SWAMP-in-a-Box Reference Manual

Version 1.37, 2020-12-30 19:58:17 -0600

Table of Contents

Chapter 1. SWAMP Web Application Backend Configuration

The file `/var/www/swamp-web-server/.env` contains various parameter names and values that are used to configure the SWAMP web application's backend. You must have `root` access to modify this file.

This file should be readable only by the `apache` system user. It should **never** be world readable, because it contains usernames and passwords for accessing various resources.

Any values that include spaces must be enclosed in double-quotes. Any values that do *not* include spaces must *not* be enclosed in double-quotes.

The remainder of this section describes the parameters. Some descriptions refer to Laravel, which is the framework that the backend is built upon.

1.1. Web Application Settings

`APP_ENV`

A description of the SWAMP's environment. This parameter is informational and does not affect the functioning of the backend. The SWAMP-in-a-Box installer sets this to "SWAMP-in-a-Box".

`APP_DEBUG`

Whether verbose debugging is enabled. When set to "true", unexpected errors in the backend return a detailed error page. When set to "false", such errors return a page that says, "Whoops, looks like something went wrong." The SWAMP-in-a-Box installer sets this to "false".

`APP_URL`

The URL used to access the SWAMP's web application routes. The SWAMP-in-a-Box installer sets this based on the hostname specified during the install process (usually, the host's detected hostname).

When the hostname changes, use the `/opt/swamp/bin/swamp_set_web_host` utility script to update this parameter, because that script will update not only this parameter but also all other configuration locations where the hostname is referenced.

`APP_CORS_URL`

The URL used to access the SWAMP's web site. The SWAMP-in-a-Box installer sets this based on the hostname specified during the install process (usually, the host's detected hostname).

When the hostname changes, use the `/opt/swamp/bin/swamp_set_web_host` utility script to update this parameter, because that script will update not only this parameter but also all other configuration locations where the hostname is referenced.

APP_FLOODLIGHT

The URL and port of the Floodlight server to contact. This is not applicable to a SWAMP-in-a-Box installation.

APP_INCOMING

The path to the directory used to temporarily store files uploaded for new packages. This should always be set to "/swamp/incoming/".

APP_KEY

An encryption key used by the Laravel framework. Allowed values are any 32 character string or a Base 64 encoded value. The SWAMP-in-a-Box installer sets this to a Base 64 encoded value. SWAMP-in-a-Box installations originally deployed using versions of SWAMP-in-a-Box prior to 1.33 will have had this set to a random 32 character string.

To generate a new Base 64 encoded value, run the following command as `root` (or using `sudo`):

```
php /var/www/swamp-web-server/artisan key:generate
```

APP_PASSWORD_ENCRYPTION_METHOD

The encryption method used to hash user passwords before either storing them in the SWAMP's SQL database or sending them to an LDAP server. Allowed values are "BCRYPT", "SSHA", "SHA1", and "NONE". The SWAMP-in-a-Box installer sets this to "BCRYPT".

This should be set to "NONE" only if `LDAP_ENABLED` is "true", `LDAP_READ_ONLY` is "false", and the LDAP server does its own encryption when given a new or changed user password. This parameter is not applicable when `LDAP_ENABLED` is "true" and `LDAP_READ_ONLY` is "true".

APP_PASSWORD_MAX

The maximum number of Application Passwords a user can create. Set this to an integer greater than zero to allow creation of one or more Application Passwords. Set this to zero to disallow creation of Application Passwords. The SWAMP-in-a-Box installer sets this to 10.

APP_LOG

How Laravel log entries are stored. Set this to "daily" or "syslog". When set to "daily", Laravel writes log entries to a new file each day at `/var/www/swamp-web-server/storage/logs/`. When set to "syslog", Laravel writes log entries to the OS syslog. The SWAMP-in-a-Box installer sets this to "daily".

APP_LOG_LEVEL

What type of notices are logged by Laravel. The SWAMP-in-a-Box installer sets this to "debug", which we recommend. Other allowed values are "emergency", "alert", "critical", "error", "warning", "notice", and "info".

APP_STATS

Whether a banner showing usage statistics is displayed on the the SWAMP home page. Set this to

"true" or "false". The SWAMP-in-a-Box installer sets this to "false". Note that in order to show lines-of-code, metric analysis must be enabled, and by default, SWAMP-in-a-Box installations do not have metric analysis enabled.

`APP_CONTACT_FORM`

Whether a web form is provided to submit Contact messages. When set to "true", and if email is enabled, the Contact Us page provides a web form to submit contact messages to the configured contact address. Likewise, the Submit Security Incident page provides a web form to submit security messages to the configures security address. When set to "false", these pages provide a mailto link to the corresponding addresses.

The SWAMP-in-a-Box installer sets this parameter to "false". This is applicable only when SWAMP-in-a-Box is configured to enable "Contact Us" or "Report Security Incident".

`APP_SIGN_UP`

Whether SWAMP-in-a-Box provides a means for new users to sign-up for accounts. When set to "false", the Sign-Up button is removed from the Home page. The SWAMP-in-a-Box installer sets this to "true"

Note that if SWAMP-in-a-Box is configured to use a read-only LDAP server for user management the "Sign-Up" button will not be present on the Home page regardless of this setting.

`APP_DEFAULT_VIEWER`

The result viewer selected by default on the Assessment Results page. Set this to either "Native" or "Code DX". The SWAMP-in-a-Box installer sets this parameter to "Native".

`APP_PYTHON`

The command used by the web server to run Python scripts. This should always be set to "python3.4".

`APP_SIMPLE_STATUS_CODES`

Whether the HTTP response status codes for all successful (200 range) responses should always be "200". Set this to "true" if you are interfacing with your SWAMP-in-a-Box using a version of java_api, java_cli, or one of the SWAMP plugins that does not support successful response codes other than "200".

The SWAMP-in-a-Box installer sets this parameter to "false".

1.2. HTCondor Settings

`HTCONDOR_COLLECTOR_HOST`

The hostname of the HTCondor collector to contact for information about the SWAMP's currently running assessments. The SWAMP-in-a-Box installer sets this to "localhost".

`HTCONDOR_ROOT`

The path to the root directory of the HT Condor process used for SWAMP-in-a-Box assessments. SWAMP-in-a-Box sets this to "/opt/swamp/htcondor", which is the location of the HT Condor instance installed for SWAMP-in-a-Box.

1.3. Mail Settings

These parameters are related to outgoing email sent by the SWAMP web application.

SWAMP-in-a-Box is installed with outgoing email disabled. Prior to enabling and configuring outgoing email (instructions can be found in the SWAMP-in-a-Box Administrator Manual), you must first configure an outgoing email server for use with the SWAMP-in-a-Box host.

`MAIL_ENABLED`

Whether the SWAMP web application is configured for outgoing email. Set this to "true" or "false". When set to "false", outgoing email is disabled, and the mail-related settings described below are not applicable. When outgoing email is disabled, all functionality that would otherwise result in an email being sent by the system runs without sending the email. Specifically:

- Username is displayed instead of email throughout the web application.
- Workflows that rely on email, such as requesting a password reset, are disabled.
- Permission requests, project invitations, and SWAMP administrator invitations are handled exclusively through the notification system.
- New user accounts do not go through a "pending" state and are instead immediately activated.
- The option to receive an email on completion of an assessment is unavailable.
- The Administrator Settings page for Restricted Domains is unavailable.
- The Administrator Settings page for System Emails is unavailable.
- The Contact Us and Report Security Incident pages do not include a means to submit a message directly through the web application.

The SWAMP-in-a-Box installer sets this parameter to "false".

`MAIL_DRIVER`

The driver used to send outgoing email. Set this to "smtp" or "sendmail". The "smtp" driver makes connections directly to the configured SMTP server (see the `MAIL_HOST` parameter below) to deliver email messages. The "sendmail" driver uses the host's postfix mail system to deliver email messages.

With the "smtp" driver, when sending a message, the SWAMP web application will wait for an acknowledgment that the message was sent. With the "sendmail" driver, the SWAMP web application will **not** necessarily wait for an acknowledgment. Instead, if there are issues with the initial attempt to send the message, the web application will rely on postfix to continue attempting to deliver the message in the background.

We recommend using the "sendmail" driver.

`MAIL_HOST`

The hostname of the SMTP server. This is applicable only if `MAIL_DRIVER` is set to "smtp".

`MAIL_PORT`

The port to connect to on the SMTP server. This is applicable only if `MAIL_DRIVER` is set to "smtp".

`MAIL_FROM_ADDRESS`

The email address to be used as the sender of outgoing SWAMP email.

`MAIL_FROM_NAME`

The name to be used as the sender of outgoing SWAMP email.

`MAIL_CONTACT_ADDRESS`

The email address to which messages submitted via the Contact Us page are sent. Use this to direct contact messages to a specific administrator or help desk. This address is also displayed in the content of some SWAMP emails.

`MAIL_CONTACT_NAME`

The name to which messages submitted via the Contact Us page are sent.

`MAIL_SECURITY_ADDRESS`

The email address to which messages submitted via the Report Security Incident page are sent. Use this to direct security messages to a specific administrator or help desk. This address is also displayed in the content of some SWAMP emails.

`MAIL_SECURITY_NAME`

The name to which messages submitted via the Report Security Incident page are sent.

`MAIL_ENCRYPTION`

If `MAIL_DRIVER` is set to "smtp" and the SMTP server uses encryption, set this to the type of encryption used. Otherwise, set this to "null".

`MAIL_USERNAME`

If `MAIL_DRIVER` is set to "smtp" and the SMTP server requires a username/password, set this to the username. Otherwise, set this to "null".

`MAIL_PASSWORD`

If `MAIL_DRIVER` is set to "smtp" and the SMTP server requires a username/password, set this to the password. Otherwise, set this to "null".

1.4. LDAP Settings

These parameters are related to configuring an LDAP server to store user-related personal information for a SWAMP instance. When the SWAMP is not configured to use an LDAP server, as is the case when SWAMP-in-a-Box is initially installed, user-related personal information is stored in the SWAMP's SQL database.

`LDAP_ENABLED`

Whether the SWAMP uses an LDAP server for user authentication and storing of user data. When set to "false", a record is created for each SWAMP user in the `project` database. When set to "true", a record is created for each SWAMP user in the LDAP server. The SWAMP-in-a-Box installer sets this to "false".

`LDAP_PASSWORD_VALIDATION`

Whether verification of a user's password on sign-in is done by LDAP. When set to "true", a user's password is authenticated through an LDAP bind. When set to "false", a user's password is authenticated in PHP by comparing it to the hash stored in LDAP.

Set this to "true" when LDAP is enabled and your LDAP server is able to validate against the type of encryption used to store passwords. Set this to "false" when LDAP is enabled and LDAP is not able to validate against the type of encryption used to store passwords, such as when `LDAP_READ_ONLY` is "false" and `APP_PASSWORD_ENCRYPTION_METHOD` is "BCRYPT".

The SWAMP-in-a-Box installer sets this to "false".

`LDAP_READ_ONLY`

Whether the SWAMP is prevented from adding or editing user records in the LDAP server. When set to "false", the SWAMP assumes that it has total control over user attributes and LDAP entries. In this case, the SWAMP should be the only client of the LDAP server. When set to "true", the SWAMP assumes that creation and editing of user attributes and LDAP entries is to be done outside of the SWAMP. In this case, the SWAMP disables any workflows that would result in the creation or editing of user records, including user passwords. Specifically:

- The sign up button is removed from the SWAMP home page. However, any user with a record in the LDAP server can sign in to the SWAMP, and supporting records in the SWAMP's SQL database will be created automatically on sign in.
- The "Reset my password" link is removed from the sign-in page.
- The Linked Account Use Policy page does not allow creation of new accounts, only linking to existing accounts.
- The user profile page displays user demographics as stored in LDAP but does not allow them to be edited in the SWAMP web application.
- The user profile page does not include options to change or reset the user's password or to delete the account.

- The SWAMP administrator Review Accounts page does not provide options to flag accounts as hibernated or to require a password reset.

This should be set to "true" if you are using a pre-existing LDAP server. The SWAMP-in-a-Box installer sets this to "false".

`LDAP_MIR_SWAMP`

Whether the LDAP server is configured with the schema used in the mir-swamp.org LDAP server. Set to "true" or "false". The purpose of this parameter is to support setting a legacy, required attribute in the LDAP server used by mir-swamp.org. In all other cases, this should be set to "false". The SWAMP-in-a-Box installer sets this to "false".

`LDAP_HOST`

The URL of the LDAP server to connect to, including the protocol and host, e.g. "ldaps://ldap.example.org". The specified LDAP server must support LDAP protocol 3. This is applicable only if `LDAP_ENABLED` is set to "true".

`LDAP_PORT`

The port to connect to on the configured `LDAP_HOST`. The SWAMP-in-a-Box installer sets this to "636". This is applicable only if `LDAP_ENABLED` is set to "true".

`LDAP_BASE_DN`

The RDN search base for LDAP searches. This needs to be set based on the configuration of the base `dn` of the LDAP directory for your users. The SWAMP-in-a-Box installer sets this to "ow=people,o=SWAMP,dc=cosalab,dc=org". This is applicable only if `LDAP_ENABLED` is set to "true".

`LDAP_USER_RDN_ATTR`

The Prefix RDN attribute for users in the LDAP server. This needs to be set based on how `dn` fields are formed in the LDAP server. The SWAMP-in-a-Box installer sets this to "swampUuid". This is applicable only if `LDAP_ENABLED` is set to "true".

`LDAP_SWAMP_UID_ATTR`

The LDAP attribute to be used as an index into the SWAMP database. This must be set to an attribute that uniquely identifies each user and is unchangeable. Often, this will be the same as `LDAP_USER_RDN_ATTR`. The SWAMP-in-a-Box installer sets this to "swampUuid". This is applicable only if `LDAP_ENABLED` is set to "true".

Note that this attribute will be used to identify users in the SWAMP's web application routes and, as such, will be displayed in URLs for the SWAMP's web pages with data for a specific user.

`LDAP_FIRSTNAME_ATTR`

The LDAP attribute for users' first names. The SWAMP-in-a-Box installer sets this to "givenName". This is applicable only if `LDAP_ENABLED` is set to "true".

If `LDAP_READ_ONLY` is set to "true" and your LDAP server does not have an attribute for users' first

names, set this to "ignore". If LDAP_READ_ONLY is set to "false", this attribute can be edited through the SWAMP web interface.

LDAP_LASTNAME_ATTR

The LDAP attribute for users' last names. The SWAMP-in-a-Box installer sets this to "sn" (surname). This is applicable only if LDAP_ENABLED is set to "true".

If LDAP_READ_ONLY is set to "true" and your LDAP server does not have an attribute for users' last names, set this to "ignore". If LDAP_READ_ONLY is set to "false", this attribute can be edited through the SWAMP web interface.

LDAP_FULLNAME_ATTR

The LDAP attribute for users' full names. The SWAMP-in-a-Box installer sets this to "cn" (common name). This is applicable only if LDAP_ENABLED is set to "true".

If your LDAP server does not have an attribute for users' full names, set this to "ignore". If LDAP_READ_ONLY is set to "false", the SWAMP will generally set this attribute to either the first and last name of the given user or to "none". It is not directly editable in the SWAMP web interface.

LDAP_PASSWORD_ATTR

The LDAP attribute for users' passwords. The SWAMP-in-a-Box installer sets this to "userPassword". This is applicable only if LDAP_ENABLED is set to "true".

If LDAP_READ_ONLY is set to "false", a user will be able to set a password on signing up for the SWAMP and later be able to change it through the SWAMP web interface.

LDAP_USERNAME_ATTR

The LDAP attribute to be mapped to the SWAMP username. The SWAMP-in-a-Box installer sets this to "uid". This is applicable only if LDAP_ENABLED is set to "true".

This must be set to an attribute that uniquely identifies each user. If LDAP_READ_ONLY is set to "false", this attribute can be edited through the SWAMP web interface as long as the new value is unique.

LDAP_EMAIL_ATTR

The LDAP attribute for users' email addresses. The SWAMP-in-a-Box installer sets this to "mail". This is applicable only if LDAP_ENABLED is set to "true".

If EMAIL_ENABLED is set to "true" and LDAP_READ_ONLY is set to "false", this attribute can be edited through the SWAMP web interface. If LDAP_READ_ONLY is set to "false" and EMAIL_ENABLED is also set to "false", you can set LDAP_EMAIL_ATTR to "ignore" and the SWAMP will not set it. Otherwise, the SWAMP will set the email attribute in LDAP to a single space character.

LDAP_ORG_ATTR

The LDAP attribute for users' affiliations. The SWAMP-in-a-Box installer sets this to "o" (organization). This is applicable only if LDAP_ENABLED is set to "true".

This should be an optional attribute in LDAP. If LDAP_READ_ONLY is set to "true" and your LDAP server does not have an attribute for users' affiliations, set this to "ignore". If LDAP_READ_ONLY is set to "false", this attribute can be edited through the SWAMP web interface.

LDAP_OBJECTCLASS

A comma-separated list of "objectClass" attributes to be set for each user. Set this to a comma-separated list of the "objectClass" attributes required by the LDAP server. The SWAMP-in-a-Box installer sets this to "top,person,organizationalPerson,inetOrgPerson,eduPerson,swampEntity", which defines the following "objectClass" attributes:

- objectClass: top
- objectClass: person
- objectClass: organizationalPerson
- objectClass: inetOrgPerson
- objectClass: eduPerson
- objectClass: swampEntity

This is applicable only if LDAP_ENABLED is set to "true" and LDAP_READ_ONLY is set to "false".

LDAP_WEB_USER

The full dn of a credentialed LDAP user with global LDAP read access. The SWAMP web server uses this to get information about SWAMP users from LDAP. This is applicable only if LDAP_ENABLED is set to "true".

LDAP_WEB_USER_PASSWORD

The password for LDAP_WEB_USER. This is applicable only if LDAP_ENABLED is set to "true".

LDAP_PASSWORD_SET_USER

The full dn of a credentialed LDAP user with permission to change other users' passwords. The SWAMP web server uses this to create and change user passwords in LDAP. This is applicable only if LDAP_ENABLED is set to "true" and LDAP_READ_ONLY is set to "false".

LDAP_PASSWORD_SET_USER_PASSWORD

The password for LDAP_SET_USER. This is applicable only if LDAP_ENABLED is set to "true" and LDAP_READ_ONLY is set to "false".

1.5. Third-Party Login Settings

These parameters can be set to allow users to sign in using credentials from third-party sites. Supported third-party sites are: GitHub, Google, and CILogon. Each site has a corresponding set of parameters; in the descriptions below, replace [SITE] with either GITHUB, GOOGLE, or CILOGON.

SWAMP-in-a-Box is installed with third-party logins disabled. Prior to enabling third-party logins for a

site, you must set up a corresponding OAuth Application with the site (instructions can be found in the SWAMP-in-a-Box User Manual).

`[SITE]_ENABLED`

Whether the SWAMP web application allows signing in via the given site. When set to "true", the SWAMP provides a means to sign up and sign in via an account with the site. The SWAMP-in-a-Box installer sets this to "false".

`[SITE]_CLIENT_ID`

The Client ID set in the OAuth Application for the site. This is applicable only when `[SITE]_ENABLED` is set to "true".

`[SITE]_CLIENT_SECRET`

The Client Secret set in the OAuth Application for the site. This is applicable only when `[SITE]_ENABLED` is set to "true".

One additional parameter is available for configuring CILogon.

`CILOGON_SKIN`

Determines the appearance of CILogon's interstitial page. The SWAMP-in-a-Box installer sets this to "default".

1.6. Session Related Settings

These parameters determine how session (logon) cookies behave.

`SESSION_DRIVER`

The driver used to manage session data. Set this to "database", "file" or "cookie". When this is set to "database", data for each user session is stored in the `project.sessions` table in the SWAMP database. When this is set to "file", data for each user session is stored in the SWAMP-in-a-Box file system. When it is set to "cookie", data for each user session is stored as a cookie on the web client. The SWAMP-in-a-Box installer sets this to "database". SWAMP-in-a-Box installations originally deployed using versions of SWAMP-in-a-Box prior to 1.34.5 may have this set to either "cookie" or "file".

When `SESSION_DRIVER` is set to "database", SWAMP administrators are able to restrict the list of users displayed on the Review Accounts page to users who are currently signed in.

When `SESSION_DRIVER` is set to "file", session data is stored in `/var/www/swamp-web-server/storage/framework/sessions/`.

`SESSION_LIFETIME`

Determines the expiration date for SWAMP session cookies, in minutes, from the time they are issued. The SWAMP-in-a-Box installer sets this to "2160" (36 hours). Set this to "0" if you are setting `SESSION_EXPIRE_ON_CLOSE` to "true".

`SESSION_EXPIRE_ON_CLOSE`

Whether SWAMP session cookies expire when the browser session ends. The SWAMP-in-a-Box installer sets this to "false". Before changing this to "true", set `SESSION_LIFETIME` to "0".

`SESSION_COOKIE`

The name of the SWAMP cookie that references a user's session data. The SWAMP-in-a-Box installer sets this to "swamp_session".

`SESSION_DOMAIN`

The name of the domain for the session cookie. Set this to "null" to use the same domain name as `APP_URL`. The SWAMP-in-a-Box installer sets this to "null".

`SESSION_SECURE_COOKIE`

Whether SWAMP session cookies are sent for secure connections only. The SWAMP-in-a-Box installer sets this to "true".

1.7. Database Settings

These parameters provide the SWAMP web application with access to the SWAMP's SQL databases. There is a set of parameters for each of the following databases: `project`, `package`, `tool`, `platform`, `assessment`, and `viewer`. Each database has a corresponding set of parameters; in the descriptions below, replace `[DB]` with `PROJECT`, `PACKAGE`, `TOOL`, `PLATFORM`, `ASSESSMENT`, or `VIEWER`.

`[DB]_HOST`

The hostname of the database server. The SWAMP-in-a-Box installer sets this to "localhost".

`[DB]_PORT`

The port to connect to on the database server. The SWAMP-in-a-Box installer sets this "3306".

`[DB]_DATABASE`

The name of the database ("project", "package", "tool", "platform", "assessment", or "viewer") for which the set of parameters applies.

`[DB]_USERNAME`

The database user whose credentials will be used by the SWAMP web application to access the database. The SWAMP-in-a-Box installer sets this to "web".

`[DB]_PASSWORD`

The password for the database user above for accessing the database. The SWAMP-in-a-Box installer sets this to the password entered during the install process.

1.8. Viewer Proxy Settings

These parameters control caching of data for integrated CodeDx results viewer web content served

from a viewer VM through the proxy. Cached data includes the IP address and corresponding SWAMP project uid returned from the viewer job in HTCondor, the user object returned from the data server, the project object returned from the data server, and return data for static web content received from the CodeDx web server (such as text/javascript files, image files, and font files).

If Code Dx has not been added to a SWAMP-in-a-Box installation, these parameters do not apply.

`VIEWER_PROXY_CACHING`

Whether information is cached for viewer proxy content. When set to "false" no information is cached. When set to "true" the information described above is cached. The SWAMP-in-a-Box installer sets this to "false".

`VIEWER_PROXY_CACHING_DURATION`

Determines the expiration time for viewer proxy cached data, in seconds, from the time it is stored or updated. The SWAMP-in-a-Box installer sets this to "1". This setting has no effect if `VIEWER_PROXY_CACHING` is set to "false". We recommend setting this to "10" when `VIEWER_PROXY_CACHING` is set to "true".

1.9. Miscellaneous Settings

These parameters control various operations of the Laravel framework. Their values should not be changed from the ones set by the SWAMP-in-a-Box installer.

`CACHE_DRIVER`

The SWAMP-in-a-Box installer sets this to "file".

`QUEUE_DRIVER`

The SWAMP-in-a-Box installer sets this to "sync".

Chapter 2. SWAMP Web Application Frontend Configuration

The file `/var/www/html/config/config.json` contains various parameter names and values that are used to configure the SWAMP web application's frontend. You must have `root` access to modify this file.

The contents of `config.json` must be a valid JSON object; the collection of values for the parameters described below are stored as nested JSON objects. Examples can be found at the end of this section.

If you have upgraded your SWAMP-in-a-Box from a previous version it is possible that `config.json` has a section of `cookie` parameters. These are no longer used by SWAMP and can be safely deleted.

The remainder of this section describes the parameters.

2.1. Contact Information

These parameters affect the display of information on the Contact Us and Report Security Incident pages. If this collection of parameters is not defined, as is the case when SWAMP-in-a-Box is initially installed, the link to the Contact page in the SWAMP web application's main menu is hidden.

2.1.1. Support

These parameters affect the display of information on the Contact Us page.

`contact.support.description`

The description of the person or team receiving messages displayed for Contact Us messages.

`contact.support.email`

The email address displayed for Contact Us messages. This should have the same value as the the `MAIL_CONTACT_ADDRESS` parameter in the backend configuration file.

`contact.support.message`

Additional text displayed for Contact Us messages.

`contact.support.phoneNumber`

The phone number displayed for Contact Us messages.

2.1.2. Security

These parameters affect the display of information on the Report Security Incident page. If the `support` section is defined but the `security` section is not, the SWAMP web application does not provide a link

from the Contact Us page to the Report Security Incident page.

`contact.security.description`

The description of the person or team receiving messages displayed for Report Security Incident messages.

`contact.security.email`

The email address displayed for Report Security Incident messages. This should have the same value as the `MAIL_SECURITY_ADDRESS` parameter in the backend configuration file.

`contact.security.message`

Additional text displayed for Report Security Incident messages.

`contact.security.phoneNumber`

The phone number displayed for Report Security Incident messages.

2.2. Welcome Message

These parameters provide a message that is displayed in a pop-up when users access the SWAMP-in-a-Box home page (not signed in). You can use it to display a Welcome message or information about the status of your system. When these parameters are not present, no message is displayed.

`notifications.welcome.message`

The content of the message, which is displayed in a pop-up.

`notifications.welcome.title`

The text displayed in the titlebar of the message pop-up.

2.3. Other Configurable Behaviors

`options.assessments.allow_multiple_tool_selection`

Whether the "All" option is present when selecting tools on the Add/Run New Assessments page. The SWAMP-in-a-Box installer sets this to "true".

`options.assessments.allow_viewing_zero_weaknesses`

Whether assessment results with zero weaknesses can be selected and sent to the Code Dx results viewer. The SWAMP-in-a-Box installer sets this to "true".

2.4. Web Services

`servers.web`

The path used to access the SWAMP web application's routes. The SWAMP-in-a-Box installer sets this based on the hostname specified during the install process (usually, the host's detected hostname). For SWAMP-in-a-Box this is set to the relative path from the SWAMP-in-a-Box URL to the API

location "/swamp-web-server/public".

When the hostname changes, use the `/opt/swamp/bin/swamp_set_web_host` utility script to update this parameter, because that script will update not only this parameter but also all other configuration locations where the hostname is referenced.

2.5. Examples

Example 1. Without the `contact` or `notifications` Sections

```
{
  "options": {
    "assessments": {
      "allow_multiple_tool_selection": true,
      "allow_viewing_zero_weaknesses": true
    }
  },

  "servers": {
    "web" : "/swamp-web-server/public"
  }
}
```

Example 2. With the `contact` and `notifications` Sections

Parameters (lines) below whose sample value include "(optional)" may be omitted.

```
{
  "contact": {
    "support": {
      "description": "Support staff",
      "email": "<Support email address (optional)>",
      "message": "Feel free to contact us with questions.",
      "phoneNumber": "<Support phone number (optional)>"
    },
    "security": {
      "description": "Security team",
      "email": "<Security email address (optional)>",
      "message": "<Security message here (optional)>",
      "phoneNumber": "<Security phone number (optional)>"
    }
  },

  "options": {
    "assessments": {
      "allow_multiple_tool_selection": true,
      "allow_viewing_zero_weaknesses": true
    }
  },

  "notifications": {
    "welcome": {
      "title": "Message Title",
      "message": "Your message here!"
    }
  }
}


  "servers": {
    "web" : "/swamp-web-server/public"
  }
}
```

Chapter 3. SWAMP-in-a-Box's File System

3.1. Configuration Files

`/var/www/swamp_web_server/.env`

`/var/www/html/config/config.json`

SWAMP web application configuration files. Directions for modifying `.env` and `config.json` can be found in this document and in the SWAMP-in-a-Box Administrator Manual.

`/opt/swamp/etc/swamp.conf`

`/opt/swamp/etc/log4perl.conf`

`/opt/swamp/etc/services.conf`

`/opt/swamp/etc/swampmonitor.conf`

SWAMP backend configuration files. Directions for modifying `swamp.conf` can be found in the SWAMP-in-a-Box Administrator Manual. There should be no need to directly modify `log4perl.conf`, `services.conf`, or `swampmonitor.conf`.

`/etc/condor/condor_config`

`/etc/condor/config.d/swampinabox_*.conf`

HTCondor configuration files. The SWAMP-in-a-Box installer preserves the version of `condor_config` installed by the HTCondor RPMs and installs several files into the `/etc/condor/config.d` directory. There should be no need to directly modify any of these files.

`/etc/httpd/conf/httpd.conf`

`/etc/httpd/conf.d/ssl.conf`

Apache configuration files. The SWAMP-in-a-Box installer replaces `httpd.conf` with a version that's included with the installer and modifies `ssl.conf` to use more secure settings for the SSL protocols and cipher suites than the settings installed by the `mod_ssl` RPM.

`/etc/php.ini`

PHP configuration file. The SWAMP-in-a-Box installer modifies this to allow uploads up to 800M.

3.2. Long-term Storage Files

`/swamp/platforms/images`

Directory containing the virtual machine images for performing assessments and running the optional Code Dx viewer.

`/swamp/SCAProjects`

Directory containing assessment results. Each sub-directory contains the results for one project.

`/swamp/store/SCAPackages`

Directory containing package archives. Each sub-directory contains the archive for one package version.

`/swamp/store/SCATools`

Directory containing assessment and metric tools. The `bundled` sub-directory contains tools that are included with the SWAMP-in-a-Box installer. The `add-on` sub-directory contains tools that were added to the system after the initial SWAMP-in-a-Box install.

`/var/lib/mysql`

Directory containing MariaDB's storage files for the SWAMP's SQL databases.

`/var/lib/docker`

Directory containing Docker's storage files for the containers used to perform assessments.

3.3. Log Files

`/opt/swamp/log`

Directory containing the SWAMP backend's log files.

`/var/log/condor`

`/var/lib/condor`

Directories containing HTCondor's log files.

`/var/log/httpd`

Directory containing Apache's log files.

`/var/log/libvirt`

Directory containing libvirt's log files.

`/var/log/mariadb`

Directory containing MariaDB's log files.

`/var/www/swamp-web-server/storage/logs`

Directory containing the SWAMP web backend's log files.

3.4. Temporary Files

`/opt/swamp/run`

`/swamp/working/project`

`/swamp/working/results`

Directories containing temporary files used by the SWAMP backend.

`/slots`

Directory containing working directories of currently executing HTCondor jobs.

`/swamp/incoming`

Directory containing user-uploaded packages.

`/swamp/outgoing`

Directory containing files that SWAMP users view or download.

`/var/lib/libvirt`

Directory containing temporary files used by libvirt.

`/var/www/swamp-web-server/storage/framework/sessions`

Directory containing data about SWAMP users' login sessions when the SWAMP web application's backend is configured to store session data on the file system.

`/var/www/swamp-web-server/storage/framework/cache`

Directory containing cached data for add-on viewers (CodeDx) when the SWAMP web application's backend is configured to cache viewer proxy data.

3.5. Reclaiming Disk Space

Log files can be deleted without impacting the normal functioning of the system, although debugging issues will be more difficult if pertinent log files are missing. Temporary files can also be deleted so long as they are not still in use.

Deleting long-term storage files **will** impact the normal functioning of the system. Deleting package archives, tool archives, platform images, and assessment results will render those objects unavailable to the system, even if they continue appear to be available in the SWAMP.