Compuware Enterprise Services User Guide

Table of Contents

Welcome to Compuware Enterprise Services

Compuware Enterprise Services (CES) is a required web platform component providing common services for both Compuware's web-based products and Topaz Workbench.

From Compuware Enterprise Services, you are able to navigate between other installed Compuware web-based products. Those products are organized within the following three product groups:

Operations

- Abend-AID
- Fault Analytics
- iStrobe
- Topaz for Java Performance
- ThruPut Manager

Build and Deploy

- ISPW

Cybersecurity

- Application Audit

To access the Administration page

In Compuware Enterprise Services, do one of the following:

- Click  and then select **Administration**.

The **Administration** page appears.

To access any of the installed Compuware web-based applications

From the Compuware Web Products Home page, do one of the following:

- Using the mouse, hover over a product category and select the appropriate product card. If a product is not installed, the card will be disabled.
- Click  and then select the product application. Only installed products will appear in the Web Products Menu.

The application's home page appears.

To access Help for any of the installed web-based applications

Click  and select **Help** from the menu. The online help for the selected page appears.

- Select **Help** from the menu. The online help for the selected page appears.
- Select **About** from the menu. The **About Compuware Enterprise Services** window appears. This allows you to view version, build, copyright, and other Compuware Enterprise Services information. It also provides information for contacting Compuware.

- Select **Collect Support Files**. The **Support file name** dialog box appears. Enter a name for the support Zip file being created and click **OK** to start the download.

To log on/log off or change host connections, or to access user profiles

If your security mode is set to either Internal or LDAP, you can log off of web products. If you are in a web product that utilizes host connections, you can log on, log off, or change host connections for that web product.

Related Topics

Administration

Database Settings

Host Connection Settings

Issue Tracking Settings

Licensing Settings

Security Settings

Update Center

Webhooks

Web Server

Administration

The Administration settings page allows you to access and manage settings within Compuware Enterprise Services. Click a function icon to access the settings for that function.

Related Topics

Welcome to Compuware Enterprise Services

Database Settings

Host Connection Settings

Issue Tracking Settings

Licensing Settings

Security Settings

Update Center

Webhooks

Web Server

Database Settings

The Database Settings option allows you to change the currently installed database used to store information related to the Compuware Enterprise Services server. By default, Compuware Enterprise Services installs and uses an Apache Derby database until you either switch or migrate to a different database.

The Database Settings option within Compuware Enterprise Services allows you to do one of the following:

- Define the currently installed database used to store information related to the Compuware Enterprise Services server.
- Have Compuware generate the data needed to run CES.
- Specify an email address to receive notifications when the database goes down or comes back up.

Change the Installed Database

If you are switching to a different database, follow the steps below.

1. Access Database Settings by selecting **Administration** from the Compuware Enterprise Services menu, and then clicking **Database**.
2. Select a **Database** from the database field:
    - **Product Database** -- This is the full operating database.
    - **SMF Archive Database** -- This allows you to set up a database for archiving iStrobe SMF data from the iStrobe database. This database must be set up before you are able to archive iStrobe SMF data. The iStrobe SMF Database is only for those enterprise-level databases supported by iStrobe.
3. Set the **DBMS Type** to any one of the following:
    - Apache Derby -- This is set by default during installation of CES. This is not an option when setting up an SMF Archive Database.
    - Microsoft SQL Server
    - IBM Db2 LUW
    - IBM Db2 z/OS
    - Oracle

     If you are using an IBM Db2 for LUW database, you must ensure that the number of local database connections which can be concurrently active exceeds the number of databases active. Review the NUMDB parameter in the DBM configuration using the configuration assistant utility.
4. Continue by entering information for the following fields as determined by the selected DBMS Type above:
    - **Database Server** -- This is the DNS name or the IP address of the server.
    - **Port** -- This is the port on which this database is listening.
    - **Instance Name** -- This is the named instance of SQL Server. If your Microsoft SQL Server database uses a port, then you don't need this.
    - **Database Location** -- This is the location name of your Db2 host.
    - **Database Name** -- This is the name of the database you wish to use. This must be created in advance. CES will not create the database programmatically.
    - **Schema** -- This is the schema you would like to associate the data objects with. This will get created if it does not already exist.

- **JDBC driver path** -- The IBM Data Server Db2 Driver for JDBC and SQLJ must be installed for that Db2 subsystem. Be sure that the driver files can be read by the CES installation program running on your system.

- **Security mode** -- The security mode feature is available for either IBM Db2 z/OS or Microsoft SQL Server. It specifies the log on mode to use when accessing the CES database. Depending on which DBMS type you've selected, choose from the following modes:

    - **Standard** -- Log on to Db2 using a user ID and password in plain text.

    - **ID Only** -- Log on to Db2 using a user ID that does not require a password.

    - **AES Encrypted Password** -- Log on to Db2 using an unencrypted user ID, and an AES encrypted password.

    - **AES Encrypted ID and Password** -- Log on to Db2 using AES encryption for both the user ID and password.

    - **PassTicket** -- This security mode can only be applied with an IBM Db2 z/OS DBMS. Log on to Db2 using a PassTicket generated by a PassTicket generator. The User ID cannot have the PROTECTED attribute enabled. Compuware uses IRRRACF.jar to generate the PassTickets.

      A Passticket is generated based on an application ID (APPLID) and a User ID.

      The APPLID is set using the *required* environment variable **ces.passticket.db2.applid**. The User ID can be set using the *optional* environment variable **ces.passticket.db2.userid**. The default is the user ID under which the CES job is running.

      If the user provides a custom PassTicket generator, then they must also specify the provider ID using the environment variable **ces.passticket.db2.provider**. The default provider name for the passticket generator provided by Compuware (for USS only) is **CES-USS-DB2**.

      In order for SMF data collection or parallel (asynchronous) profile processing to work with PassTickets, CES must also have the class name and bundle name for the PassTicket generator. These values must be provided in the new PassTicket fields *PassTIcket Class* and *PassTicket Bundle Name* on the database configuration screen. These fields are only visible when the security mode is set to PassTicket.

      When using the Passticket generator provided by Compuware (for USS only), the Passticket Class must be set to **com.compuware.ces.passticket.provider.PassTicketProvider**, and the PassTicket Bundle Name must be set to **com.compuware.ces.passticket.provider** .

    - **None** -- SSL is not requested or used. This is the default.
    - **Request** -- SSL is requested. If the server does not support it, then a plain connection is used.
    - **Require** -- SSL is requested. If the server does not support it, then an exception is thrown.
    - **Authenticate** -- SSL is requested. If the server does not support it, then an exception is thrown and the server's certificate must be signed by a trusted CA.

- **Use Windows Authentication**-- This is only visible when the DBMS Type above is set to Microsoft SQL Server. Switching it to **On** allows you to use Windows Authorization when logging on to the Microsoft SQL Server Database.

- **Database User ID** -- This ID is required. If the Database administrator ID is not specified, then this ID will be used to create the tables, indexes, and views used by CES. Otherwise, the ID is for use by the CES application. The ID must have one of the following privileges:

- **CREATETAB** authority for the database; USE privilege for its table space
- **DBADM** authority for the database
- **SYSADM** authority

- **Database User Password** -- This is the user's password associated with the database.

   You are able to use Windows Authority for SQL server databases with CES on Windows under the following conditions:

  - Your SQL Server is configured for Windows Authority.

  - CES may run as either the local system (default) or a user account. If using LDAP, then CES must run as the user account.

- **Secondary Authorization ID** -- When specified, this ID will be used in a 'SET CURRENT SQLID' statement prior to any execution of DDL. It is used when the Database user ID and/or Database administrator ID does not have the privileges to create the CES tables, indexes and views. The ID must have the minimum Db2 authorizations, outlined under the Database User ID and Database Administrator ID options.

  To use the secondary authorization ID for updating data or inserting data into the database, check the box labeled **Use secondary authorization ID for updating data**. By leaving it unchecked, the secondary authorization ID is used only during the creation of the database.

- **Database Administrator ID** -- This is the Administrator ID associated with this database. When specified, it will only be used to create the tables, indexes, and views used by CES. This is an optional field and only required if the Database User ID does not have the following roles:

  - **CREATETAB** authority for the database; USE privilege for its table space
  - **DBADM** authority for the database
  - **SYSADM** authority

- **Database Administrator Password** -- This is the password associated with the Database Administrator ID.

   Changing either the database user ID or the database user password fields will change the credentials only.

   The Database Administrator ID and Database Administrator Password are not required if the user ID and user password entered have sufficient authority to set up the database. This includes creation of tables, views, indexes, stored procedures, functions and triggers.

   If you have changed either the user ID or the user password associated with the iStrobe database, you must also reflect those changes in the database user ID and password.

- **Use SSL connection to database** -- Indicates whether or not to use a secure socket connection to the database.

- **SSL connection keystore** -- Identifies where the key is stored.

- **Keystore password** -- Identifies the password for the keystore.

- **Email Notification** -- Optional field that allows a user to specify an email address to receive an email notification when the database goes down. If the database comes back up at any point, CES will resume functioning automatically and notify that address as well.

 To have the email sent to multiple recipients, specify an email address associated with a distribution list.

5. Click **Apply** to apply the changes.

6. You are prompted to either create a new database, switch databases, or migrate data from an existing Apache Derby database.

   - **New** database: CES supports the assignment of the storage group and buffer pools when creating a new database. These changes do not affect the upgrading of an existing database.

     When creating a new database, you are prompted for the storage group name and buffer pools. The storage group name is required. The buffer pool names will default to BP0, BP8K0, BP16K0 and BP32K. CES will assign tables to all 4 buffer pool sizes, so at least one buffer pool must exist for each.

     The storage group name and buffer pool selections will be included in the DDL generated when using the Generate DDL function, so the assignments can be reviewed or modified before executing the DDL.

   - **Switch** databases: When using any Compuware Enterprise Services database, you can switch to a different database type. This can happen with a new database or one that was previously used. If the database is from an older version of CES, you are prompted to upgrade.

     Before upgrading a database you should consider making a backup as the upgrade process is not reversible. If the upgrade fails, address the cause of the failure and rerun the upgrade. The upgrade will continue from the point of failure. Continue this process until the upgrade completes successfully.

      When upgrading a Db2 database to CES 18.2 or later, and using both a user and administrator ID, grants will be executed giving the user ID the following authorities:

     - For CES database tables, the authority to *select, update, delete, and insert.*
     - For CES database views,the authority to *select*.

      If grants fail, the database will still be upgraded and the updated database configuration saved in CES. The user will then be given the ability to download the grants DDL script to manually execute the grants. The grants DDL script will grant authorities on the following views:

     - CICS_SERVICE_TIME_VIEW
     - DDF_SQL_ACTIVITY_EXEC_VIEW
     - DDF_SQL_ACTIVITY_TARGET_VIEW
     - FOLDERACL_VIEW
     - PRF_DBRM_SEARCH_VIEW
     - PRF_DDNAME_DSNAME_SEARCH_VIEW
     - PRF_INDEX_VIEW
     - PRF_MODULE_SEARCH_VIEW
     - PUP_SUBSYS_VIEW
     - VIP_USAGE_VIEW

   - **Migrate** data: When using a Derby database, you can migrate the existing data into a new Compuware Enterprise Services database.

Update the Installed Database Configuration Settings

If your database configuration has changed, after a driver upgrade for example, follow the same steps detailed above in the Change the Installed Database section to make the necessary modifications.

Generate DDL (does not apply to Derby databases)

You may choose to have Compuware generate DDL that your database administrator can manually run to either create a new database for use by CES or upgrade an existing Db2 z/OS database used by a previous version of CES.

To create a new database through generated DDL

1. Access Database Settings by selecting **Administration** from the Compuware Enterprise Services menu, and then clicking **Database**.
2. Select the database type.
3. If provided by your database administrator, enter the following:
    - Database name
    - Schema
    - Secondary auth ID if required (when using Db2 for z/OS)

4. Click **Generate DDL** to save the generated DDL as a file named **ddlCreationScripts.zip** by default.

    CAUTION: If you see a default filename of **ddlUpgradeScripts.zip**, CES connected to an existing database requiring an upgrade, and CES generated upgrade scripts instead. If that is not your intention, review your configuration before proceeding.

5. If your chosen database was Db2 z/OS, you may be prompted for storage group and bufferpool settings. Enter those settings and click **OK** to continue.

6. After the database administrator has extracted and run the generated DDL to create the database, access the Database Settings within CES again to enter your database settings and click **Apply**.

To upgrade an existing database through generated DDL

1. Access Database Settings by selecting **Administration** from the Compuware Enterprise Services menu, and then clicking **Database**.
2. Confirm your existing database connection settings, being sure to enter the Database user password if applicable.

     CES must be able to connect to the database to generate upgrade DDL. If it cannot connect, CES will instead generate DDL to create a new database.

3. Click **Generate DDL** to save the generated DDL in the Downloads folder as a file named **ddlUpgradeScripts.zip**.

    CAUTION: If you see a default filename of **ddlCreationScripts.zip** , CES could not connect to the specified database or a database upgrade was not required, and CES generated creation scripts instead. If that is not your intention, review your configuration before proceeding.

4. If your chosen database was Db2 z/OS, you may be prompted for storage group and bufferpool settings. Enter those settings and click **OK** to continue.

5. After the database administrator has extracted and run the generated DDL to upgrade the database, access the Database Settings within CES again to confirm your database settings and click **Apply**.

Related Topics

Welcome to Compuware Enterprise Services

Enterprise Services

Host Connection Settings

Issue Tracking Settings

Licensing Settings

Security Settings

Update Center

Webhooks

Web Server Settings

Host Connection Settings

Host Connection settings are used to configure connections to the mainframe using Compuware's Host Communications Interface (HCI). Multiple connections can be defined since multiple HCI instances can be deployed on your mainframe systems. The connections can be associated with security groups to restrict user access to specific connections. The communications through this connection can also be secured using an encryption protocol to ensure the data being sent back and forth is secure and private.

If Compuware Enterprise Services has security enabled—refer to the Security Settings Help topic for more information—then the connection can be associated with security groups. This will restrict access to the connection to only those users belonging to that security group.

A table displays all the configured connections. The page displays 25 connections per page in the table by default. More, or fewer, connections can be displayed per page by changing the value of “Show N entries”. The list of connections can also be filtered by clicking on the filter icon and providing filter criteria in the filter field. The order of the connections can be altered by clicking on a column header to change the sorting. Multiple columns can be sorted by holding the shift key when clicking on the column headers.

The status of the connection is displayed allowing a quick overview as to which connections are currently up and running. A green arrow pointing up indicates that the connection is currently running. A red arrow pointing down indicates that the connection is currently not running. A question mark indicates that the status of the connection is unknown. If the status is unknown, click the information icon to update the status. You can also update the status by clicking **Test** in the Edit dialog box, and the clicking **OK**.

Further details about a connection can be obtained by clicking on the information icon when hovering the mouse over a connection. The details will describe which Topaz products are currently licensed and information about the Compuware Shared Services that are associated with that HCI.

To access the Host Connection Settings page, click Administration from the Compuware Enterprise Services menu, then click the Host Connections icon. If security has been enabled for Compuware Enterprise Services, access to the Host Connection Settings page is restricted to users with administrative privileges.

Topaz Workbench can synchronize with this list of connections. When synchronizing the list of connections, only ungrouped connections, as well as those connections associated with a group to which that Topaz Workbench user belongs, will be displayed. Refer to the Topaz Workbench User Guide for complete details on synchronizing host connections. Refer to the Strobe/HCI configuration documentation for more information on details to support multiple Strobe instances. If you wish to use this web service, contact Compuware Customer Support for full documentation.

When updating from a release prior to 18.02.02, all existing groups will be migrated to match any defined security groups. If a matching security group cannot be found, the connection will be ungrouped.

The buttons above the columns include:

Set Filters: To filter the contents of the **Host Connection Settings** table, click , then enter the value you want to filter by. Everything not containing that value will be hidden. To clear the filter, click.

Show Event History: To show the history of HCI events, click .

To create a new connection

1. From the **Host Connection Settings** page, click **Add**. A form appears with several fields:

   - **Description** – A text description of the connection. This field is required and must be unique. When accessing a configured connection, this description will be presented to the user.
   - **Host** – The z/OS host system name or IP address on which the HCI is running. This field is required.
   - **Port** – The port number which the HCI uses for listening for client requests. This field is required.
   - **Encryption Protocol** – The encryption protocol to use for securing the communications with the HCI. For this to work properly, the HCI must be configured with that protocol on the port specified above. The default for this field is “None”.

- **Groups** – The security groups that are to be associated with this connection. The default for the connection is to be “Ungrouped” by having no security groups associated.

  Only users belonging to this group have access to this connection. Any ungrouped connections are available to all users.

2. Optionally, click **Test** to test the values entered. A status message displays indicating whether a successful connection could be made using the values entered.

3. After entering values in the required fields, click **OK**. The new connection appears in the list of connections.

To edit a connection

1. From the **Host Connection Settings** page, select the Host Connection to be edited and click **Edit**. The same form that is presented for creating a new connection will be displayed, however, the fields will be populated with the values assigned to the connection being edited.

2. Modify the values in the fields and click **OK**.

 The Test button can be optionally clicked before clicking the OK button, and will perform the same test as in creating a new connection, but with the modified values.

To remove a connection

1. From the **Host Connection Settings** page, select one or more connections in the table.

2. Click **Remove**. The selected connections are removed from the list of connections.

Related Topics

Welcome to Compuware Enterprise Services

Administration

Database Settings

Issue Tracking Settings

Licensing Settings

Security Settings

Update Center

Webhooks

Web Server Settings

Issue Tracking Settings

The **Issue Tracking Settings** page allows an administrator to configure integration between Compuware's products and Atlassian's JIRA issue tracking system. This integration can be leveraged from Abend-AID web viewer or iStrobe to log issues directly in JIRA from the **Submit Fix Request** page.

The integration enables the rich issue recreation and debugging information to be stored in JIRA, which can then be used to track the issue and assign it to an application development team for resolution. Users of Topaz Workbench can access the JIRA and import the Fix Request attachment to automatically configure a debugging session to recreate and fix the issue.

From the **Issue Tracking Settings** page, you can add, edit, or remove configuration settings.

To add an Issue Tracking configuration

1. From the **Issue Tracking Settings** page, click **Add**. The Location & Credentials step appears.
2. Complete the following fields:
    - In the **Name** field, enter a descriptive name for the issue. This is used as an identifier in iStrobe.
    - In the **Type** field, select the type of issue tracking system being used. Currently, JIRA is the only tracking system supported by Compuware Enterprise Services.
    - In the **Server** field, enter the location of the server on which the issue tracking system resides.
    - In the **User Name** field, enter your user name. You must have authority to create JIRA issues.
    - In the **Password** field, enter the password associated with your user name.
3. Click **Next**. The Project Information step appears.
4. Choose the appropriate project information for the selected issue tracking system.
    - In the **Project** field, select a project from the list.
    - In the **Issue Type** field, select an issue type from the list.
5. Click **Next**. The Field Mappings step appears. The Field Mappings step identifies those fields within the issue tracking system.
6. Select appropriate values for each of the fields. These fields will vary and correspond specifically with those in the selected issue tracking system.
7. Click **Finish**. The issue tracking configuration is added to the list of configurations.

To edit an Issue Tracking configuration

1. From the **Issue Tracking Settings** page, point to an issue tracking configuration and click on it. The configuration is selected.
2. Click **Edit**. The Location & Credentials step appears. Change the fields as needed.
3. Click **Next** to advance through the steps, changing content of fields within those steps as needed.
4. Click **Finish**. The issue tracking configuration is edited and saved within the list of configurations.

To remove an Issue Tracking configuration

1. From the **Issue Tracking Settings** page, point to an issue tracking configuration and click on it. The configuration is selected.
2. Click **Remove**. The issue tracking configuration is removed from the list of configurations.

Related Topics

Welcome to Compuware Enterprise Services

Administration

Database Settings

Host Connection Settings

Licensing Settings

Security Settings

Update Center

Webhooks

Web Server

Topaz License Settings

Topaz License Settings allows you to configure license lease durations and display a list of license holders for those Topaz licenses being used at your site. This function is specific only to those sites using either Topaz or Topaz for Java Performance.

Topaz License Settings also allows you to view license usage history and export that history to a .csv file.

To view a list of licenses being used by a feature pack

Select one of three feature packs from the drop-down list:

- **Topaz for Enterprise Data** is a timed license with a specific duration measured in hours. Changing the lease duration affects the duration of future leases only. Set the duration by adjusting the hours under Configuration and clicking **Apply**. When leased, the unique identifier displays as the IP address for the Topaz user.
- **Topaz for Program Analysis** is a timed license with a specific duration measured in hours. Changing the lease duration affects the duration of future leases only. Set the duration by adjusting the hours under Configuration and clicking **Apply**. When leased, the unique identifier displays as the IP address for the Topaz user.
- **Topaz for Java Performance** is not a timed license, but rather it is licensed by the connected agent within the LPAR. The license can be held for an indefinite period. Selecting an LPAR allows you to view those licenses associated with the LPAR. When leased, the unique identifier displays as the agent name.
- **Topaz for Total Test** is a timed license with a specific duration measured in hours. Changing the lease duration affects the duration of future leases only. Set the duration by adjusting the hours under Configuration and clicking **Apply**. When leased, the unique identifier displays as the IP address for the Topaz user.

To view license usage history

Click **License Usage History** from the Leases section to navigate to the **Topaz License History** page. This page displays a list of all license events and identifies when the license was obtained and when it was released. It also identifies any errors that occurred while trying to obtain or release a license.

You can also remove entries from the usage history based on age by clicking **Clear History** and selecting an appropriate time period.

Related Topics

Welcome to Compuware Enterprise Services

Administration

Database Settings

Host Connection Settings

Issue Tracking Settings

Security Settings

Update Center

Webhooks

Web Server

Security

Compuware Enterprise Services provides the ability to secure access to Compuware web products, product functions, administrative functions, and REST endpoints. With security enabled, a user must provide credentials to access Compuware web products. By default, administrative functions are restricted and users will only have access to the base web product functions. Restricted functions do not display in the user interface and REST endpoints will be inaccessible.

The Security page has five tabs:

- Personal Access Tokens tab
- Security tab
- Users tab
- Groups tab
- Roles tab

Personal Access Tokens tab

The Personal Access Tokens tab allows you to manage personal access tokens. Personal access tokens are used in place of your credentials when performing ISPW operations using the ISPW API. Personal access tokens are a widespread standard used across well-known organizations and services.

A personal access token is required to authenticate with ISPW when using the ISPW API.

When accessing the Personal Access Tokens tab, a list of configured personal access tokens are displayed which show the user name, generated token, host, and port. The number of personal access tokens displayed in the list at a given time can be changed by selecting a different value in the option field below the list. The default is 25 entries per page but can be changed to 10, 25, 50, 100, 500, or all.

To access a Personal Access Token

In Compuware Enterprise Services, select **Administration >Security**, and then select the **Personal Access Tokens** tab.

To add a Personal Access Token

1. From the **Personal Access Tokens** tab, click **Add**.

2. Complete each of the required fields. If you choose to create a secure host connection, be sure that the port used is already defined as a secure port on the host mainframe.

    - **User Name** – The RACF login name that will be associated with the token.
    - **Token** – A generated token used when making API requests.
    - **Host Connection** – z/OS host system name or IP address that is running ISPW.

3. When complete, click **OK** to add the personal access token to the list of personal access tokens.

To edit a Personal Access Token

1. From the **Personal Access Tokens** tab, select the personal access token to be edited by clicking on it, and then click **Edit**.

2. Modify the content of the field(s) as needed. If you choose to create a secure host connection, be sure that the port used is already defined as a secure port on the host mainframe. You may also modify the password.

3. When complete, click **OK**. The personal access token has been edited and returned to the list of personal access tokens.

To remove a Personal Access Token

1. From the **Personal Access Tokens** tab, select the Personal Access Token to be removed. You may remove more than one at a time.
2. Click **Remove**. The selected Personal Access Token is removed from the list.

Security tab

The Security tab allows you to enable secure access to administrative functions of Compuware Enterprise Services.

User authentication is achieved through the use of Compuware Enterprise Services internal authentication system, or by utilizing your existing LDAP, X.509, or Kerberos enterprise authentication system. By enabling security, you are able to manage Users, Groups, and Roles.

Although you are not required to secure access to Compuware web products, you should consult with the network security group at your site to determine whether or not to enable security for Compuware Web Products.

To access security settings in Compuware Enterprise Services, select **Administration >Security**, and then select the **Security** tab.

Authentication Mode

The authentication mode provides the ability to enable or disable security, configure settings that apply to all authentication systems, and configure an authentication system. To enable security, set the authentication mode switch to **On**.

To support older versions of integrated Compuware products that do not support Compuware Enterprise Services security, options are available to disable security for those specific products. By default, security is disabled (Off) for all of the integrated Compuware products to ensure that these integrations continue to work with Compuware Enterprise Services. Security can be enabled (On) for those Compuware products which have a release version compatible with Compuware Enterprise Services security.

- **Require CMSC authentication** requires CMSC to authenticate via a preshared key. To enable CMSC authentication, set the switch to **On**.
- **Require Topaz Workbench user authentication** requires Topaz Workbench to authenticate using any of the four authentication modes. Without this enabled, Topaz users authenticate anonymously. To enable Topaz Workbench user authentication, set the switch to **On**.
- **Disable Abend-AID Viewer Find and Fix requests** Abend-AID Viewer does not support authentication. To disable Abend-AID Viewer Find and Fix requests, set the switch to **On**.

Internal

With security mode set to Internal

When security is enabled with the Internal authentication mode, Compuware Enterprise Services manages authenticating users, as well as managing user names and passwords. This mode is appropriate when do not have an enterprise authentication system, or you do not wish integrate with an enterprise authentication system. This mode replaces previous functionality in Compuware Enterprise Services and iStrobe where passwords were required for administrator access. It also replaces the functionality in iStrobe that required authentication with a user name only.

1. From the **Security** window in **Administration**, toggle the Authentication Mode to **On**.
2. Select the Internal option.

3. To allow new users to self register when they authenticate for the first time in a Compuware web product, toggle **Allow new users to self register** to **On**.

4. Enter a user name and password for the main administrator of Compuware Enterprise Services.

5. Click **Apply** to save and apply the security settings. Compuware Enterprise Services will restart to implement the changes to the security settings.

LDAP

To configure and enable security using LDAP

When security is enabled with an **LDAP** authentication server, Compuware web products will authenticate users with that LDAP server. This mode offers better user management since user accounts are stored in a centralized LDAP server. Valid LDAP users are registered with Compuware Enterprise Services during the users initial login to a Compuware web product.

1. From the **Security** window in **Administration**, toggle the Authentication Mode to **On**.

2. Select the LDAP option.

3. Enter the following required information in each of the fields:

   - LDAP server URL
   - LDAP server port number
   - Bind with, either Search filter or User DN
   - Distinguished Name (DN)
   - Password for DN (only required when binding with a search filter)
   - Search base (only required when binding with a search filter)
   - Search filter (only required when binding with a search filter)
   - Administrator(s). Do not include the domain name in this field

4. Click **LDAP Server Connection Test**. If an LDAP server connection is available, you will be able to apply this security configuration.

5. Click **Apply** to save and apply the security settings. Compuware Enterprise Services will restart to implement the changes to the security settings.

Kerberos

To configure and enable security using Kerberos

Enabling security with **Kerberos** single sign on offers additional advantages over LDAP, such as faster and more secure authentication, as well as users being automatically authenticated when accessing a Compuware web product.

1. From the **Security** window in **Administration**, toggle the Authentication Mode to **On**.

2. Select the Kerberos option.

3. Enter the following required information in each of the fields:

   - Service principal
   - Keytab location
   - Administrator(s)

4. Click **Kerberos login test**. If you are able to log in, you will be able to apply this security configuration.

5. Click **Apply** to save and apply the security settings. Compuware Enterprise Services will restart to implement the changes to the security settings.

Client Certificate

To configure and enable security using a client certificate (X.509)

When security is enabled with a **client certificate (X.509)**, it uses an SSL client certificate to authenticate users. Compuware Enterprise Services must be configured to use HTTPS when using Client certificate as the authentication mode.

1. From the **Security** window in **Administration**, toggle the Authentication Mode to **On**.
2. Select the Client certificate option.
3. Enter the following required information in the field:
   - X.509 mask – The X.509 mask is a regular expression used to extract the user name from the X.509 certificate. The user name extracted is used to log into Compuware Web Products. The default mask, as shown below, extracts the contents of the Common Name (CN) field from the certificate.

     ```
     CN=(.*?),
     ```
4. Click **Apply** to save and apply the security settings. Compuware Enterprise Services will restart to implement the changes to the security settings.

Users tab

The Users tab allows you to manage the users that have access to the Compuware web applications. When accessing the users tab, a list of configured users are displayed showing the name of the user, the email address associated with that user, the groups to which the user is assigned, and the individual roles assigned to that user.

You can create and delete users and assign roles to users. Users can also be granted permissions individually by selecting an individual user and editing.

The list of users can be filtered by clicking the filter icon above the list and entering the filter criteria. For example, to filter the list to only those users having the iStrobe User role, click the filter icon and type **iStrobe User**. If you wanted to further filter the list to those users who also have the ISPW User role, you would type **iStrobe User ISPW User** into the filter.

The number of users displayed in the list at a given time can be changed by selecting a different value in the option field below the list. The default is 25 entries per page but can be changed to 10, 25, 50, 100, 500, or all.

There are four ways to add users to the list of users:

- Migrating from a previous release, existing users will be automatically migrated to CES. There are several special cases to be aware of when coming from a previous release.
  - Existing CES or iStrobe installs may have the 'Require administrative password' checkbox enabled. CES will be placed in the 'Internal' mode security on upgrade. In this case, a 18.2.1 CES user will be created called 'CESAdmin' or 'iStrobeAdmin' with the password that was defined in the previous releases user interface.
  - Existing iStrobe customers that have the 'Require user login' option selected will be upgraded to the 'Internal' mode security and asked to define a password to be used with the user ID on the upgrade to 18.2.1.
- Enabling LDAP, Kerberos, or Client Certificates authentication mode which will cause any authenticated user to be automatically added to the list. Any authenticated user will be automatically created in CES. The users will inherit the permissions of any groups that have Automatic-Assign' option checked.
- Enabling Internal authentication mode as well as enabling the 'Allow users to self-register' option. This allows users to register themselves and will add those users to the list.

- Manually adding users to the list.

To manually add a user

1. From the **Users** tab, click **Add**.
2. Complete each of the required fields.
    - **Name**: The name of the user.
    - **Password**:Add a temporary password assigned to the user. When the user first logs in they will be required to change their password.
    - **Email**: An email address associated with the user.
    - **Roles**: This list of roles that can be assigned to the user. To assign a role to a user, click the toggle to On.
3. Click **OK**. The user appears in the Users table.

To edit a user

1. From the **Users** tab, select a user from the list and click **Edit**.
2. Modify the content of the field(s) as needed. If you edit a user that is not yourself and change their password, that user will be required to change their password at their next login. Changes to any roles assigned to the user will not take effect until their next login. When you've completed editing the user, click **OK** to update the user in the list of users.

To remove a user

1. From the **Users** tab, select a user to be removed by clicking on the user name in the table. You may remove more than one at a time. You cannot remove yourself from the list of users.
2. Click **Remove**.
3. When prompted, click **Yes** to remove the user.

To modify the roles assigned to a user

1. From the **Users** tab, select a user by clicking on the user name in the table.
2. Click **Edit**.
3. Edit the roles assigned to the user as is appropriate.
4. Click **OK** to apply those roles to that user.

Groups tab

The Groups tab allows you to manage security groups. Groups provide the ability to easily assign roles to many users at a time as well as automatically assign roles to new users. Groups can also be associated with host connections to restrict user access to specific host connections. When accessing the groups tab, a list of configured groups are displayed which show the name of the group, a description of the group, the roles associated with the group, and whether or not new users are auto assigned to the group. The group is also expandable to show the list of users that belong to that group.

The list of groups can be filtered by clicking the filter icon above the list and entering the filter criteria. For example, to filter the list to only those groups that have the iStrobe User role, you would click the filter icon and type **iStrobe User**. If you wanted to further filter the list to the users that also have the ISPW User role, you would type **iStrobe User ISPW User** into the filter.

The number of groups displayed in the list at a given time can be changed by selecting a different value in the option field below the list. The default is 25 entries per page but can be changed to 10, 25, 50, 100, 500, or all.

To add a group

1. From the **Groups** tab, click **Add**.
2. Under **Group Name**, add the name of the group, and optionally add a description for the group.
3. Under **Roles**,click the toggle switch to **On** for those roles you would like assigned to the group.
4. Under **User Assignment**, click the toggle switch to **On** for those users you would like assigned to the group. To automatically assign new users to the group, click the **Auto assign users** toggle switch to **On**.
5. Click **OK** to create the group and save the settings. The group appears in the Groups table.

To edit a group

1. From the **Groups** tab, select a group by clicking on the group name to highlight it in the table.
2. Click **Edit** to reveal the attributes of the group, including the users.
3. Under **User Assignment**, click the toggle switch to **On** for those users you would like added to the group.
4. Click **OK** to save the settings for the group.

To remove a group

1. From the **Groups** tab, select a group by clicking on the group name to highlight it in the table.
2. Click **Remove**. The group is deleted from the table.

To remove a user from a group

1. From the **Groups** tab, expand the group from which you would like to delete a user by clicking the plus sign next to the group name.
2. Click **Edit**.
3. Under **User Assignment,** click the toggle switch to **Off** for the user you would like removed from the group. The user is deleted from the group.

Roles tab

The Roles tab allows you to manage security roles. Roles control the access rights to Compuware web products and functionality. By default, a number of roles are provided to cover most situations. You can customize many of the existing roles or create new roles to suit your security needs. When accessing the roles tab, a list of configured roles are displayed which show the name of the role, and a description of the role.

 The Compuware Enterprise Services Administrator and the Super Administrator roles cannot be edited or removed.

The number of roles displayed in the list at a given time can be changed by selecting a different value in the option field below the list. The default is 25 entries per page but can be changed to 10, 25, 50, 100, 500, or all.

Product Roles and Rights

Product	Default Roles	Description	Access/Rights

CES	CES Administrator	Users assigned this role have access to Compuware Enterprise Services configuration settings for Database, Host Connections, Licensing, Issue Tracking, Update Center, Security and Web Server.	• Database • Host Connections • Licensing • Issue Tracking • Update Center • Security • Web Server
	Super Admin	Users assigned this role have access to administrative functionality for all Compuware web products.	• Access to all product Administrator functionality.
iStrobe Administrator	iStrobe Administrator		• Administration • Submit Strobe Measurements • Strobe Administration • Use Performance Tracker • Folder Creation • Folder Management • Strobe Insight Reports Access
	iStrobe Performance Tracker	Users assigned this role have access to use iStrobe Performance Tracker functionality.	• Use Performance Tracker
	iStrobe User	User assigned this role have access to Submit Strobe Measurements and create Folders in iStrobe.	• Submit Strobe Measurements • Folder Creation
ISPW	ISPW Admin	Users assigned this role have access to manage ISPW server connections for use in the ISPW Web Interface.	• Access to ISPW Admin Area (until this is removed)
	ISPW User	Users assigned this role have access to the ISPW web Deployment application as well as the ISPW Mobile and Web applications.	• Mobile / Web Approvals • Deployments

	ISPW Approver	Users assigned this role have access to the ISPW Mobile and Web applications.	• Mobile / Web Approvals
Fault Analytics	Fault Analytics Administrator	Users assigned this role have access to Abend-Aid Fault Analytics' Administration, Preferences and Reports screens.	• Administration • Preferences • Reports
	Fault Analytics User	Users assigned this role have access to Abend-Aid Fault Analytics' Preferences and Reports screens.	• Preferences • Reports
TJP	Topaz for Java Performance User	Users assigned this role have full access to Topaz for Java Performance.	• Full Access to TJP
Application Audit	Application Audit User	Users assigned this role have full access to Application Audit.	• Full access to Application Audit

To add a role

1. From the **Roles** tab, click **Add**. The role appears in the Roles box. You can rename the role by clicking it and typing a new name in the Roles field.
2. Complete each of the required fields.
   - **Name**: The name of the role.
   - **Description**: An optional description of the role.
   - **Rights**: The list of rights that can be assigned to the role listed by Compuware web product. To assign a right to a role, click the toggle to **On**.
3. When the appropriate rights have been selected for a role, click **OK**. The role is saved with the given name and associated functions.

To modify functions assigned to a role

1. From the **Roles** tab, select the role to be modified by clicking it, and then click **Edit**.
2. Modify the functions assigned to the role by resetting toggle switches for various functions.
3. Click **OK**. The role is modified with the associated functions.

To delete a role

1. From the **Roles** tab, select the role to be deleted by clicking it.
2. Click **Remove** next to the role name. When prompted, click **Yes** to delete the role.

Related Topics

Welcome to Compuware Enterprise Services

Update Center

The Update Center provides a means of centrally administering updates for Compuware web-based products and Topaz Workbench. Updates are provided by obtaining an update repository, either online or manually.

- **Online** -- Update repositories can be retrieved from Compuware's cloud-based update server.

  Check with your network administrator to be sure you can issue HTTPS requests to **`update.compuware.com`** on port **`443`**. Depending on your network settings, you may need to configure proxy server settings. Refer to the Proxy settings on the Web Server Settings help page.

- **Manual** -- Updates can be performed manually by uploading a repository file.

Users have the option to opt out of automatic database upgrades when applying maintenance. In those instances, however, CES will be unusable until the database is manually upgraded. The user can have CES upgrade the database by either connecting at the Database Settings page or by generating upgrade ddl as detailed in the Database Settings online help page under **Generate DDL**.

Updating Compuware Web Products

Follow the instructions below to update Compuware Web Products, either online or manually.

To update Compuware Web Products online

1. From the Compuware Enterprise Services menu, click **Administration** and then click **Update Center**. The Update Center page appears.
2. Click the **Updates** tab.
3. Set the **Check for updates online** switch to **On**.
4. To show the latest versions only of the web-based products, set the **Show latest versions only** switch to **On**.
5. Under **Compuware Web Products**, click **Download** to download and process the repository. The progress bar indicates when the download has completed.
6. Click **Apply** to apply the update. Compuware Enterprise Services automatically restarts to complete the maintenance operation. If a database upgrade is necessary, the database will then be automatically upgraded.

   For instruction on manually updating a database, refer to the topic in the Database Settings section of this online help.

   It is recommended that users log out before applying an update. Active users may experience inconsistent behavior during the upgrade process.

7. At the end of the upgrade process, a status message appears indicating that product updates were applied and the Compuware Enterprise Services server successfully restarted.

To manually update Compuware Web Products

This process presumes you have downloaded the update file from the Compuware Support Center website. Be sure that the update file you've downloaded is the appropriate version for the Compuware web-based product.

1. After downloading the update file, launch the Compuware Enterprise Services application.
2. From Compuware Enterprise Services menu, click **Administration** and then click **Update Center**. The Update Center page appears.
3. Click the **Updates** tab.

4. Set the **Check for updates online** switch to **Off**.

5. Under **Manual Compuware Web Products Update**, click **Upload**. Select the update file you wish to apply, and click **Open**. The upload process runs and the progress bar indicates when the upload is complete.

6. Click **Apply** to apply the update. Compuware Enterprise Services automatically restarts to complete the maintenance operation. If a database upgrade is necessary, the database will then be automatically upgraded.

 It is recommended that users log out before applying an update. Active users may experience inconsistent behavior during the upgrade process.

7. At the end of the upgrade process, a status message appears indicating that product updates were applied and the Compuware Enterprise Services server successfully restarted.

Updating Topaz Workbench

Follow the instructions below to allow Topaz Workbench users to update the Topaz Workbench repository, either online or manually.

To update Topaz Workbench online

1. From the Compuware Enterprise Services menu, click **Administration** and then click **Update Center**. The Update Center page appears.

2. Click the **Updates** tab.

3. Set the **Check for updates online** switch to **On**.

4. To show the latest versions only of the web-based products, set the **Show latest versions only** switch to **On**.

5. Under **Topaz Workbench**, click **Download** to download and process the downloaded repository. The progress bar indicates when the download has completed.

6. Click **Done**. The p2 repository file download is complete and the repository is hosted for access by Topaz Workbench.

7. Instruct Topaz Workbench users to perform an update by navigating to the **Topaz Workbench Help Menu** and selecting **Check for Updates**.

To manually update Topaz Workbench

This process presumes you have downloaded the Topaz Workbench P2 Repository from the Compuware Support Center website. Be sure that the p2 repository you've downloaded is appropriate for your version of Topaz Workbench.

1. After downloading the p2 repository for the Topaz Workbench, launch the Compuware Enterprise Services application.

2. From Compuware Enterprise Services menu, click **Administration** and then click **Update Center**. The Update Center page appears.

3. Click the **Updates** tab.

4. Set the **Check for updates online** switch to **Off**.

5. Under **Manual Topaz Workbench Update**, click **Upload**. Select the update file you wish to host, and click **Open**. The upload process runs and the progress bar indicates when the upload is complete.

6. Click **Done**. The p2 repository file upload is complete and the repository is hosted for access by Topaz Workbench.

7. Instruct Topaz Workbench users to perform an update by navigating to the **Topaz Workbench Help Menu** and selecting **Check for Updates**.

Related Topics

Welcome to Compuware Enterprise Services

Administration

Database Settings

Host Connection Settings

Issue Tracking Settings

Licensing Settings

Security Settings

Webhooks

Web Server

Web Server Settings

The Web Server Settings page allows you configure and manage settings for the following:

- Web Server
- Proxy
- Ports
- Email
- Logging

Web Server

The Web Server settings tab allows you to change the following server settings established during installation:

- **Protocol** established (HTTP or HTTPS).
  You can choose to enable either protocol or enable both protocols by clicking the **On/Off** switch for each.

- **Port settings** established.
  You can choose to change the established port for each protocol.

If you choose to enable **HTTPS**, you must be prepared to provide a keystore and, optionally, a truststore as follows:

For Windows or Linux:

- When using the **Java Keystore** type, you must provide the location of the Java keystore file (.jks) on the server, as well as the Java keystore password.

- When selecting **TrustStore** for client certificate authentication, you must provide the location of the TrustStore on the server. The TrustStore can be the same as the Java Keystore.

For USS:

- When using the **Java Keystore** type, you must provide the location of the Java keystore file (.jks) on the server, as well as the Java keystore password.

- When using either the **Keyring** or the **Keyring with Hardware CCA** type, you must provide the Keyring username, as well as the Keyring name.

- When selecting **TrustStore** for client certificate authentication, you must provide the location of the TrustStore on the server. The TrustStore can be the same as the Java Keystore or the provided Keyring or Keyring with Hardware CCA type.

Proxy

The Proxy settings tab allows you to establish proxy settings for outbound HTTP requests. By toggling the **On/Off** switch for each, you can choose to enable either the HTTP proxy or the secured HTTPS proxy. You can also enable both proxy settings.

At a minimum, you must provide both the Host and Port settings. If your site has established a user name and password for each proxy, you must provide that information as well.

 If you want to use the Compuware Update Center through an HTTP proxy, you must configure using Secure Proxy.

Ports

The Ports settings tab allows you to optionally change the port settings that were established when installing Compuware Web Products. Those ports include the following:

Compuware Enterprise Services

- **Strobe Communication** - Used for communication between the mainframe and the client.
- **Compuware Enterprise Services Shutdown** - Used to stop the web application.
- **Internal Messaging** - Provides additional processing capacity.
- **Derby** - Used to start the embedded Derby database.

Abend-AID Fault Analytics

This is listed only if Abend-AID Fault Analytics has been installed.

- **Abend-AID Communication** - Used by Abend-AID Fault Analytics to transmit messages.

Topaz for Java Performance

This is listed only if Topaz for Java Performance has been installed.

- **Agent Communication** - Used for communication between the agent and the server. TJP listens on this.

iStrobe

This is listed only if iStrobe has been installed.

- **SMF Collection** - Used by iStrobe to collect SMF data.

Communication Port Security

Use the toggle switches to selectively enable and configure support for IBM AT-TLS on the communication ports. The following ports will be configured:

- Strobe communication
- SMF collection (iStrobe only)
- Agent communication (TJP only)
- Abend-AID communication (Fault Analytics only).

For more information on IBM AT-TLS, refer to the IBM documentation.

AT-TLS is only supported when HTTPS is configured and enabled. When the Communication Port Security settings are changed without HTTPS in use, the settings will not be used until HTTPS is configured and enabled.

This setting is not applicable for USS installs and will not display.

TLS Settings

Although the settings for the SSL/TLS protocol for CES can be set manually, this option is recommended for advanced users only . If the SSL/TLS protocol is manually set, CES *will not* be able to connect to applications without a matching SSL/TLS protocol until the process is undone.

To manually change the protocol, follow these steps:

1. Open the file located at **CES_DATA_DIR/jetty/etc/jetty-selector.xml**.
2. Find the line beginning with
   <New id="sslContextFactory"
   class="com.compuware.jetty.security.extension.CompuwareSslContextFactory">.
3. Find the corresponding close tag **</New>**.

4. Create a blank line immediately above the close tag **</new>**.

5. Insert the following line: **<Set name="protocol">TLSv1.2</Set>**.
   If a security level other than TLS v1.2 is required, replace where necessary.

Security levels other than TLS v1.2 have been decremented and are no longer considered secure, and are not recommended for use.

Email

The Compuware Enterprise Services email notification option allows automated email messages to be sent to users when profiles have been downloaded. You must set up the email server and sender addresses to values appropriate for your site.

To access the Email Settings, select **Administration** from the Compuware Enterprise Services menu, and click **Email**.

- **SMTP server address** – Contact your email administrator for the name or IP address of your email server. The SMTP server address length is limited to a maximum of 255 characters.

- **From address** – The sender's address appears on all email messages sent when it receives a profile. You should use a valid SMTP format address that is associated with a mailbox that you monitor. You may want to have a mailbox setup specifically for iStrobe. This email will receive all non-deliverable notifications and any other exceptions that may occur when an e-mail is sent. The From address length is limited to a maximum of 255 characters.

- **Default host** – CES installs with a default host name that is used for generating links in emails that are sent from other Compuware web applications. You can change the default host name by selecting the Custom host radio button.

- **Custom host** – To use a custom host name instead of the default host name, select this option and enter a custom host name for generating the links in the email that point to the iStrobe reports. Choosing this will override the Default host name.

Refer to your Strobe documentation to set up email notification using Strobe's SMTP E-mail Notification Address field on the iStrobe Performance Profile Options panel.

Logging

Settings in the **Logging Level** box should not be changed. The defaults are shipped for minimal logging for all Compuware web-based product log files. These settings are used for diagnostics and should only be changed when instructed to by Compuware Product Support.

You may download a log file by selecting the row in the table and clicking  above the table. You may select multiple log files for download with **ctrl+click** and/or **shift+click**. Clicking  with multiple rows selected allows you to download all of these files at once.

Clicking on a log component name presents that log's contents. Clicking  refreshes the contents of the log, and clicking  allows you to download the log.

Related Topics

Welcome to Compuware Enterprise Services

Administration

Database Settings

Webhooks

Compuware Web Products communicate with Compuware mainframe products, such as ISPW, by issuing requests and receiving responses to those requests. For example, a Deploy request can be made through Compuware Web Products to an instance of ISPW running on a mainframe. That instance of ISPW will return a response to that request, at a future time, indicating the success or failure of the Deploy action. As part of a DevOps environment, you might be interested in having a third-party application notified when ISPW actions have occurred from either Compuware Web Products or any other source. This type of integration can be achieved through the use of webhooks.

Compuware Enterprise Services Webhooks

A webhook allows third-party applications, such as Slack™, to receive notifications when an action has occurred in a Compuware mainframe product. For instance, a notification could be sent to Jenkins™ to kick off a build whenever a Promotion occurred in ISPW.

When accessing the Webhooks page in Compuware Enterprise Services, a list of configured webhooks are displayed which show the user-defined name of the webhook, the URL to where the response will be forwarded, and the type of HTTP method that will be used when forwarding the response.

The list of webhooks can be filtered by clicking the filter icon above the list and entering the filter criteria. For example, to filter the list to all POST methods you would click the filter icon and type “POST” (without quotes). If you wanted to further filter the list to all POST methods being sent to a URL containing the domain test.com, you would type “POST test.com” (without quotes) into the filter.

The number of webhooks displayed in the list at a given time can be changed by selecting a different value in the option field below the list. The default is 25 entries per page but can be changed to 10, 25, 50, 100, 500, or all.

If you have management rights then you can also add, edit, and remove webhooks.

ISPW *must* be configured to push notifications to your CES installation.

To add a webhook

1. Click **Add** below the list of webhooks. The Webhook Information page appears.
2. Configure a webhook by completing the following fields:

- **Webhook enabled**: Toggle On or Off. This specifies whether the webhook is enabled. If it is not enabled then the request to the Compuware mainframe product will not be sent and thus no responses will be received. If the webhook was previously enabled, disabling it will tell the Compuware mainframe product to stop sending any future responses.
- **Name**: This is a user-defined name for the webhook so that the webhook is easier to identify when viewing the list of webhooks.
- **URL**: This is the URL location where the Compuware mainframe product responses will be sent.

  The URL entered must begin with http:// or https://.
- **Request method**: This is the HTTP method used when the response from a Compuware mainframe product is forwarded to the specified URL. The following methods are available for selection: DELETE, GET, POST, and PUT. If the third-party application follows common conventions, then DELETE will delete a resource, GET will retrieve a resource, POST will create a resource, and PUT will edit or modify, a resource. For example, to create a new item in a third-party application when the response was received, choose the POST option.
- **Request headers**: This allows you to define any HTTP headers that need to be sent along with the response to the third-party application. For example, to provide authentication information to a third-party application, click **Add Header**. In the **Header name** field type **Authorization** and in the **Header value** field type your credential information, such as **Basic dXNlcjpwYXNzd29yZA==ik**.

- **Request body**: This specifies the information that will be sent in the body of the HTTP request to the third-party application. This is a free-form field where any text can be entered, so you can enter JSON, XML, or whatever format is required by the third-party application.

- **Product**: This specifies which Compuware mainframe product is going to receive the request.

- **Product specific fields**: The remaining fields are specific to the Compuware mainframe product selected, and will dynamically change based upon that selection. For **ISPW**, the following fields are used:

    - **Applications**: The names of the applications of an ISPW resource. Each application name must not exceed four characters with each name separated by a comma.
    - **Levels**: The current levels of an ISPW resource. Each level must not exceed four characters with each level separated by a comma.
    - **Event names**: The current names of events associated with an ISPW resource. Each event name must be separated by a comma.
    - **Operations**: The operations for which you want responses. For example, if you want to receive responses when a Deploy or Promote occurs, then you would select Deploy and Promote.

Variable substitution

Variable substitution is allowed in the URL, request headers, and request body fields. A string enclosed with $$ will be replaced with an associated value. For example, if the mainframe product supplied an ID when a notification was sent, the ID could be dynamically added to the URL by placing a variable in the URL like this:

```
http://sample.com/endpoint/$$ID$$
```

If the ID that was sent was 123-456-789 then the URL would end up looking like this:

```
http://sample.com/endpoint/123-456-789
```

The following variables are available for substituting values from ISPW:

- $$application$$ *(The names of the applications in ISPW)*
- $$deployDate$$ *(The date the resource was deployed in ISPW)*
- $$deployTime$$ *(The time the resource was deployed in ISPW)*
- $$event$$ *(The event names associated with an ISPW resource)*
- $$levels$$ *(The current levels of an ISPW resource.)*
- $$message$$ *(A message about the operation that was performed in ISPW)*
- $$notificationID$$ *(The ID associated with the notification in ISPW)*
- $$operation$$ *(The operations to be performed in ISPW)*
- $$owner$$ *(The owner of the resource in ISPW)*
- $$release$$ *(The release of ISPW)*
- $$setID$$ *(The ID of the set in ISPW)*
- $$startDate$$ *(The date the operation was started)*
- $$startTime$$ *(The time the operation was started)*
- $$stream$$ *(The stream in ISPW)*

3. After configuring the webhook, click **OK** to submit the request to the selected mainframe product, if the webhook is enabled. The webhook will then appear in the list of webhooks.

To edit a webhook

1. From the Webhook Information page, select a webhook from the list and click **Edit**. The Webhook Information page appears. The fields will be populated with the values for that webhook.

2. Edit the fields as needed.

3. Click **OK** to submit the request to the selected mainframe product.

To remove a webhook

1. Select one or more webhooks from the list.
2. Click **Remove**. The webhook is removed from the list of webhooks and the request is removed from the associated mainframe products.

Webhook Example

As a company practicing DevOps, you are using Compuware Web Products, Compuware ISPW, and Slack™. You want a notification sent to Slack™ whenever a promote occurs in ISPW. To achieve this, you would create a webhook in Compuware Web Products with the following configuration options:

- **Webhook enabled**: On
- **Name**: ISPW Promote Slack Notification
- **URL**: https://hooks.slack.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX
- **Request method**: POST
- **Request headers**: Content-type application/json
- **Request body**: { “text” : “A promote occurred in ISPW” }
- **Product**: ISPW
- **Event Type**: Promote

The “Event Criteria” was left empty so as not to filter the responses to a specific application, level, or event name. As a result, you will receive a message in Slack™ for all promotes that occur in ISPW.

Webhook Example with Variable Substitution

As a company practicing DevOps, you are using Compuware Web Products, Compuware ISPW, and Slack™. You want a notification sent to Slack™ whenever a promote occurs in ISPW. To achieve this, you would create a webhook in Compuware Web Products with the following configuration options:

- **Webhook enabled**: On
- **Name**: ISPW Promote Slack Notification
- **URL**: https://hooks.slack.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX
- **Request method**: POST
- **Request headers**: Content-type application/json
- **Request body**: {"text" : "A promote occurred in ISPW for set: $$setID$$ at levels: $$levels$$ with a status of: $$eventNames$$"}
- **Product**: ISPW
- **Event Type**: Promote

The URL would receive a POST request with the following JSON body looking like this:

```
{
   "text" : "A promote occurred in ISPW for set: S000000021 at level: DEV1 with a
status of: success"
}
```

The “Event Criteria” was left empty so as not to filter the responses to a specific application, level, or event name. As a result, you will receive a message in Slack™ for all promotes that occur in ISPW.

Related Topics

Welcome to Compuware Enterprise Services

Administration

Database Settings

Host Connection Settings

Issue Tracking Settings

Licensing Settings

Security Settings

Update Center

Web Server Settings