Service Architecture Leveraging Tuxedo (SALT)
Configuration Guide
12c Release 2 (12.1.3)

April 2014
Configuring a SALT Application

Configuring Oracle Tuxedo Web Services ......................................................... 1
    Using Oracle Tuxedo Service Metadata Repository for SALT .......................... 2
    Defining Service-Level Keywords for SALT .................................................. 2
    Defining Service Parameters for SALT ....................................................... 6
Configuring Native Oracle Tuxedo Services ...................................................... 8
    Creating a Native WSDF .............................................................................. 9
    Defining the SOAP Header ......................................................................... 9
    Defining WSBinding Object ....................................................................... 10
    Defining Service Object ........................................................................... 11
    Configuring Message Conversion Handler .................................................. 12
Using WS-Policy Files ......................................................................................... 13
Generating a WSDL File from a Native WSDF .................................................... 15
Using Oracle Tuxedo Version-Based Routing (Inbound) ........................................ 15
Configuring External Web Services .................................................................... 16
    Web Console SALT Configuration ............................................................... 16
    Manual SALT Configuration ....................................................................... 17
    Converting a WSDL File into Oracle Tuxedo Definitions ............................. 17
    Post Conversion Tasks .............................................................................. 21
    Using Oracle Tuxedo Version-Based Routing (Outbound) ............................. 23
Configuring Multiple Bindings ........................................................................... 24
    SALT inbound services ............................................................................. 24
    SALT outbound services .......................................................................... 24
Creating the SALT Deployment File .................................................................... 24
    Importing the WSDF Files ........................................................................ 25
    Configuring the GWWS Servers ................................................................... 25
    Configuring GWWS Server-Level Properties ............................................. 26
Configuring Multiple Encoding Support ........................................... 28
Configuring System-Level Resources ............................................. 30
Configuring Certificates ............................................................... 30
Configuring Plug-in Libraries ....................................................... 31
Configuring Advanced Web Service Messaging Features ................. 32
Web Service Addressing ............................................................... 32
Configuring the Addressing Endpoint for Outbound Services .......... 32
Disabling WS-Addressing ............................................................. 34
Web Service Reliable Messaging .................................................. 34
Creating the Reliable Messaging Policy File ................................ 35
Specifying the Reliable Messaging Policy File in the WSDF File ....... 35
Message Transmission Optimization Mechanism (MTOM) .............. 36
Configuring Security Features ....................................................... 37
Configuring Transport-Level Security .......................................... 37
  Setting Up SSL Link-Level Security ........................................... 37
  Configuring Inbound HTTP Basic Authentication ....................... 37
  Configuring Outbound HTTP Basic Authentication .................... 38
Configuring Message-Level Web Service Security ....................... 39
  Main Use Cases of Web Service Security ................................. 39
  Using WS-Security Policy Files .............................................. 40
Configuring SAML Single Sign-On .............................................. 41
  Transport Protection .............................................................. 42
  SAML Key File .................................................................. 42
  Configuring X.509-Based Authentication ................................. 48
  Certificate Sources ............................................................... 50
  Properties ....................................................................... 51
Compiling SALT Configuration .................................................... 58
Configuring a SALT Application

This section contains the following topics:

- Configuring Oracle Tuxedo Web Services
- Configuring Service Contract Discovery
- Configuring SALT WS-TX Support
- SALT Configuration Tool

**Configuring Oracle Tuxedo Web Services**

- Using Oracle Tuxedo Service Metadata Repository for SALT
- Configuring Native Oracle Tuxedo Services
- Configuring External Web Services
- Configuring Multiple Bindings
- Creating the SALT Deployment File
- Configuring Advanced Web Service Messaging Features
- Configuring Security Features
- Compiling SALT Configuration
- Configuring the UBBCONFIG File for SALT
Configuring SALT In Oracle Tuxedo MP Mode

Migrating from SALT 1.1

Using Oracle Tuxedo Service Metadata Repository for SALT

SALT leverages the Oracle Tuxedo Service Metadata Repository to define service contract information for both existing Oracle Tuxedo services and SALT proxy services. Service contract information for all listed Oracle Tuxedo services is obtained by accessing the Oracle Tuxedo Service Metadata Repository system service provided by the local Oracle Tuxedo domain. Typically, SALT calls the `TMMETADATA` system as follows:

- **During GWWS server run-time.**
  It calls the Oracle Tuxedo Service Metadata Repository to retrieve necessary Oracle Tuxedo service definition at the appropriate time.

- **When tmwsdlgen generates a WSDL file.**
  It calls the Oracle Tuxedo Service Metadata Repository to retrieve necessary Oracle Tuxedo service definitions and converts them to the WSDL description.

The following topics provide SALT-specific usage of Oracle Tuxedo Service Metadata Repository keywords and parameters:

- **Defining Service-Level Keywords for SALT**
- **Defining Service Parameters for SALT**

Defining Service-Level Keywords for SALT

Table 1 lists the Oracle Tuxedo Service Metadata Repository service-level keywords used and interpreted by SALT.

**Note:** Metadata Repository service-level keywords that are not listed have no relevance to SALT and are ignored when SALT components load the Oracle Tuxedo Service Metadata Repository.
### Table 1 SALT Usage of Service-Level Keywords in Oracle Tuxedo Service Metadata Repository

<table>
<thead>
<tr>
<th>Service-Level Keyword</th>
<th>SALT Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>The unique key value of the service. This value is referenced in the SALT WSDF file. For native Oracle Tuxedo services, this value can be the same as the Oracle Tuxedo advertised service name or an alias name different from the actual Oracle Tuxedo advertised service name. For SALT proxy services, this value typically is the Web service operation local name.</td>
</tr>
<tr>
<td>servicemode</td>
<td>Determines the service mode (i.e., native Oracle Tuxedo service or SALT proxy service. The valid values are:  • tuxedo represents a native Oracle Tuxedo service  • webservice represents an SALT proxy service, i.e. a service definition converted from a wsdl:operation  Do not use “webservice” to define a native Oracle Tuxedo service. This value is always used to define services converted from external Web services.</td>
</tr>
<tr>
<td>tuxservice</td>
<td>The actual Oracle Tuxedo advertised service name. If no value is specified, then the value is the same as the value in the service keyword. For native Oracle Tuxedo service, SALT invokes the Oracle Tuxedo service defined using this keyword. For SALT proxy service, GWWS server advertises the service name using this keyword value.</td>
</tr>
</tbody>
</table>
Configuring a SALT Application

Table 1  SALT Usage of Service-Level Keywords in Oracle Tuxedo Service Metadata Repository

<table>
<thead>
<tr>
<th>Service-Level Keyword</th>
<th>SALT Usage</th>
</tr>
</thead>
</table>
| servicetype           | Determines the service message exchange pattern for the specified Oracle Tuxedo service. The following values specify mapping rules between the Oracle Tuxedo service types and Web Service message exchange pattern (MEP):  
  • service  
    corresponds to request-response MEP  
  • oneway  
    corresponds to oneway request MEP  
  • queue  
    corresponds to request-response MEP |
| inbuf                 | Specifies the input buffer (request buffer) type for the service. For native Oracle Tuxedo services, the value can be any Oracle Tuxedo typed buffer type. The following values are Oracle Tuxedo reserved buffer types:  
  STRING, CARRAY, XML, MBSTRING, VIEW, VIEW32, FML, FML32, X_C_TYPE, X_COMMON, X_OCTET, NULL (input buffer is empty)  
  
  **Note:** The value is case sensitive, if *inbuf* specifies any other type other than the previous buffer types, the buffer is treated as a custom buffer type.  
  For SALT proxy services, the value is always FML32. |
| outbuf                | Specifies the output buffer (response buffer with TPSUCCESS), type for the service. For native Oracle Tuxedo services, the value can be any Oracle Tuxedo typed buffer type. The following values are Oracle Tuxedo reserved buffer types:  
  STRING, CARRAY, XML, MBSTRING, VIEW, VIEW32, FML, FML32, X_C_TYPE, X_COMMON, X_OCTET, NULL (input buffer is empty)  
  
  **Note:** The value is case sensitive, if *outbuf* specifies any other type other than the previous buffer types, the buffer is treated as a custom buffer type.  
  For SALT proxy services, the value is always FML32. |
Using Oracle Tuxedo Service Metadata Repository for SALT

Table 1  SALT Usage of Service-Level Keywords in Oracle Tuxedo Service Metadata Repository

<table>
<thead>
<tr>
<th>Service-Level Keyword</th>
<th>SALT Usage</th>
</tr>
</thead>
</table>
| **errbuf**             | Specifies the error buffer (response buffer with TPFAIL) type for the service.  
For native Oracle Tuxedo services, the value can be any Oracle Tuxedo typed buffer type. The following values are Oracle Tuxedo reserved buffer types:  
STRING, CARRAY, XML, MBSTRING, VIEW, VIEW32, FML, FML32, X_C_TYPE, X_COMMON, X_OCTET, NULL (input buffer is empty).  
**Note:** The value is case sensitive, if errbuf specifies any other type other than the previous buffer types, the buffer is treated as a custom buffer type.  
For SALT proxy services, the value is always FML32. |
| **inview**             | Specifies the view name used by the service for the following input buffer types:  
VIEW, VIEW32, X_C_TYPE, X_COMMON  
SALT requires that you specify the view name rather than accept the default inview setting.  
This keyword is for native Oracle Tuxedo services only. |
| **outview**            | Specifies the view name used by the service for the following output buffer types:  
VIEW, VIEW32, X_C_TYPE, X_COMMON  
SALT requires that you specify the view name rather than accept the default outview setting.  
This keyword is for native Oracle Tuxedo services only. |
| **errview**            | Specifies the view name used by the service for the following error buffer types:  
VIEW, VIEW32, X_C_TYPE, X_COMMON  
SALT requires that you specify the view name rather than accept the default errview setting.  
This keyword is for native Oracle Tuxedo services only. |
Defining Service Parameters for SALT

The Oracle Tuxedo Service Metadata Repository interprets parameters as sub-elements encapsulated in an Oracle Tuxedo service typed buffer. Each parameter can have its own data type, occurrences in the buffer, size restrictions, and other Oracle Tuxedo-specific restrictions. Please note:

- VIEW, VIEW32, X_C_TYPE, or X_COMMON typed buffers
  Each parameter of the buffer should represent a VIEW/VIEW32 structure member.

- FML or FML32 typed buffers
  Each parameter of the buffer should represent an FML/FML32 field element that may be present in the buffer.

- STRING, CARRAY, XML, MBSTRING, and X_OCTET typed buffers
  Oracle Tuxedo treats these buffers holistically. At most, one parameter is permitted for the buffer to define restriction facets (such as buffer size threshold).

- Custom typed buffers

<table>
<thead>
<tr>
<th>Service-Level Keyword</th>
<th>SALT Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>inbufschema</td>
<td>Specifies external XML Schema element associated with the service input buffer. If this value is specified, SALT incorporates the external schema in the generated WSDL to replace the default data type mapping rule for the service input buffer. This keyword is for native Oracle Tuxedo services only.</td>
</tr>
<tr>
<td>outbufschema</td>
<td>Specifies external XML Schema element associated with the service output buffer. If this value is specified, SALT incorporates the external schema in the generated WSDL to replace the default data type mapping rule for the service output buffer. This keyword is for native Oracle Tuxedo services only.</td>
</tr>
<tr>
<td>errbufschema</td>
<td>Specifies external XML Schema element associated with the service error buffer. If this value is specified, SALT incorporates the external schema in the generated WSDL to replace the default data type mapping rule for the service error buffer. This keyword is for native Oracle Tuxedo services only.</td>
</tr>
</tbody>
</table>
Parameters facilitate describing details about the buffer type.

- FML32 typed buffers that support embedded VIEW32 and FML32 buffers
  Embedded parameters provide support.
- View32 typed buffers that support embedded VIEW32 buffers
  Embedded parameters provide support.

Table 2 lists the Oracle Tuxedo Service Metadata Repository parameter-level keywords used and interpreted by SALT.

**Note:** Metadata Repository parameter-level keywords that are not listed have no relevance to SALT and are ignored when SALT components load the Oracle Tuxedo Service Metadata Repository.

### Table 2: SALT Usage of Parameter-Level Keyword in Oracle Tuxedo Service Metadata Repository

<table>
<thead>
<tr>
<th>Parameter-level Keyword</th>
<th>SALT Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>param</strong></td>
<td>Specifies the parameter name.</td>
</tr>
<tr>
<td></td>
<td>• VIEW, VIEW32, X_C_TYPE, or X_COMMON</td>
</tr>
<tr>
<td></td>
<td>• FML, FML32</td>
</tr>
<tr>
<td></td>
<td>• Specifies the view structure member name in the param keyword.</td>
</tr>
<tr>
<td></td>
<td>• Specifies the FML/FML32 field name in the param keyword.</td>
</tr>
<tr>
<td></td>
<td>• STRING, CARRAY, XML, MBSTRING, or X_OCTET</td>
</tr>
<tr>
<td></td>
<td>SALT ignores the parameter definitions.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Specifies the data type of the parameter.</td>
</tr>
<tr>
<td><strong>subtype</strong></td>
<td>Specifies the view structure name if the parameter type is view32. For any other typed parameter, SALT ignores this value.</td>
</tr>
<tr>
<td><strong>access</strong></td>
<td>The general definition applies for this parameter. To support an Oracle Tuxedo TPFAIL scenario, the access attribute value has been enhanced.</td>
</tr>
<tr>
<td></td>
<td><strong>Original values:</strong> in, out, inout, noaccess.</td>
</tr>
<tr>
<td></td>
<td><strong>New added values:</strong> err, inerr, outerr, inouterr.</td>
</tr>
</tbody>
</table>

Note: SALT does not support dec_t and ptr data types.
Configuring Native Oracle Tuxedo Services

This section describes the required and optional configuration tasks for exposing native Oracle Tuxedo services as Web services:

- Creating a Native WSDF
- Using WS-Policy Files
- Generating a WSDL File from a Native WSDF
- Using Oracle Tuxedo Version-Based Routing (Inbound)

<table>
<thead>
<tr>
<th>Parameter-level Keyword</th>
<th>SALT Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>The general definition applies for this parameter. For SALT, the value for the count parameter must be greater than or equal to requiredcount.</td>
</tr>
<tr>
<td>requiredcount</td>
<td>The general definition applies for this parameter. The default is 1. For SALT, the value for the count parameter must be greater than or equal to requiredcount.</td>
</tr>
<tr>
<td>size</td>
<td>This optional keyword restricts the maximum byte length of the parameter. It is only valid for the following parameter types: STRING, CARRAY, XML, and MBSTRING. If this keyword is not set, there is no maximum byte length restriction for this parameter. The value range is $[0, 2^{31}-1]$.</td>
</tr>
<tr>
<td>paramschema</td>
<td>Specifies the corresponding XML Schema element name of the parameter. It is generated by the SALT WSDL converter. This keyword is for SALT proxy service only. Do not specify this keyword for native Oracle Tuxedo services.</td>
</tr>
<tr>
<td>primetype</td>
<td>Specifies the corresponding XML primitive data type of the parameter. It is generated by SALT WSDL converter according to SALT pre-defined XML-to-Tuxedo data type mapping rules. This keyword is for SALT proxy service only. Do not specify this keyword for native Oracle Tuxedo services.</td>
</tr>
</tbody>
</table>
Creating a Native WSDF

To expose a set of Oracle Tuxedo services as Web services through one or more HTTP/S endpoints, a native WSDF must be defined.

Each native WSDF must be defined with a unique WSDF name. A WSDF can define one or more <WSBinding> elements for more Web service application details (such as SOAP protocol details, the Oracle Tuxedo service list to be exposed as web service operations, and so on).

This section contains the following topics:

- Defining the SOAP Header
- Defining WSBinding Object
- Defining Service Object
- Configuring Message Conversion Handler

Defining the SOAP Header

The mapsoapheader attribute is used to configure SOAP headers. It defines an FML32 field that represents the SOAP header. It is TA_WS_SOAP_HEADER STRING type.

Note: The mapsoapheader attribute is defined in wssoapflds.h file shipped with SALT. Listing 1 shows a SOAP header definition example.

Listing 1  SOAP Header Definition

```xml
<Definition ...>
  <WSBinding id="simpapp_binding">
    <Servicegroup id="simpapp">
      <Service name="toupper">
        <Property name="mapsoapheader" value="true" />
      </Service>
    </Servicegroup>
    ....
  </WSBinding>
```

The `mapsoapheader` attribute default value is "false" which indicates the GWWS does not execute mapping between the SOAP header and FML fields.

If `mapsoapheader` is set to `true`, the mapping behavior is as follows for inbound and outbound services:

- **Inbound**
  
  For inbound services, the GWWS translates the SOAP header as shown in **Listing 2**.

**Listing 2   GWWS Soap Header Translation**

```
<cup:SoapHeader xmlns:cup='http://www.xxx.com/soa/esb/message/1_0'>
  <cup:Head>
    <cup:Name>xxx</cup:Name>
    <cup:Value>xxx</cup:Value>
  </cup:Head>
</cup:SoapHeader>
```

The string buffer is assigned to the `TA_WS_SOAP_HEADER` field and injects the target FML32 buffer. If the target buffer type is not FML32, the translation will not take effect.

- **Out Bound**
  
  For outbound services, the GWWS receives the `TA_WS_SOAP_HEADER` from the request buffer and places it in the SOAP header when the SOAP package is composed.

### Defining WSBinding Object

Each WSBinding object is defined using the `<WSBinding>` element. Each WSBinding object must be defined with a unique WSBinding id within the `WSDF`. The WSBinding id is a required indicator for the `SALTDEPLOY` file reference used by the `GWWS`.

Each WSBinding object can be associated with SOAP protocol details by using the `<SOAP>` sub-element. By default, SOAP 1.1, document/literal styled SOAP messages are applied to the WSBinding object.

Listing 3 shows how SOAP protocol details are redefined using the `<SOAP>` sub-element.

**Listing 3  Defining SOAP Protocol Details for a WSBinding**

```xml
<Definition ...>
  <WSBinding id="simpapp_binding">
    <Servicegroup id="simpapp">
      <Service name="toupper" />
      <Service name="tolower" />
    </Servicegroup>
    <SOAP version="1.2" style="rpc" use="encoded">
      <AccessingPoints>
        ...  
      </AccessingPoints>
    </SOAP>
  </WSBinding>
</Definition>
```

Within the `<SOAP>` element, a set of access endpoints can be specified. The URL value of these access endpoints are used by corresponding GWWS servers to create the listen HTTP/S protocol port. It is recommended to specify one HTTP and HTTPS endpoint (at most), for each GWWS server for an inbound WSBinding object.

Each WSBinding object must be defined with a group of Oracle Tuxedo services using the `<Servicegroup>` sub-element. Each `<Service>` element under `<Servicegroup>` represents an Oracle Tuxedo service that can be accessed from a Web service client.

**Defining Service Object**

Each service object is defined using the `<Service>` element. Each service must be specified with the “name” attribute to indicate which Oracle Tuxedo service is exposed. Usually, the “name” value is used as the key value for obtaining Oracle Tuxedo service contract information from the Oracle Tuxedo Service Metadata Repository.
Listing 4 shows how a group of services are defined for WSBinding.

Listing 4  Defining a Group of Services for a WSBinding

<Definition ...>
  <WSBinding id="simpapp_binding">
    <Servicegroup id="simpapp">
      <Service name="toupper" />
      <Service name="tolower" />
    </Servicegroup>
    ...
  </WSBinding>
</Definition>

Configuring Message Conversion Handler

You can create your own plug-in functions to customize SOAP XML payloads and Oracle Tuxedo typed buffer conversion routines. For more information, see Using SALT Plug-ins in SALT Programming Web Services and “Configuring Plug-in Libraries” on page 31.

Once a plug-in is created and configured, it can be referenced using the <service> element to specify user-defined data mapping rules for that service. The <Msghandler> element can be defined at the message level (<Input>, <Output> or <Fault>) to specify which implementation of “P_CUSTOM_TYPE” category plug-in should be used to do the message conversion. The <Msghandler> element content is the Plug-in name.

Listing 5 shows a service that uses the “MBCONV” custom plug-in to convert input and “XMLCONV” custom plug-in to convert output.

Listing 5  Configuring Message Conversion Handler for a Service

<Definition ...>
  <WSBinding id="simpapp_binding">
    <Servicegroup id="simpapp">
      <Service name="toupper">
        <Input>
          <Msghandler>MBCONV</Msghandler>
        </Input>
      </Service>
    </Servicegroup>
    ...
  </WSBinding>
</Definition>
Using WS-Policy Files

Advanced Web service features can be enabled by configuring WS-Policy files (for example, Reliable Messaging and Web Service Message-Level Security). You may need to create WS-Policy files to use these features. The Web Service Policy Framework specifications provides a general purpose model and syntax to describe and communicate the policies of a Web Service.

To use WS-Policy files, the <Policy> element should be defined in the WSDF to incorporate these separate WS-Policy files. The location attribute is used to specify the policy file path; both abstract and relative file path are allowed. The use attribute is optionally used by message-level assertion policy files to specify the applied messages, request (input) message, response (output) message, fault message, or the combination of the three.

There are two different sub-elements in the WSDF that reference WS-Policy files:

- <Servicegroup>
  - If a WS-Policy file consists of Web Service Endpoint-level Assertions (for example, Reliable Messaging Assertion), the WS-Policy file applies to all endpoints serving the <Servicegroup> element.
  
  - If a WS-Policy file consists of Web Service Operation-level Assertions (for example, Security Identity Assertion), the WS-Policy file applies to all services listed in the <Servicegroup> element.

  - If a WS-Policy file consists of Web Service Message level Assertions (for example, Security SignedParts Assertion), the WS-Policy file applies to input, output and/or fault messages of all services listed in the <Servicegroup> element.
Configuring a SALT Application

- Note: SALT only supports request message-level assertions for the current release. You must only specify `use="input"` for message-level assertion policy files.

- `<Service>`
  - If a WS-Policy file consists of Web Service Operation-level Assertions (for example, Security Identity Assertion), the WS-Policy file applies to this particular service.
  - If a WS-Policy file consists of Web Service Message-level Assertions (for example, Security SignedParts Assertion), the WS-Policy file applies to input, output and/or fault messages of this particular service.

- Note: SALT only supports request message-level assertions for the current release. You must specify `use="input"` for message-level assertion policy files.

SALT provides some pre-packaged WS-Policy files for most frequently used cases. These WS-Policy files are located under directory `$/TUXDIR/udataobj/salt/policy`. These files can be referenced using `location="salt:<policy_file_name>"`.

Listing 6 shows a sample of using WS-Policy Files in the native `WSDF` file.

**Listing 6  A Sample of Defining WS-Policy Files in the WSDF File**

```xml
<Definition ...>
  <WSBinding id="simpapp_binding">
    <Servicegroup id="simpapp">
      <Policy location="./endpoint_policy.xml" />
      <Policy location="/usr/resc/all_input_msg_policy.xml" use="input" />
      <Service name="toupper">
        <Policy location="service_policy.xml" />
        <Policy location="/usr/resc/input_message_policy.xml"
          use="input" />
      </Service>
      <Service name="tolower" />
    </Servicegroup>
  ....
</WSBinding>
</Definition>
```
Configuring Native Oracle Tuxedo Services

Generating a WSDL File from a Native WSDF

Once an Oracle Tuxedo native WSDF is created, the corresponding WSDL file can be generated using the SALT WSDL generation utility, `tmwsdlgen`. The following example command generates a WSDL file named “appl.wsdl” from a given WSDF named “appl.wsdf”:

```
tmwsdlgen -c appl.wsdf -o appl.wsdl
```

**Note:** Before executing `tmwsdlgen`, the `TUXCONFIG` environment variable must be set correctly and the relevant Oracle Tuxedo application using `TMMETADATA` must be booted.

You can optionally specify the output WSDL file name using the `'-o'` option. Otherwise, `tmwsdlgen` creates a default WSDL file named “tuxedo.wsdl”.

If the native WSDF file contains Oracle Tuxedo services that use `CARRAY` buffers, you can specify `tmwsdlgen` options to generate different styled WSDL files for `CARRAY` buffer mapping. By default, `CARRAY` buffers are mapped as `xsd:base64Binary` XML data types in the SOAP message. For more information, see Data Type Mapping and Conversions in SALT Programming Web Services and `tmwsdlgen` in the SALT Reference Guide.

Using Oracle Tuxedo Version-Based Routing (Inbound)

Using Oracle Tuxedo version-based routing with Oracle Tuxedo services exposed as Web services involves the following:

- GWWS gets `REQUEST_VERSION` and `VERSION_RANGE` from the `UBBCONFIG` file.
- Calling service with request version
- If different settings are needed (such as specific traffic from specific gateway to be routed to specific services), another gateway instance can be configured in a group with different `REQUEST_VERSION` value and started for this.

Listing 7 shows an example where GWWS inherits a request version "1" from its `UBBCONFIG` settings, and therefore exposes services that are advertised by Oracle Tuxedo application servers which include "1" in their `VERSION_RANGE` settings (such as `GROUP1` here). If a service exposed by GWWS is actually performed by a server in `GROUP2`, the result is a `TPENOENT` error forwarded to the remote Web Services client.
Listing 7  Using Tuxedo Version Based Routing with Tuxedo Services Exposed as Web Services

...  
GROUP1
LMID=L1 GRPNO=2 VERSION_RANGE="1-2"
GROUP2
LMID=L1 GRPNO=2 VERSION_RANGE="3-4"
GWWS_GRP
LMID=L1 GRPNO=3 REQUEST_VERSION=1
...
|mySERVER SRVGRP=GROUP2 SRVID=30
...
GWWS SRVGRP=GWWS_GRP SRVID=30
...

Configuring External Web Services

You can configure external web service via SALT web console or manually.

- Web Console SALT Configuration  
- Manual SALT Configuration  
- Using Oracle Tuxedo Version-Based Routing (Outbound)

Web Console SALT Configuration

A web console is a GUI based SALT configuration tool. One of its features is to import external web services by providing a WSDL file.

The WSDL file is provided as input to the "Import External Web Services" in the SALT web console main web page. The input file can exists locally from where the web console is launched or on the server (remote) where the GWWS server is actively running.

The GWWS Server upon receiving the WSDL file uses the wsdlcvt tool to generate the following files corresponding to their extensions in the APPDIR directory:

    wsdlcvt -y -f -i <input_WSDL_file> -o <base_name>
Configuring External Web Services

XSD - XML schema file.
MIF - Metadata repository file.
FML32 - FML32 field table file.
WSDF - Non-native WSDF file.

Please note that the user has to just input the WSDL file the above files are generated internally by the GWWS server without the intervention of the user.

After the files are successful generated, the user has to then set the following environment variables in the APPDIR directory:

FLDTBLDIR32
FIELDTBL$32
XSDDIR
XSDFILES

The GWWS server reloads the Service Metadata Repository and the SALT configuration file (SALTCONFIG) with the new services/operations and Bindings that were imported from the WSDL file.

The web services that were imported are displayed in the SALT web console main page under the "Imported Web Services" section. For more information, see .

Manual SALT Configuration

- Converting a WSDL File into Oracle Tuxedo Definitions
- Post Conversion Tasks

Converting a WSDL File into Oracle Tuxedo Definitions

SALT provides a WSDL conversion command utility to convert external WSDL files into Oracle Tuxedo definitions. The WSDL file is converted using Extensible Stylesheet Language Transformations (XSLT) technology. Apache Xalan Java 2.7.0 is bundled in the SALT installation package and is used as the default XSLT toolkit.

The SALT WSDL converter is composed of two parts:

- The xsl files, which process the WSDL file.
- The command utility, wsdlcvt, invokes the Xalan toolkit. This wrapper script provides a user friendly WSDL Converter interface.
The following sample command converts an external WSDL file and generates Oracle Tuxedo definition files.

```shell
cvtoolcvt -i GoogleSearch.wsdl -o GSearch
```

Table 3 lists the Oracle Tuxedo definition files generated by SALT WSDL Converter.

<table>
<thead>
<tr>
<th>Generated File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Tuxedo Service Metadata Repository input file</td>
<td>SALT WSDL Converter converts each <code>wsdl:operation</code> to a Oracle Tuxedo service metadata syntax compliant service called SALT proxy service. SALT proxy services are advertised by GWWS servers to accept ATMI calls from Oracle Tuxedo applications.</td>
</tr>
<tr>
<td>FML32 field table definition file</td>
<td>SALT maps each <code>wsdl:message</code> to an Oracle Tuxedo FML32 typed buffer. The SALT WSDL Converter decomposes XML Schema of each message and maps each basic XML snippet as an FML32 field. The generated FML32 fields are defined in a definition table file, and the field name equals to the XML element local name by default. To access an SALT proxy service, Oracle Tuxedo applications must refer to the generated FML32 fields to handle the request and response message. FML32 environment variables must be set accordingly so that both Oracle Tuxedo applications and GWWS servers can map between field names and field identifier values. Note: You may want to re-define the generated field names due to field name conflict or some other reason. In that case, both Oracle Tuxedo Service Metadata Definition input file and FML32 field table definition file must be changed accordingly. For more information, see “Resolving Naming Conflict For the Generated SALT Proxy Service Definitions”.</td>
</tr>
</tbody>
</table>
Configuring External Web Services

Table 3  Tuxedo Definition Files generated by SALT WSDL Converter

<table>
<thead>
<tr>
<th>Generated File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-native WSDF file</td>
<td>SALT WSDL Converter converts the WSDL file into a WSDF file, which can be deployed to GWWS servers in the SALT deployment file for outbound direction. The generated WSDF file is anon-native WSDF file.</td>
</tr>
<tr>
<td>Note:</td>
<td>Please do not deploy non-native WSDF files for inbound direction.</td>
</tr>
<tr>
<td>XML Schema files</td>
<td>WSDL embedded XML Schema and imported XML Schema (XML Schema content referenced with <a href="">xsd:import</a>) are saved locally as .xsd files. These files are used by GWWS servers and need to be saved under the same directory.</td>
</tr>
<tr>
<td>Note:</td>
<td>New XML Schema environment variables XSDDIR and XSDFILES must be set accordingly so that GWWS servers can load these .xsd files.</td>
</tr>
</tbody>
</table>

WSDL-to-Tuxedo Service Metadata Keyword Mapping

Table 4 lists WSDL Element-to-Tuxedo Service Metadata Definition Keyword mapping rules.

Table 4  WSDL Element-to-Tuxedo Service Metadata Definition Mapping

<table>
<thead>
<tr>
<th>WSDL Element</th>
<th>Corresponding Oracle Tuxedo Service Metadata Definition Keyword</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>/wsdl:definitions</td>
<td>service</td>
<td>SALT proxy service name. The keyword value equals to the operation local name.</td>
</tr>
<tr>
<td>/wsdl:portType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>@name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tuxservice</td>
<td></td>
<td>SALT proxy service advertised name in Oracle Tuxedo system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the wsdl operation local name is less than 15 characters, the keyword value equals to the operation local name, otherwise the keyword value is the first 15 characters of the operation local name.</td>
</tr>
</tbody>
</table>
Configuring a SALT Application

### WSDL-to-WSDF Mapping

Table 5 lists WSDL Element-to-WSDF Element mapping rules.

<table>
<thead>
<tr>
<th>WSDL Element</th>
<th>Corresponding Oracle Tuxedo Service Metadata Definition Keyword</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>/wsdl:definitions</td>
<td>inbuf=FML32</td>
<td>WSDL operation messages are always mapped as Oracle Tuxedo FML32 buffer types. Please do not change the buffer type any way.</td>
</tr>
<tr>
<td>/wsdl:portType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:input</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:definitions</td>
<td>outbuf=FML32</td>
<td>Note: For more information about wsdl message and FML32 buffer mapping, see XML-to-Tuxedo Data Type Mapping for External Web Services in the SALT Programming Web Services.</td>
</tr>
<tr>
<td>/wsdl:portType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:definitions</td>
<td>errbuf=FML32</td>
<td></td>
</tr>
<tr>
<td>/wsdl:portType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:fault</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### WSDL-to-WSDF Mapping

Table 4 WSDL Element-to-Tuxedo Service Metadata Definition Mapping

<table>
<thead>
<tr>
<th>WSDL Element</th>
<th>Corresponding Oracle Tuxedo Service Metadata Definition Keyword</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>/wsdl:definitions</td>
<td>inbuf=FML32</td>
<td>WSDL operation messages are always mapped as Oracle Tuxedo FML32 buffer types. Please do not change the buffer type any way.</td>
</tr>
<tr>
<td>/wsdl:portType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:input</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:definitions</td>
<td>outbuf=FML32</td>
<td>Note: For more information about wsdl message and FML32 buffer mapping, see XML-to-Tuxedo Data Type Mapping for External Web Services in the SALT Programming Web Services.</td>
</tr>
<tr>
<td>/wsdl:portType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:definitions</td>
<td>errbuf=FML32</td>
<td></td>
</tr>
<tr>
<td>/wsdl:portType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/wsdl:fault</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring External Web Services

#### Post Conversion Tasks

The following post conversion tasks must be performed for configuring outbound Web service applications:

- Resolving Naming Conflict For the Generated SALT Proxy Service Definitions
- Loading the Generated SALT Proxy Service Metadata Definitions
- Setting Environment Variables for GWWS Runtime

### Resolving Naming Conflict For the Generated SALT Proxy Service Definitions

When converting a WSDL file, unexpected naming conflicts may arise due to truncation or lost context information. Before using the generated Service Metadata Definitions and FML32 field table files, the following potential naming conflicts must be eliminated first.

---

<table>
<thead>
<tr>
<th>WSDL Element</th>
<th>WSDL Element</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>/wsdl:definitions</td>
<td>/Definition</td>
<td>If namespace prefix “soap” refers to URI “<a href="http://schemas.xmlsoap.org/wsdl/soap/%E2%80%9D">http://schemas.xmlsoap.org/wsdl/soap/”</a>, the SOAP version attribute value is “1.1”; If namespace prefix “soap” refers to URI “<a href="http://schemas.xmlsoap.org/wsdl/soap12/%E2%80%9D">http://schemas.xmlsoap.org/wsdl/soap12/”</a>, the SOAP version attribute value is “1.2”.</td>
</tr>
<tr>
<td>/wsdl:binding</td>
<td>/WSBinding</td>
<td>The WSDF WSBinding SOAP message style setting is equal to the corresponding WSDL soap binding message style setting (“rpc” or “document”).</td>
</tr>
<tr>
<td>/soap:binding</td>
<td>/SOAP @version</td>
<td>Each wsdl:operation object maps to a Service element of the corresponding WSBinding element.</td>
</tr>
<tr>
<td>@style</td>
<td>/style</td>
<td>Each soap:address endpoint defined for a wsdl:binding object maps to a Endpoint element of the corresponding WSBinding element.</td>
</tr>
</tbody>
</table>

---

Table 5  WSDL Element-to-WSDF Element Mapping
Eliminating the duplicated service metadata keyword “tuxservice” definitions

The keyword tuxservice in the SALT proxy service metadata definition is the truncated value of the original Web Service operation local name if the operation name is more than 15 characters.

The truncated tuxservice value may be duplicated for multiple SALT proxy service entries. Since GWWS server uses tuxservice values as the advertised service names, you must manually resolve the naming conflict among multiple SALT proxy services to avoid uncertain service request delivery. To resolve the naming conflict, you should assign a unique and meaningful name to tuxservice.

Eliminating the duplicated FML32 field definitions

When converting an external WSDL file into Oracle Tuxedo definitions, each wsdl:message is parsed and mapped as an FML32 buffer format which contains a set of FML32 fields to represent the basic XML snippets of the wsdl:message. By default, The generated FML32 fields are named using the corresponding XML element local names.

The FML32 field definitions in the generated field table file are sorted by field name so that duplicated names can be found easily. In order to achieve a certain SOAP/FML32 mapping, the field name conflicts must be resolved. You should modify the generated duplicated field name with other unique and meaningful FML32 field name values. The corresponding Service Metadata Keyword param values in the generated SALT proxy service definition must be modified accordingly. The generated comments of the FML32 fields and Service Metadata Keyword “param” definitions are helpful in locating the corresponding name and param.

Loading the Generated SALT Proxy Service Metadata Definitions

After potential naming conflicts are resolved, you should load the SALT proxy service metadata definitions into the Oracle Tuxedo Service Metadata Repository through tmloadrepos utility. For more information, see tmloadrepos, in the Oracle Tuxedo Command Reference Guide.

Setting Environment Variables for GWWS Runtime

Before booting GWWS servers for outbound Web services, the following environment variable settings must be performed.

- Update FLDTBLDIR32 and FIELDTBLS32 environment variables to add the generated FML32 field table files.
- Place all excerpted XML Schema files into one directory and set the XSDDIR and XSDFILES environment variables accordingly.
– The `XSDDIR` and `XSDFILES` environment variables are introduced in the SALT 2.0 release. They are used by the GWWS server to load all external XML Schema files at runtime. Multiple XML Schema file names should be delimited with comma `,`. For instance, if you placed XML Schema files: `a.xsd, b.xsd` and `c.xsd` in directory `/home/user/myxsd`, you must set environment variable `XSDDIR` and `XSDFILES` as follows before booting the GWWS server:

```
XSDDIR=/home/user/myxsd
XSDFILES=a.xsd,b.xsd,c.xsd
```

### Using Oracle Tuxedo Version-Based Routing (Outbound)

When using Oracle Tuxedo version-based routing with External Web services imported into Tuxedo using SALT, please note:

- Since one GWWS instance cannot advertise more than one service with same name, that same service has to be in a different instance.
- Based on the above, the existing mechanism can simply be used; configure multiple GWWS instances with `VERSION_RANGE` in its `*GROUP` settings accordingly.

**Listing** shows an example where Oracle Tuxedo programs (client or server) call an external Web service exposed by both GWWS in groups `GROUP2` and `GROUP3`. Programs using version 1 or 2 are routed to the service exposed by GWWS in `GROUP2` which may connect to endpoint 1, and programs using version 3 or 4 are routed to the service exposed by GWWS in `GROUP3` which may connect to a different endpoint than GWWS in `GROUP2`.

**Listing 8  Oracle Tuxedo Version-Based Routing with External Web Services**

```
GROUP2
LMID=L1 GRPNO=2 VERSION_RANGE="1-2"
GROUP3
LMID=L1 GRPNO=3 REQUEST_VERSION=1 VERSION_RANGE="3-4"
...
GWWS SRVGRP=GROUP2 SRVID=30
...
GWWS SRVGRP=GROUP3 SRVID=30
...
```
Configuring Multiple Bindings

SALT inbound services
The users are allowed to create multiple bindings for the same service group and service operation. However, it does not allow creating multiple bindings for different service groups and operation.

Multiple Bindings can be created for inbound services for the following:

- The users can add endpoint addresses for each of the binding created. This is useful when there is "http" and "https" needed per service.
- The users can add more than one SOAP attribute values.
  - To specify different SOAP versions. For e.g.: SOAP version 1.1, or 1.2.
  - To specify Encoding styles. For e.g.: RPC/encoded or Doc/Literal.

You must use the web console to add multiple bindings.

SALT outbound services
The web services that are imported using the WSDL file are outbound services, where a Tuxedo client can send a request and receive response from the external web service.

The users for the imported web service can change the value of the end point address via web console and the Policy files. However, the users are not allowed to add any multiple bindings or add SOAP attributes.

Creating the SALT Deployment File
The SALT Deployment file (SALTDEPLOY) defines a SALT Web service application. The SALTDEPLOY file is the major input for Web service application in the binary SALTCONFIG file.

To create a SALTDEPLOY file, do the following steps:

1. Importing the WSDF Files
2. Configuring the GWWS Servers
3. Configuring System-Level Resources

For more information, see SALT Deployment File Reference in the Oracle SALT Reference Guide.
Importing the WSDF Files

You should import all your required WSDF files to the SALT deployment file. Each imported WSDF file must have a unique WSDF name which is used by the GWWS servers to make deployment associations. Each imported WSDF file must be accessible through the location specified in the SALTDEPLOY file.

Listing 9 shows how to import WSDF files in the SALTDEPLOY file.

Listing 9  Importing WSDF Files in the SALTDEPLOY File

```xml
<Deployment ..>
  <WSDF>
    <Import location="/home/user/simpapp_wsdf.xml" />
    <Import location="/home/user/rmapp_wsdf.xml" />
    <Import location="/home/user/google_search.wsdf" />
  </WSDF>
  ...
</Deployment>
```

Configuring the GWWS Servers

Each GWWS server can be deployed with a group of inbound WSBinding objects and a group of outbound WSBinding objects defined in the imported WSDF files. Each WSBinding object is referenced using attribute “ref=<wsdf_name>:<WSBinding id>”. For inbound WSBinding objects, each GWWS server must specify at least one access endpoint as an inbound endpoint from the endpoint list in the WSBinding object. For outbound WSBinding objects, each GWWS server can specify zero or more access endpoints as outbound endpoints from the endpoint list in the WSBinding object.

Listing 10 shows how to configure GWWS servers with both inbound and outbound endpoints.

Listing 10  GWWS Server Defined In the SALTDEPLOY File

```xml
<Deployment ..>
  ...
  <WSGateway>
```
Configuring a SALT Application

```xml
<GWInstance id="GWWS1">
  <Inbound>
    <Binding ref="app1:app1_binding">
      <Endpoint use="simpapp_GWWS1_HTTPPort" />
      <Endpoint use="simpapp_GWWS1_HTTPSPort" />
    </Binding>
  </Inbound>
  <Outbound>
    <Binding ref="app2:app2_binding">
      <Endpoint use="simpapp_GWWS1_HTTPPort" />
      <Endpoint use="simpapp_GWWS1_HTTPSPort" />
    </Binding>
    <Binding ref="app3:app3_binding" />
  </Outbound>
</GWInstance>
</WSGateway>
...
Creating the SALT Deployment File

Configuring a SALT Application

---

**Table 6  GWWS Server Level Properties**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
<th>Value Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_content_length</td>
<td>Specifies the maximum allowed incoming HTTP message content length.</td>
<td>[0, 1G] (byte)</td>
<td>0 (means no limit)</td>
</tr>
<tr>
<td></td>
<td>(Can set suffix 'M', 'G', e.g. 1.5M, 0.2G)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thread_pool_size</td>
<td>Specifies the GWWS server thread pool size.</td>
<td>[1, 1024]</td>
<td>16</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the network timeout in seconds.</td>
<td>[1, 65535]</td>
<td>300</td>
</tr>
<tr>
<td></td>
<td>(unit: sec)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wsrn_acktime</td>
<td>Specifies the Reliable Messaging Acknowledgement message reply policy. GWWS servers support replying acknowledgement messages either after receiving the SOAP request from network immediately or after the Oracle Tuxedo service returns the response message.</td>
<td>&quot;NETRECV&quot;</td>
<td>&quot;NETRECV&quot;</td>
</tr>
</tbody>
</table>

**Note:** For more information, see “Configuring Multiple Encoding Support”.

For more information, see “Tuning the GWWS Server” in Administering SALT at Runtime.

Listing 11 shows an example of how GWWS properties are configured.

**Listing 11  Configuring GWWS Server Properties**

```xml
<Deployment ..>
  ...
  <WSGateway>  
    <GWInstance id="GWWS1">  
      ....
      <Properties>
        <Property name="thread_pool_size" value="20"/>
        <Property name="enableMultiEncoding" value="true"/>
      </Properties>
    </GWInstance>
  </WSGateway>
</Deployment>
```
Configuring a SALT Application

```xml
<Property name="timeout" value="600"/>
</Properties>
</GWInstance>
</WSGateway>
...
</Deployment>
```

**Configuring Multiple Encoding Support**

SALT supports multiple encoding SOAP messages and the encoding mappings between SOAP message and Oracle Tuxedo buffer. SALT supports the following character encoding:


To enable the GWWS multiple encoding support, GWWS server-level “enableMultiEncoding” property should be set to “true” as shown in **Listing 12**.

**Note:** GWWS internally converts non UTF-8 external messages into UTF-8. However, encoding conversion hurts server performance. By default, encoding conversion is turned off and messages that are not UTF-8 encoded are rejected.

**Listing 12  Configuring GWWS Server Multiple Encoding Property**

```xml
<Deployment ..>
...
<WSGateway>
  <GWInstance id="GWWS1">
    ......
  </GWInstance>
  <Properties>
    <Property name="enableMultiEncoding" value="true"/>
  </Properties>
</GWInstance>
</WSGateway>
```
Table 7 explains the detailed SOAP message and Oracle Tuxedo buffer encoding mapping rules if the GWWS server level multiple encoding switch is turned on.

<table>
<thead>
<tr>
<th>Mapping from ...</th>
<th>Mapping to ...</th>
<th>Encoding Mapping Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP/XML</td>
<td>Oracle Tuxedo Typed Buffer</td>
<td>string/mbstring/xml buffer or field character encoding equals to SOAP xml encoding.</td>
</tr>
<tr>
<td>STRING Typed Buffer</td>
<td>SOAP/XML</td>
<td>GWWS sets the target SOAP message in UTF-8 encoding, and assumes the original STRING buffer contains only UTF-8 encoding characters.</td>
</tr>
<tr>
<td>Note: Oracle Tuxedo Developers must ensure the STRING characters are UTF-8 encoded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MBSTRING/XML Typed Buffer</td>
<td>SOAP/XML</td>
<td>SOAP xml encoding equals to MBSTRING/XML encoding.</td>
</tr>
<tr>
<td>FML/32, VIEW/32 Typed Buffer that containing the same encoding setting for multiple FLD_MBSTRING fields</td>
<td>SOAP/XML</td>
<td>SOAP xml encoding is set to FLD_MBSTRING encoding, the original Typed buffer field characters are not changed in the SOAP message.</td>
</tr>
<tr>
<td>Note: Oracle Tuxedo Developers must ensure the FLD_STRING characters in the same buffer are consistent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FML/32, VIEW/32 Typed Buffer that containing the different encoding for multiple FLD_MBSTRING fields</td>
<td>SOAP/XML</td>
<td>SOAP xml encoding is set to UTF-8, the original Typed buffer FLD_MBSTRING field characters in other encoding are converted into UTF-8 in the SOAP message.</td>
</tr>
<tr>
<td>Note: Oracle Tuxedo Developers must ensure the FLD_STRING characters in the same buffer are UTF-8 encoded.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring System-Level Resources

SALT defines a set of global resources shared by all GWWS servers in the SALTDEPLOY file. The following system-level resources can be configured in the SALTDEPLOY file:

- Certificates
- Plug-in load libraries

Configuring Certificates

Certificate information must be configured in order for the GWWS server to create an SSL listen endpoint, or to use X.509 certificates for authentication and/or message signature. All GWWS servers defined in the same deployment file share the same certificate settings, including the private key file, trusted certificate directory, and so on.

The private key file is configured using the <Certificate>/<PrivateKey> sub-element. The private key file must be in PEM file format and stored locally. SSL clients can optionally be verified if the <Certificate>/<VerifyClient> sub-element is set to true.

Note: By default, the GWWS server does not verify SSL clients.

If SSL clients are to be verified, and/or the X.509 certificate authentication feature is enabled, a set of trusted certificates must be stored locally and located by the GWWS server. There are two ways to define GWWS server trusted certificates:

1. Include all certificates in one PEM format file and define the file path using the <<Certificate>/<TrustedCert> sub-element.

2. Save separate certificate PEM format files in one directory and define the directory path using the <<Certificate>/<CertPath> sub-element.

Note: The "cn" attribute of a distinguished name is used as a key for certificate lookup. Wildcards used in a name are not supported. Empty subject fields are not allowed. This limitation is also found in Oracle Tuxedo.

Listing 13 shows a SALTDEPLOY file segment configuring GWWS server certificates.

Listing 13 Configuring Certificates In the SALTDEPLOY File

```xml
<Deployment ..>

... <System>

<Certificates>
```
Creating the SALT Deployment File

```xml
<PrivateKey>/home/user/gwws_cert.pem</PrivateKey>
<VerifyClient>true</VerifyClient>
<CertPath>/home/user/trusted_cert</CertPath>
</Certificates>
</System>
</Deployment>

Configuring Plug-in Libraries

A plug-in is a set of functions that are called when the GWWS server is running. SALT provides a plug-in framework as a common interface for defining and implementing plug-ins. Plug-in implementation is carried out through a dynamic library that contains the actual function code. The implementation library can be loaded dynamically during GWWS server start up. The functions are registered as the implementation of the plug-in interface.

In order for the GWWS server to load the library, the library must be specified using the `<Plugin>/<Interface>` element in the SALTDEPLOY file. Listing 14 shows a SALTDEPLOY file segment configuring multiple customized plug-in libraries to be loaded by the GWWS servers.

Listing 14 Configuring Plug-in Libraries In the SALTDEPLOY File

```xml
<Deployment ..>
...
<System>
  <Plugin>
    <Interface lib="plugin_1.so" />
    <Interface lib="plugin_2.so" />
  </Plugin>
</System>
</Deployment>
```

Note: If the plug-in library is developed using the SALT 2.0 plug-in interface, the “id” and “name” attributes for the interface do not need to be specified. These values can be obtained through plug-in interfaces.
For more information, see Using Plug-ins with SALT in Oracle SALT Programming with Web Services.

**Configuring Advanced Web Service Messaging Features**

SALT currently supports the following advanced Web Service Messaging features:

- **Web Service Addressing**
  
  Supports both inbound and outbound asynchronous Web service messaging.

- **Web Service Reliable Messaging**
  
  Supports inbound Web Service reliable message delivery.

- **Message Transmission Optimization Mechanism (MTOM)**
  
  Supports binary attachment in native and external web services.

**Web Service Addressing**

SALT supports Web service addressing for both inbound and outbound services. The Web service addressing (WS-Addressing) messages used by the GWWS server must comply with the Web Service Addressing standard (W3C Member Submission 10 August 2004).

Inbound services do not require specific Web service addressing configuration. The GWWS server accepts and responds accordingly to both WS-Addressing request messages and non WS-Addressing request messages.

Outbound services require Web service addressing configuration as described in the following sections:

- **Configuring the Addressing Endpoint for Outbound Services**
- **Disabling WS-Addressing**

**Configuring the Addressing Endpoint for Outbound Services**

For outbound services, Web service addressing is configured at the Web service binding level. In the SALTDEPLOY file, each GWWS server can specify a WS-Addressing endpoint by using the &lt;WSAddressing&gt; element for any referenced outbound WSBinding object to enable WS-Addressing.

Once the WS-Addressing endpoint is configured, the GWWS server creates a listen endpoint at start up. All services defined in the outbound WSBinding are invoked with WS-Addressing messages.
Configuring Advanced Web Service Messaging Features

Listing 15 shows a SALTDEPLOY file segment enabling WS-Addressing for a referenced outbound Web service binding.

**Listing 15  WS-Addressing Endpoint Defined for Outbound Web Service Binding**

```
<Deployment ..>
  ...
  <WSGateway>
    <GWInstance id="GWWS1">
      ...
      <Outbound>
        <Binding ref="app1:app1_binding">
          <WSAddressing>
            <Endpoint address="https://myhost:8801/app1_async_point">
              <Endpoint use="simpapp_GWWS1_HTTPPort" />
              <Endpoint use="simpapp_GWWS1_HTTPSPort" />
            </WSAddressing>
          </Binding>
        </Binding>
        <Binding ref="app2:app2_binding">
          <WSAddressing>
            <Endpoint address="https://myhost:8802/app2_async_point">
              <Endpoint use="simpapp_GWWS1_HTTPPort" />
              <Endpoint use="simpapp_GWWS1_HTTPSPort" />
            </WSAddressing>
          </Binding>
        </Outbound>
      ...
    </GWInstance>
  </WSGateway>
  ...
</Deployment>
```

**Notes:** In a GWWS server, each outbound Web Service binding can be associated with a particular WS-Addressing endpoint address. These endpoints can be defined with the same
hostname and port number, but the context path portion of the endpoint addresses must be different.

If the external Web service binding does not support WS-Addressing messages, configuring Addressing endpoints may result in run time failure.

**Disabling WS-Addressing**

If you create a WS-Addressing endpoint in the SALTDEPLOY file or not, you can explicitly disable the Addressing capability for particular outbound services in the WSDF. To disable the Addressing capability for a particular outbound service, you should use the property name “disableWSAddressing” with a value set to “true” in the corresponding <Service> definition in the WSDF file. This property has no impact on any inbound services.

Listing 16 shows WSDF file segment disabling Addressing capability.

Listing 16  Disabling Service-Level WS-Addressing

```xml
<Definition ...
   <WSBinding id="simpapp_binding">
     <Servicegroup id="simpapp">
       <Service name="toupper">
         <Property name="disableWSAddressing" value="true" />
       </Service>
       <Service name="tolower" />
     </Servicegroup>
     ....
   </WSBinding>
</Definition>
```

**Web Service Reliable Messaging**

SALT currently supports Reliable Messaging for inbound services only. To enable Reliable Messaging functionality, you must create a Web Service Reliable Messaging policy file and include the policy file in the WSDF. The policy file must comply with the WS-ReliableMessaging Policy Assertion Specification (February 2005).

**Note:** A WSDF containing a Reliable Messaging policy definition should be used by the GWS server for inbound direction only.
Creating the Reliable Messaging Policy File

A Reliable Messaging Policy file is a general WS-Policy file containing WS-ReliableMessaging Assertions. The WS-ReliableMessaging Assertion is an XML segment that describes features such as the version of the supported WS-ReliableMessage specification, the source endpoint’s retransmission interval, the destination endpoint’s acknowledge interval, and so on.

For more information, see the SALT WS-ReliableMessaging Policy Assertion Reference in the SALT Reference Guide.

Listing 17 shows a Reliable Messaging policy file example.

Listing 17  Reliable Messaging Policy File Example

```xml
<?xml version="1.0"?>
<wsp:Policy wsp:Name="ReliableSomeServicePolicy"
 xmlns:wrm="http://schemas.xmlsoap.org/ws/2005/02/rm/policy"
 xmlns:beapolicy="http://www.bea.com/wrm/policy">
  <wrm:RMAssertion>
    <wrm:InactivityTimeout Milliseconds="600000" />
    <wrm:AcknowledgementInterval Milliseconds="2000" />
    <wrm:BaseRetransmissionInterval Milliseconds="500"/>
    <wrm:ExponentialBackoff />
    <beapolicy:Expires Expires="P1D" />
    <beapolicy:QOS QOS="ExactlyOnce InOrder" />
  </wrm:RMAssertion>
</wsp:Policy>
```

Specifying the Reliable Messaging Policy File in the WSDF File

You must reference the WS-ReliableMessaging policy file at the `<Servicegroup>` level in the native WSDF file. Listing 18 shows how to reference the WS-ReliableMessaging policy file.

Listing 18  Reference the WS-ReliableMessaging Policy At the Endpoint Level

```xml
<Definition ...>
  <WSBinding ...>
```
Configuring a SALT Application

<Servicegroup ...
  <Policy location="RMPolicy.xml" />
<Service ...
<Service ...
...
</Servicegroup ...
</WSBinding>
</Definition>

**Note:** Reliable Messaging in SALT does not support process/system failure scenarios, which means SALT does not store the message in a persistent storage area. SALT works in a *direct mode* with the SOAP client. Usually, system failure recovery requires business logic synchronization between the client and server.

**Message Transmission Optimization Mechanism (MTOM)**

SALT supports binary attachments for CARRAY typed buffers or CARRAY fields in fielded buffers (VIEW, VIEW32, FML or FML32). By default binary buffers/fields are base64 encoded. As shown in Listing 19, in order to enable MTOM the configuration must be added to a service or service group in a WSDF file.

**Listing 19** <Policy location="salt:ws-mtom.xml"/>

<Definition ...
<WSBinding id="simpapp_binding">
<Servicegroup id="simpapp">
  <Service name="toupper">
    <Policy location="salt:ws-mtom.xml"/>
  </Service>
  <Service name="tolower" />
</Servicegroup>
....
Configuring Security Features

SALT provides security support at both the transport level and SOAP message level. The following topics explain how to configure security features for each level:

- Configuring Transport-Level Security
- Configuring Message-Level Web Service Security
- Configuring SAML Single Sign-On
- Configuring X.509-Based Authentication

Configuring Transport-Level Security

SALT provides point-to-point security using SSL link-level security and supports HTTP basic authentication mechanisms for both inbound and outbound service authentication.

Setting Up SSL Link-Level Security

To set up link-level security using SSL at inbound endpoints, you can simply specify the endpoint address with prefix “https://”. The GWWS server who uses this inbound endpoint creates SSL listen port and make SSL secured connections with Web Service Clients. SSL features need to specify certificates settings. For more information, see “Configuring Certificates”.

The GWWS server automatically creates SSL secured connection to outbound endpoints that are published with URLs that having prefix “https://”.

Configuring Inbound HTTP Basic Authentication

SALT depends on the Oracle Tuxedo security framework for Web Service client authentication. There is no special SALT configuration required to enable inbound HTTP Basic Authentication. If the Oracle Tuxedo system requires user credentials, HTTP Basic Authentication is an alternative for Web Service client programs to carry user credentials.

The GWWS gateway supports Oracle Tuxedo domain security configuration for the following two authentication patterns:
• Application password (APP_PW)

• User-level authentication (USER_AUTH)

The GWWS server passes the following string from the HTTP header of the client SOAP request for Oracle Tuxedo authentication.

Authorization: Basic <base64Binary of username:password>

The following is an example of a string from the HTTP header:

Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

In this example, the client sends the Oracle Tuxedo username “Aladdin” and the password “open sesame”, and uses this paired value for Oracle Tuxedo authentication.

• Using Application Password (APP_PW)

If Oracle Tuxedo uses APP_PW, then the HTTP username value is ignored and the GWWS server only uses the password string as the Oracle Tuxedo application password to check the authentication.

• Using User-level Authentication (USER_AUTH)

If Oracle Tuxedo uses USER_AUTH, then both the HTTP username and password value are used. In this case, the GWWS server does not check the Oracle Tuxedo application password.

Configuring Outbound HTTP Basic Authentication

SALT supports authentication plug-in development to prepare user credentials for outbound HTTP Basic Authentication. Outbound HTTP Basic Authentication is configured at Endpoint-level. If an outbound Endpoint requires a user profile in the HTTP message, you must specify the HTTP Realm for the HTTP endpoint in the WSDF file. The GWWS server invokes the authentication plug-in library to prepare usernames and passwords, and sends them using HTTP Basic Authentication mechanism in the request message.

Listing 20 shows how to enable HTTP Basic Authentication for the outbound endpoints.

Listing 20   Enabling HTTP Basic Authentication For the Outbound Endpoint

<Definition ...>
<WSBinding id="simpapp_binding">
  <SOAP>
    <AccessingPoints>
Once a service request is sent to an outbound endpoint using `<Realm>` element, the GWWS server passes the Oracle Tuxedo client uid and gid to the authentication plug-in function, so that the plug-in can determine HTTP Basic Authentication username/password according to the Oracle Tuxedo client information. To obtain Oracle Tuxedo client uid / gid for HTTP basic authentication username/password mapping, Oracle Tuxedo security level may also need to be configured in the UBBCONFIG file. For more information, see “Configuring Oracle Tuxedo Security Level for Outbound HTTP Basic Authentication” and “Programming Outbound Authentication Plug-ins” in the SALT Programming Web Services.

**Configuring Message-Level Web Service Security**

SALT supports Web Service Security 1.0 and 1.1 specification for message level security. You can use message-level security in SALT to assure:

- Authentication, by requiring username or X.509 tokens
- Inbound request message integrity, by requiring the soap body signature

**Main Use Cases of Web Service Security**

SALT implementation of the *Web Service Security: SOAP Message Security specification* supports the following use cases:

- Include a token (username, or X.509) in the SOAP message for authentication.
- Include a token (X.509) and the soap body signature in the SOAP message for integrity.
Configuring a SALT Application

Using WS-Security Policy Files
SALT includes a number of WS-Security Policy 1.0 and 1.2 files you can use for message level security use cases.

The WS-Policy files can be found at $TUXDIR/udataobj/salt/policy once you have successfully installed SALT.

Table 8 lists the default WS-Security Policy files bundled by SALT.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>wssp1.0-username-auth.xml</td>
<td>WS-Security Policy 1.0. Plain Text Username Token for Service Authentication</td>
</tr>
<tr>
<td>wssp1.0-x509v3-auth.xml</td>
<td>WS-Security Policy 1.0. X.509 V3 Certificate Token for Service Authentication</td>
</tr>
<tr>
<td>wssp1.0-signbody.xml</td>
<td>WS-Security Policy 1.0. Signature on SOAP:Body for verification of X.509 Certificate Token</td>
</tr>
<tr>
<td>wssp1.2-Wss1.0-UsernameToken-plain-auth.xml</td>
<td>WS-Security Policy 1.2. Plain Text Username Token for Service Authentication</td>
</tr>
<tr>
<td>wssp1.2-Wss1.1-X509V3-auth.xml</td>
<td>WS-Security Policy 1.2. X.509 V3 Certificate Token for Service Authentication</td>
</tr>
<tr>
<td>wssp1.2-signbody.xml</td>
<td>WS-Security Policy 1.2. Signature on SOAP:Body for verification of X.509 Certificate Token</td>
</tr>
</tbody>
</table>

The above policy files (with the exception of the WS-Security Policy 1.2 UserToken file), can be referenced using <Servicegroup> or <Service> elements in the native WSDF file. The WSSP 1.2 UserToken file can only be referenced using <Servicegroup>.

Listing 21 shows a combination of policy assignment making that the service “TOUPPER” requires client send a UsernameToken (in plain text format) and an X509v3Token in request, and also requires the SOAP:Body part of message to be signed with the X.509 token. The sample “wsseapp” shows how to clip the WSSP 1.2 UserToken file used in the <Service> element.
Policy is referred using the "location" attribute of the <Policy> element. A prefix "salt:" means an SALT default bundled policy file is used. User-defined policy file can be used by directly specifying the file path.

Notes: If a policy is referred at the <Servicegroup> level, it applies to all services in this service group.

The "signbody" policy must be used with the attribute "use" set as "input", which specifies the policy applied only for input message. This is necessary because the SOAP:Body of the output message is not signed.

Configuring SAML Single Sign-On

SALT supports SAML 1.1 and SAML 2.0 Single Sign-On (SSO). You can use Single Sign-On to process a secure incoming request by performing authentication on behalf of the end user, without having to request their credentials.

The SALT implementation of SAML SSO supports the sender-vouches confirmation method. With this method, SALT represents a back-end system, and a Web Service intermediary sits between the back-end and the end user. In this case, the Web Service intermediary "vouches" for the end user using SAML token mechanisms.
Note: In order to use SAML SSO, make sure you have correctly configured the `<Certificates>` element in the SALTDEPLOY file.

- Transport Protection
- SAML Key File

Transport Protection
Although it is not required to use TLS/SSL as a transport to carry an SAML security token to access Oracle Tuxedo through GWWS, it is recommended that the Web Service intermediary use TLS/SSL to access Oracle Tuxedo through GWWS using an SAML security token. The use of TLS/SSL ensures the SOAP message content from being disclosed or modified without detection. This is particularly important when accessing Oracle Tuxedo services through a wide area network outside of a fire wall.

SAML Key File
The public key certificate of trusted SAML assertion issuers must be located in the $APPDIR directory. These certificates must be in PEM format. The name of the certificate must reflect the issuer name. For instance, if the issuer id is "ws_1" then the certificate name should be "ws_1.pem".

However, for long issuer names the key file provides the ability to correlate between the real issuer name and its local reference name so that the PEM file name can be much more concise but still remain useful to the administrator.

For example, if the assertion issuer name is web.abc.com/saml/authenticator, then the PEM file name for its public key certificate can be called "abc.pem" instead of "www.abc.com/saml/authenticator.pem".

This is especially useful when in a UNIX environment where the "/" symbol also works as a path separator. This translation is required when confusion like this may arise.

The key file name is fixed to "saml_key.meta". It should be located in the same file folder specified by "CertPath". This file should be protected by the file system and is in XML format.

This section contains the following topics:

- Key File Format
- File Information
- GWWS Key
Configuring Security Features

- Assertion Issuer Information
- Key File Generation
- Procedure to Manage Key File
- WS-Policy Files
- Mapping SAML Elements with Oracle Tuxedo Security

**Key File Format**

The key file is an XML file. There are three types of information stored in this file: file information, GWWS key, and issuer information.

**Note:** You should not modify this file manually since this will cause the file to fail integrity checking.

**File Information**

The file information section contains the version number of the tool generated this file, a random key, administrative password, and digital signature.

**GWWS Key**

This GWWS key section contains one GWWS symmetric key. There can be only one symmetric configured for GWWS to simplify the validation task. This key is encrypted with obfuscated key. This section is optional and is missing if no GWWS symmetric key is configured.

In MP configuration with multiple GWWS on different machine nodes, this file needs to be replicated on each node; however, if a different GWWS key is desired, then a similar key file but with a different GWWS key record can be copied to a different node.

**Assertion Issuer Information**

This section contains multiple records, one for each trusted assertion issuer. It contains issuer identifier, local issuer identifier, symmetric key, and whether a public key certificate also exists or not.

The issuer identifier is the value presented in the "issuer" attribute of "<saml:Assertion>" element in the WSSE security header.

The local issuer identifier is the abbreviated name for the issuer. The purpose is to make any long issuer identifier become shorter and easier to memorize, but still remain locally unique. This data is optional; if it exists and a certificate also exists, then the certificate must take the name of this local issuer identifier with ‘pem” as file extension.
Configuring a SALT Application

The symmetric key is the shared secret that issuer used to sign the assertion. This data is optional. The length of the key also dictates which algorithm can be used for signing.

The public key certificate exists field tells whether a public key certificate exists. If it exists, the certificate should be located in the folder specified by the "CertPath" element. This field can be true while the symmetric key field also exists. At runtime, GWWS detects which key to use to validate the signature.

**Key File Generation**

A new command is added to *wsadmin* to manage the key file. This new command is used to generate new key file, add new record, delete existing record, and modify record. The name of the file it managed is "saml_key.meta" in the current working directory.

To create the key file issues the following *wsadmin* command:

```bash
saml create -p password
```

Where the "-p password" is for the administrative password to access the newly created key file. A key file with name "saml_key.meta" is created in the current working directory.

To add a trusted issuer, input the following command:

```bash
saml add -i -n authority.abc.com -l abc -c -p password
```

Where "-i" tells it to add an issuer with name "authority.abc.com" with short local reference name "abc" and the access password to access the key file. The key file "saml_key.meta" must exist in current working directory. Since "-c" option is given, a public key certificate named "abc.pem" must exist in the "CertPath".

For more information, see *wsadmin* the SALT Command Reference.

**Procedure to Manage Key File**

The following procedure describes a SALT administrator setting up GWWS to be able to handle SAML assertion for the first time.

1. Change directory to `/APPDIR` and start *wsadmin*.
2. Use "saml create" command to create the key file.
3. Use "saml add -g" command to add GWWS record.
4. Use "saml add -i" command to add trusted assertion issuer record for every trusted assertion issuer.
5. Copy the file "saml_key.meta" to the directory described in the SALT deployment descriptor file "CertPath" element under "Certificate".
6. Change directory to Oracle Tuxedo application domain, and use "tmboot -y" to boot the Oracle Tuxedo application domain.

In MP mode configuration, it is possible to have a different GWWS record in the key file for a different GWWS instance. The following procedure creates the key file for a GWWS instance on a different node.

1. Copy the original key file to different directory or machine.
2. Use "saml delete -g" to delete existing GWWS record.
3. Use "saml add -g" to add a different GWWS record.

**WS-Policy Files**

SALT includes a number of WS-Policy files that you can use for configuring services for SAML SSO as listed in Table 9

<table>
<thead>
<tr>
<th>File Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wssp1.2-2007-Saml1.1-SenderVouches-Https.xml</td>
<td>SAML 1.1 support (with SSL)</td>
</tr>
<tr>
<td>Wssp1.2-2007-Saml2.0-SenderVouches-Https.xml</td>
<td>SAML 2.0 support (with SSL)</td>
</tr>
<tr>
<td>Wssp1.2-2007-Saml1.1-SenderVouches.xml</td>
<td>SAML 1.1 support (without SSL)</td>
</tr>
<tr>
<td>Wssp1.2-2007-Saml2.0-SenderVouches.xml</td>
<td>SAML 2.0 support (without SSL)</td>
</tr>
</tbody>
</table>

The above files can be referenced at the `<ServiceGroup>` or `<Service>` level in the native WSDF file.

This policy may be combined with other WS-Security policies (such as inbound body signature). For more information, see Configuring Message-Level Web Service Security.

For example, Listing 22 shows the SAML 1.1 policy file with supported capabilities outlined.

**Listing 22  SAML 1.1 Policy File**

```xml
<?xml version="1.0"?>
```
Configuring a SALT Application

```xml
    xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
  <sp:AsymmetricBinding>
    <wsp:Policy>
      <sp:InitiatorToken>
        <wsp:Policy>
          <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Always">
            <wsp:Policy>
              <sp:WssX509V3Token/>
            </wsp:Policy>
          </sp:X509Token>
        </wsp:Policy>
      </sp:InitiatorToken>
    </wsp:Policy>
  </sp:AsymmetricBinding>
  <sp:AlgorithmSuite>
    <wsp:Policy>
      <sp:Basic256/>
    </wsp:Policy>
  </sp:AlgorithmSuite>
  <sp:Layout>
    <wsp:Policy>
      <sp:Lax/>
    </wsp:Policy>
  </sp:Layout>
  <sp:IncludeTimestamp/>
  <sp:ProtectTokens/>
</wsp:Policy>
```
Mapping SAML Elements with Oracle Tuxedo Security

Table 10 lists what optional SAML assertion elements must present.

Table 10  Optional SAML Assertion Elements

<table>
<thead>
<tr>
<th>Oracle Tuxedo SECURITY Level</th>
<th>Additional SAML Assertion Elements Required</th>
<th>Access Principal</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>None</td>
<td>Anonymous, Subject/NameID</td>
</tr>
<tr>
<td>APP_PW</td>
<td>None</td>
<td>Anonymous, Subject/NameID</td>
</tr>
<tr>
<td>USER_PW</td>
<td>Subject</td>
<td>Subject/NameID</td>
</tr>
<tr>
<td>ACL</td>
<td>Subject</td>
<td>Subject/NameID</td>
</tr>
<tr>
<td>MANDATORY_ACL</td>
<td>Subject</td>
<td>Subject/NameID</td>
</tr>
</tbody>
</table>

In NONE and APP_PW cases, if the optional element "Subject" exists, then "NameID" is used to access Oracle Tuxedo. If the optional element "Subject" does not exist, then the client assumes anonymous user identity to access Oracle Tuxedo. If the anonymous access is not allowed (i.e. no credential mapping for anonymous), then the request fails.
Configuring X.509-Based Authentication

A X.509 V3 public key certificate is required for X.509 based authentication for an outbound GWWS SOAP message. The public key certificate used for this purpose can be configured as either one certificate for all the requests targeted for the same Web Service or per request invocation if Tuxedo SECURITY is set at USER_AUTH or higher. In the later case, the certificate must have the same name as the Tuxedo user identification or the mapped remote user name if identity mapping plug-in is installed.

The configured X.509 public key certificate will be used for:

1. Mutual Authentication for Transport Layer security (i.e. SSL/TLS)
2. Message signing
3. Part of the SOAP message that can be used to authenticate user at message-level (as oppose to transport layer)

Whether all 3 tasks will be performed or only partial of the 3 tasks depends on the WS policy used by the Web Service.

Since message encryption will not be supported as it is not required it is recommended to use SSL/TLS as the preferred transport mechanism to protect the integrity and privacy of the message. The X.509 Public Key certificate used for SSL/TLS can be different from the one used for signing depends on how user configure it.

When GWWS received a request from client it will process the message, optionally it will sign the message and attach the certificate as the binary security token to the SOAP request message if WS policy requires it; and then send the request to remote Web Service through SSL/TLS. Depends on the WS policy this SSL/TLS connection can be either one-way or two-way SSL. During the SSL/TLS connection establishing process the application server will validate the client certificate if the connection is two-way SSL; and forward the request to Web Service.

When Web Service received the request it will validate the certificate, verify the signature if Web Service requires it. If the request is good it will send reply back. The reply send back by Web Service may be also signed depends on WS policy.

When GWWS received the reply it will forward reply back to actual SALT client. In the case that reply is signed GWWS will validate the certificate and verify the signature before forwarding the reply back to SALT client.
Listing 23  SOAP message based on X.509 Authentication

```xml
<S11:Envelope xmlns:S11="…” ">
  <S11:Header>
    <wsse:Security xmlns:wsse="…” xmlns:wsu="…”>
      <wsse:BinarySecurityToken
          wsu:id="binarytoken"
          ValueType="wsse:X590v3"
          EncodingType="wsse:Base64Binary">
        MIIEzzCCA9CgAwIBAgIQEmtJZc0...
      </wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:Reference URI="#body">…</ds:Reference>
          <ds:Reference URI="#binarytoken">…</ds:Reference>
        </ds:SignedInfo>
        ...
      </ds:Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body" xmlns:wsu="…”>
    ...
  </S11:Body>
</S11:Envelope>
```

For user to successfully access Web Service through GWWS user must configure a valid client certificate and private key that is accessible to GWWS at runtime. This certificate and private
key can be used by transport level security or message level security, or even both depend on Web Service' requirement.

Currently Tuxedo SALT only support single certificate which is configured through the "System" element in the deployment descriptor, with this limitation all the requests going through different instances of GWWS gateway will use same certificate to establish SSL/TLS connection. Invariably, in the eyes of the Web Service they all come from the same user; thus same access privilege. This new feature will remove this constraint and make it possible to use different certificate to represent different client or gateway.

SALT configuration consists of a deployment descriptor (DEP) and multiple web service definition files (WSDF). This new feature will use "Property" to configure default user identity to be used for this purpose, or to instruct GWWS to how to use filters/mappers to map Tuxedo user identity to a X.509 certificate. The "Property" which is used for configuration is an XML element that is available as configurable child element to both "GWInstance" and "Service". "GWInstance" is configured in SALT deployment descriptor while "Service" is configured in SALT web service definition file.

When a Web Service' WS-Security policy requires message level security, GWWS will use the private key to perform message signing, and attach the certificate to the SOAP message as Binary Security Token to be used by target Web Service to validate the message and authenticate the user. Otherwise, it will only use the certificate and private key to create a secured transport layer connection, i.e. SSL/TLS.

Whether a service request will use "X.509" security token for user identity is determined by the WS Security Policy associated with the Web Service.

Note: This feature only supports X.509 V3 Public Key Certificate; other versions are not supported

Certificate Sources

The X.509 V3 Public Key Certificate used for message level security can come from one of the following sources:

1. The X.509 Certificate configured for the transport security.
2. The X.509 Certificate associates with a particular instance of GWWS gateway.
3. The X.509 Certificate associates with the preset principal of the Web Service.
4. The X.509 Certificates associate with SALT clients.
Properties
There are three new properties added to the configuration to aid different security configurations. All 3 properties are available in "GWInstance" and "Service". The "Service" element is available in WSDF, and the "GWInstance" is available in SALT deployment descriptor.

- defaultClientIdentification
- useSingleClientIdentification
- allowAnonymousAccess

defaultClientIdentification
This property defines the default client name to be used for X.509 certificate lookup. The one configured in the "Service" has precedence over the one configured in "GWInstance". The following example shows the effective default client name will be "catalina" for service "GetData".

Listing 24

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!- Sample.wsdf
 -->
<Definition ...>
  <WSBinding id="sample_Binding">
    <SOAP>
      <AccessingPoints>
        ...
      </AccessingPoint>
    </SOAP>
  </WSBinding>
  <ServiceGroup id="SampleSrvGrp">
    <Service name="GetData">
      <Property name="defaultClientIdentification" value="catalina"/>
    </Service>
  </ServiceGroup>
</Definition>
```
Configuring a SALT Application

Listing 25

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!- sample.dep
-->
  <WSDF>
    <Import location="c:/salt/x.509/Sample.wsdf"></Import>
  </WSDF>
  <WSGateway>
    <GWInstance id="INSTANCE1">
      <Outbound>
        ...
      </Outbound>
      <Properties>
        <Property name="defaultClientIdentification" value="melbourne"/>
      </Properties>
    </GWInstance>
  </WSGateway>
  <System>
    <Certificate>
      ...
    </Certificate>
  </System>
</Deployment>
```
For all other services provided by GWWS instance "INSTANCE1" without their own "defaultClientId" configured then they will use the default client id of the GWWS and in this case it will be "melbourne".

**useSingleClientIdentification**

"useSingleClientIdentification" tells whether it is desirable for any Web Service use the same client X.509 certificate. When the decision is to enable this filter then all the SALT client request will use the identity configured in "defaultClientIdentification", if "defaultClientIdentification" is not configured then it is a configuration error and "wsloadcf" will issue an error. By default it is disabled.

This filter only affects the runtime client X.509 certificate selection when Tuxedo "SECURITY" is configured at least at "USER_AUTH" level. If Tuxedo SECURITY is configured as "NONE" or "APP_PW" then this filter will not be used for client certificate selection. The error condition described in previous paragraph will still be true even if this attribute is disabled at runtime.

The following is the matrix table for decision to enable this single client identification filter.

### Table 11  Single Client Identification Filter Matrix

<table>
<thead>
<tr>
<th>Service</th>
<th>GWInstance</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unconfigured</td>
<td>Unconfigured</td>
<td>Disable</td>
</tr>
<tr>
<td>Unconfigured</td>
<td>Configured TRUE</td>
<td>Enable</td>
</tr>
<tr>
<td>Unconfigured</td>
<td>Configured FALSE</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configure TRUE</td>
<td>Unconfigured</td>
<td>Enable</td>
</tr>
<tr>
<td>Configure TRUE</td>
<td>Configured TRUE</td>
<td>Enable</td>
</tr>
<tr>
<td>Configure TRUE</td>
<td>Configured FALSE</td>
<td>Enable</td>
</tr>
<tr>
<td>Configure FALSE</td>
<td>Unconfigured</td>
<td>Disable</td>
</tr>
</tbody>
</table>
Configuring a SALT Application

Table 11 Single Client Identification Filter Matrix

<table>
<thead>
<tr>
<th>Service</th>
<th>GWInstance</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure FALSE</td>
<td>Configured TRUE</td>
<td>Disable</td>
</tr>
<tr>
<td>Configure FALSE</td>
<td>Configured FALSE</td>
<td>Disable</td>
</tr>
</tbody>
</table>

The example in the previous section will have this filter "disabled" since both places omitted this property. The following example will have this filter "enabled".

Listing 26

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!-- Sample.wsdf

<Definition _>

<WSBinding id="sample_Binding">
  <SOAP>
    <AccessingPoints>
      ...
    </AccessingPoints>
  </SOAP>
  <ServiceGroup id="SampleSrvGrp">
    <Service name="GetData">
      <Property name="defaultClientIdentification" value="catalina"/>
      <Property name="useSingleClientIdentification" value="true" />
    </Service>
  </ServiceGroup>
</WSBinding>
```
Listing 27

<?xml version="1.0" encoding="UTF-8"?>
<!- sample.dep
-->
    <WSDF>
        <Import location="c:/salt/x.509/Sample.wsdf"></Import>
    </WSDF>
    <WSGateway>
        <GWInstance id="INSTANCE1">
            <Outbound>
                ...
            </Outbound>
            <Properties>
                <Property name="defaultClientIdentification" value="melbourne"/>
            </Properties>
        </GWInstance>
    </WSGateway>
    <System>
        <Certificate>
            ...
        </Certificate>
    </System>
</Deployment>
allowAnonymousAccess

This property only affects the X.509 certificate selection when Tuxedo SECURITY is configured at least at "USER_AUTH" level. This property allows users without their own X.509 certificate to use a default client identification when access a Web Service. By default it is disabled.

The following is the matrix table for decision to enable this anonymous client access filter.

Table 12  Anonymous Client Access Filter Matrix

<table>
<thead>
<tr>
<th>Service</th>
<th>GWInstance</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unconfigured</td>
<td>Unconfigured</td>
<td>Disabled</td>
</tr>
<tr>
<td>Unconfigured</td>
<td>Configured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unconfigured</td>
<td>Configured</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configure TRUE</td>
<td>Unconfigured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configure TRUE</td>
<td>Configured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configure TRUE</td>
<td>Configured</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configure FALSE</td>
<td>Unconfigured</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configure FALSE</td>
<td>Configured</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configure FALSE</td>
<td>Configured</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

If the decision is to enable this filter then "defaultClientIdentification" must be configured; if "defaultClientIdentivation" is not configured then "wsloadcf" will fail and return an error.

The following is the sample configuration.
Listing 28

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!- Sample.wsdf -->
<Definition ...>
  <WSBinding id="sample_Binding">
    <SOAP>
      <AccessingPoints>
        ...
      </AccessingPoints>
    </SOAP>
    <Servicegroup id="SampleSrvGrp">
      <Service name="GetData">
        <Property name="defaultClientIdentification" value="catalina"/>
        <Property name="allowAnonymousAccess" value="true" />
      </Service>
    </Servicegroup>
  </WSBinding>
</Definition>
```

Listing 29

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!- sample.dep -->
  <WSDF>
```

Configuring Security Features
Compiling a SALT Application

<Import location="c:/salt/x.509/Sample.wsdf"></Import>
</WSDF>
<WSGateway>
  <GWInstance id="INSTANCE1">
    <Outbound>
      ...
    </Outbound>
  </GWInstance>
  <Properties>
    <Property name="defaultClientIdentification" value="melbourne"/>
    <Property name="allowAnonymousAccess" value="false" />
  </Properties>
</GWInstance>
</WSGateway>
<System>
  <Certificate>
    ...
  </Certificate>
</System>
</Deployment>

Compiling SALT Configuration

Compiling a SALT configuration file means generating a binary version of the file (SALTCONFIG) from the XML version SALTDEPLOY file. To compile a configuration file, run the wsloadcf command. wsloadcf parses a deployment file and loads the binary file.

wsloadcf reads a deployment file and all imported WSDF files and WS-Policy files referenced in the deployment file, checks the syntax according to the XML schema of each file format, and optionally loads a binary configuration file called SALTCONFIG. The SALTCONFIG and
Configuring the UBBCONFIG File for SALT

(Optionally) `SALTOFFSET` environment variables point to the `SALTCONFIG` file and (optional) offset where the information should be stored.

`wsloadcf` validates the given SALT configuration files according to the predefined XML Schema files. XML Schema files needed by SALT can be found at directory: `$/TUXDIR/udataobj/salt`.

`wsloadcf` can execute for validating purpose only without generating the binary version `SALTCONFIG` once option `"-n"` is specified.

For more information, see `wsloadcf` reference in the SALT Reference Guide.

Configuring the UBBCONFIG File for SALT

After configuring and compiling the SALT configuration, the Oracle Tuxedo `UBBCONFIG` file needs to be updated to apply SALT components in the Oracle Tuxedo application. Table 13 lists the `UBBCONFIG` file configuration tasks for SALT.

<table>
<thead>
<tr>
<th>Configuration Tasks</th>
<th>Required</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the TMMETADATA Server in the *SERVERS Section</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configuring the GWWS Servers in the *SERVERS Section</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Updating System Limitations in the UBBCONFIG File</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configuring Certificate Password Phrase For the GWWS Servers</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configuring Oracle Tuxedo Authentication for Web Service Clients</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configuring Oracle Tuxedo Security Level for Outbound HTTP Basic Authentication</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the TMMETADATA Server in the *SERVERS Section

SALT requires at least one `TMMETADATA` server defined in the `UBBCONFIG` file. Multiple `TMMETADATA` servers are also allowed to increase the throughput of accessing the Oracle Tuxedo service definitions.

Listing 30 lists a segment of the `UBBCONFIG` file that shows how to define `TMMETADATA` servers in an Oracle Tuxedo application.
Configuring a SALT Application

### Listing 30  TMMETADATA Servers Defined In the UBBCONFIG File *SERVERS Section

```
......
*SERVERS
TMMETADATA SRVGRP=GROUP1 SRVID=1
  CLOPT="-A -- -f domain_repository_file -r"
TMMETADATA SRVGRP=GROUP1 SRVID=2
  CLOPT="-A -- -f domain_repository_file"
......
```

**Note:** Maintaining only one Service Metadata Repository file for the entire Oracle Tuxedo domain is highly recommended. To ensure this, multiple **TMMETADATA** servers running in the Oracle Tuxedo domain must point to the same repository file.

For more information, see “Managing The Tuxedo Service Metadata Repository” in the Oracle Tuxedo documentation.

### Configuring the GWWS Servers in the *SERVERS Section

To boot GWWS instances defined in the SALTDEPLOY file, the **GWWS** servers must be defined in the *SERVERS section of the UBBCONFIG file. You can define one or more **GWWS** server instances concurrently in the UBBCONFIG file. Each **GWWS** server must be assigned with a unique instance id with the option “-i” within the Oracle Tuxedo domain. The instance id must be present in the XML version SALTDEPLOY file and the generated binary version SALTCONFIG file.

**Listing 31** lists a segment of the UBBCONFIG file that shows how to define **GWWS** servers in an Oracle Tuxedo application.

### Listing 31  GWWS Servers Defined In the UBBCONFIG File *SERVERS Section

```
......
*SERVERS
GWWS SRVGRP=GROUP1 SRVID=10
  CLOPT="-A -- -i GW1"
GWWS SRVGRP=GROUP1 SRVID=11
  CLOPT="-A -- -i GW2"
GWWS SRVGRP=GROUP2 SRVID=20
```
CLOPT="-A -- -c saltconf_2.xml -i GW3"

For more information, see “GWWS” in the Oracle SALT Reference Guide.

**Notes:** Be sure that the TMMETADATA system server is set up in the UBBCONFIG file to start before the GWWS server boots. Because the GWWS server calls services provided by TMMETADATA, it must boot after TMMETADATA.

To ensure TMMETADATA is started prior to being called by the GWWS server, put TMMETADATA before GWWS in the UBBCONFIG file or use SEQUENCE parameters in *SERVERS definition in the UBBCONFIG file.

SALT configuration information is pre-compiled with wsloadcf to generate the SALTCONFIG file binary. GWWS server reads the SALTCONFIG file at start up. The SALTCONFIG environment variable must be set correctly with the SALTCONFIG file entity before booting GWWS servers.

Option “-c” is deprecated in the current version SALT. In SALT 1.1 release, option “-c” is used to specify SALT 1.1 configuration file for the GWWS server. In SALT 2.0, GWWS server reads SALTCONFIG file at start up. GWWS server specified with this option can be booted with a warning message to indicate this depreciation. The specified file can be arbitrary and is not read by the GWWS server.

**Updating System Limitations in the UBBCONFIG File**

When configuring the Oracle Tuxedo domain with SALT GWWS servers, you must plan and update Oracle Tuxedo system limitations defined in the UBBCONFIG file according to your SALT application requirements.

**Tip:** Define an adequate MAXSERVERS number in the *RESOURCES section

SALT requires the following system servers to be started in an Oracle Tuxedo domain: TMMETADATA and GWWS. The number of TMMETADATA and GWWS server must be accounted for in the MAXSERVERS value.

**Tip:** Define an adequate MAXSERVICES number in the *RESOURCES section
When the GWWS server working in the outbound direction, external wsdl operations are mapped with Oracle Tuxedo services and advertised via the GWWS servers. The number of the advertised services by all GWWS servers must be accounted for in the MAXSERVICES value.

**Tip:** Define an adequate MAXACCESSERS number in the *RESOURCES section

The MAXACCESSERS value is used to specify the default maximum number of clients and servers that can be simultaneously connected to the Oracle Tuxedo bulletin board on any particular machine in this application. The number of TMMETADATA and GWWS server, maximum concurrent Web Service client requests must be accounted for in the MAXACCESSERS value.

**Tip:** Define an adequate MAXWSCLIENTS number in the *MACHINES section

When the GWWS server operating in the inbound direction, each Web Service client is deemed a workstation client in the Oracle Tuxedo system; therefore, MAXWSCLIENTS must be configured with a valid number in the UBBCONFIG file for the machine where the GWWS server is deployed. The number is shared.

Configuring Certificate Password Phrase For the GWWS Servers

Configuring a security password phrase is required when setting up certificates for SALT. The certificates setting is desired when the GWWS servers enable SSL link-level encryption and/or Web Service Security X.509 Token and signature features. The certificate private key file must be created and encrypted with a password phrase.

When GWWS servers are specified with certificate-related features, they are required to read the private key file and decrypt it using the password phrase. To configure a password phrase for each GWWS server, the keywords SEC_PRINCIPAL_NAME and SEC_PRINCIPAL_PASSVAR must be specified under each desired GWWS server entry in the *SERVERS section. During compiling the UBBCONFIG file with tmloadcf, the administrator must type the password phrase, which can be used to decrypt the private key file correctly.

**Note:** Only one private key file can be specified in the SALT deployment file. All the GWWS servers defined in the SALT deployment file must be provided the same password phrase for the private key file decryption.

Listing 32 shows a segment of the UBBCONFIG file that defines a security password phrase for the GWWS servers.
**Listing 32**  Security Password Phrase Defined in the UBBCONFIG File For the GWWS Servers

```
.....
*SERVERS
GWWS SRVGRP=GROUP1 SRVID=10
  SEC_PRINCIPAL_NAME="gwws_certkey"
  SEC_PRINCIPAL_VAR="gwws_certkey"
  CLOPT="-A -- -i GW1"
GWWS SRVGRP=GROUP1 SRVID=11
  SEC_PRINCIPAL_NAME="gwws_certkey"
  SEC_PRINCIPAL_PASSVAR="gwws_certkey"
  CLOPT="-A -- -i GW2"
.....
```

For more information, see **UBBCONFIG(5)** in the Oracle Tuxedo 12cR2 documentation.

**Configuring Oracle Tuxedo Authentication for Web Service Clients**

SALT GWWS servers rely on Oracle Tuxedo authentication framework to check the validity of the Web Service clients. If your existing Oracle Tuxedo application is already applied, Web Service clients must send user credentials using one of the following:

- HTTP Basic Authentication in the HTTP message header
- Web Service Security Username Token in the SOAP message header

Contrarily, if you want to authenticate Web Service clients for SALT, you must configure Oracle Tuxedo authentication in the Oracle Tuxedo domain.

For more information, see **Administering Authentication** in the *Oracle Tuxedo 12cR2 Documentation*.

**Configuring Oracle Tuxedo Security Level for Outbound HTTP Basic Authentication**

To obtain Oracle Tuxedo client *uid/gid* for outbound HTTP Basic Authentication *username/password* mapping, you must configure the Oracle Tuxedo Security level as **USER_AUTH, ACL** or **MANDATORY_ACL** in the **UBBCONFIG** file.
Listing 33 shows a segment of the UBBCONFIG file that defines security-level ACL in the UBBCONFIG file.

Listing 33  Security-Level ACL Defined in the UBBCONFIG File For Outbound HTTP Basic Authentication

*RESOURCES
IPCKEY ... 
......
SECURITY ACL
......

Configuring SALT In Oracle Tuxedo MP Mode

To set up GWWS servers running on multiple machines within an MP mode Oracle Tuxedo domain, each Oracle Tuxedo machine must be defined with a separate SALTDEPLOY file and a set of separate other components.

You must propagate the following global resources across different machines:

- Certificates.

  Private key file and the trusted certificate files must be accessible from each machine according to the settings defined in the SALTDEPLOY file.

- Plug-in load libraries.

  Plug-in shared libraries must be compiled on each machine and must be accessible according to the settings defined in the SALTDEPLOY file.

You may define two GWWS servers running on different machine with the same functionality by associating the same WSDF files. But it requires manual propagation of the following artifacts:

- The WSDF files
- The WS-Policy files
- FML32 field table definition files if Oracle Tuxedo Services consume FML32 typed buffers
- XML Schema files excerpted by wsd1cvt.
Migrating from SALT 1.1

This section describes the following two possible migrating approaches for SALT 1.1 customers who plan to upgrade to SALT 2.0 release:

- Running GWWS servers with SALT 1.1 Configuration File
- Adopting SALT 2.0 Configuration Style by Converting SALT 1.1 Configuration File

Running GWWS servers with SALT 1.1 Configuration File

After upgrading from SALT 1.1 to SALT 2.0 release, you may still want to run your existing SALT applications with the original SALT 1.1 configuration file. This is supported in SALT 2.0.

The SALT configuration compiler utility, wsloadcf, supports loading the binary version SALTCONFIG from one SALT 1.1 format configuration file.

To run SALT 2.0 GWWS servers with SALT 1.1 configuration file, you must perform the following steps:

1. Load the binary version SALTCONFIG from the SALT 1.1 format configuration file via wsloadcf.
2. Set the SALTCONFIG environment variable before booting the GWWS servers.
3. Boot the GWWS servers associated with this SALT 1.1 configuration file.

Note: If you have more than one SALT 1.1 configuration files defined in an Oracle Tuxedo domain, you must follow steps 1 - 3 to generate more binary SALTCONFIG files and boot corresponding GWWS servers.

Adopting SALT 2.0 Configuration Style by Converting SALT 1.1 Configuration File

When wsloadcf loads a binary SALTCONFIG from a SALT 1.1 configuration file, it also converts this SALT 1.1 configuration file into one WSDF file and one SALTDEPLOY file.

It is highly recommended to start using the SALT 2.0 styled configuration once you get the converted files from SALT 1.1 configuration. If you want to incorporate more than one SALT 1.1 configuration file into one SALT 2.0 deployment, you must manually edit the SALTDEPLOY file for importing the other WSDF files.

Listing 34 shows the converted SALTDEPLOY file and WSDF file from a given SALT 1.1 configuration file.
Configuring a SALT Application

Listing 34  A Sample of SALT 1.1 Configuration File (simpapp.xml)

```
<Configuration xmlns="http://www.bea.com/Tuxedo/Salt/200606">
  <Servicelist id="simpapp">
    <Service name="toupper" />
    <Service name="tolower" />
  </Servicelist>
  <Policy />
  <System />
  <WSGateway>
    <GWInstance id="GWWS1">
      <HTTP address="/127.0.0.1:7805" />
      <HTTPS address="127.0.0.1:7806" />
      <Property name="timeout" value="300" />
    </GWInstance>
  </WSGateway>
</Configuration>
```

The converted SALT 2.0 WSDF file and deployment file are shown in Listing 35 and Listing 36 respectively.

Listing 35  Converted WSDF File for SALT 1.1 Configuration File (simpapp.xml.wsdf)

```
<Definition name="simpapp" wsdlNamespace="urn:simpapp.wsd1" xmlns="http://www.bea.com/Tuxedo/WSDF/2007">
  <WSBinding id="simpapp_binding">
    <Servicegroup id="simpapp">
      <Service name="toupper" />
      <Service name="tolower" />
    </Servicegroup>
    <SOAP>
      <AccessingPoints>
        <Endpoint id="simpapp_GWWS1_HTTPPort"
          address=http://127.0.0.1:7805/simpapp />
        <Endpoint id="simpapp_GWWS1_HTTPSPort"
          address="https://127.0.0.1:7806/simpapp />
      </AccessingPoints>
    </SOAP>
  </WSBinding>
</Definition>
```
Configuring Service Contract Discovery

When discovery is activated for a service, the server that provides the service collects service contract information and sends the information to an internal service implemented by TMMETADATA(5). The same service contract is only sent once to reduce communication overhead.

Listing 36  Converted SALTDDEPLOY File for SALT 1.1 Configuration File (simpapp.xml.dep)

  <WSDF>
    <Import location="/home/myapp/simpapp.wsdf" />
  </WSDF>
  <WSGateway>
    <GWInstance id="GWWS1">
      <Inbound>
        <Binding ref="simpapp:simpapp_binding">
          <Endpoint use="simpapp_GWWS1_HTTPPort" />
          <Endpoint use="simpapp_GWWS1_HTTPSPort" />
        </Binding>
      </Inbound>
      <Properties>
        <Property name="timeout" value="300" />
      </Properties>
    </GWInstance>
  </WSGateway>
</Deployment>
The **TMMETADATA** server summarizes the collected data and generates a service contract. The contract information can either be stored in the metadata repository, or output to a text file (which is then loaded to the metadata repository using `tmloadrepos`). SALT uses the `tmscd` command to control the service contract runtime collection. For more information, see `tmscd` in the SALT Command Reference Guide.

Generated service contract information contains the service name, request buffer information, response buffer information, and error buffer information if there is a failure. The collected service contract information is discarded if it fails to send information to the **TMMETADATA** server. The buffer information includes buffer type and subtype, and field information for FML/FML32 (`name,type,subtype`). Discovery is supported for any embedded buffer in FML32 buffer. For FML/FML32 field occurrences, the discovery automatically updates the pattern for the `count(requiredcount)` in metadata repository. Field occurrence does not impact the pattern, but the minimum occurrence is the "requiredcount". The maximum occurrence is the "count" of the entire contract discovery period.

For VIEW/VIEW32/X_C_TYPE/X_COMMON, only the view name is discovered. SALT can generate a detailed description by view name when using metadata repository.

**Note:** Patterns flagged with `autodiscovery` (see Table 14) are compared. If the same `autodiscovery` pattern already exists in the metadata repository, then the newer pattern is ignored.

Only application ATMI services (local, or imported via `/TDOMAIN` gateway) are supported. Service contract discovery does not support the following services:

- system services (name starts with '.' or '..')
- conversational services
- CORBA services
- `/Q and SALT proxy services

**Note:** Services without a reply are mapped as "oneway" services in the metadata repository.

**tpforward Support**

If a service issues `tpforward()` instead of `tpreturn()`, its reply buffer information is the same as the reply buffer of the service which it forwards to. For example:

- client calls SVCA with a STRING typed buffer
SVCA processes the request, and then creates a new FML32 typed buffer as the request is forwarded to SVCB.

SVCB handles the request and returns a STRING buffer to the client. The SVCA contract is STRING+STRING. The SVCB contract is FML32+STRING.

**Service Contract Text File Output**

If you want collected service contract discovery information logged to a file instead of directly to the metadata repository, you must use the `TMMETADATA(5) -o<filename>` option and then use `tmloadrepos` to manually load the file to the metadata repository. For more information, see `tmloadrepos` in the Oracle Tuxedo Command Reference Guide.

The output complies with the format imposed by `tmloadrepos` if a file is used as storage instead of the metadata repository. The file contains a service header section and a parameter section for each parameter. Service header contains items listed in Table 14. The "service" field format is `<TuxedoServiceName>+'_'+<SequenceNo>`. The suffix `<SequenceNo>` is used to avoid name conflict when multiple patterns are recognized for an Oracle Tuxedo service.

**Note:** `<SequenceNo>` starts from the last `<SequenceNo>` number already stored in the metadata repository.

Service parameter contains information is listed in Table 15.

**Table 14  Service Level Attributes**

<table>
<thead>
<tr>
<th>Keyword (abbreviation)</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service(sv)</td>
<td>TOUPPER_1</td>
<td>&lt;RealServiceName&gt;_&lt;SequenceNo&gt;.</td>
</tr>
<tr>
<td>tuxservice(tsv)</td>
<td>TOUPPER</td>
<td>The service name.</td>
</tr>
<tr>
<td>servicetype(st)</td>
<td>service</td>
<td>oneway</td>
</tr>
<tr>
<td>inbuf(bt)</td>
<td>STRING</td>
<td>FML, FML32, VIEW, VIEW32, STRING, CARRAY, XML, X_OCTET, X_COMMON, X_C_TYPE, MBSTRING or other arbitrary string representing an application defined custom buffer type.</td>
</tr>
</tbody>
</table>
### Table 14 Service Level Attributes

<table>
<thead>
<tr>
<th>Keyword (abbreviation)</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outbuf (BT)</td>
<td>FML32</td>
<td>set to &quot;NULL&quot; if it is an error reply.</td>
</tr>
<tr>
<td>errbuf (ebt)</td>
<td>STRING</td>
<td>present only when it is an error reply.</td>
</tr>
<tr>
<td>inview</td>
<td></td>
<td>View name. Present only when inbuf is of type VIEW or VIEW32.</td>
</tr>
<tr>
<td>outview</td>
<td></td>
<td>View name. Present only when outbuf is of type VIEW or VIEW32.</td>
</tr>
<tr>
<td>errview</td>
<td></td>
<td>View name. Present only when errbuf is of type VIEW or VIEW32.</td>
</tr>
<tr>
<td>autodiscovery</td>
<td>true</td>
<td>Set to &quot;true&quot;.</td>
</tr>
</tbody>
</table>

### Table 15 Parameter Level Attributes

<table>
<thead>
<tr>
<th>Keyword (abbreviation)</th>
<th>Sample</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>param (pn)</td>
<td>USER_INFO</td>
<td></td>
</tr>
<tr>
<td>paramdescription (pd)</td>
<td>service parameter</td>
<td></td>
</tr>
<tr>
<td>access (pa)</td>
<td>in</td>
<td>A combination of {in} {out} {err}.</td>
</tr>
<tr>
<td>type (pt)</td>
<td>.fml32</td>
<td>byte, short, integer, float, double, string, carray, dec_t, xml, ptr, fml32, view32, mbstring.</td>
</tr>
<tr>
<td>subtype (pst)</td>
<td></td>
<td>A view name for a view or view32 typed parameter.</td>
</tr>
</tbody>
</table>
Table 15 Parameter Level Attributes

<table>
<thead>
<tr>
<th>Keyword (abbreviation)</th>
<th>Sample</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>100</td>
<td>The maximum occurrence of FML/FML32 field watched during the collection period</td>
</tr>
<tr>
<td>requiredcount</td>
<td>1</td>
<td>The minimum occurrence of FML/FML32 field watched during the collection period.</td>
</tr>
</tbody>
</table>

Examples

Example 1:
Input: service=SVC, request=STRING, reply = TPSUCCESS + STRING
Output Pattern: service=SVC_1, tuxservice=SVC, inbuf=STRING, outbuf=STRING

Example 2:
Input: service=SVC, request=STRING, reply = TPFAIL + STRING
Output Pattern (partial): Service=SVC_1, tuxservice=SVC, inbuf=STRING, outbuf=NULL, errbuf=STRING

Example 3:
Input:
service=SVC, request=STRING, reply = TPSUCCESS + STRING
service=SVC, request=STRING, reply = TPFAIL + STRING
Output Pattern:
service=SVC_1, tuxservice=SVC, inbuf=STRING, outbuf=STRING
Service=SVC_2, tuxservice=SVC, inbuf=STRING, outbuf=NULL, errbuf=STRING

Example 4:
Input: service=FMLS, request=FML32(name,pwd), reply=TPSUCCESS+FML32(id)
Output Pattern:
service=FMLS_1, tuxservice=FMLS, inbuf=FML32, outbuf=FML32
param: input(name, pwd), output(id)
Example 5:

Input:

\[
\text{service=FMLS, request=FML32 (name, pwd), reply=TPSUCCESS+FML32(id)}
\]

\[
\text{service=FMLS, request=FML32 (name, pwd, token), reply=TPSUCCESS+FML32(id)}
\]

Output Pattern:

\[
\text{service=FMLS_1, tuxservice=FMLS, inbuf=FML32, outbuf=FML32}
\]

\[
\text{param: input(name, pwd), output(id)}
\]

\[
\text{service=FMLS_2, tuxservice=FMLS, inbuf=FML32, outbuf=FML32}
\]

\[
\text{param: input(name, pwd, token), output(id)}
\]

Configuring SALT WS-TX Support

This section contains the following topics:

- Configuring Transaction Log Device
- Registration Protocol
- Configuring WS-TX Transactions
- Configuring Maximum Number of Transactions
- Configuring Policy Assertions
- WSDL Generation
- WSDL Conversion

Notes: These configuration changes are summarized in the SALTDEPLOY additions pseudo-schema and WSDF additions pseudo-schema Appendix.

For additional information, see the SALT Interoperability Guide.

Configuring Transaction Log Device

The GWWS system server must be configured using the transaction log (TLogDevice) element (similar to the Oracle Tuxedo or /Domains TLog files). The TLOGDevice element is added to the SALTCONFIG source file (SALTDEPLOY) as shown in Listing 37.

A TLOGName element is also added to allow sharing the same TLog device across GWWS instances.
Only one TLog device per Web services Gateway instance is permitted (that is, the transaction log element is a child element of /Deployment/WSGateway/GWInstance).

Listing 37  TLOG Element Added to SALTDEPLOY File

```
  <WSDF>
    ...
  </WSDF>
  <WSGateway>
    <GWInstance id="GW1">
      <TLogDevice location="/app/GWTLOG"/>
      <TLogName id="GW1TLOG"/>
      ...
    </GWInstance>
  </WSGateway>
  ...
</Deployment>
```

Registration Protocol

Oracle Tuxedo-based services are registered with a Durable 2PC protocol with coordinators. When Oracle Tuxedo is the coordinator (outbound direction), the GWWS system server allows either Volatile 2PC or Durable 2PC registration requests and handles them accordingly.

Configuring WS-TX Transactions

Figure 2 illustrates the application and protocol flows of a typical WS-AT context service invocation.
The configuration steps and runtime behavior of the SALT GWWS gateway are outlined in the following sections (depending on the role of the Oracle Tuxedo domain as shown in Figure 2):

- **Configuring Incoming Transactions**
- **Configuring Outbound Transactions**

**Configuring Incoming Transactions**

Oracle Tuxedo services exposed as Web services do not require any specific configuration other than creating a transaction log file and adding it to the GWWS deploy configuration file in order to initiate a local transaction associated with an incoming WS-AT transaction request.

To ensure a transaction can be propagated into an Oracle Tuxedo domain, do the following steps:

1. Ensure that the Oracle Tuxedo service called supports transactions.
2. Configure a transaction log file in the GWWS deployment file. For more information, see Configuring Transaction Log Device.

3. Configure a policy file containing a WS-AT Assertion corresponding to the desired behavior with respect to the external Web Service called. For more information, see Configuring Policy Assertions.

4. Incoming calls containing a CoordinationContext element creates an Oracle Tuxedo global transaction.

**Error Conditions**

Error conditions are handled as follows:

- No log file is configured for the gateway. A wscoor:InvalidState fault is sent back to the caller. The Detail field contains a corresponding message.

- The target Oracle Tuxedo service does not support transactions. An application fault with a TPETRAN error code is returned to the caller.

- For all other applications, configuration (such as TPENSENT) or system errors are handled the same way that normal (non-transactional) requests are handled.

**Configuring Outbound Transactions**

In order for Oracle Tuxedo clients to propagate an Oracle Tuxedo global transaction to external Web services, do the following steps:

1. Configure a transaction log file in the GWWS deployment file. For more information, see Configuring Transaction Log Device.

2. Configure a policy file containing a WS-AT Assertion corresponding to the desired behavior with respect to the external Web Service called. For more information, see Configuring Policy Assertions.

3. Depending on the assertion setting and presence of an Oracle Tuxedo transaction context, a CoordinationContext element is created and sent in the SOAP header along with the application request.

4. An endpoint reference is automatically generated and sent along with the CoordinationContext element for the remote RegistrationService element to enlist in the transaction. This step, along with the protocol exchanges (Prepare/Commit or Rollback etc.) is transparent on both sides.
Error Conditions

Error conditions are handled as follows:

- If the remote system does not support transactions and the WS-AT Assertion/transaction context call has *must* create transaction semantics, a TPESYSTEM error is returned to the client.

- Errors generated remotely are returned to the Oracle Tuxedo client in the same manner as regular, non-transactional calls. The fault Reason and Detail fields returned describe the nature of the failure (which is environment dependent).

Configuring Maximum Number of Transactions

The MaxTran element allows you to configure the size of the internal transaction table as shown in Listing 1. The default is MAXGTT.

**Note:** The MaxTran value is optional. If the configured value is greater than MAXGTT, it is ignored and MAXGTT is used instead

Listing 1  MaxTran Element

```xml
  <WSDF>
    ...
  </WSDF>
  <WSGateway>
    <GWInstance id="GW1">
      ...
      <MaxTran value="500"/>
      ...
    </GWInstance>
  </WSGateway>
  ...
</Deployment>
```
Configuring Policy Assertions

WS-AT defines a policy assertion that allows requests to indicate whether an operation call must or may be made as part of an Atomic Transaction.

Policy. xml File

The policy.xml file includes WS-AT policy elements. WS-AT defines the ATAssertion element, with an Optional attribute, as follows:

```
<wsat:ATAssertion wsp:Optional="true"/>
```

as shown in Listing 2.

Listing 2  Policy .XML ATAssertion Element

```xml
<?xml version="1.0"?>
<wsp:Policy wsp:Name="TransactionalServicePolicy"
    xmlns:wsat="http://docs.oasis-open.org/ws-tx/wsat/2006/06">
  <wsat:ATAssertion wsp:Optional="true"/>
</wsp:Policy>
```

Note: In order to correctly import external WSDL files, the wsdlcvt command is modified to generate a policy.xml file containing the ATAssertion element when one is present in the WSDL. For outbound requests, a policy.xml file containing an ATAssertion element must be created and properly pointed to in the SALTDEPLOY source.

Inbound Transactions

For inbound transactions, no particular behavior change takes place at runtime. The client consuming the WSDL takes the decision based on the configured value and runtime behavior is the same for the normal cases.
Outbound Transactions

- When an ATAssertion with no "Optional=true" is configured, the call must be made in a transaction. If no corresponding XA transaction exists, the WS-TX transaction is initiated but not associated with any Oracle Tuxedo XA transaction. If an XA transaction exists, there is no change in behavior.

- When an ATAssertion with "Optional=true" is configured, an outbound transaction context is requested only if a corresponding Oracle Tuxedo XA transaction exists in the context of the call.

- When no ATAssertion is configured for this service, the corresponding service call is made outside of any transaction. If a call is made to an external Web service in the context of an Oracle Tuxedo XA transaction, the Web service call will not propagate the transaction.

This allows excluding certain Web service calls from a global transaction, and represents the default for most existing Web services calls (that do not support WS-TX).

WSDL Generation

WSDL generation is enhanced to generate an ATAssertion element corresponding to the assertion configured in the policy file for the corresponding service.

WSDL Conversion

For outbound requests, the WSDL conversion tool, wsdlcvt, generates a policy.xml file containing the ATAssertion element when one is present in the processed WSDL. You must properly configure the location of the policy.xml file in the SALTDEPLOY source.

SALT Configuration Tool

The SALT configuration tool allows you to view and modify your configuration. Oracle Tuxedo services can be exposed as Web Services without having to edit configuration files.

Enabling the SALT Configuration Tool

- GWWS Option
- Custom HTTP Header Option
- REpresentational State Transfer (REST) Option
- MIB Class Interface
- Security

Note: With Internet Explorer 9, web pages are displayed without CSS information by default. In order to display the pages properly, Internet Explorer 8 document compatibility mode should be used. Do the following:
  - Click on tools (little gear icon on the right) then select "Developer Tools" or hit F12
  - Select "Document mode" and "IE8 standards"

GWWS Option

Web administration is disabled by default. In order to enable admin capabilities, the GWWS server must be configured as such in `UBBCONFIG`, using the `-a` option as follows:

```
-a <scheme>: //<host>:<port>
```

- `<scheme>` can be 'http' or 'https'. If using 'https', GWWS must be configured for SSL capabilities by adding private-key and certificates in the same manner as securing application Web Services with SSL.
- `<host>` is the name or IP address of the admin URL listening endpoint.
- `<port>` is the port value of the admin URL listening endpoint.

Use the following URL to access the Web Admin Console:

```
<scheme>://<host>:<port>/admin
```

For example: `https://server.company.com:3333/admin`.

Custom HTTP Header Option

Custom HTTP headers allow Oracle Tuxedo to interoperate with servers or clients that use HTTP headers to transmit data. You must use the `enableCustomHTTPHeaders` property to enable/activate this option as shown in Listing 3

Listing 3  Custom HTTP Header Configuration

```
  <WSDF>
    ...
  </WSDF>
</Deployment>
```
Configuring a SALT Application

```xml
<WSDF>
  <WSGateway>
    <GWInstance id="GW1">
      ...
      <Inbound>
      ...
      </Inbound>
      <Outbound>
      ...
      </Outbound>
      <Properties>
        <Property name="enableCustomHTTPHeaders" value="true">
      </Property>
      </Properties>
      ...
  </GWInstance>
  ...
</WSGateway>
```

**Representational State Transfer (REST) Option**

REST mode is disabled by default. In order to enable REST mode, the GWWS server will have to be configured as such in `SALTDEPLOY`.

**Note:** SALT GWWS always generates XML headers with a `<?xml version="1.0" encoding="UTF-8"?>` prolog. This is currently a limitation and does not affect encoding handling, as those are processed at the HTTP level.

- **Inbound**
- **Outbound**

**Inbound**

The following sections have been added to `SALTDEPLOY`:

```
/Deployment/WSGateway/GWInstance/Inbound/REST/Network
```

This element contains two attributes to specify http or https REST listening endpoints, as follows:
<HTTP>
<Network http="host:port" https="host:port"/>
...
</HTTP>

Only one <Network> element is allowed. The http and https elements are optional, but at least one will have to be specified. The http and https attributes are constructed as follows:

- <host> is the name or IP address of the REST listening endpoint.
- <port> is the port value of the REST listening endpoint.

All REST requests are performed by the same <host>:<port> combination, i.e., it’s not possible to use more than one such combination per gateway per protocol (http and https).

Service calls will use the above pattern as the basis for constructing URLs. For example:

(http://host:1234/myTOUPPER)

By default, if services are not explicitly and individually specified as advertised using REST, they will not be callable. See Service.

**Service Configuration**

An element has been to SALTDEPLOY to specify which services are accessible when REST is configured through the command-line switch described above.

The way Oracle Tuxedo services are exposed using a CRUD (Create Read Update Delete) mapping to take advantage of the REST paradigm. For example, a REST service named bankAccount has an HTTP method to Oracle Tuxedo service mapping as shown in Table 1.

<table>
<thead>
<tr>
<th>Method</th>
<th>Oracle Tuxedo Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>ACCOUNT_INFO</td>
</tr>
<tr>
<td>POST</td>
<td>OPEN_ACCOUNT</td>
</tr>
<tr>
<td>DELETE</td>
<td>CLOSE_ACCOUNT</td>
</tr>
<tr>
<td>PUT</td>
<td>UPDATE_ACCOUNT</td>
</tr>
</tbody>
</table>

Clients invoke the service as follows:
URL: http://host:1234/bankAccount?account=1234

Data exchanged:

Request:
GET /bankAccount?account=1234 HTTP/1.0
Content-Type: application/json

Response:

{{'account':1234},{'balance':1000}...}

The following elements are added to SALTDEPLOY:

- /Deployment/WSGateway/GWInstance/Inbound/REST/Service
- /Deployment/WSGateway/GWInstance/Inbound/REST/Service/Method

There will be zero or one <RESTHTTP> element in <Inbound> and one or more <Service> element in <HTTPREST>. <Service> contains the following attributes:

- name: logical name of a REST service. This is the value passed in the URI which combined with the method will map to the actual Tuxedo service.

There will be at least one <Method> element per <Service>, and at most four (one per supported method). The <Method> element contains the following attributes:

- name: name of the method being mapped GET, POST, DELETE, PUT value. Any other value will result in a configuration error at wsloadcf time.

- reposservice
  name of the Tuxedo Metadata Repository service to use as interface. This value will be optional and will be used as an indication of what buffer-type and/or parameter list to use when generating test code on the configuration tool test page. This value will be generated by the configuration console when exposing Tuxedo services as RESTful services.

- tuxservice
  The Oracle Tuxedo service being mapped.

- inputbuffer
  Oracle Tuxedo buffer type/optionally subtype used for input conversion. Values are the same as all existing Oracle Tuxedo buffer types. For VIEW/VIEW32 buffer types, the
notion of subtype is conveyed by using the notation: \{VIEW\|VIEW32\}/<Subtype>, for example: 'VIEW32/customer'.

For more information, see Data Type Mapping and Message Conversion Services in the SALT Programming Guide.

There is no checking as to whether a service is already advertised or not, since Oracle Tuxedo services can be advertised dynamically. As indicated, if a service is not listed in this section it will not be possible to call it using REST means.

Listing 4  REST Inbound Example

```xml
  <WSDF>
    ...
  </WSDF>
</WSDF>
<WSGateway>
  <GWInstance id="GW1">
    <Inbound>
      <Binding ref="bankapp:bankapp Binding">
        <Endpoint use="http1"/>
        <Endpoint use="https1"/>
      </Binding>
      <RESTHTTP>
        <Network http="host:1234" https="host:1235"/>
        <Service name="bankAccount">
          <Method name="GET"
            reposservice="ACCOUNT_INFO"
            service="ACCOUNT_INFO"
            inputbuffer="FML32"/>
          <Method name="POST"
```
Configuring a SALT Application

```xml
reposservice="OPEN_ACCOUNT"
service="OPEN_ACCOUNT"
inputbuffer="FML32"/>

<Method name="DELETE"
reposservice="CLOSE_ACCOUNT"
service="CLOSE_ACCOUNT"
inputbuffer="FML32"/>

<Method name="PUT"
reposservice="UPDATE_ACCOUNT"
service="UPDATE_ACCOUNT"
inputbuffer="FML32"/>

</Service>
</RESTHTTP>
</Inbound>
...
```

**Outbound**

The following element will be added to SALTDEPLOY:
/Deployment/WSGateway/GWInstance/Oubound/HTTP/Service.

There will be zero or one <HTTP> element(s) in <Outbound> and one or more <Service> element(s) in <HTTP>. <Service> will contain the following attributes:

- **name**: Tuxedo service name to be advertised. This needs to be unique in the Tuxedo domain.
- **method**: HTTP method that will be used to perform the HTTP call.
- **address**: URL of the external HTTP service to call.
- **content-type**: Content type to use for complex data encoding: JSON or XML.
Enabling the SALT Configuration Tool

Configuring a SALT Application

outputbuffer: Tuxedo buffer type/optionally subtype used for response conversion. Values will be the same as all existing Tuxedo buffer types. For VIEW/VIEW32 buffer types, the notion of subtype will be conveyed by using the notation: {VIEW|VIEW32}/<Subtype>, for example: 'VIEW32/customer'. See Data Mapping paragraph for details.

Note: A Tuxedo service must be mapped to a combination of URL + HTTP method + HTTP mapping (JSON or XML) - unlike HTTP/REST inbound, since on the Tuxedo side there is only the notion of Tuxedo service.

Listing 5  REST Outbound Example

  <WSDF>
    ...
  </WSDF>
  <WSGateway>
    <GWInstance id="GW1">
      ...
      <Outbound>
        <Binding ref="bankapp:bankapp_binding">
          <Endpoint use="http1"/>
          <Endpoint use="https1"/>
        </Binding>
        <HTTP>
          <Service name="BANK_GET"
            method="GET"
            address="http://some.org/bankAccount"
            content-type="JSON"
            outputbuffer="FML32"/>
          <Service name="HTTPSvcGet"
            method="GET"
Configuring a SALT Application

```xml
<HTTP>
  <Outbound>
    ...
    
    <Service name="HTTPSvcPost"
      method="POST"
      address="http://some.org/some/path"
      content-type="JSON"
      outputbuffer="FML32"/>
    
    </Outbound>
    </HTTP>
```

MIB Class Interface

SALT MIB interface is called using `tpcall(".wm" + GWWSID,...)`. It provides the following classes defined:

- T_WSRELOAD Class
- T_WSGW Class
- T_WSWEBSERVICE Class
- T_WSBINDING Class
- T_WSOPERATION Class
- T_WSHTTPSERVICE Class
- T_WSTRANSACTION Class

Usage

- T_WSRELOAD Class
Listing 6  T_WSRELOAD Class Usage Example

$ ud32 < reload.ud32
with reload.ud32 containing:
SRVCNM .wmGW1
TA_OPERATION GET

TA_CLASS T_WSRELOAD

".wmGW1" above is this particular instance and must match the gateway id as specified in the UBBCONFIG file in the "-i" option of the GWWS system server.

Example of a reply:
RTN pkt(1) is :

TA_ERROR 0
TA_MORE 0
TA_OCCURS 1

TA_CLASS T_WSRELOAD

TA_STATUS Config reloaded

- All Other Classes

Listing 7  Example of call, to get T_SALTGW information, in ud32 format

$ ud32 < saltgw.ud32
SENT pkt(1) is :
SRVCNM .wmgw1
TA_CLASS T_SALTGW
TA_OPERATION GET
Configuring a SALT Application

RTN pkt(1) is :
TA_ERROR 0
TA_MORE 0
TA_OCCURS 1
TA_INSTANCEID gw1
TA_TLOGDEVICE
TA_TLOGNAME
TA_WSATENDPOINT
TA_MAXTRAN
TA_SOCKSADDRLIST
TA_MAXCONTENTLEN 0
TA_THREADPOOLSIZE 16
TA_TIMEOUT 300
TA_MAXBACKLOG 20
TA_ENABLEMULTIENC true
TA_ENABLESOAPVAL false
TA_PRIVATEKEY
TA_VERIFYCLIENT
TA_TRUSTEDCERT
TA_CERTPATH
TA_PLUGINLIBRARIES
TA_PLUGINPARAMS
TA_RESTHTTPADDRESS localhost:1111
TA_RESTHTTPSADDRESS

Class Definitions

T_WSRELOAD Class
Invoking this class with GET operation will result in reloading of the SALTCORE file. This will be equivalent to re-starting GWWS, but without actually shutting it down then re-booting it.
**T_WSGW Class**

The T_WSGW class represents attributes of gateway instances such as number of threads, TLOG device and name.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_INSTANCEID(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..12]</td>
<td></td>
</tr>
<tr>
<td>TA_TLOGDEVICE</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..256]</td>
<td></td>
</tr>
<tr>
<td>TA_TLOGNAME</td>
<td>string</td>
<td>r--r--r--</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>TA_WSATENDPOINT</td>
<td>string</td>
<td>r--r--r--</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>TA_MAXTRAN</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXGTT</td>
<td>MAXGTT</td>
</tr>
<tr>
<td>TA.SOCKSADDRLIST</td>
<td>string</td>
<td>r--r--r--</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>TA_MAXCONTENTLEN</td>
<td>string</td>
<td>r--r--r--</td>
<td>1b &lt;= string byte size &lt;= 1G</td>
<td></td>
</tr>
<tr>
<td>TA_THREADPOOLSIZE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= 1024</td>
<td>16</td>
</tr>
<tr>
<td>TA_NWTIMEOUT</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= 65535</td>
<td>300</td>
</tr>
<tr>
<td>TA_MAXBACKLOG</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= 255</td>
<td>16</td>
</tr>
<tr>
<td>TA_ENABLEMULTIENC</td>
<td>string</td>
<td>r--r--r--</td>
<td>{true, false}</td>
<td></td>
</tr>
<tr>
<td>TA_ENABLESOAPVAL</td>
<td>string</td>
<td>r--r--r--</td>
<td>{true, false}</td>
<td></td>
</tr>
<tr>
<td>TA_PRIVATEKEY</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..12]</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2  T_WSGW Class Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_VERIFYCLIENT</td>
<td>string</td>
<td>r--r--r--</td>
<td>{true, false}</td>
<td>false</td>
</tr>
<tr>
<td>TA_TRUSTEDCERT</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..128]</td>
<td></td>
</tr>
<tr>
<td>TA_CERTPATH</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..128]</td>
<td></td>
</tr>
<tr>
<td>TA_PLUGINLIBRARIES</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..256]</td>
<td></td>
</tr>
<tr>
<td>TA_PLUGINPARAMS</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..256]</td>
<td></td>
</tr>
<tr>
<td>TA_RESTHTTPADDRESS</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..256]</td>
<td></td>
</tr>
<tr>
<td>TA_RESTHTTPSADDRESS</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..256]</td>
<td></td>
</tr>
<tr>
<td>TA_WS_REQREPDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_REQREPFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_ONEWAYDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_ONEWAYFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUNDDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUNDFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUND_ONEWAYDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUND_ONEWAYFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
</tbody>
</table>
Attribute Semantics

**TA_INSTANCEID**
Gateway instance identifier. This attribute value may contain a maximum of 12 characters (excluding the terminating NULL character). The identifier value must be unique within the SALTDEPLOY file.

**TA_TLOGDEVICE**
One attribute "location" describes the location of the Transaction file. This is required if WS-TX transaction support is required.

**TA_TLOGNAME**
One attribute "id" describes the name of the transaction log inside a Transaction file. This is required if WS-TX transaction support is required.

**TA_WSATENDPOINT**
One attribute "address" describes the WS-AT protocol end point.

---

### Table 2 T_WSGW Class Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_WS_INBOUNDTIME</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUNDTIME</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_THREADS</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_TOTALPENDING</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_RESTDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_RESTFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_RESTPENDING</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_RESTTIME</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a SALT Application

**TA_MAXTRAN**
One attribute "value" describes the maximum number of concurrent WS-TX transactions allowed. This is bounded by Oracle Tuxedo MAXGTT.

**TA_SOCKSADDRLIST**
String type containing a list of proxy server URLs. For example:
proxy.server1.com,10.123.1.1:1080

**TA_MAXCONTENTLENGTH**
Enables the GWWS server to deny the HTTP requests when the content length is larger than the property setting. If not specified, the GWWS server does not check for it. The string value can be one of the following three formats:

- Integer number in bytes. No suffix means the unit is bytes.
- Float number in kilobytes. The suffix must be 'K'. For instance, 10.4K, 40K, etc.
- Float number in megabytes. The suffix must be 'M'. For instance, 100M, 20.6M, etc.

**TA_THREADPOOLSIZE**
Specifies the maximum thread pool size for the GWWS server.

*Note:* This value defines the maximum possible threads that may be spawned in the GWWS server. When the GWWS server is running, the actual spawned threads may be less than this value.

**TA_NWTIMEOUT**
Specifies the network time-out value, in seconds.

**TA_MAXBACKLOG**
Specifies the backlog listen socket value. It controls the maximum queue length of pending connections by operating system.

*Note:* Generally no tuning is needed for this value.

**TA_ENABLEMULTIENC**
Toggles on/off multiple encoding message support for the GWWS server. If multiple encoding support property is turned off, only UTF-8 HTTP / SOAP messages can be accepted by the GWWS server.

**TA_ENABLESOAPVAL**
Toggles on/off XML Schema validation for inbound SOAP request messages if the corresponding Tuxedo input buffer is associated with a customized XML Schema.

**TA_PRIVATEKEY**
When using an Oracle wallet, specifies the location of a directory that contains an Oracle Wallet.
Notes: Oracle SALT does not have the concept of a security principal name like Oracle Tuxedo does, so the Wallet is located in the specified directory and not in a subdirectory.

Note: To configure server identity certificates (SALT deploy configuration file `<PrivateKey>` element), it is required that the root certificate authority be present in the SSL configuration file. Proper configuration is:

- root CA certificate
- intermediate certificate(s) (if any)
- server certificate
- server private key

in PEM format.

When using the legacy security credentials format, specifies the PEM format private key file. The key file path is specified as the text value for this element. The server certificate is also stored in this private key file. The value of this element may contain a maximum of 256 characters (excluding the terminating NULL character).

With either security credential format, the password for the Oracle Wallet or the GWWS private key file is specified in the TUXCONFIG file using the `SEC_PRINCIPAL_PASSVAR="environment_variable_name"` parameter. The TUXCONFIG file must also set the `SEC_PRINCIPAL_NAME="any_non-null_string(not_used)"` parameter so that `SEC_PRINCIPAL_PASSVAR` will be properly processed in the configuration file.

This element is mandatory if the parent `<Certificate>` element is configured.

**TA_VERIFYCLIENT**
Optional.

Specifies if Web service clients are required to send a certificate via HTTP over SSL connections. The valid element values are "true" and "false".

**TA_TRUSTEDCERT**
Optional.

Specifies the file name of the trusted PEM format certificate files. The value of this element may contain a maximum of 256 characters (excluding the terminating NULL character).
Configuring a SALT Application

**TA_CERTPATH**
Specifies the local directory where the trusted certificates are located. The value of this element may contain a maximum of 256 characters (excluding the terminating NULL character).

This element is optional.

Note: If TA_VERIFYCLIENT is set to "true", or if WS-Addressing is used with SSL, trusted certificates must be stored in the directory setting with this element.

**TA_PLUGINLIBRARIES**
Comma-separated list of local shared library file paths.

**TA_PLUGINPARAMS**
Comma-separated list specifying string values that are passed to the library when initialized by the GWWS server at boot time.

Each item in the list is passed in order to the corresponding item in the TA_PLUGINLIBRARIES attribute.

Note: The statistics fields below may not be present if no corresponding action has been performed. For example if no one-way call has been made T_WS_ONEWAYDONE will not be returned.

**TA_WS_REQREPDONE**
Number of inbound request-reply calls performed.

**TA_WS_REQREPFAIL**
Number of inbound failed request-reply calls.

**TA_WS_ONEWAYDONE**
Number of inbound one-way calls performed.

**TA_WS_ONEWAYFAIL**
Number of inbound failed one-way calls.

**TA_WS_OUTBOUNDDONE**
Number of outbound request-reply calls performed.

**TA_WS_OUTBOUNDFAIL**
Number of outbound failed request-reply calls.

**TA_WS_OUTBOUND_ONEWAYDONE**
Number of outbound one-way calls performed.

**TA_WS_OUTBOUND_ONEWAYFAIL**
Number of outbound failed one-way calls.
**TA_WS_INBOUNTIME**
Average processing time of inbound calls.

**TA_WS_OUTBOUNTIME**
Average processing time of outbound calls.

**TA_WS_THREADS**
Number of active threads.

**TA_WS_TOTALPENDING**
Total average processing time across all SOAP services.

**TA_RESTINBOUNDDONE**
Number of successful inbound REST calls.

**TA_RESTINBOUNDFAIL**
Number of failed outbound REST calls.

**TA_RESTINBOUNDTIME**
Total average processing time for inbound REST calls.

**TA_RESTOUTBOUNDDONE**
Number of successful inbound REST calls.

**TA_RESTOUTBOUNDFAIL**
Number of failed outbound REST calls.

**TA_RESTOUTBOUNDTIME**
Total average processing time for inbound REST calls.

**Limitations**
None

**T_WSWEBSERVICE Class**
The T_WSWEBSERVICE class represents configuration attributes of SOAP Web Services. Each Web Service identified by a WSDFNAME can contain one or more instance of bindings, which will be returned as one or more instances of this class, for example for a Web Service named 'ACCOUNT':

- **TA_OCCURS**
- **TA_WSDFNAME**
- **TA_WSDFNAME**
- **TA_BINDINGID**
- **TA_BINDINGID**
Configuring a SALT Application

Table 3 T_WSWEBSERVICE Class Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_WSDFNAME(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_BINDINGID(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..78]</td>
<td></td>
</tr>
<tr>
<td>TA_INSTANCEID</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..12]</td>
<td></td>
</tr>
<tr>
<td>TA_WSDFDIRECTION</td>
<td>string</td>
<td>r--r--r--</td>
<td>(INBOUND</td>
<td>OUTBOUND)</td>
</tr>
<tr>
<td>TA_ENDPOINTIDLIST</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..1024]</td>
<td></td>
</tr>
<tr>
<td>TA_WSAENDPOINT</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..1024]</td>
<td></td>
</tr>
<tr>
<td>TA_REALM</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..1024]</td>
<td></td>
</tr>
</tbody>
</table>

Attribute Semantics

**TA_WSDFNAME**
WSDF name. Identifies this web service definition.

**TA_BINDINGID**
Binding id. Links with a T_SALTBINDING class instance, see T_SALTBINDING class definition.

**TA_INSTANCEID**
Gateway instance identifier of gateway this web service is deployed on.

**TA_WSDFDIRECTION**
Native Web Service: this attribute will contain the "INBOUND" value.
Non-native Web Service: this attribute will contain the "OUTBOUND" value.

**TA_ENDPOINTIDLIST**
Comma-separated list of WSBinding object endpoint references.

If the referenced endpoint is specified as an inbound endpoint, the GWWS server creates the corresponding HTTP and/or HTTPS listen endpoint. At least one inbound endpoint must be specified for one inbound WSBinding object.
If the referenced endpoint is specified as an outbound endpoint, the GWWS server creates HTTP and/or HTTPS connections per SOAP requests for the outbound WSBinding object.

If an outbound endpoint is not specified for the outbound WSBinding object, the first 10 endpoints (at most) are auto-selected.

The referenced endpoint must already be defined in the TA_SALTWSDF class.

**TA_WSAENDPOINT (outbound only)**

Specifies the WS-Addressing listen endpoint address.

If this attribute is not empty, by default all SOAP messages are sent out with a Web Service Addressing message header.

The address value must be in the following format:

"http(s)://<host>:<port>/<context_path>"

The GWWS server creates listen endpoints and usage for receiving WS-Addressing SOAP response messages.

**TA_REALM (outbound only)**

Specifies the HTTP Realm attribute of an HTTP and/or HTTP/S endpoint. If this element is configured for one endpoint, the GWWS tries to incorporate HTTP basic authentication information in the request messages when issuing outbound calls through this endpoint.

**Limitations**

None

**T_WSBINDING Class**

The T_WSBINDING class represents configuration attributes of SOAP bindings.

Required key fields: TA_BINDINGID and TA_WSFNAME

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_BINDINGID(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..78]</td>
<td></td>
</tr>
<tr>
<td>TA_WSFNAME(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_SOAPVERSION</td>
<td>string</td>
<td>r--r--r--</td>
<td>{1.1</td>
<td>1.2}</td>
</tr>
</tbody>
</table>
Configuring a SALT Application

Table 4  T_WSBINDING Class Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_SOAPSTYLE</td>
<td>string</td>
<td>r--r--r--</td>
<td>{rpc</td>
<td>document}</td>
</tr>
<tr>
<td>TA_SOAPENCODING</td>
<td>string</td>
<td>r--r--r--</td>
<td>{encoded</td>
<td>literal}</td>
</tr>
<tr>
<td>TA_POLICIES</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..2570]</td>
<td></td>
</tr>
<tr>
<td>TA_ENDPOINTS</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..2570]</td>
<td></td>
</tr>
</tbody>
</table>

**TA_BINDINGID**
Identifies the WSBinding object. The value must be unique within the WSDF.

Native WSDF: the value is specified by customers and is used as the wsdl:binding name in the generated WSDL document.

Non-native WSDF: the value is the wsdl:binding name defined in the external WSDL document.

**TA_WSDFNAME**
WSDF name. Links with a T_SALTWSDF class instance, see T_SALTWSDF class definition.

**TA_SOAPVERSION**
Specifies SOAP version for this WSBinding object.

**TA_SOAPSTYLE**
Specifies SOAP message style for this WSBinding object.

**TA_SOAPENCODING**
Specifies SOAP message encoding style for this WSBinding object.

**TA_POLICIES**
Specifies a comma-separated list of local file paths for the referenced WS-Policy file(s).

Specifically, Oracle SALT pre-defines WS-Policy template files for typical WS-* scenarios. These files can be found under the STUXDIR/udataobj/salt/policy directory. These template files can be referenced using the string format "salt:<template_file_name>".
Enabling the SALT Configuration Tool

For example, the SALT WS-SecurityPolicy 1.0 template file "wssp1.0-signbody.xml" is represented as the following string value in the TA_POLICIES attribute:

```
salt:wssp1.0-signbody.xml
```

**TA_ENDPOINTS**
Comma-separated list of endpoints representing each access endpoint for this TA_SALTBINDING class instance.

**Limitations**
None

**T_WSOPERATION Class**
The T_WSOPERATION class represents configuration attributes of SOAP operations.
Required key fields: TA_BINDINGID and TA_WSDFNAME.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_BINDINGID(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_SERVICENAME(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..255]</td>
<td></td>
</tr>
<tr>
<td>TA_WSDFNAME(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..255]</td>
<td></td>
</tr>
<tr>
<td>TA_TUXEDOREF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..128]</td>
<td></td>
</tr>
<tr>
<td>TA_NAMESPACE</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..255]</td>
<td></td>
</tr>
<tr>
<td>TA_SOAPACTION</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..255]</td>
<td></td>
</tr>
<tr>
<td>TA_POLICIES</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..2570]</td>
<td></td>
</tr>
<tr>
<td>TAASYNCTIMEOUT</td>
<td>long</td>
<td>r--r--r--</td>
<td>0 &lt;= num &lt;= 32767</td>
<td>60</td>
</tr>
<tr>
<td>TA_DISABLEWSA</td>
<td>string</td>
<td>r--r--r--</td>
<td>{True</td>
<td>False}</td>
</tr>
</tbody>
</table>
Configuring a SALT Application

Table 5  T_WSOPERATION Class Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_INPUTMSGNAME</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_INPUTWSACTION</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_INPUTMSGHANDLER</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_OUTPUTMSGNAME</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_OUTPUTWSACTION</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_OUTPUTMSGHANDLER</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_ERRMSGNAME</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_ERRWSACTION</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_ERRMSGHANDLER</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..30]</td>
<td></td>
</tr>
<tr>
<td>TA_WS_REQREPFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_REQREPDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_ONEDWAYFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_ONEDWAYDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_INBOUNDTIME</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUNDFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUNDDONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_OUTBOUND_ONEWAYFAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
</tbody>
</table>
Attribute Semantics

**TA_BINDINGID**
Binding id. Links with a T_SALTBINDING class instance, see T_SALTBINDING class definition.

**TA_SERVICENAME**
Specifies the service name.

Native WSDF: the service name value is used as the wsdl:operation name in the generated WSDL document.

Non-native WSDF: the service name is equal to the wsdl:operation name defined in the external WSDL document.

**TA_WSDFNAME**
WSDF name. Links with a T_SALTWSDF class instance, see T_SALTWSDF class definition.

**TA_TUXEDOREF**
An optional attribute used to reference the service definition in the Tuxedo Service Metadata Repository.

If not specified, attribute TA_SERVICENAME value is used as the reference value.

**TA_NAMESPACE**
Specifies service namespace attribute. This is a non-native WSDF attribute. It is used to save the namespace setting for each wsdl:operation defined in the external WSDL document.

Note: Do not specify this attribute for a native WSDF.

**TA_SOAPACTION**
Specifies the service soapAction attribute. This is a non-native WSDF attribute. It is used to save the soapAction setting for each wsdl:operation defined in the external WSDL document.
Note: Do not specify this attribute for a native WSDF.

**TA_POLICIES**
Specifies a comma-separated list of local file paths for the referenced WS-Policy file(s).

Specifically, Oracle SALT pre-defines WS-Policy template files for typical WS-* scenarios. These files can be found under the $TUXDIR/udataobj/salt/policy directory. These template files can be referenced using the string format "salt:<template_file_name>".

For example, the SALT WS-SecurityPolicy 1.0 template file "wssp1.0-signbody.xml" is represented as the following string value in the TA_POLICIES attribute:

salt:wssp1.0-signbody.xml

**TAASYNCTIMEOUT**
Outbound service: Specifies a time in seconds to wait for a SOAP response.
Inbound service: No behavior impact.

**TA_DISABLEWSA**
Outbound service: Disables explicit Web Service Addressing requests with this property.
Inbound service: No behavior impact.

**TA_INPUTMSGNAME**
Specifies the service input message name attribute. This is a non-native WSDF attribute. It is used to save the name for the input wsdl:message defined in the external WSDL document.

Note: Do not specify this attribute for a native WSDF.

**TA_INPUTWSAACTION**
Specifies the service input message wsaAction attribute. This is a non-native WSDF attribute. It is used to save the wsaAction attribute of the input wsdl:message defined in the external WSDL document.

Note: Do not specify this attribute for a native WSDF.

**TA_INPUTMSGHANDLER**
Specifies a customized message conversion handler. Optional for <Input>, <Output> and/or <Fault> elements of any service. The value of this element is the handler name.

The GWWS server looks for the message conversion handler from all known message conversion plug-in shared libraries using the handler name. The message conversion handler allows you to develop customized Tuxedo buffer and SOAP message payload transformation functions to replace the default GWWS message conversions.
**TA_OUTPUTMSGNAME**

Specifies the service output message name attribute. This is a non-native WSDF attribute. It is used to save the name for the output wsdl:message defined in the external WSDL document.

Note: Do not specify this attribute for a native WSDF.

**TA_OUTPUTWSAACTION**

Specifies the service output message name attribute. This is a non-native WSDF attribute. It is used to save the wsaAction attribute of the output wsdl:message defined in the external WSDL document.

Note: Do not specify this attribute for a native WSDF.

**TA_OUTPUTMSGHANDLER**

Specifies a customized message conversion handler. Optional for <Input>, <Output> and/or <Fault> elements of any service. The value of this element is the handler name.

The GWWS server looks for the message conversion handler from all known message conversion plug-in shared libraries using the handler name. The message conversion handler allows you to develop customized Tuxedo buffer and SOAP message payload transformation functions to replace the default GWWS message conversions.

**TA_FAULTMSGNAME**

Specifies the service fault message name attribute. This is a non-native WSDF attribute. It is used to save the name for the fault wsdl:message defined in the external WSDL document.

Note: Do not specify this attribute for a native WSDF.

**TA_FAULTWSAACTION**

Specifies the service fault message wsaAction attribute. This is a non-native WSDF attribute. It is used to save the wsaAction attribute of the fault wsdl:message defined in the external WSDL document.

Note: Do not specify this attribute for a native WSDF.

**TA_FAULTMSGHANDLER**

Specifies a customized message conversion handler. Optional for <Input>, <Output> and/or <Fault> elements of any service. The value of this element is the handler name.

The GWWS server looks for the message conversion handler from all known message conversion plug-in shared libraries using the handler name. The message conversion handler allows you to develop customized Tuxedo buffer and SOAP message payload transformation functions to replace the default GWWS message conversions.
Note: The statistics fields below may not be present if no corresponding action has been performed. For example if no one-way call has been made T_WS_ONEWAYDONE will not be returned.

**TA_WS_REQREPDONE**
Number of inbound request-reply calls performed.

**TA_WS_REQREPFAIL**
Number of inbound failed request-reply calls.

**TA_WS_ONEWAYDONE**
Number of inbound one-way calls performed.

**TA_WS_ONEWAYFAIL**
Number of inbound failed one-way calls.

**TA_WS_INBOUNTIME**
Average processing time of inbound calls.

**TA_WS_OUTBOUNDDONE**
Number of outbound request-reply calls performed.

**TA_WS_OUTBOUNDFAIL**
Number of outbound failed request-reply calls.

**TA_WS_OUTBOUND_ONEWAYDONE**
Number of outbound one-way calls performed.

**TA_WS_OUTBOUND_ONEWAYFAIL**
Number of outbound failed one-way calls.

**TA_WS_OUTBOUNTIME**
Average processing time of outbound calls.

**Limitations**
None

**T_WSHTTPSERVICE Class**
The T_WSHTTPSERVICE class represents configuration attributes of SALT REST services.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_HTTPSVNAME(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPDIRECTION</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..8]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPMETHOD</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..10]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPOUTBUF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..17]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPOUTADDRESS</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..25]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPCONTENTTYPE</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[0..25]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPPOSTSERVICE</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPPUTSERVICE</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPGETSERVICE</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPDELETESERVICE</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPPOSTINBUF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..17]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPPUTINBUF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..17]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPGETINBUF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..17]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPDELETEINBUF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..17]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPPOSTTUXREF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25]</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a SALT Application

Table 6  T_WSHTTPSERVICE Class Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_HTTPPUTTUXREF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25 6]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPGETTUXREF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25 6]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTPDELETETUXREF</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25 6]</td>
<td></td>
</tr>
<tr>
<td>TA_HTTP_DONE</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_HTTP_FAIL</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_HTTP_TIME</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
</tbody>
</table>

**TA_RESTSVCNAME**
Name to be used in URL to call a Tuxedo service. Note that this is not the actual Tuxedo service, that is configured using the <Method> element described below.

**TA_RESTPOSTSERVICE**
Name of Tuxedo service being mapped to the HTTP POST method.

**TA_RESTPUTSERVICE**
Name of Tuxedo service being mapped to the HTTP PUT method.

**TA_RESTGETSERVICE**
Name of Tuxedo service being mapped to the HTTP GET method.

**TA_RESTDELETESERVICE**
Name of Tuxedo service being mapped to the HTTP DELETE method.

**TA_RESTPOSTINBUF**
Tuxedo buffer typeoptionally subtype used for input conversion. Values will be the same as all existing Tuxedo buffer types. For VIEW/VIEW32 buffer types, the notion of subtype will be conveyed by using the notation: {VIEW|VIEW32}/<Subtype>, for example: 'VIEW32/customer'.

This is the value associate with the HTTP POST method for this REST service.
Enabling the SALT Configuration Tool

**TA_RESTPUTINBUF**
Tuxedo buffer type/optionally subtype used for input conversion. Values will be the same as all existing Tuxedo buffer types. For VIEW/VIEW32 buffer types, the notion of subtype will be conveyed by using the notation: {VIEW|VIEW32}/<Subtype>, for example: 'VIEW32/customer'.

This is the value associate with the HTTP PUT method for this REST service.

**TA_RESTGETINBUF**
Tuxedo buffer type/optionally subtype used for input conversion. Values will be the same as all existing Tuxedo buffer types. For VIEW/VIEW32 buffer types, the notion of subtype will be conveyed by using the notation: {VIEW|VIEW32}/<Subtype>, for example: 'VIEW32/customer'.

This is the value associate with the HTTP GET method for this REST service.

**TA_RESTDELETEINBUF**
Tuxedo buffer type/optionally subtype used for input conversion. Values will be the same as all existing Tuxedo buffer types. For VIEW/VIEW32 buffer types, the notion of subtype will be conveyed by using the notation: {VIEW|VIEW32}/<Subtype>, for example: 'VIEW32/customer'.

This is the value associate with the HTTP DELETE method for this REST service.

**TA_RESTPOSTTUXREF**
Reference to a metadata repository entry. This is used to associate interface data with a REST service and method. One use is for the configuration tool to generate automatic test code based on service metadata (interface).

This is the value associate with the HTTP POST method for this REST service.

**TA_RESTPUTTUXREF**
Reference to a metadata repository entry. This is used to associate interface data with a REST service and method. One use is for the configuration tool to generate automatic test code based on service metadata (interface).

This is the value associate with the HTTP PUT method for this REST service.

**TA_RESTGETTUXREF**
Reference to a metadata repository entry. This is used to associate interface data with a REST service and method. One use is for the configuration tool to generate automatic test code based on service metadata (interface).

This is the value associate with the HTTP GET method for this REST service.
Configuring a SALT Application

**TA_RESTDELETETUXREF**
Reference to a metadata repository entry. This is used to associate interface data with a
REST service and method. One use is for the configuration tool to generate automatic test
code based on service metadata (interface).

This is the value associate with the HTTP DELETE method for this REST service.

**TA_RESTDONE**
Number of successful calls.

**TA_RESTFAIL**
Number of failed calls.

**TA_RESTPENDING**
Number of requests being processed.

**TA_RESTTIME**
Average time processing time.

Limitations
None

**T_WSTRANSACTION Class**
The T_WSTRANSACTION class represents runtime attributes of WS-TX transactions.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_INSTANCEID(k)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string</td>
<td>[1..12]</td>
</tr>
<tr>
<td>TA_WS_TRANPROCESSID</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;=</td>
<td>MAXLONG</td>
</tr>
<tr>
<td>TA_WS_TRANSVCNAME</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25</td>
<td>6]</td>
</tr>
<tr>
<td>TA_WS_TRANGTRID</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..78]</td>
<td></td>
</tr>
<tr>
<td>TA_WS_TRANCOORCONTEXT</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..25</td>
<td>6]</td>
</tr>
<tr>
<td>TA_WS_TRANTRANID(*)</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..78]</td>
<td></td>
</tr>
</tbody>
</table>
Table 7 T_WSTRANSACTION Class Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Permissions</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA_STATE(k)</td>
<td>string</td>
<td>R-XR-XR--</td>
<td>GET: &quot;{ACT</td>
<td>COM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SET: &quot;FOR&quot;</td>
<td>&quot;N/A&quot;</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TA_WS_TRANTIMESTAMP</td>
<td>long</td>
<td>r--r--r--</td>
<td>1 &lt;= num &lt;= MAXLONG</td>
<td></td>
</tr>
<tr>
<td>TA_WS_TRANBRANCHES</td>
<td>fml32</td>
<td>r--r--r--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TA_WS_TRANBRANCH</td>
<td>string</td>
<td>r--r--r--</td>
<td>string[1..256]</td>
<td></td>
</tr>
</tbody>
</table>

**TA_INSTANCEID**

Gateway instance identifier.

**TA_WS_TRANPROCESSID**

Process id of the gateway.

**TA_WS_TRANSVCNAME**

Currently unused.

**TA_WS_TRANGTRID**

Tuxedo side global transaction identifier.

**TA_WS_TRANCOORDCONTEXT**

Web services side coordination context.

**TA_STATE**

GET: "{ACTive | COMcalled | REAdy | HEUristic | HEuristic Hazard }

A GET operation will retrieve run-time information for the selected T_WSTRANSACTION object(s). The following states indicate the meaning of a TA_STATE returned in response to a GET request.

SET: "{FORget}"

A SET operation will update run-time information for the selected T_WSTRANSACTION object. The following states indicate the meaning of a TA_STATE set in a SET request. States not listed may not be set.
Configuring a SALT Application

FORget: Resolve a Heuristic or Heuristic Hazard transaction by removing its transaction log record. State change allowed only when in the HEUristic or HEuristic Hazard state.

**TA_WS_TRANTIMESTAMP**
- Transaction time stamp.

**TA_WS_BRANCHES**
- Comma-separated transaction branch identifiers.

**Limitations**
None

**Security**

**Note:** It is recommended that you use SSL/TLS to protect user name and password in order to integrate the SALT Configuration Tool with Oracle Tuxedo security.

For Oracle Tuxedo application domains that requires **ACL** or **MANDATORY_ACL** security, a console service must be configured in the Oracle Tuxedo security data files. This added information is used for Oracle Tuxedo access control to the Configuration Tool service. By default, the Configuration Tool service name is "SALTWEBCONSOLE", but you can modify it using the GWWS option "-C <CONSOLE SERVICE NAME>". For example:

```
GWWS SRVGRP=GROUP1 SRVID=3
  CLOPT="-A -- -iGWWS1 -a
http://server.company.com:3333/admin -C CONSOLE"
```

This tells GWWS to use "CONSOLE" as the service name for access control.

**Note:** You should also use "tpacladd" to add this Web Console service into the security data file. For example: $ tpacladd -g 1000 CONSOLE.

This will add CONSOLE as an Oracle Tuxedo SERVICE into the security data file and restrict the access only to user belongs to the group with group id 1000.

**Configuring Configuration Tool Security**

**No Security**

Without configuring **SECURITY** in the "*RESOURCES" section of the UBBCONFIG file or configuring it with a value of "NONE", no security is used for accessing the SALT Configuration Tool. Anyone who knows the URL of the tool can access it. Listing 8 shows a UBBCONFIG file "*RESOURCES" section example.

```
110 Configuring a SALT Application
```
Enabling the SALT Configuration Tool

Listing 8  No Security UBBCONFIG *RESOURCES Section Example

*RESOURCES
IPCKEY 15301
DOMAIN mydomain
MASTER machine1
MAXACCESSERS 50
MAXSERVERS 10
MAXSERVICES 40
MODEL SHM
LDBAL N

Application Password Security
Configuring SECURITY in the "*RESOURCES" section with a value of APP_PW causes Oracle Tuxedo application password security to be enabled. Users who want to access the SALT configuration tool are requested to present this password; failure to do so results in denied access. Listing 9 shows a UBBCONFIG file "*RESOURCES" section example.

Listing 9  Application Password Security UBBCONFIG *RESOURCES Section Example

*RESOURCES
IPCKEY 15301
DOMAIN mydomain
MASTER machine1
MAXACCESSERS 50
MAXSERVERS 10
MAXSERVICES 40
MODEL SHM
LDBAL N
User Authentication Security

Configuring SECURITY in the "*RESOURCES" section with a value of USER_AUTH causes Oracle Tuxedo user authentication security to be enabled. To access the SALT configuration tool users are requested to present a valid Oracle Tuxedo user name and password; failure to do so results in denied access. Listing 10 shows a UBBCONFIG file "*RESOURCES" section example.

Listing 10  User Authentication Security UBBCONFIG *RESOURCES Section Example

<table>
<thead>
<tr>
<th>SECURITY</th>
<th>APP_PW</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_AUTH</td>
<td></td>
</tr>
</tbody>
</table>

A user can be added using the "tpusradd" command. The following example adds user "tom" to the group with group id 1000 in the Oracle Tuxedo application domain.

$ tpusradd -u 2503 -g 1000 tom

Access Control List Security

Configuring SECURITY in the "*RESOURCES" section with a value of ACL causes Oracle Tuxedo access control list security to be enabled. Anyone who wants to access the SALT configuration tool is requested to present a valid Oracle Tuxedo user name and password that belongs to the
Enabling the SALT Configuration Tool

Listing 11  Access Control List Security UBBCONFIG *RESOURCES Section Example

*RESOURCES
IPCKEY       15301
DOMAIN       mydomain
MASTER       machinel
MAXACCESSERS 50
MAXSERVERS   10
MAXSERVICES  40
MODEL        SHM
LDBAL        N
SECURITY     ACL

Access control to the configuration tool can be added using the "tpacladd" command. The following example adds Configuration Tool service "SALTWEBCONSOLE" to the access control list in an Oracle Tuxedo application domain.

$ tpacladd -g 1000 SALTWEBCONSOLE

If the service is not added to the Oracle Tuxedo access control security data file, any user with a valid Oracle Tuxedo user name and password can access the SALT Web Console.

Mandatory Access Control List Security

Configuring SECURITY in the "*RESOURCES" section with a value of MANDATORY_ACL causes Oracle Tuxedo access control list security to be enabled. Anyone who wants to access the SALT configuration tool is requested to present a valid Oracle Tuxedo user name and password that belongs to the group(s) allowed to access the configuration tool; failure to do so results in denied access. Listing 12 shows a UBBCONFIG file "*RESOURCES" section example.
Listing 12  Mandatory Access Control List Security UBBCONFIG *RESOURCES Section Example

*RESOURCES
IPCKEY                  15301
DOMAIN                  mydomain
MASTER                  machine1
MAXACCESSERS            50
MAXSERVERS              10
MAXSERVICES             40
MODEL                   SHM
LDBAL                   N
SECURITY                MANDATORY_ACL

Access control to the configuration tool can be added using the "tpacladd" command. The following example adds the configuration tool service "SALTWEBCONSOLE" to the access control list in the Oracle Tuxedo application domain.

$ tpacladd -g 1000 SALTWEBCONSOLE

If the service is not added to the Oracle Tuxedo access control security data file, then you cannot access the SALT Web Console.

See Also

- tmadnin
- tmloadrepos
- ubbconfig
- WSDF documentation
- SALT Programming Guide
- SALT Reference Guide
- SALT Interoperability Guide