink, "Home > Custom Reports > USMC" at the top of the page, click "USMC" (circled above) and return to the USMC tree.

This time, I will click on the "Reports" sub-folder to open the following screen:

Note that a BUILDER report can be called from various levels in the BUILDER hierarchy. The source code for the report should be written to feed one of the four levels and the parameter in the report must be set to receive one of the following: ORGANIZATION_ID, the SITE_ID, the COMPLEX_ID or the FACILITY_ID. Bear in mind that there may be multiple versions of the "Final 1 - Facility Summary Report", for instance. The code in each will be slightly different to accommodate the different levels. The report MUST be loaded into the REPORT SERVER at the level for which it is written or you will get a run-time error. At CERL, we keep the file name the same, but keep the source code files stored in separate folders to distin-



guish them. But the user could change the report name slightly, to make the level perfectly obvious, for example, ”Final 1 (Site) - Facility Summary”, ”Final 1 (Complex) - Facility Summary”, etc.

8.3 How to Load a Custom Report into SMS

To load a custom report into SMS:

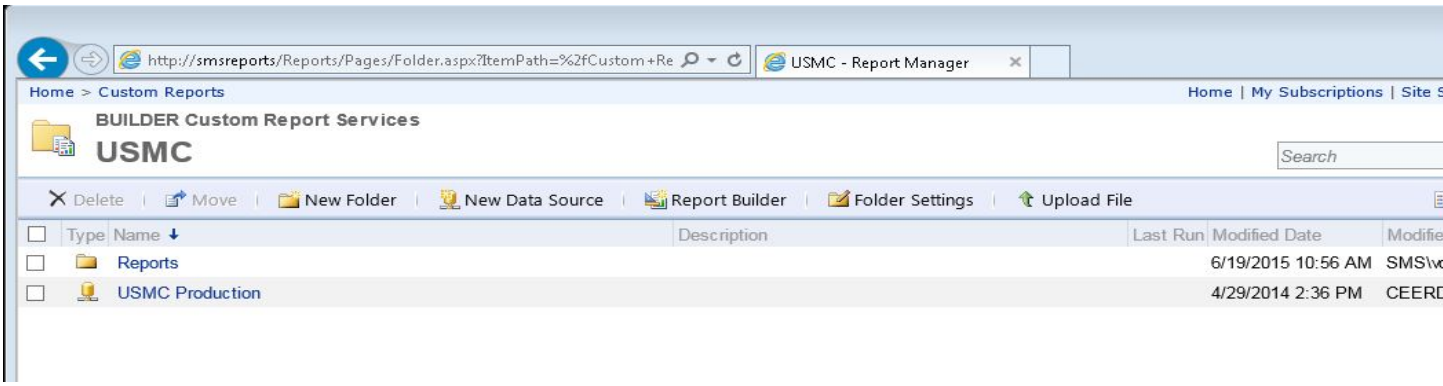
1. Drill down to the level at which you want to load your report. In this particular case, we are uploading a SITE-LEVEL report. So we drilled down into the ”Site” Folder. It looks like the following screen shot.

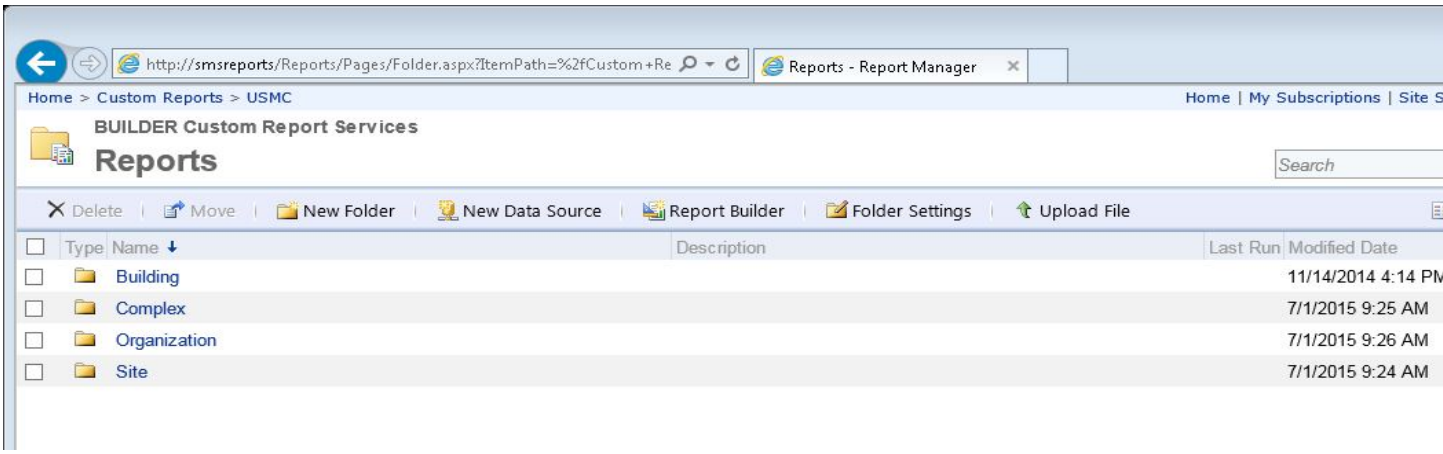
2. Once there, click the ”Upload File” button.

This brings up the UPLOAD dialog screen:

3. Use the ”Browse...” button to locate your report (.RDL file). Then click OK. If you were reloading an updated report and the report already existed in the REPORT SERVER previously, then you would need to check the ”Overwrite item if it exists” check-box. Locate your report in the report list and note the ”Modified Date” and ”Modified By” columns.

4. The next is an important step is to set the data source in the report. (This actually can be done BEFORE you upload the report if you have access to the REPORT SERVER from your development environment. Or you can wait and just do it once you have it loaded in the REPORT SERVER.) Hover your mouse over the report that you are configuring until the drop-down menu appears. From this menu, choose ”Manage” ...





This brings up the "Manage Report" dialog box ...

5. Click the "Data Source" menu to reveal the "Manage Data Sources" dialog box ...

6. Choose the "A shared data source" radio button and use the "Browse" button under that button to select the "USMC Production" data source. Click Apply. Use the bread-crumb trail hyperlink menu and click on "Site" to return to the Site folder.

7. Login to the BUILDER Inventory Module. Navigate down to a SITE. Select the new report from the Reports Menu / Custom Reports Sub-menu. Click View Report.

8.4 SQL Configuration

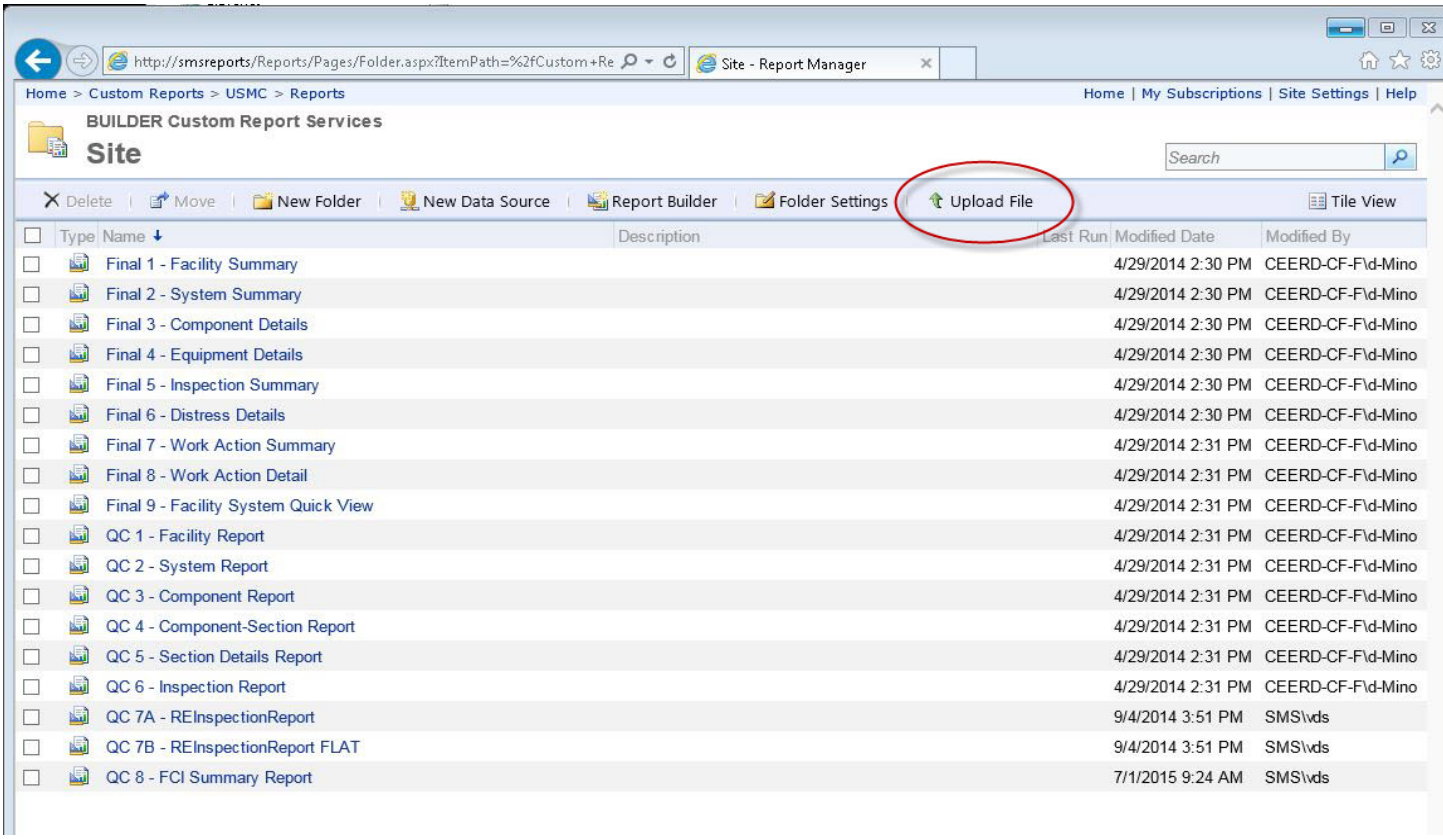
Once the reports are set up in your reporting server, and before accessing the reports, you will need to make some changes to the configuration table in your SQL server INVENTORY table. There are three fields that must be changed:

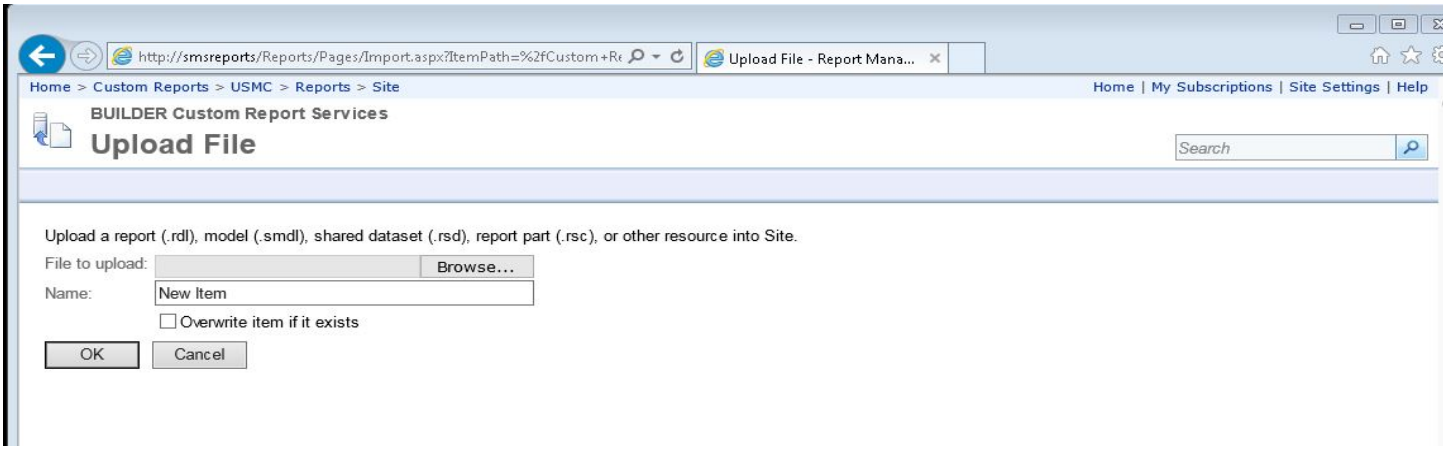
1. UseRemoteCstmRpts needs to be changed to True.

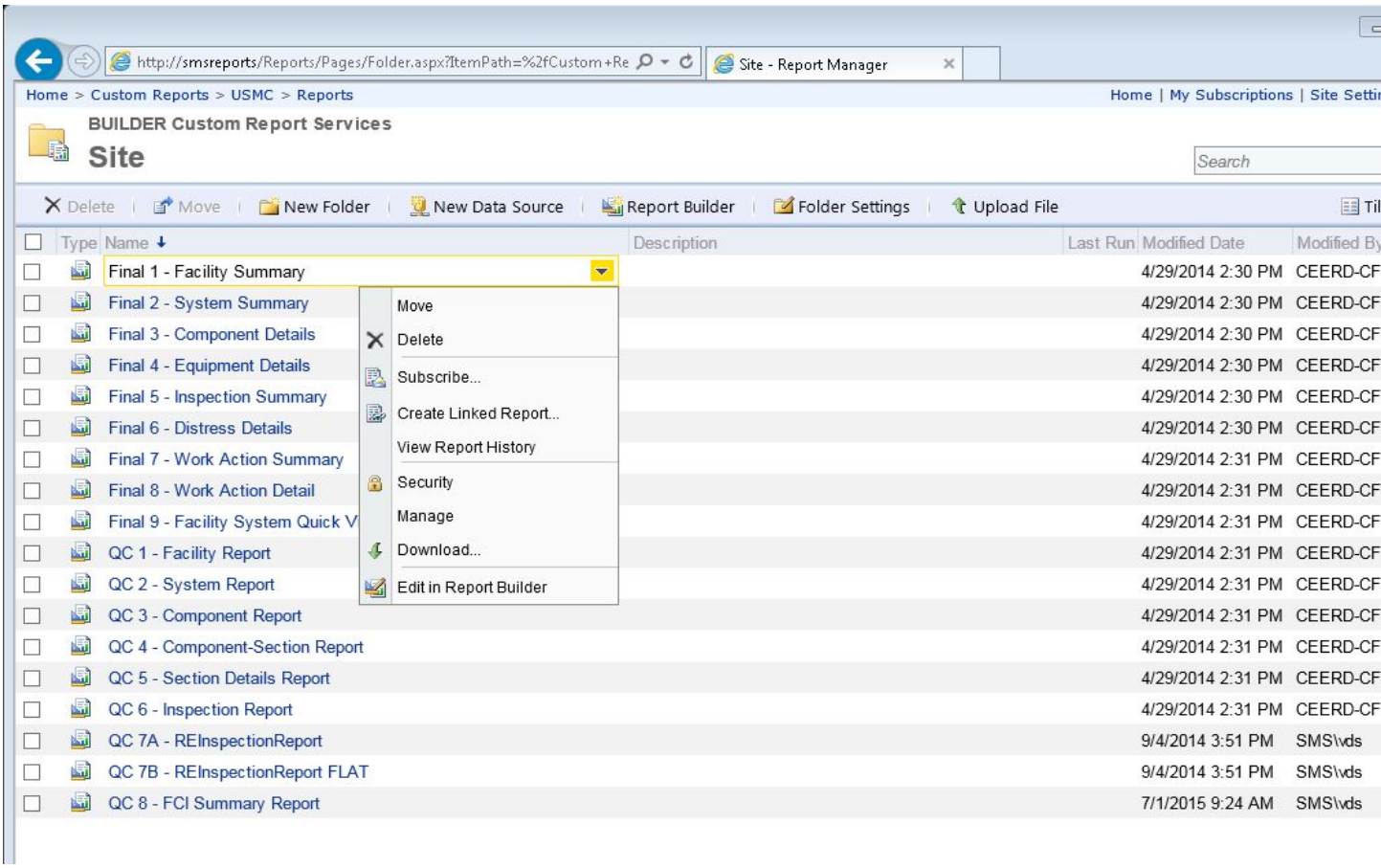
2. CstmRptSvrURI needs to be changed to the address of the report server concatenated with the virtual folder address.

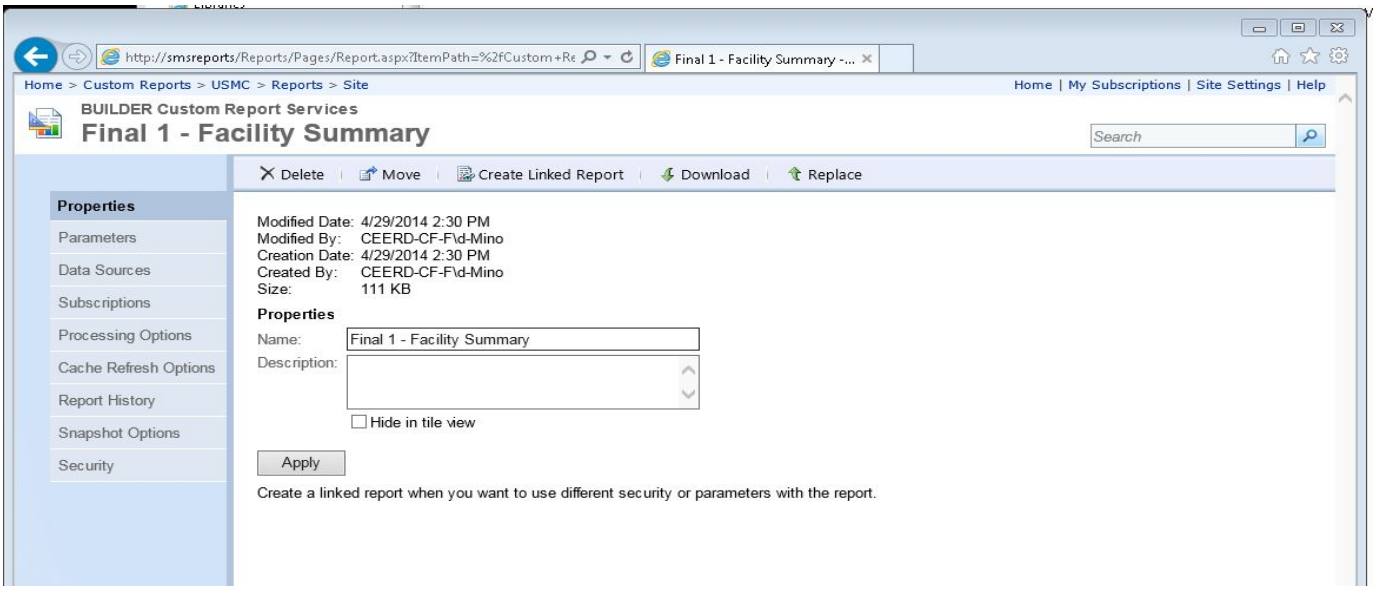
3. CstmRptSvrRoot needs to be changed to reflect the root folder that holds your reports.

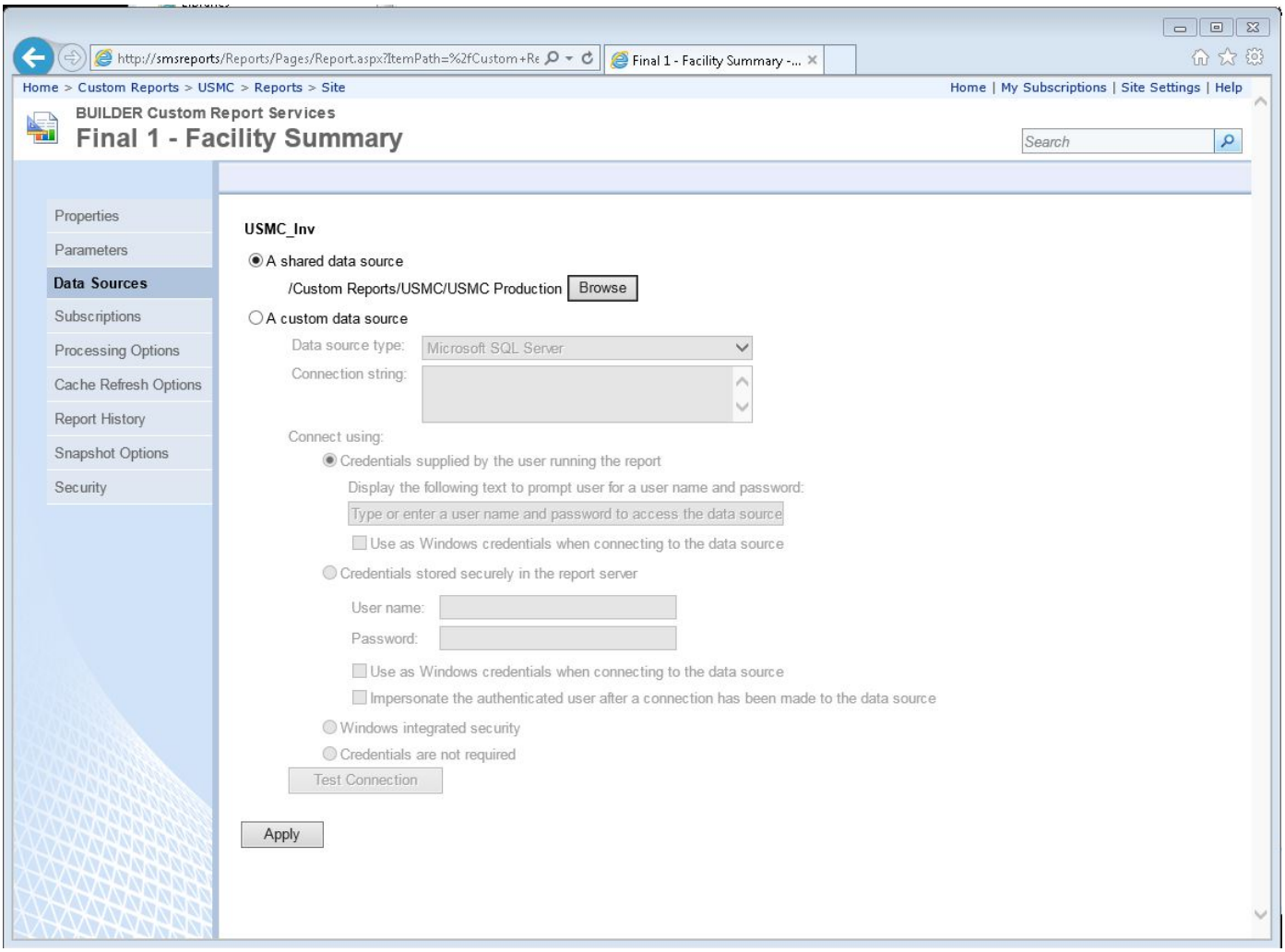
After these are changed, the APP POOL will need to be recycled; then your report should be accessible in the application.


http://smsreports/Reports/Pages/Folder.aspx?ItemPath=%2fCustom+Re
Site - Report Manager
Home > Custom Reports > USMC > Reports
Home | My Subscriptions | Site Settings | Help
BUILDER Custom Report Services
Site
Search
Delete
Move
New Folder
New Data Source
Report Builder
Folder Settings
Upload File
Tile View
Type
Name
Description
Last Run
Modified Date
Modified By
Final 1 - Facility Summary 4/29/2014 2:30 PM CEERD-CF-F\d-Mino
Final 2 - System Summary 4/29/2014 2:30 PM CEERD-CF-F\d-Mino
Final 3 - Component Details 4/29/2014 2:30 PM CEERD-CF-F\d-Mino
Final 4 - Equipment Details 4/29/2014 2:30 PM CEERD-CF-F\d-Mino
Final 5 - Inspection Summary 4/29/2014 2:30 PM CEERD-CF-F\d-Mino
Final 6 - Distress Details 4/29/2014 2:30 PM CEERD-CF-F\d-Mino
Final 7 - Work Action Summary 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
Final 8 - Work Action Detail 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
Final 9 - Facility System Quick View 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
QC 1 - Facility Report 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
QC 2 - System Report 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
QC 3 - Component Report 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
QC 4 - Component-Section Report 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
QC 5 - Section Details Report 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
QC 6 - Inspection Report 4/29/2014 2:31 PM CEERD-CF-F\d-Mino
QC 7A - REInspectionReport 9/4/2014 3:51 PM SMS\vds
QC 7B - REInspectionReport FLAT 9/4/2014 3:51 PM SMS\vds
QC 8 - FCI Summary Report 7/1/2015 9:24 AM SMS\vds


http://smsreports/Reports/Pages/Import.aspx?ItemPath=%2fCustom+Re
Upload File - Report Mana...
Home > Custom Reports > USMC > Reports > Site
Home | My Subscriptions | Site Settings | Help
BUILDER Custom Report Services
Upload File
Search
Upload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc), or other resource into Site.
File to upload:
Browse...
Name:
New Item
Overwrite item if it exists
OK
Cancel


http://smsreports/Reports/Pages/Folder.aspx?ItemPath=%2fCustom+Re
Site - Report Manager
Home > Custom Reports > USMC > Reports
Home | My Subscriptions | Site Settin
BUILDER Custom Report Services
Site
Search
Delete
Move
New Folder
New Data Source
Report Builder
Folder Settings
Upload File
Type
Name
Description
Last Run
Modified Date
Modified By
Final 1 - Facility Summary
Final 2 - System Summary
Final 3 - Component Details
Final 4 - Equipment Details
Final 5 - Inspection Summary
Final 6 - Distress Details
Final 7 - Work Action Summary
Final 8 - Work Action Detail
Final 9 - Facility System Quick V
QC 1 - Facility Report
QC 2 - System Report
QC 3 - Component Report
QC 4 - Component-Section Report
QC 5 - Section Details Report
QC 6 - Inspection Report
QC 7A - REInspectionReport
QC 7B - REInspectionReport FLAT
QC 8 - FCI Summary Report
4/29/2014 2:30 PM CEERD-CF
4/29/2014 2:31 PM CEERD-CF
9/4/2014 3:51 PM SMS\vds
7/1/2015 9:24 AM SMS\vds
Move
Delete
Subscribe...
Create Linked Report...
View Report History
Security
Manage
Download...
Edit in Report Builder


http://smsreports/Reports/Pages/Report.aspx?ItemPath=%2fCustom+Re
Final 1 - Facility Summary -...
Home > Custom Reports > USMC > Reports > Site
Home | My Subscriptions | Site Settings | Help
BUILDER Custom Report Services
Final 1 - Facility Summary
Search
Delete
Move
Create Linked Report
Download
Replace
Properties
Parameters
Data Sources
Subscriptions
Processing Options
Cache Refresh Options
Report History
Snapshot Options
Security
Modified Date: 4/29/2014 2:30 PM
Modified By: CEERD-CF-F\d-Mino
Creation Date: 4/29/2014 2:30 PM
Created By: CEERD-CF-F\d-Mino
Size: 111 KB
Properties
Name: Final 1 - Facility Summary
Description:
Hide in tile view
Apply
Create a linked report when you want to use different security or parameters with the report.


http://smsreports/Reports/Pages/Report.aspx?ItemPath=%2fCustom+Re
Final 1 - Facility Summary -...
Home > Custom Reports > USMC > Reports > Site
Home | My Subscriptions | Site Settings | Help
BUILDER Custom Report Services
Final 1 - Facility Summary
Search
Properties
Parameters
Data Sources
Subscriptions
Processing Options
Cache Refresh Options
Report History
Snapshot Options
Security
USMC_Inv
A shared data source
/Custom Reports/USMC/USMC Production
Browse
A custom data source
Data source type:
Microsoft SQL Server
Connection string:
Connect using:
Credentials supplied by the user running the report
Display the following text to prompt user for a user name and password:
Type or enter a user name and password to access the data source
Use as Windows credentials when connecting to the data source
Credentials stored securely in the report server
User name:
Password:
Use as Windows credentials when connecting to the data source
Impersonate the authenticated user after a connection has been made to the data source
Windows integrated security
Credentials are not required
Test Connection
Apply

Part III

Operational Administration

Chapter 9

Application Settings

As an administrator in the application (BUILDER), you will have a variety of permissions and settings that are not available to normal users. Here we will take a look at these. To access the Application Settings, select **Tools**, followed by **Administration**, and then **Application Settings** (*See Figure 9.1*). Here we will have seven different tabs with different settings or editable material in each one.

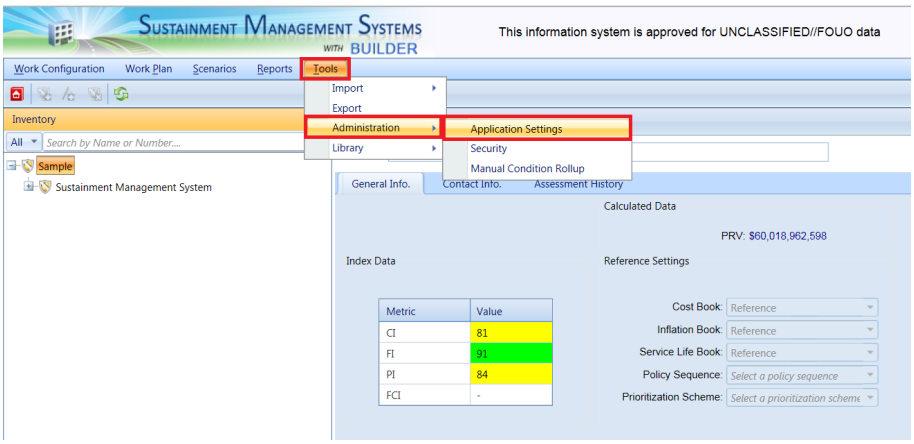


Figure 9.1: Application Settings

9.1 Settings Tab

Refer to Figure 9.2 for the Settings tab options described below.

9.1.1 User Category

Here is where you as Administrator will select the User Category for the application. For this example we have used Air Force. The settings allow this to limit the amount of data available to be shown to the users. This will personalize the application data and make it faster, as there will be options available for some agencies that are not needed for others. Once this is selected, the only choice that is available afterwards is the one selected, or all.

9.1.2 User's Default Unit of Measure

This is where you pick the default unit of measure for the application. You can choose either **English** or **Metric**.

Figure 9.2: Settings Tab

9.1.3 Fiscal Year Start Date

When running simulations for Long Term Planning, the fiscal start date determines when items are estimated to be completed, and when new work items will evaluated.

9.1.4 Critical Work Items

When this check box is selected, sections containing distresses marked as critical will have work items created, even if the CSCI is above the standard assigned to that section.

9.2 Systems Tab

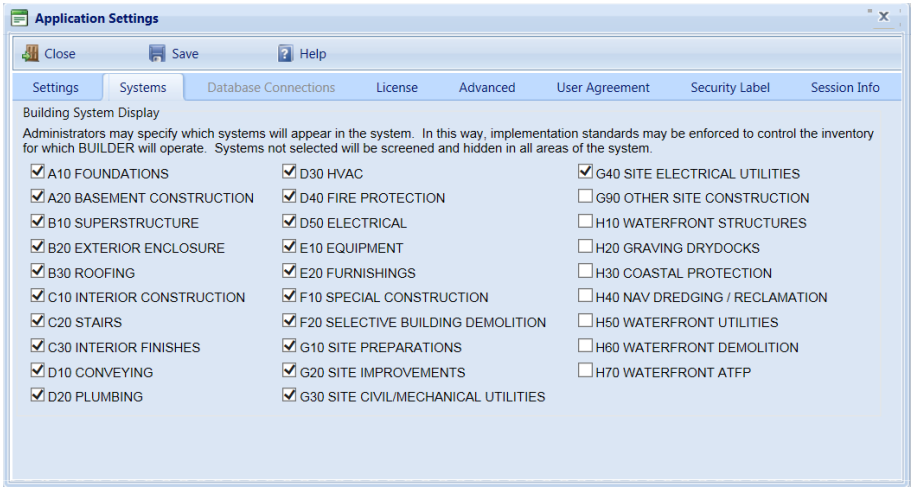


Figure 9.3: Systems Tab

At the Systems tab (*See Figure 9.3*), Administrators may specify which systems will appear in the system. In this way, implementation standards may be enforced to control the inventory for which BUILDER will operate. Systems not selected will be hidden and not made available in the system selection.

9.3 License Tab

The Engineered Management Systems use an encrypted license to determine which applications you have access to; as well as to enforce licensing on the quantity of inventory you are managing. This license information will be supplied to you by your support agent.

9.4 Advanced Tab

Refer to Figure 9.4 for the Advanced tab options described below.

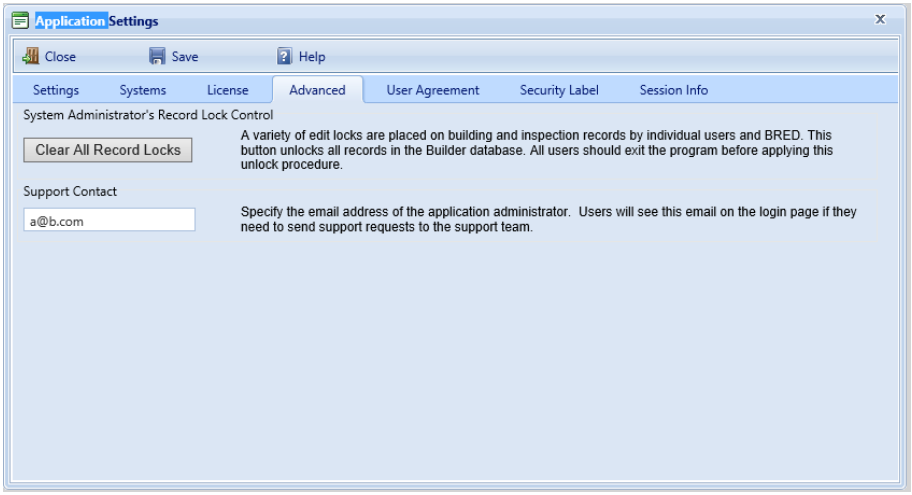


Figure 9.4: Advanced Tab

9.4.1 System Administrators Record Lock Control

A variety of edit locks are placed on building and inspection records, both by individual users and by the the BRED application itself. This button unlocks all records in the BUILDER database.

> ***Important:*** *All users should exit the program before applying this unlock procedure.*

9.4.2 Support Contact

Specify the email address of the application administrator. Users will see this email on the login page if they need to send support requests to the support team.

9.5 User Agreement

As an administrator you may define text that will be displayed to a user before the user is allowed to login to the application. The user will be required to click a button labeled **I Agree** before the login options are displayed. If you do not define this text, users will be taken directly to the login options.

9.6 Security Label Tab

At the Security Label tab (*See Figure 9.5*), the Administrator can enter text that will be presented to the user about security. After editing the statement, click **Save** to have the text displayed.

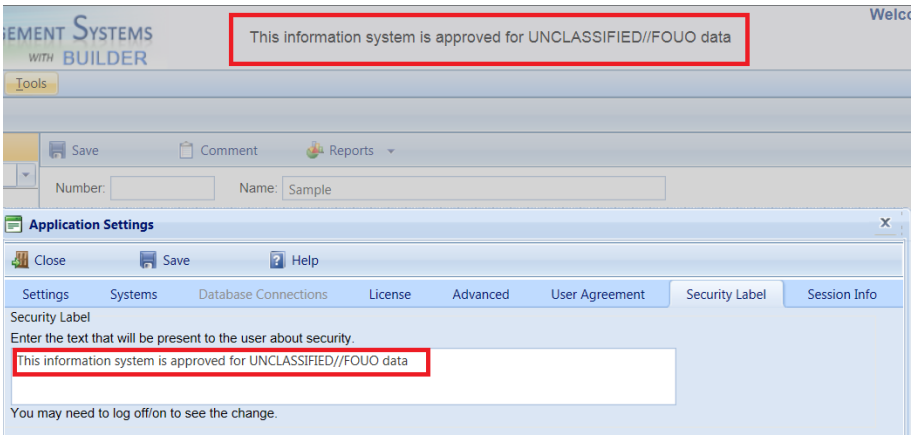


Figure 9.5: Security Tab

9.7 Session Info Tab

This tab will let you know the current number of Sessions, number of users, and if there are any long Running Processes. There is a refresh button there to refresh the information if needed.

Chapter 10

Application Security

10.1 Password Policy

This will give the administrator the ability to set criteria for passwords.

10.1.1 Bad Logins

This option determines how many times a user can try to login to their account with an incorrect password before their account is locked.

10.1.2 History

This option sets the number of previous passwords that cannot be used. For example, if 10 is used, then a user resetting their password cannot use any of the previous 10 passwords used.

10.1.3 Maximum Age

This option sets the amount of time that a user has before they must use another password. Once this limit has been reached, a user will be presented with a change password dialogue that will let the user change his or her password.

10.1.4 Maximum and Minimum Length

These options set the minimum and maximum length requirements for passwords.

10.2 Managing Users, Rights, and Roles

10.2.1 User Accounts

This is where an administrator will manage users' accounts and add the users to the correct Role and Organization.

10.2.1.1 Add User Account

To add a user, click the **Add** button in the Security toolbar. (See Figure 10.1) From here you will add the information for the user including first name, last name, username (login name), and the password. At this screen you can also specify the Unit of Measure as either English or Metric, as well as specifying whether the user must login with their CAC card. After entering in the information, click **Save**, and then close to save the user. (See Figure 10.2)

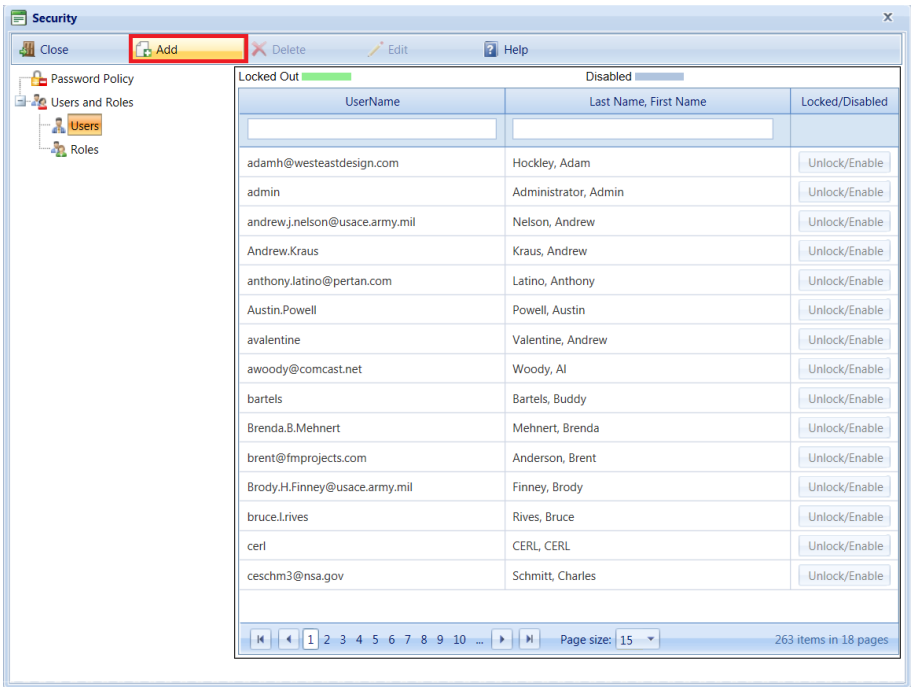


Figure 10.1: Add User Account

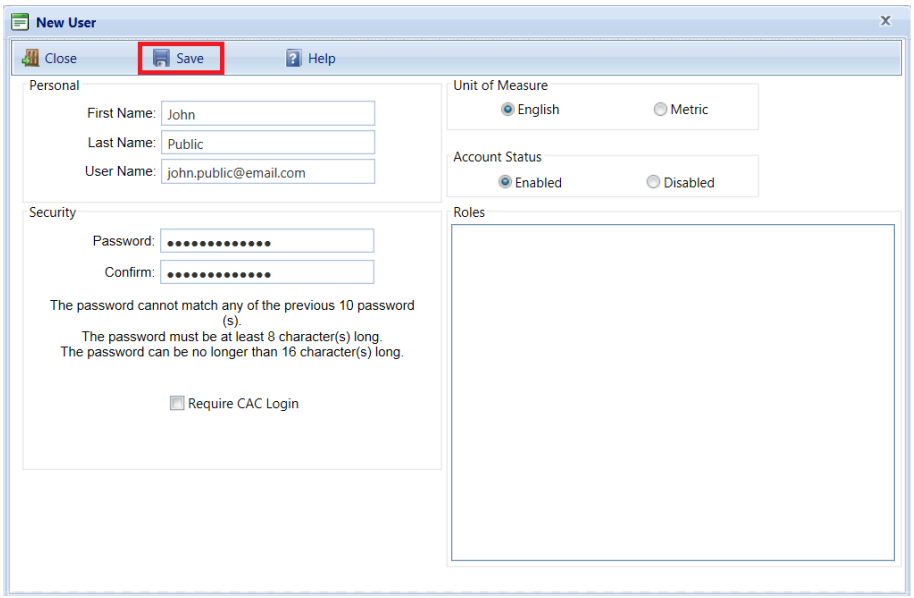


Figure 10.2: Save User Account

10.2.1.2 Delete User Account

To delete an account, you can search for the account you need to delete with our user search feature. You can search by username, by first name, or by last name. (See Figure 10.3) After finding the user that you want to delete, simply highlight the user, and then click **Delete** in the toolbar. You will see a dialogue box that asks if you are sure that you want to delete the user. If yes, click **yes** and the user will be deleted.

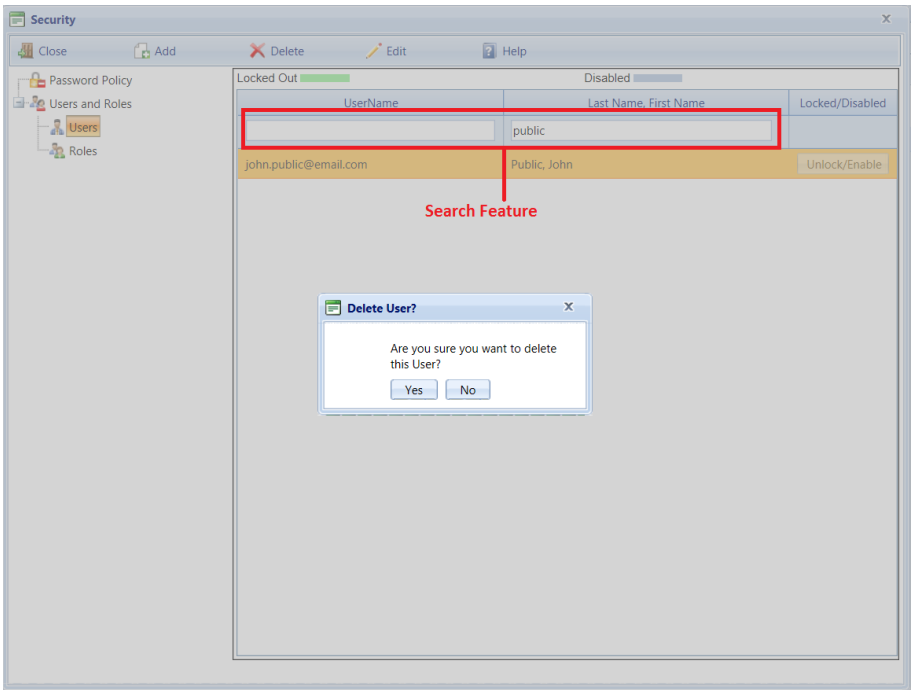


Figure 10.3: Delete User Account

WARNING: *It is recommended to* disable *users that are not needed, instead of deleting them. This will ensure that any assessment records tied to the user being deleted are not affected.*

10.2.1.3 Edit User Account

To edit an account, simply search for the account in the search bar, and then click **Edit** on the toolbar. From here you can edit any of the data related to the users account. After editing any of the data, you must click **Save** before **Close**, to save the data you have edited.

10.2.1.4 Disable User Account

Disabling an account is done in the Edit options. When in edit, there is an Account Status section with two options, Enabled and Disabled. To disable an account, just select **Disabled** then **Save**, and then **Close**.

10.2.1.5 Locked User Account

An account will get locked after a user has entered their password 3 times incorrectly (according to default settings, but this can be changed by an Administrator). When a user's account is locked, they will be notified that their account is disabled and that they must contact an Administrator. (*See Figure 10.4*) In the Administrator view, a locked account will be highlighted green if it has been locked. (*See Figure 10.5*). To unlock an account, select the account. Click **Edit**, and then **Enabled** in the Account Status selection. After that is completed, click **Save**, and then Close.

10.2.2 Roles

This is where an Administrator will add the users that have been created to the Roles needed to accomplish their goals. Varying levels of permissions are available, with the most common being:

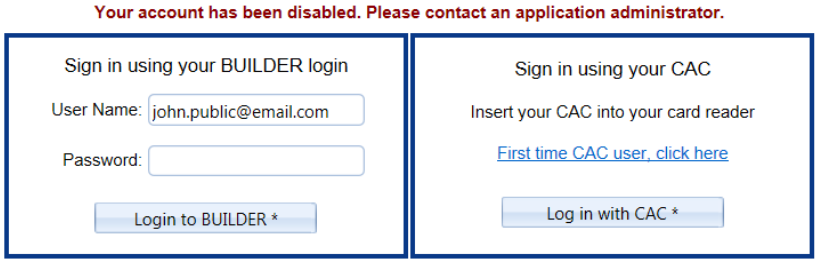


Figure 10.4: Locked User Account

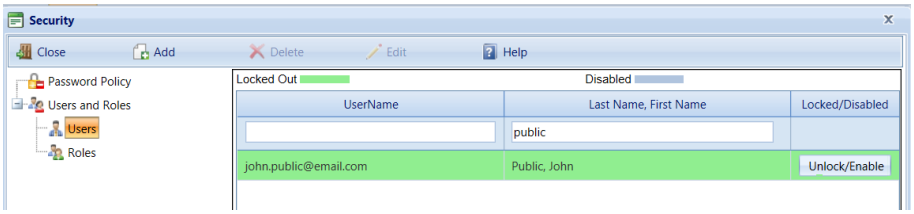


Figure 10.5: Locked Disabled User Account

10.2.2.1 Inspection Supervisor

This Role is often assigned to the Assessor in the field. Being assigned to this Role adds the user to the list of users selectable in the BUILDER Remote Entry Database (BRED) application. Users assigned the Inspection Supervisor role can perform their job duties in the field under their own user account using the BRED application.

10.2.2.2 Work Planner (Data Manager)

Also called Data Manager, this Role is often assigned to the person editing information done by the Inspection Supervisor in the field. The Work Planner is able to view and edit all data within an Organization; add Facilities and Complexes; create and edit Work Plans; and generate multi-year Scenarios.

10.2.2.3 Master Planner

This Role has no restrictions on what the user can edit, create or delete within the application.

> ***Note:*** *This is the highest privilege level and should be assigned sparingly.*

For more information on user Roles, please refer to the SMS support site and search for either **Roles** or **roles** (the search feature is not case-sensitive). The site is located at `https://support.sms.erdc.dren.mil`

10.2.2.4 Assigning Roles

Now that we have some idea as to what the available Roles are and what they are used for, we will look at assigning users to these Roles. The steps taken to assign the Role is the same for all.

1. Under **Tools** and then **Administration**, open the **Security** Feature. Select **Roles** in the left pane as shown. (*See Figure 10.6*) From there, navigate the tree until you find the Organization or Site that you want to assign the user to.

   > ***Note:*** *When an Organization has multiple Sites under it, a user can be assigned at the Organizational level and have access to all Sites under that Organization at the Role level assigned. If a user is assigned a lesser Role at a Site under the Organization, the Role that is higher is the one*

that is assigned. For example, if a user is assigned as a Data Manager at the Organizational level, but assigned as an Inspector Supervisor at a Site under that Organization, then the user will have Data Manager privileges at that site. If the user is assigned as a Data Manager at Organizational level, and as a Master Planner at the Site level, then the user will have Data Manager privileges throughout the Organization except for the Site, where they are assigned as a Master Planner.

2. Select the Role you want to assign the user to. Then click **Edit** in the toolbar. The **Edit Group** popup window will appear.

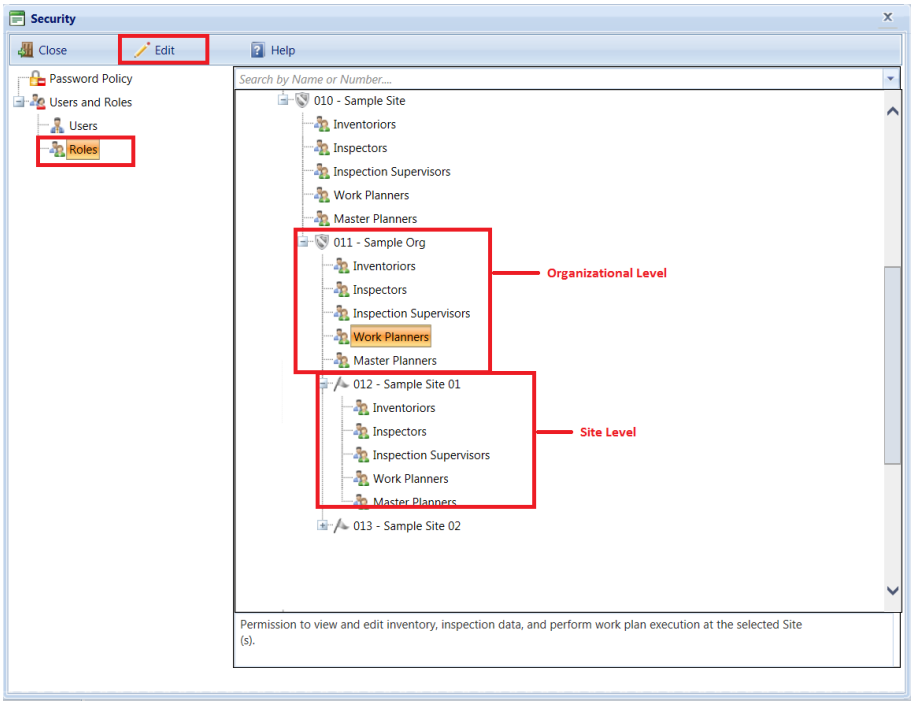


Figure 10.6: User Roles

3. In the left panel of the **Edit Group** popup, select the user to be assigned to a Role, then click the right arrow between the two panels to move the user to the right panel. (See Figure 10.7) After the user is moved, then click **Save** to save the changes you have made. Click **Close** when finished.

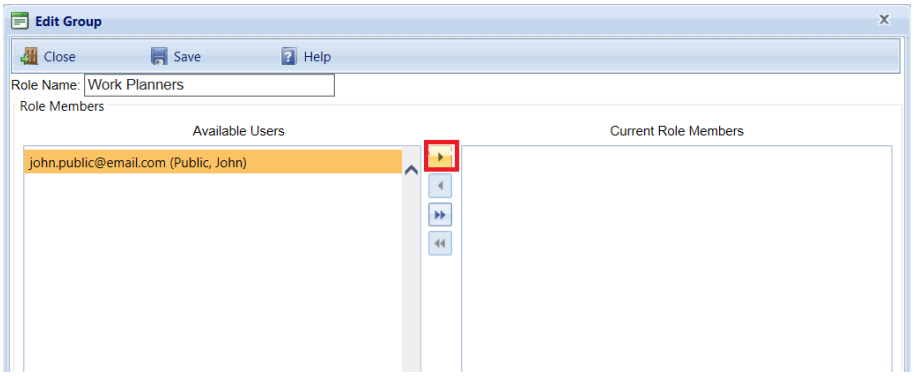


Figure 10.7: User Groups

In addition to assigning Roles to users at Organizations and Sites, an Administrator can also limit a user's account to Read-Only, or elevate a user to an Administrator Role. You do this in the same way that you assign users to Roles within Organizations and Sites.

10.2.3 User-Created Locks

Users can create locks on records for the purpose of editing information. This is accomplished through exporting the Facility or Systems to a BRED file. When these locks are created, they lock the Facility to prevent further editing to the Facility or System so that two people cannot edit the same information at the same time.

Administrators have the ability to unlock these locked Facilities. They can do so in two different ways: One is by using **System Administrators Record Lock Control** under Application Settings, described earlier on page 59. The second way is through the User Preferences dialog. The User Preferences dialog is located in the upper right corner of the application. Here users can change their passwords, change Unit of Measure, clear their own locks, or register their CAC card.

The difference between a user clearing locks and an Administrator clearing locks is that when an Administrator clears locks, it is for the entire application. This can lead to multiple users having the ability to edit the same information at the same time. If a user has an issue and needs a Facility or System unlocked, there is a report available to determine who has locked the Facility or System. It is always best to contact the user who originally locked the System or Facility and determine if they can unlock it themselves. If something has happened to the BRED file and they cannot unlock the Facility or System by importing that file, instruct them on how to unlock the Facility or System by using the user Preferences dialog.

Part IV

Appendixes

Appendix A

User Roles Appendix

A.1 Available User Roles

A.1.1 Read-only

Users assigned to the Read-Only role can export both Standard and Custom reports, but can *not* download a BRED file (see the **Inspector Supervisor** role below).

A.1.2 Inspection Supervisor

Also referred to as Assessor, this Role is often assigned to the assessor in the field. Being assigned to this Role adds the user to the list of users selectable in the BUILDER Remote Entry Database (BRED) application. He or she can import and export BRED data files at the BUILDER web application.

Users assigned the Inspection Supervisor role can perform their job duties in the field under their own user account using the BRED application. They have permission to view and edit *their own* inventory and inspection data.

A.1.3 Work Planner (Data Manager)

Also called Data Manager, this Role is often assigned to the person editing information done by the Inspection Supervisor in the field. Work Planners are able to view and edit all data within an Organization; add Facilities and Complexes; create and edit Work Plans; and generate multi-year Scenarios. They have permission to view and edit inventory and inspection data for their *entire assigned installation*.

A.1.4 Master Planner

This Role has no restrictions on what the user can edit, create or delete within the application.

> ***Note:*** *This is the highest privilege level and should be assigned sparingly.*

In addition to unrestricted ability to create and data within the program, the Master Planner has the potential to powerfully influence the effectiveness of SMS implementation by assigning such things as standards, policies, prioritization schemes, and RSL (remaining service life) and cost books.

A.2 Additional Resources

For more information on user Roles, please refer to the SMS site and search for either **Roles** or **roles** (the search feature is not case-sensitive). The site is located at `https://support.sms.edrc.dren.mil`.

Appendix B

Configuration Appendix

B.1 Configuration Table Options

B.1.1 AutoCreateCritical

Default Value: True
Configurable in Application Settings: Yes

B.1.2 Branch

Configures the DoD service branch.
Configurable in Application Settings: Yes

B.1.3 DefaultMetric

Default Value: True
Configurable in Application Settings: Yes

B.1.4 FiscalStartDate

Fiscal year start date.
Configurable in Application Settings: Yes

B.1.5 LookupDatabase

Default Value: Lookup
Configurable in Application Settings: No

B.1.6 ScenarioMaxYears

Sets the maximum years defined in a scenario.
Default Value: 10
Configurable in Application Settings: No

B.1.7 UseUniformat

Rescinded. This should always be 1. All Lookup databases use Uniformat.
Default Value: 1
Configurable in Application Settings: No

B.1.8 UseBREDEnergyForm

Rescinded. Legacy BRED 3.0 setting.
Default Value: True
Configurable in Application Settings: No

B.1.9 UseBREDMCForm

Rescinded. Legacy BRED 3.0 setting.
Default Value: True
Configurable in Application Settings: No

B.1.10 UseBREDADAForm

Rescinded. Legacy BRED 3.0 setting.
Default Value: True
Configurable in Application Settings: No

B.1.11 UseBREDSeismicForm

Rescinded. Legacy BRED 3.0 setting.
Default Value: True
Configurable in Application Settings: No

B.1.12 AvailableSystems

Comma delimited list of available systems.
Configurable in Application Settings: Yes

B.1.13 BuildingFolderSize

Maximum facilities to expand in the navigation tree view
Default Value: 10000
Configurable in Application Settings: No

B.1.14 HasImpProcs

Should always be True. Are Impact stored procedures located in the database?
Default Value: True
Configurable in Application Settings: No

B.1.15 LoginAgreement

The text displayed in the user agreement
Configurable in Application Settings: Yes

B.1.16 SmartCardName

If this column is not NULL, smart cards will be enabled.
Default Value: NULL
Configurable in Application Settings: No

B.1.17 SupportEmail

Email address of the administrator of the application.
Default Value: NULL
Configurable in Application Settings: Yes

B.1.18 SecureInfo

The text displayed in the security banner.
Default Value: NULL
Configurable in Application Settings: Yes

B.1.19 ZipBredFile

Compress BRED file?
Default Value: False
Configurable in Application Settings: No

B.1.20 BREDImport_NullChk

Validate NULL data during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.21 BREDImport_TypeChk

Validate data types during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.22 BREDImport_NameChk

Validate name data during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.23 BREDImport_YearChk

Validate year data during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.24 BREDImport_CharsCk

Validate character data during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.25 BREDImport_DateChk

Validate date data during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.26 BREDImportSqlInjCk

Validate SQL injection code during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.27 BREDImportClWdthCk

Validate column width during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.28 BREDImportGuidCk

Validate GUID data during BRED import?
Default Value: True
Configurable in Application Settings: No

B.1.29 BREDImportCMCsCk

Validate CMC data during BRED import?
Default Value: False
Configurable in Application Settings: No

B.1.30 InspWindowInDays

Number of days between valid inspections.
Default Value: 30
Configurable in Application Settings: No

B.1.31 UseRemoteCstmRpts

Use SQL Server Reporting Services on a remote server.
Default Value: True
Configurable in Application Settings: No

B.1.32 CstmRptSvrURI

URI of Report Server.
Default Value: http://localhost/ReportServer
Configurable in Application Settings: No

B.1.33 CstmRptSvrRoot

Root folder of the reports on the SSRS report server.
Default Value: /Custom Reports
Configurable in Application Settings: No

B.1.34 BredLkpUri

URI of BRED lookup database.
Default Value: http://sms.cecer.army.mil/bred/lookups
Configurable in Application Settings: No

B.1.35 BredLkpVersion

Version of the BRED Lookup database. Value depends on BRED Version.
Value: 3.110.1510.822
Configurable in Application Settings: No

B.1.36 License

The installed license.
Value: (License Hash)
Configurable in Application Settings: No

B.1.37 RSAVersion

Use RSA authentication. If this column is not NULL, RSA will be enabled.
Default Value: NULL
Configurable in Application Settings: No

Appendix C

System Configuration Worksheet

Note that values for these variables may have already been entered into the Appendix of the *Sustainment Management System™ Installation Guide*

Variable	*Description*	*Value*
<ADMIN_NAME>	System administrator user name	For basic installation this will always be "Administrator"
<ADMIN_PASSWORD>	System administrator password	
<DEFAULT_WEBSITE>	Default web domain for the SMS application	By default, this is "Default Web Site"
<LICENSEE>	Licensee alias as issued by the SMS vendor	
<POOL_IDENTITY>	Domain or Local user that the application will run-as	
<SQL_AUTH_USERNAME>	SQL Authentication user name	
<SQL_SERVER_NAME>	Name of the SQL server	
<SSRS_NAME>	Name of the server where SSRS is installed	
<VERSION_NUMBER>	SMS version number being installed	
<WEB_APP_NAME>	Name of the web application that the SMS is installed into	
<WEB_APP_ROOT>	The path to the web application root directory*	

*The path to the web application root directory will be the concatenation of three items, connected by two single backslashes:

1. Where the inetpub directory is (followed by a backslash)
2. The value of <DEFAULT_WEBSITE> (followed by a backslash)
3. The value of <WEB_APP_NAME>

Appendix D

SMS PowerShell Command Reference

D.1 Information

D.1.1 Get-SMSApplication [-Name <String>] [-Site <String>]

This command returns SMS application objects that describe the configuration and versions of the application and database.

1. To return *all* SMS application objects for *all* sites, type `Get-SMSApplication` with no parameters.
2. To return *one* object for *all* sites, include the **[-Name** <**String**>**]** parameter and *omit* the **[-Site** <**String**>**]** parameter. Type either:
   - `Get-SMSApplication -Name <String>` *or*
   - `Get-SMSApplication <String>`

   where <String> represents the name of the SMS application.
3. To return *all* SMS application objects for *one* site, *omit* the **[-Name** <**String**>**]** parameter and include the **[-Site** <**String**>**]** parameter by typing:
   - `Get-SMSApplication -Site <String>`

   where <String> is the designation of the desired site.
4. To return *one* object for *one* site, add both parameters in this order: **[-Name** <**String**>**]** followed by **[-Site** <**String**>**]**. You can do this in either explicit or abbreviated form by typing one of the following:
   - `Get-SMSApplication -Name <String> -Site <String>` *or*
   - `Get-SMSApplication <String> <String>`

   where the first <String> represents the name of the SMS application, and the second <String> is the designation of the desired site.

D.1.1.1 [-Name <String>]

Optional: Specifies which SMS application object. If omitted, the default is all SMS application objects. If both **[-Name]** and **[-Site]** are omitted, all SMS application objects for all sites will be returned.

D.1.1.2 [-Site <String>]

Optional: Designates the site for which the SMS application object(s) will be returned. If omitted, the default is all sites. If both **[-Name]** and **[-Site]** are omitted, all SMS application objects for all sites will be returned.

Note: *This may be abbreviated to <String> only if the* ***-Name*** *parameter has been included before it.*

D.1.2 Get-SMSApplicationState [-Name <String>] [-Site <String>] [-verbose]

This command returns the state of or more SMS applications. The state will be either Starting, Started, Stopping, or Stopped. The state is returned as an object; if you need to use it as a string, type (for example)
`$myStateString = (Get-SMSApplicationState usaf).value`

D.1.2.1 [-Name <String>]

Optional: Specifies the SMS application to return the state of. If omitted, the default is all SMS applications. If both **[-Name]** and **[-Site]** are omitted, the state of all SMS applications for all sites will be returned; in this case, using the **[-verbose]** parameter is highly recommended.

D.1.2.2 [-Site <String>]

Optional: Designates the site for which the state of the SMS application(s) will be returned. If omitted, the default is all sites. If both **[-Name]** and **[-Site]** are omitted, the state of all SMS applications on all sites will be returned; in this case, using the **[-verbose]** parameter is highly recommended.

> ***Note:*** *This may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

D.1.2.3 [-verbose]

Optional: Although optional, this parameter is *recommended* when querying the state of more than one site or more than one SMS application. A greater amount of detail is provided in that the states of all sites and all applications are broken out separately.

> ***Note****: Using the **[-verbose]** parameter also results in the value of the object returned being longer and more complex.*

D.2 Control

D.2.1 Start-SMSApplication [-Name <String>] [-Site <String>]

This command starts one or more SMS applications. Parameters are described below.

D.2.1.1 [-Name <String>]

Optional: Specifies the SMS application to be started. If omitted, the default is all SMS applications. If both **[-Name]** and **[-Site]** are omitted, all SMS applications for all sites will be started.

D.2.1.2 [-Site <String>]

Optional: Designates the site where the SMS application(s) will be started. If omitted, the default is all sites. If both **[-Name]** and **[-Site]** are omitted, all SMS applications for all sites will be started.

Note: *This may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

D.2.2 Stop-SMSApplication [-Name <String>] [-Site <String>]

This command stops one or more SMS applications. The application state will change to "Stopping" and then "Stopped." Parameters are described below.

D.2.2.1 [-Name <String>]

Optional: Specifies the SMS application to be stopped. If omitted, the default is all SMS applications. If both **[-Name]** and **[-Site]** parameters are omitted, all SMS applications on all sites will be stopped.

D.2.2.2 [-Site <String>]

Optional: Designates the site where the SMS application(s) will be stopped. If omitted, the default is all sites. If both the **[-Name]** and **[-Site]** are omitted, all SMS applications on all sites will be stopped.

Note: *This may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

D.2.3 Restart-SMSApplication [-Name <String>] [-Site <String>]

This command restarts one or more SMS applications. Parameters are described below.

D.2.3.1 [-Name <String>]

Optional: Specifies which SMS application to restart. If omitted, the default is all SMS applications. If both **[-Name]** and **[-Site]** are omitted, all SMS applications on all sites will be restarted.

D.2.3.2 [-Site <String>]

Optional: Designates the site where the SMS application(s) will be restarted. If omitted, the default is all sites. If both **[-Name]** and **[-Site]** are omitted, all SMS applications on all sites will be restarted.

Note: *This may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

D.3 Product Installation and Removal

D.3.1 Set-SMSDatabaseNames

This command sets the Inventory database name for the remainder of the current session. It allows you to either A. specify a prefix to prepend to the default database name, or B. enter the name for the Inventory database.

A. To attach a prefix, use this parameter:

D.3.1.1 -DatabasePrefix <String>

Type `-databasePrefix` and enter the prefix to be prepended to the default database name.

B. Alternatively, to enter name for the Inventory database, use the parameter below:

D.3.1.2 -InventoryDatabaseName <String>

Type `-InventoryDatabaseName` and enter the desired name for the Inventory database.

To see optional parameters for the **Set-SMSDatabaseNames** command, visit Get-Help Set-SMSDatabaseNames.

D.3.2 Export-SMSDatabaseScripts (Using Windows Authentication)

Export-SMSDatabaseScripts -DatabaseServer <String> -winAuthentication [-SourcePath <String>]

This command creates the customer-specific database scripts and files that accomplish bulk loading of data. It creates two scripts: (1) a SQL script to create your databases with all tables, views and stored procedures; and (2) a batch file to bulk load all required data. The most common parameters are listed under the headers below; visit Get-Help Export-SMSDatabaseScripts to see additional optional parameters.

The following SQL Server tools are required:

1. SQL Server Management Studio
2. SQL Server BCP, the bulk copy commandline utility.

Also, unless you have SQL Server tools installed on your webserver, you will need to copy the custom scripts and the data files to your database server after the `Export-SMSDatabaseScripts` command finishes and before continuing with `Install-SMSApplication`. The default location for these scripts is the **%ProgramFiles%\ERDC-CERL\SMS\Database\Create Scripts** folder.

D.3.2.1 -DatabaseServer <String>

REQUIRED: Specifies the name of the database server. This will be the value of <SQL_SERVER_NAME>.

D.3.2.2 -winAuthentication

REQUIRED: If you are using Windows authentication, use the **-winAuthentication** parameter.

D.3.2.3 [-SourcePath <String>]

Optional: Specifies the full path where the scripts are located. If omitted, the default path is the **%ProgramFiles%\ERDC-CERL\SMS\Database\Create Scripts** folder.

Visit Get-Help Export-SMSDatabaseScripts to see additional optional parameters for this command.

D.3.3 Install-SMSApplication (using Windows Authentication)

Install-SMSApplication -Site <String> -Name <String> -DatabaseServer <String> -ApplicationPoolUser <String> -winAuthentication

This command installs an SMS application to the IIS Server as a web application. The required parameters are listed below; refer to the System Configuration Worksheet (Appendix C on page 77) for values to be entered.

Important: Before running this script, please ensure that:

1. A web site exists, such as "Default Web Site". It can be named differently, but you must know the name of the site this application should install to;
2. The Application Pool user exists and you know the password;
3. If using Windows Authentication to your database, you are logged-in as a user with permissions to connect to the SMS application's database;
4. Your database has already been created AND data has been bulk copied. If not, please refer to the **Export-SMSDatabaseScripts (Using Windows Authentication)** command on page 82. Depending on your environment, you may need to run the resulting scripts on your database server.

D.3.3.1 -Site <String>

REQUIRED: Designates the site where the SMS application will be installed. Type `-Site` and enter the value of <DEFAULT_WEBSITE> from the System Configuration Worksheet. Alternatively, just enter the value of <DEFAULT_WEBSITE>.

D.3.3.2 -Name <String>

REQUIRED: Specifies which SMS application is to be installed. Type `-Name` and enter the value of <WEB_APP_NAME> from the System Configuration Worksheet. Alternatively, just enter the value of <WEB_APP_NAME>.

D.3.3.3 -DatabaseServer <String>

REQUIRED: This is the same as the **-databaseServer** parameter used with `Export-SMSDatabaseScripts`. Type `-databaseServer` and enter the value of <SQL_SERVER_NAME> from the System Configuration Worksheet.

D.3.3.4 -ApplicationPoolUser <Value>

Type `-ApplicationPoolUser` and enter the value of <POOL_IDENTITY> from the System Configuration Worksheet. When prompted, enter the associated password.

D.3.3.5 -winAuthentication

REQUIRED: Type `-winAuthentication` if you are using Windows Authentication for your database.

Visit Get-Help Install-SMSApplication to see optional parameters for this command.

D.3.4 Export-SMSDatabaseScripts (Using SQL Authentication)

Export-SMSDatabaseScripts -DatabaseServer <String> -sqlAuthentication -DatabaseUser <String> [-SourcePath <String>]

This command creates the customer-specific database scripts and files that accomplish bulk loading of data. It creates two scripts: (1) a SQL script to create your databases with all tables, views and stored procedures; and (2) a batch file to bulk load all required data. The most common parameters are listed under the headers below; visit Get-Help Export-SMSDatabaseScripts to see additional optional parameters.

The following SQL Server tools are required:

1. SQL Server Management Studio
2. SQL Server BCP, the bulk copy commandline utility.

Also, unless you have SQL Server tools installed on your webserver, you will need to copy the custom scripts and the data files to your database server after the `Export-SMSDatabaseScripts` command finishes and before continuing with `Install-SMSApplication`. The default location for these scripts is the **%ProgramFiles%\ERDC-CERL\SMS\Database\Create Scripts** folder.

D.3.4.1 -DatabaseServer <String>

REQUIRED: Specifies the name of the database server. This will be <SQL_SERVER_NAME>.

D.3.4.2 -sqlAuthentication

REQUIRED: If you are using SQL authentication, use the **-sqlAuthentication** parameter. You will also need the **-DatabaseUser** parameter as described in the following subsection.

D.3.4.3 -DatabaseUser <String>

REQUIRED: This value is required only when SQL Authentication is being used. Type `-databaseUser` and enter the SQL Authentication username. (In the System Configuration Worksheet, this is the value for <SQL_AUTH_USERNAME>.) You will be prompted for the SQL Authentication password for the database user. The password parameter must be entered when prompted and cannot be supplied at the command line.

D.3.4.4 [-SourcePath <String>]

Optional: Specifies the full path where the scripts are located. If omitted, the default is the **%ProgramFiles%\ERDC-CERL\SMS\Database\Create Scripts** folder.

Visit Get-Help Export-SMSDatabaseScripts to see additional optional parameters for this command.

D.3.5 Install-SMSApplication (using SQL Authentication)

Install-SMSApplication -Site <String> -Name <String> -DatabaseServer <String> -ApplicationPoolUser <String> -sqlAuthentication -DatabaseUser <String>

This command installs an SMS application to the IIS Server as a web application. The required parameters are listed below; refer to the System Configuration Worksheet (Appendix C) for values to be entered.

Important: Before running this script, please ensure that:

1. A website exists, such as "Default Web Site". It can be named differently, but you must know the name of the site this application should install to;

2. The Application Pool (AppPool) user exists and you know the password;
3. If using SQL Authentication to your database, you know the username and password of the user that will connect to the database on behalf of the SMS application, because you will be prompted for this information;
4. Your database has already been created AND data has been bulk copied. If not, please refer to the **Export-SMSDatabaseScripts (Using SQL Authentication)** command on page 83. Depending on your environment, you may need to run the resulting scripts on your database server.

D.3.5.1 -Site <Value>

REQUIRED: Designates the site for installing the SMS application. Type `-Site` and enter <DEFAULT_WEBSITE> from the System Configuration Worksheet. Alternatively, just enter <DEFAULT_WEBSITE>.

D.3.5.2 -Name <Value>

REQUIRED: Specifies which SMS application is to be installed. Type `-Name` and enter <WEB_APP_NAME> from the System Configuration Worksheet. Alternatively, just enter <WEB_APP_NAME>.

D.3.5.3 -DatabaseServer <Value>

REQUIRED: Type `-DatabaseServer` and enter the value of <SQL_SERVER_NAME> from the System Configuration Worksheet.

D.3.5.4 -ApplicationPoolUser <Value>

REQUIRED: Type `-ApplicationPoolUser` and enter the value of <POOL_IDENTITY> from the System Configuration Worksheet. When prompted, enter the associated password.

D.3.5.5 -sqlAuthentication

REQUIRED: Type `-sqlAuthentication` if you are using SQL Authentication for your database.

D.3.5.6 -DatabaseUser <String>

REQUIRED: This value is required only when SQL Authentication is being used. Type `-DatabaseUser` and enter the SQL Authentication username. (In the System Configuration Worksheet, this is the value for <SQL_AUTH_USERNAME>.) When prompted, enter the associated password.

Visit Get-Help Install-SMSApplication to see optional parameters for this command.

D.3.6 Remove-SMSApplication -Name <String> -Site <String>

This command removes one or more SMS applications from the IIS Server. The required parameters are:

D.3.6.1 -Name <String>

REQUIRED: Specifies the SMS application to be removed.

D.3.6.2 -Site <String>

REQUIRED: Designates the site from which the SMS application(s) will be removed.

Visit Get-Help Remove-SMSApplication for description of optional parameters for this command.

D.4 Administration

D.4.1 Backup-SMSApplication -BackupPath <String> [-Name <String>] [-Site <String>]

The SMS PowerShell module includes a backup utility that archives the application, configuration, and user files. It does *not* backup the databases; this will need to be configured and scheduled with a SQL Server Management Studio maintenance plan or with a third party backup application.

D.4.1.1 -BackupPath <String>

REQUIRED: Designates the path and filename that the archive will be stored to. This string should be enclosed in quotation marks if there are spaces in the path. The filename should have the .zip extension appended.

D.4.1.2 [-Name <String>]

Optional: Specifies the SMS application to be backed up. If omitted, the default is all SMS applications. If both the **[-Name]** and **[-Site]** parameters are omitted, all SMS applications for all sites will be backed up.

D.4.1.3 [-Site <String>]

Optional: Designates the site for which the SMS application(s) will be backed up. If omitted, the default is all sites. If both the **[-Name]** and **[-Site]** parameters are omitted, all SMS applications on all sites will be backed up.

> ***Note:*** *This parameter may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

Update-SMSApplication [-Name <String>] [-Site <String> [-BackupPath <String>] [-All] [-NoBackup] [-NoDatabaseUpdate]

This command updates one or more SMS applications. By default this command will backup the application, configuration, and user files to the **C:\Temp** directory.

D.4.1.4 [-Name] <String>

Optional: Specifies the SMS application to be updated. The **[-All]** switch may be used instead.

D.4.1.5 [-Site <String>]

Optional: Designates the site on which the SMS application(s) will be updated.

> ***Note:*** *This parameter may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

D.4.1.6 [-BackupPath <String>]

Optional: Designates the path that the backup archive will be stored to. The <String>should be enclosed in quotation marks if there are spaces in the path. The default path is **C:\Temp**.

D.4.1.7 [-All]

Optional: Update all SMS applications.

Unlike many other commands, omitting **[-Name]** <**String**>**]** and **[[-Site]** <**String**> will *not* perform the command on all SMS applications by default.

D.4.1.8 [-NoBackup]

Optional: Forces an update without backing up files.

D.4.1.9 [-NoDatabaseUpdate]

Optional: Forces an update without upgrading the database. Database upgrade must then be added manually (*see section 7.5.3*).

D.4.2 Set-SMSMessage -Message <String> [-Name <String>] [-Site <String>]

This command displays a message on one or more SMS application login pages. If neither the **[-Name]** nor **[-Site]** parameter is specified, the default is the login page of all SMS applications in all sites.

D.4.2.1 -Message <String>

REQUIRED: The first <String> you provide is the message string. This needs to be a "quoted" string (enclosed in quotation marks).

D.4.2.2 [-Name <String>]

Optional: Specifies which SMS application. If omitted, the default is all SMS applications. If both the **[-Name]** and **[-Site]** parameters are omitted, the message will be displayed on the login page of all SMS applications on all sites.

D.4.2.3 [-Site <String>]

Optional: The <String> following the **[-Site]** parameter is the name of the designated site. If the **[-Site]** parameter is omitted, the default is all sites. If both the **[-Name]** and **[-Site]** parameters are omitted, the message will be displayed on the login page of all SMS applications on all sites.

> ***Note:*** *This parameter may be abbreviated to <String> only if the **[-Name]** parameter has been included before it.*

D.4.3 Reset-SMSMessage [-Name <String>] [-Site <String>]

This command removes the message from one or more SMS application login pages. If neither the **[-Name]** nor **[-Site]** parameter is specified, it removes any messages from the login page of all SMS applications in all sites.

D.4.3.1 [-Name<String>]

Optional: Specifies which SMS application. If omitted, the default is all SMS applications. If both the **[-Name]** and **[-Site]** parameters are omitted, all messages will be removed from the login pages of all SMS applications on all sites.

D.4.3.2 [-Site <String>]

Optional: The <String> following the **[-Site]** parameter is the name of the designated site. If this parameter is omitted, the default is all sites. If both the **[-Name]** and **[-Site]** parameters are omitted, all messages will be removed from the login pages of all SMS applications on all sites.

Note: *This parameter may be abbreviated to <String> only if the* ***[-Name]*** *parameter has been included before it.*

D.4.4 Set-SMSAdministratorPassword -Name <String> [-Site <String>]

This command sets the SMS Administrator password for one or more SMS applications. You will be prompted to enter the administrator password; if this was entered in the Configuration Worksheet, it will be the value of <ADMIN_PASSWORD>. The parameters for this command are described below.

D.4.4.1 -Name <String>

REQUIRED: Specifies which SMS application.

D.4.4.2 [-Site <String>]

Optional: Designates the site on which the SMS Administrator password will be set for the applicable SMS application. If omitted, the default is all sites.