Oracle® Fusion Middleware

Release Notes for Oracle Web Cache

11g Release 1 (11.1.1)

E64094-01

June 2015

This document describes issues and release-specific user information associated with Oracle Web Cache. It includes the following topics:

1 Oracle Web Tier—Statement of Direction

The Oracle Web Cache product has been deprecated. The *Administrator's Guide for Oracle Web Cache* dates from the 11.1.1.7 release. For more information on the current (11.1.1.9) release of Oracle Web Cache, see *Oracle Web Tier - Statement of Direction (Doc ID 1576588.1)* available at the following URL:

`https://support.oracle.com`

2 New Security Protocols and Ciphers

The 11.1.1.9 release of Oracle Web Cache adds support for the TLSv1.1 and TSLv1.2 security protocols.

3 Enabling TLS Security Protocols

The current release of Oracle Web Cache adds support for the TLSv1.1 and TLSv1.2 security protocols. The security protocol used by Oracle Web Cache is indicated by the value of the SSLENABLED parameter of the LISTEN directive in the webcache.xml file.

The default value of the SSLENABLED parameter is `SSL` (this is because the `SSL` value included the SSLv2 and SSLv3 protocols in past releases). In the 11.1.1.9 release, the `SSL` value indicates that the security protocols TLSv1.0, TLSv1.1, and TLSv1.2, will be used.

To set different protocols or combinations of protocols, you must manually edit the webcache.xml file. There is no GUI support for the new protocols.

The following table describes the value you must set for the SSLENABLED parameter to enable various protocols or protocol combinations.

To enable these security protocols...	Set this value for the SSLENABLED attribute...
TLS1.1	`TLSV1_1`
TLS1.2	`TLSV1_2`
TLS1.0 and TLS1.1	`TLSV1V1_1`
TLS1.0 and TLS1.2	`TLSV1V1_2`
TLS1.1 and TLS1.2	`TLSV1_1V1_2`
TLS1.0, TLS1.1 and TLS1.2	`TLSV1V1_1V1_2`

4 Ciphers Supported by the STRONG_CRYPTO_ONLY Parameter

The STRONG_CRYPTO_ONLY parameter of the LISTEN directive is used to restrict the use of weak and anonymous ciphers by Oracle Web Cache. If this parameter is set to YES (the default), then Oracle Web Cache will use only strong ciphers. Following is the list of ciphers that are used:

- `SSL_RSA_WITH_RC4_128_SHA`
- `SSL_RSA_WITH_AES_128_CBC_SHA`
- `SSL_RSA_WITH_AES_256_CBC_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

If the STRONG_CRYPTO_ONLY parameter is set to NO, then Oracle Web Cache will include the following ciphers in addition to the ones listed above.

> **Note:** The NO setting might be important in upgrade scenarios. The Patch Set installer (or the 10*g* Upgrade Assistant) does not perform any reconfiguration. You should check to ensure that the STRONG_CRYPTO_ONLY parameter is set to the new optimal YES setting.

- `SSL_RSA_WITH_3DES_EDE_CBC_SHA`

- SSL_RSA_WITH_RC4_128_MD5
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5

5 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds. It includes the following topics:

5.1 Using Oracle Web Cache with Oracle Portal, Forms, Reports, and Discoverer

Oracle Web Cache cannot be updated to 11.1.1.9 in a Portal, Forms, Reports, and Discoverer (PFRD) home. Also, you cannot install Oracle Web Cache separately, because PFRD is not certified with any 11.1.1.9 products.

5.2 Running Oracle Web Cache Processes as a Different User Is Not Supported

Running Oracle Web Cache as a user other than the installed user through the use of the `webcache_setuser.sh setidentity` command is not supported.

Specifically, you *cannot* change the user ID with the following sequence:

1. Change the process identity of the Oracle Web Cache processes in the Process Identity page using Oracle Web Cache Manager (**Properties** > **Process Identity**).
2. Use the `webcache_setuser.sh` script as follows to change file and directory ownership:

   ```
   webcache_setuser.sh setidentity user_ID
   ```

   user_ID is the user you specified in the **User ID** field of the Process Identity page.
3. Restart Oracle Web Cache using `opmnctl`.

   Oracle Web Cache will start and then immediately shut down.

   In addition, messages similar to the following are displayed in the event log:

   ```
   [2009-06-02T21:22:46+00:00] [webcache] [ERROR:1] [WXE-13212] [logging] [ecid: ]
   Access log file
   /scratch/webtier/home/instances/instance1/diagnostics/logs/WebCache/webcache1/a
   ccess_log could not be opened.
   [2009-06-02T21:22:46+00:00] [webcache] [WARNING:1] [WXE-13310] [io] [ecid: ]
   Problem opening file
   /scratch/webtier/home/instances/instance1/config/WebCache/webcache1/webcache.pi
   d (Access Denied).
   [2009-06-02T21:22:46+00:00] [webcache] [ERROR:1] [WXE-11985] [esi] [ecid: ]
   Oracle Web Cache is unable to obtain the size of the default ESI fragment page
   /scratch/webtier/home/instances/instance1/config/WebCache/webcache1/files/esi_
   ```

```
fragment_error.txt.
[2009-06-02T21:22:46+00:00] [webcache] [WARNING:1] [WXE-11905] [security]
[ecid: ] SSL additional information: The system could not open the specified
file.
```

For more information about the `webcache_setuser.sh` script, see "Running webcached with Root Privilege" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Web Cache*.

5.3 SSLENABLED Values and Limitations on the Administration Server

The default value of the SSLENABLED parameter, `SSL`, configures the Web Cache administration server to listen with combination of the TLSv1.0, TLSv1.1, and TLSv1.2 security protocols.

However, the SSLENABLED values introduced in the current release (`TLSV1_1`, `TLSV_1_2`, `TLSV1V1_1`, `TLSV1V1_2`, `TLSV1_1V1_2`, and `TLSV1V1_1V1_2`) cannot be used by the administration server.

To workaround this issue, either use the `SSL` value or do not start the Web Cache Administration component to use the features it provides.

For more information, see "New for 11.1.1.9 only" in *How to Configure Oracle Web Cache 11g to Use a Specific SSL Protocol (Doc ID 1263526.1)* at the following URL:

`https://support.oracle.com/`

6 Documentation Errata

This section provides clarifications for errors in Oracle Web Cache documentation. It includes the following topics:

- Section 6.1, "Procedure to Enable Generation of Core Dump"
- Section 6.2, "Clarification About Support for CRLs"
- Section 6.3, "Clarifications About Configuring the CRL Location"

6.1 Procedure to Enable Generation of Core Dump

Information about enabling generation of core dump is not available in the *Oracle Fusion Middleware Administrator's Guide for Oracle Web Cache*.

To enable generation of a core dump when Oracle Web Cache is shut down, add `CORE="YES"` to the `TRACEDUMP` element in the `$INSTANCE_HOME/config/WebCache/`*`webcache_name`*`/webcache.xml` file.

The updated `TRACEDUMP` element would look like the following:

```
<TRACEDUMP FILENAME=file_name CORE="YES"/>
```

The core dump file with the specified name is created in the `$INSTANCE_HOME/config/WebCache/`*`webcache_name`* directory.

6.2 Clarification About Support for CRLs

Section 5.1.1.2.2, "Certificate" of the *Oracle Fusion Middleware Administrator's Guide for Oracle Web Cache* states the following:

"Although the Oracle HTTP Server supports OpenSSL certificate revocation lists, Oracle Web Cache does not."

This statement is incorrect. Oracle Web Cache *does* support CRLs.

6.3 Clarifications About Configuring the CRL Location

Section 5.5.3, "Configuring Certificate Revocation Lists (CRLs)" of the *Oracle Fusion Middleware Administrator's Guide for Oracle Web Cache* has the following incorrect statements:

- **Incorrect statement**: "Fusion Middleware Control or Oracle Web Cache Manager do not provide support for client certificate validation with Certificate Revocation Lists (CRLs). You can configure this support by manually editing the `webcache.xml` file."

  Clarification: This statement is incorrect. You can enable and configure support for CRLs by using the Oracle Web Cache Manager, as follows:

  1. Go to the **Listen Ports** page.
  2. Select the HTTPS port for which you want to configure CRL settings, and click **Edit Selected**.

     The **Edit/Add Listen Port** dialog box is displayed.
  3. Select the **Certificate Revocation List Enabled** option.
  4. In the **CRL Path** field, specify the fully qualified path to the directory in which the CRLs are stored. For example, `/home/crl`.
  5. In the **CRL File** field, specify the fully qualified path and filename of the CRL file. For example, `/home/oracle/crl/CA/crl`.

- **Incorrect statement**: Step 4 of the procedure to configure certificate validation using CRLs: "Configure CRL file location by adding the `SSLCRLPATH` and `SSLCRLFILE` parameters to the `HTTPS LISTEN` directive."

  Clarification: This statement is incorrect. You must add *either* `SSLCRLPATH` *or* `SSLCRLFILE` to the `HTTPS LISTEN` directive, not both.

7 Resolved Issues

- Due to security concerns, the SSLV3 security protocol has been disabled by default.
- Support for the TLSv1.1 and TLSv1.2 security protocols have been added. Section 2, "New Security Protocols and Ciphers," Section 3, "Enabling TLS Security Protocols," and Section 4, "Ciphers Supported by the STRONG_CRYPTO_ONLY Parameter."
- The default value of the STRONG_CRYPTO_ONLY parameter has been set to YES. For more information, see Section 4, "Ciphers Supported by the STRONG_CRYPTO_ONLY Parameter."

8 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle Fusion Middleware Release Notes for Oracle Web Cache, 11g Release 1 (11.1.1)
E64094-01