**********

webMethods
CentraSite (v9.6)
for Windows
and UNIX Platforms

Post-Installation README File

This file contains important information you must read before using CentraSite. You can find additional information about CentraSite in the documentation area of Empower (https://empower.softwareag.com), Software AG's global extranet.

April 15th, 2014

**********

Table of Contents
=================

**********

# 1 Readme and Last Minute Information

The content of this readme file represents the state of the software to the best knowledge of all involved at the time when the final distribution was built.

Any further changes to the content of this file are available at https://empower.softwareag.com/.

** IMPORTANT: Software AG strongly recommends that you install the latest fix of your currently installed product version before you install the new product version. **

Please note that some of the entries of this readme file do not apply to the CentraSite Community Edition. For more information on the features available with the CentraSite, see the online documentation section "Introducing CentraSite" > "CentraSite Editions".

For release information concerning the security package distributed with CentraSite, see the Software AG Security Infrastructure readme file available from the Software AG Installer or from https://empower.softwareag.com/.

In the following descriptions of the known issues, the term <SuiteInstallDir> indicates the root directory for all products in the webMethods suite, and "<CentraSiteInstallDir>" indicates the installation directory of the CentraSite.

# 2 Known Issues for CentraSite

## 2.1 Installation and Configuration Issues

### 2.1.1 Upgrade procedure does not update custom SSL client configurations

If you perform an upgrade from CentraSite version 9.0 or version 9.5 to version 9.6, the upgrade does not automatically upgrade your custom SSL configurations for communication between clients and the CentraSite Registry Repository. As a result, some of your existing CentraSite 9.0 or 9.5 custom configurations might not be valid for CentraSite 9.6.

Therefore, you need to adjust your custom SSL configurations after upgrading to CentraSite 9.6. Please check the online documentation section "Basic Operations" > "Configuring Secure Communication between CentraSite Components" for the description of how to set up SSL configurations from clients to the CentraSite Registry Repository.

### 2.1.2 Installing CentraSite 9.6 with older webMethods products throws a java.lang.UnsupportedClassVersionError exception

If you install CentraSite 9.6 on webMethods Product Suite 8.2 SP2, for example, Software AG Designer 8.2 SP2 and Integration

Server 8.2 SP2, and try to establish a connection with Designer and Integration Server, both the Designer and Integration Server throw a java.lang.UnsupportedClassVersionError exception. This situation occurs because the older webMethods products (that is, Designer 8.2 SP2 and Integration Server 8.2 SP2) are still using the older version of Java 6.

Note that webMethods Product Suite 8.2 SP2 products are now certified to use Java 7. You can download the Java 7 from Software AG Update Manager.

This issue is resolved with a workaround, as follows:

Modify the Software AG Designer configuration

1. Shut down Software AG Designer 8.2 SP2.
2. Locate the following file in your Software AG Designer installation:
   <SuiteInstallDir>\eclipse\v36\eclipse.ini
3. Open the file in a text editor.
4. Locate the -vm parameter.
5. In a new line below the parameter, add the following:
   <SuiteInstallDir>/jvm/jvm/jre/bin/javaw.exe
6. Save the file and restart Software AG Designer.

Modify the webMethods Integration Server configuration

1. Shut down webMethods Integration Server 8.2 SP2.
2. Locate the following file in your Software AG Designer installation:
   <SuiteInstallDir>\eclipse\v36\eclipse.ini
3. Go to the <IntegrationServer_directory>\bin directory and open the setenv.bat or setenv.sh file in a text editor.
4. Edit the JAVA_DIR parameter to point to the JDK7 directory. For example:
   SET JAVA_DIR=<SuiteInstallDir>\jvm\jvm\jre
5. Save the file and restart Software AG Designer.

(INM-17009)

## 2.2 CentraSite Control

### 2.2.1 IE11 Browser: CentraSite Control not displaying correctly

When accessing CentraSite Control using Microsoft Internet Explorer version 11 and attempting to change the screen orientation (right-to-left), the UI is not displayed correctly. This issue occurs because the right-to-left (RTL) screen orientation does not work correctly if Microsoft Internet Explorer version 11 is in Quirks mode. This is an

issue with Microsoft Internet Explorer version 11 in Quirks mode.

There is currently no workaround for this issue.

This issue applies only when using Internet Explorer 11 with CentraSite Control. If you use an earlier version of the Internet Explorer, the issue does not occur.

(NJX-1334)

## 2.3 CentraSite Business UI

### 2.3.1 Restricted availability of roles "API Runtime Provider" and "API Publisher" for Organization Administrator

The roles "API Runtime Provider" and "API Publisher" are required to perform virtualization or publishing of APIs. Currently, these roles are not implicitly assigned to a user with the "Organization Administrator" role. The Renew and Revoke icons for API keys in the "Consumers" popup of the API details page are also not displayed for that user.

In the absence of these roles, a user with the "Organization Administrator" role cannot virtualize or publish APIs.

A user with the "Organization Administrator" role must explicitly be assigned with the "API Runtime Provider" and "API Publisher" roles to virtualize and/or publish APIs.

(INM-17051)

### 2.3.2 Email notifications sent to users contain the ${user.displayname} token and not the recipient's name

When the approval workflow system sends email notifications that uses the predefined email templates, the body of the email shows the ${user.displayname} token.

To substitute the ${user.displayname} token correctly, specify the user's First Name and Last Name in the User Preferences page. For more information about these settings, see the online documentation section "Administering the CentraSite Business UI" > "Working with the Business User Interface" > "Setting User Preferences".

(INM-17125)

### 2.3.3 Extension points in the Business UI are not working correctly

Business UI extensions may not display correctly.

This issue is resolved with a workaround as follows:

1. Open the MANIFEST.MF file in a text editor. This file is located in the <CentraSiteInstallDir>\cast\cswebapps\BusinessUI\META-INF directory.
2. Under the section Bundle-ClassPath, append the relative path of the following JAR files available in the WEB-INF/lib folder, as a comma-separated list.
   CentraSiteBUIExtension.jar
   CentraSiteBUIExtensionCore.jar
   For example,
   WEB-INF/lib/CentraSiteBUIExtension.jar,WEB-INF/lib/CentraSiteBUI
   BUIExtensionCore.jar

   Note: If you have created custom extensions, make sure you include the associated jar files in the META-INF folder.
3. Add the extension's associated Java archives to the <CentraSiteInstallDir>\cast\cswebapps\BusinessUI\META-INF directory.
4. Save your modifications.
5. Delete files under <SuiteInstallDir>\profiles\CTP\configuration\org.eclipse.osgi folder.

6. Restart the Software AG Runtime.

(INM-17218)

## 2.4 Asset Handling

### 2.4.1 Potential conflicts between predefined profiles and user-defined profiles

In the user interface, the sequence number plays a vital role in the profile display order and the instance level profile permission. In general, the sequence numbers assigned to the predefined profiles and computed profiles are odd numbers, and even numbers are assigned to the user-defined profiles. But, some predefined profiles are designated with an even sequence number. When a user creates a new profile, consider the system assigns an even sequence number that matches with one of the predefined profiles. When the user sets the profile-level permissions for the new profile, the same permissions are also assigned to the predefined profile that has the same even sequence number within the asset type. As a result, the user might get permissions to more profiles than intended.

The following list shows some of the predefined profiles that

has an even sequence number.

- Identification

- Summary

- Technical Details

- Default

- Details

- Specification

- Support

There is currently no workaround for this issue. However, Software AG strongly recommends that you create a new profile and delete the conflicting user-defined profile within the asset type.

(INM-16782)

## 2.5 Import/Export Issues

### 2.5.1 Importing older versions of predefined asset types no longer allowed

Importing predefined asset types is no longer possible if the asset type is exported from a CentraSite installation prior to 9.6. For example, a predefined asset type from version 8.2 cannot be imported to CentraSite 9.6.

You can, however, import asset instances of older versions if the predefined asset type definition in the export archive matches with the existing asset type definition in the version 9.6 registry.

(INM-17023)

## 2.6 API Management

### 2.6.1 Configuring the API consumption settings after clearing the Require Approval checkbox renders an empty Subject line in the email notification

When configuring the API consumption settings, after you select the Require Approval checkbox, CentraSite automatically populates the Key Generation Settings panel and the Key Renewal Settings panel with three rows. Each row displays the

predefined email subject and template as configured for the individual approval actions (Approved, Rejected, and Approval Request) in the centrasite.xml file. If you delete the rows that pertains to Approved actions from the Key Generation Settings and Key Renewal Settings, clear the Require Approval checkbox, and then do a Configure again, the email Subject fields for Key Generation Settings and Key Renewal Settings is empty.

This issue is resolved with a workaround, as follows: specify the email Subject fields for the Key Generation Settings and Key Renewal Settings manually. For more information about these settings, see the online documentation section "API Management Solutions" > "Configuring an API for Consumption".

(INM-17129)

### 2.6.2 Invalid Access URI displayed in Consumer Overview profile

The Consumer Overview profile of an API contains an invalid Access URI value. This is because a resource name is missing in the Access URI.

This issue is resolved with a workaround as follows: append "/" followed by the resource name to construct the absolute URI.

(INM-17110)

### 2.6.3 Native API is exposed to consumers

If you mark the checkbox "Expose to Consumers" when you publish your (proxy) API, the instance-level View permission (which is assigned to the Everyone group in the API) is also automatically propagated to the native API.

This issue is resolved with a workaround as follows:

1. In CentraSite Control, display the policy list: Policies > Design/Change Time
2. Enable the "Show Predefined Policies" option.
3. Locate the "Set API Publish Permissions" policy.
4. In the Policy Information panel, click "Change State". (If you do not see the Change State button, it is probably because you do not have permission to change the lifecycle state of a policy.)
5. In the Change Lifecycle Stage dialog box, select the "Suspended" state (to deactivate it temporarily), then click OK.
6. Click the "Permissions" action.
7. Check the "Propagate permissions to dependent objects" radio button.

8. Click "Save" to save the updated policy.
9. Activate the policy by changing its lifecycle state to the "Productive" state.

(INM-16625)

### 2.6.4 Unable to renew expired API keys in CentraSite

In CentraSite, it is not possible to renew an API key that has expired. Therefore, it is necessary to renew the API key before it expires.

To work around this issue, request a new key for consuming the API whose key has expired. You will also need to update the applications of that particular API to use the new API key.

(INM-17284)

## 2.7 Runtime Security Authentication Handling

### 2.7.1 NTLM Transparent Mode with Kerberos Authentication Support

When a virtual service is configured for NTLM authentication scheme in transparent mode, Mediator will behave in "pass by" mode, allowing an NTLM handshake to occur between the client and server. This kind of NTLM handshake becomes unreliable on certain circumstances.

Mediator now supports Kerberos handshake in Transparent mode. If you choose to use the NTLM Transparent mode with Kerberos authentication, set the value of the watt.pg.disableNtlmAuthHandler property to "true" in the extended settings for the Integration Server. For information about the watt.pg.disableNtlmAuthHandler property, see the document Administering webMethods Mediator (version 9.6). For more information about working with extended configuration settings, see the document webMethods Integration Server Administrator's Guide.

(INM-17243)

## 2.8 Pluggable UI

### 2.8.1 PluggableUIRegistryProvider moved to a new package

Any implementation that uses the PluggableUIRegistryProvider class will receive an exception:

Java.lang.ClassNotFoundException:

com.softwareag.centrasite.appl.framework.util.PluggableUIRegistryProv
ider.

Ensure that any implementation that uses the
PluggableUIRegistryProvider class is referencing it from the
PluggableUIRegistryProvider.jar. Also note that the package
has been changed from
"com.softwareag.centrasite.appl.framework.util" to
"com.softwareag.centrasite.appl.framework.util.pui".

(INM-16612)

## 2.9 Platform Issues

### 2.9.1 Platform Manager does not support overinstall

If you have CentraSite, Platform Manager 9.5 and Platform
Manager Plug-ins installed, and you upgrade CentraSite from
version 9.5 to version 9.6 using the overinstall method (as
opposed to the side-by-side method), it can happen that the
overinstall might corrupt your CentraSite installation. This
is because Platform Manager does not support overinstallation.

** Important: Software AG strongly recommends that you
uninstall the Platform Manager 9.5 and Platform Manager
Plug-ins of your currently installed CentraSite version 9.5
before you overinstall the new CentraSite version 9.6. And,
when you upgrade CentraSite to 9.6 using the overinstall, make
sure you select all the three CentraSite components:
CentraSite, Platform Manager 9.6 and Platform Manager Plug-ins
in the Software AG Installer, if you would like to continue
with the Platform Manager. Because if you try later to install
the Platform Manager 9.6 and the Platform Manager Plug-ins on
the overinstalled CentraSite, it might again corrupt the
installation. For complete information about using the
overinstallation procedure to upgrade from CentraSite 9.5 to
9.6, see the online documentation section "Upgrading from a
Previous Version" > "Upgrading CentraSite 9.5 to 9.6 Using
Overinstall".

# 3 Deprecation Notices

## 3.1 Local OS Authentication

Because of architectural changes in the security
infrastructure the local operating system authentication
mechanism is set to deprecated and will be removed in future

releases.

Software AG recommends using the LDAP or "Internal" authentication (set by default) instead.

(RGHINM-13362)

### 3.2 Active Directory Authentication other than LDAP

Because of architectural changes in the security infrastructure only LDAP authentication with Microsoft Active Directory is supported.

(RGHINM-13362)

### 3.3 CentraSite WebDAV API

The CentraSite WebDAV API is set to deprecated and should no longer be used. It will be removed in future releases. The WebDAV API-specific Javadoc has already been removed in this version from the online documentation.

(RGHINM-13261)

### 3.4 CentraSite Extensions for XQJ API

The support of CentraSite Extensions for XQJ API is set to deprecated and will be removed in future releases.

(RGHINM-13261)

### 3.5 CentraSite Control API

The CentraSite Control API is set to deprecated and will be removed in future releases.

(RGHINM-13261)

### 3.6 Restriction for ESB Types in Type Management page

The following ESB (Enterprise Service Bus) types that appear in the Type Management page of CentraSite Control should no longer be used:

- ESB Document

- ESB Document Field

- ESB Document Type

- ESB Folder

- ESB Package

- ESB Service

- ESB Specification

- ESB WS Descriptor

- ESB WS Operation

# 4 Documentation Addenda and Errata

## 4.1 Setting up Secure Communication and Tomcat Ports

The section "Configuring Secure Communication between CentraSite Components" in the product documentation is no longer strictly correct. Please use the following procedures instead.

### 4.1.1 Secure Communication

Software AG recommends that you not make changes to the webapp configuration files because they could be overwritten by hotfixes and upgrades.

Instead, use the command line tool "CentraSiteCommand" with the option "set SSL RR" or "set SSL AST", as in the following description:

We advise you to run the "set SSL RR" command before "set SSL AST". The commands attempt to check that the new configurations have been successfully applied. If the reconfiguration fails the original configuration is reinstated. The original configuration files are archived to <SuiteInstallDir>/CentraSite/cfg/archive. You can use the same input configuration file for the "set SSL AST" and "set SSL RR" commands.

set SSL RR
==========

```
    -url: CentraSite URL using https
    -user: User to log in to CentraSite
    -password: Password to log in to CentraSite
```

-file: Configuration file containing the security properties

The following properties need to be supplied in .xml format:

com.softwareag.centrasite.security.keyStore
com.softwareag.centrasite.security.keyStorePassword
com.softwareag.centrasite.security.keyStoreType

com.softwareag.centrasite.security.trustStore
com.softwareag.centrasite.security.trustStorePassword
com.softwareag.centrasite.security.trustStoreType

com.softwareag.centrasite.security.crr.trustStore
com.softwareag.centrasite.security.crr.certificate
com.softwareag.centrasite.security.crr.keyFile
com.softwareag.centrasite.security.crr.storePassword

Example
-------

CentraSiteCommand set SSL RR
-url https://localhost:53313/CentraSite/CentraSite
-user AdminUser -password AdminPwd
-file C:\SoftwareAG\CentraSite\utilities\RR-config.xml

RR-config.xml
-------------

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="com.softwareag.centrasite.security.keyStore">C:/SoftwareAG/CentraSite/test/files/certs/castcert.p12</entry>
<entry key="com.softwareag.centrasite.security.keyStorePassword">cscert</entry>
<entry key="com.softwareag.centrasite.security.keyStoreType">PKCS12</entry>
<entry key="com.softwareag.centrasite.security.trustStore">C:/SoftwareAG/CentraSite/test/files/certs/casttrust.p12</entry>
<entry key="com.softwareag.centrasite.security.trustStorePassword">cscert</entry>
<entry key="com.softwareag.centrasite.security.trustStoreType">PKCS12</entry>
<entry key="com.softwareag.centrasite.security.crr.trustStore">C:/SoftwareAG/CentraSite/test/files/certs/crrtrust.pem</entry>
<entry key="com.softwareag.centrasite.security.crr.certificate">C:/SoftwareAG/CentraSite/test/files/certs/crrcert.crt</entry>
<entry key="com.softwareag.centrasite.security.crr.keyFile">C:/SoftwareAG/CentraSite/test/files/certs/crr.key</entry>
<entry key="com.softwareag.centrasite.security.crr.storePassword">cscert</entry>
</properties>
```

set SSL AST
===========

-url: CentraSite URL using https
-user: User to log in to CentraSite
-password: Password to log in to CentraSite
-file: Configuration file containing the security properties

Note that the Software AG Runtime must be shut down before
this command is run, and can be restarted after the command
has been executed.

The following properties need to be supplied in .xml format:

com.softwareag.centrasite.security.keyStore
com.softwareag.centrasite.security.keyStorePassword
com.softwareag.centrasite.security.keyStoreType

com.softwareag.centrasite.security.trustStore
com.softwareag.centrasite.security.trustStorePassword
com.softwareag.centrasite.security.trustStoreType

Example
-------

[shut down Software AG Runtime]

CentraSiteCommand set SSL AST
    -url https://localhost:53313/CentraSite/CentraSite
    -user AdminUser -password AdminPwd
    -file C:\SoftwareAG\CentraSite\utilities\AST-config.xml

[start Software AG Runtime]

AST-config.xml
--------------

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="com.softwareag.centrasite.security.keyStore">C:/SoftwareAG/CentraSite/test/files/certs/castcert.p12</entry>
<entry key="com.softwareag.centrasite.security.keyStorePassword">cscert</entry>
<entry key="com.softwareag.centrasite.security.keyStoreType">PKCS12</entry>
<entry key="com.softwareag.centrasite.security.trustStore">C:/SoftwareAG/CentraSite/test/files/certs/casttrust.p12</entry>
<entry key="com.softwareag.centrasite.security.trustStorePassword">cscert</entry>
<entry key="com.softwareag.centrasite.security.trustStoreType">PKCS12</entry>
</properties>
```

### 4.1.2 Tomcat ports

The Tomcat ports also need to be propagated to the CentraSite webapps. This is done in the following manner:

1. Set the ports in the configuration file
   <SuiteInstallDir>/CentraSite/cfg/cast-config.xml.
2. Stop the Software AG Runtime.
3. Run the command
   <SuiteInstallDir>/CentraSite/bin/cfg/OverInstallAfterCopy
   as follows:
   OverInstallAfterCopy -ast -fromVersion 9.5.1.0.nnn
   Example:
   OverInstallAfterCopy -ast -fromVersion 9.5.1.0.524
4. Start the Software AG Runtime.

Note that you can determine the correct 9.5.1.0.nnn value by examining the install log file <SuiteInstallDir>/install/logs/installLog.txt. Search for the

string "newINMJVersion"; this will be a value such as 9.5.1.0.524. Use this value as the -fromVersion parameter.

Note also that the Software AG Runtime has to be stopped before you run the OverInstallAfterCopy command. The file name of the OverInstallAfterCopy command ends with ".cmd" or ".sh", depending on the host operating system.

(INM-15376)

## 4.2 Problems when Starting the Documentation's Java-Based Search/Navigation

If you encounter security warnings when starting the documentation's search/navigation applet (security warning) try changing to a previous version of Java in the Java Runtime Environment Settings (Control Panel > Java Control Panel > Java > View).

Note: This workaround only applies to the documentation's search/navigation applet.

## 4.3 Viewing Software AG Product Documentation under Windows

Current operating systems of Microsoft Windows incorporate a range of specific security features that restrict active content that runs locally on the user's computer.

Active content includes ActiveX controls, Java applets and JavaScript.

Software AG's documentation web pages contain JavaScript, and the SEARCH, INDEX and CONTENTS features are implemented as Java applets. As a result, when viewing documentation web pages that reside on the user's PC, users of Internet Explorer and Mozilla Firefox are informed that active content is blocked.

The user must explicitly and repeatedly allow active content if he or she wants to make use of the documentation's full navigation features.

Note that this behavior is only observed when reading web pages installed locally on the user's PC, i.e. on a local hard disk or CD-ROM drive.

The active content for which Software AG is responsible, that is, the JavaScript code in our HTML documentation pages, will not harm the user's computer. The risk in using the navigation applets is negligible: Software AG has received no reports

from users concerning any harm caused to a computer by the applets. We therefore suggest that when reading Software AG documentation in a local context, the user allow active content via the Security settings in the browser (with Internet Explorer, usually found under Tools > Internet Options > Advanced).

Full details of alternatives can be found on the home page of the supplier of the navigation applets: http://www.phdcc.com/xpsp2.htm

# 5 Legal Notices

## 5.1 Source Code of Third Party Software

Certain third party products require that the source code must be made available. In case of any particular request please contact your software supplier.

# 6 Miscellaneous

## 6.1 Diagnostic Tools

For inspecting or testing the underlying structures of the internal databases of CentraSite, a set of diagnostic tools can be obtained using the Software AG Installer by selecting the entry "Tamino Server 9.5 > XTools 9.SP1".

INM-RM-96-20140415