GroundWork Monitor Professional 5.1.3 Configuration Guide

PURPOSE

This purpose of this document is to provide configuration notes for use after installing the GroundWork Monitor Professional 5.1.x product.

DISTRIBUTION NOTES

In addition to this Configuration Guide, Readme, Release Notes, and an Installation Guide accompany this release. These documents contain important information regarding bug fixes, known issues, new features, and installation notes.

SUPPORT

Product support is available through a GroundWork subscription agreement. For more information, go to GroundWork Support at: http://www.groundworkconnect.com

CONTENTS

SECTION 1 – ENABLE SSL SUPPORT FOR APACHE

The binaries and libraries necessary to enable SSL support are included in the Groundwork Monitor distribution. The steps below outline how to enable SSL for Apache Web Server.

TO ENABLE SSL SUPPORT IN GROUNDWORK MONITOR:

1. Edit **/usr/local/groundwork/apache2/conf/httpd.conf** and find the line that states:
   #Include conf/extra/httpd-ssl.conf
2. Remove the # symbol.
3. Save the file.

PERFORM THESE STEPS TO CREATE YOUR OWN SELF-SIGNED CERTIFICATE

1. Create private key and self-signed cert in the **/usr/local/groundwork/apache2/conf/** directory.

   openssl genrsa -out server.key 2048
   openssl req -new -x509 -key server.key -out server.crt -days 1095
2. When prompted, answer the appropriate questions

IF YOU HAVE YOUR OWN CERTIFICATE

1. Modify **/usr/local/groundwork/apache2/conf/extras/httpd-ssl.conf** and modify the line to point to your already existing certificate:

   SSLCertificateFile /usr/local/groundwork/apache2/conf/server.crt

RESTART APACHE AND TEST

1. Restart Apache with the following command: **/etc/init.d/httpd restart**
2. View the site using: **https://<yourserver>/**

SECTION 2 – ENABLE FIREFOX 1.5.x SUPPORT

In order to restrict access to various applications such as Advance Reports, Performance, etc, the Groundwork Apache web server is configured to only allow access to these applications from certain resources. This is accomplished by restricting access to defined http referer header values. This restricted access forces users to be logged into Groundwork Monitor in order to access these applications. The problem with Firefox 1.5.x is that for resource requests that are generated in javascript the http referer header is not set therefore Apache does not allow the resource request to be fulfilled.

In Firefox 2.0.x and supported Internet Explorer versions, javascript generated requests contain the appropriate http referer header information. It is recommended all clients use one of the supported browsers.

If it is mandatory to use Firefox 1.5.x then follow the instructions below which configure Apache to allow requests from Firefox 1.5.x to be served. Please note, the configuration below will open up security holes with the Firefox 1.5.x browser. Apache will allow requests from the Firefox 1.5.x browser to the resources configured below. The configuration limits access to only to the necessary resources, but there are potentially sensitive resources that are exposed.

APACHE CONFIGURATION

Make the following edits to your Apache configuration to allow access for the Firefox 1.5.x browser.

1. Make the following changes to the Apache Configuration File: **/usr/local/groundwork/apache2/conf/httpd.conf**

   a) Add the following line which defines a request environment variable. This variable will be used to allow Firefox 1.5.x access. Add the line below the other **SetEnvIf** entries.

   ```
   SetEnvIf User-Agent Firefox/1\.5 firefox_1_5
   ```

   b) Add the following Location directives after the existing Location directive for **/reportserver**. These directives will provide access control to the necessary resources.

   ```
   <!-- Add after this existing directive -->

   <Location /reportserver />
    Order Deny,Allow
    Deny from all
    Allow from env=framework_referer
   </Location>

   <!-- New directives to Add -->

   <Location /reportserver/scripts/dojo/>
    Order Deny,Allow
    Deny from all
    Allow from env=firefox_1_5
    Allow from env=framework_referer
   </Location>

   <Location /reportserver/reports.jsp>
    Order Deny,Allow
    Deny from all
    Allow from env=firefox_1_5
    Allow from env=framework_referer
   </Location>

   <Location /reportserver/admin-directories.jsp>
    Order Deny,Allow
   ```

```
 Deny from all
 Allow from env=firefox_1_5
 Allow from env=framework_referer
</Location>
```

c) Add the following line to the existing Location directive for **/birtviewer**:

```
Allow from env=firefox_1_5
```

The Location directive should look like the following after the above line has been added.

```
<Location /birtviewer/>
 Order Deny,Allow
 Deny from all
 Allow from env=firefox_1_5
 Allow from env=framework_referer
</Location>
```

2. Update the file **/usr/local/groundwork/config/gwreportserver.properties**

   a) Change the org.groundwork.report.firefox_1_5.support property to be equal to true:

   ```
   org.groundwork.report.firefox_1_5.support=true
   ```

3. Restart gwservices: **/etc/init.d/gwservices restart**
4. Restart Apache: **/etc/init.d/httpd restart**

SECTION 3 – ENABLE LDAP AUTHENTICATION FOR MONITOR USERS

Groundwork Monitor allows LDAP authentication for users by means of an external Directory source (Example: Active Directory, eDirectory, OpenLDAP). LDAP Authentication is setup on a per user basis. This means some users can authenticate against LDAP while others can authenticate normally. This provides a flexible authentication scheme with redundant backup users in case of LDAP connection failure.

In order to configure LDAP authentication, you must know the Distinguished Name of the context that your users reside in. You will use this information later on.

You must first configure the global LDAP settings.

1. Log into Groundwork Monitor as an Administrator.
2. Navigate to Administration and click on the Guava Core package.
3. Choose Package Configuration
4. In the Directory Host field, enter the hostname or ip address of the server which will service LDAP requests.
5. In the Prefix field, enter the portion of the DN that comes before the username (Example: uid=)
6. In the Suffix field, enter the portion of the DN that comes after the username (Example: ,ou=people,dc=myorganization,dc=com)
7. Click Change Settings to save the LDAP authentication settings.

Now that the global LDAP settings are saved, you can configure the users you want to use LDAP authentication.

1. Log into Groundwork Monitor as an Administrator.
2. Navigate to Administration and edit the user you want to enable LDAP authentication for.
3. Change Authentication Mode to GuavaLDAPModule
4. Save the user.

The next time the user logs in GroundWork Monitor will attempt to bind to the LDAP directory server using the configuration settings you provided. For example, if user Joe attempts to log in, it will attempt to bind to the LDAP directory server using the distinguised name uid=joe,ou=people,dc=myorganization,dc=com (using the settings from above). Be sure to use the DN components that are relevant to your directory configuration.