Securing your server to IP address or hostname.

This section will outline how to secure the SOA Gateway Web Services to a specific IP address/hostname.

All examples have been enclosed in <IfModule> directives. This means that the security directives will be ignored automatically if the Apache web server does not have SOA Gateway enabled.

- Example 1
- Example 2
- Example 3
- Example 4
- Example 5

Example 1

This example will show how to allow a request to the configuration service from only the local machine. This is local to where the SOA Gateway server is running, not where the Eclipse IDE is running (if different).

1. Edit the SOA Gateway Apache configuration file.
2. Enter the following directives.

```
<IfModule mod_xmiddle.c>
  <Location /configurationService>
      Allow from 127.0.0.1
      Deny from all
  </Location>
</IfModule>
```

3. Restart the server

This would only allow access to the configuration web service from the local machine. All remote clients would be denied access.

Example 2

Only allow a remote machine to configure the SOA Gateway server.

1. Edit the SOA Gateway Apache configuration file
2. Enter the following directives.

```
<IfModule mod_xmiddle.c>
    <Location /configurationService>
        Allow from adminHost
        Deny from all
    </Location>
</IfModule>
```

3. Restart the server

This example would only allow the machines adminHost to configure the SOA Gateway server. All others machines would be rejected access.

Example 3

Only allow a remote machine to configure SOA Gateway, but allow any client to access the Web Service WSDL.

1. Edit the SOA Gateway Apache configuration file
2. Enter the following directives:

```
<IfModule mod_xmiddle.c>
    <Location /configurationService>
        <Limit POST>
            Allow from adminHost
            Deny from all
        </Limit>
    </Location>
</IfModule>
```

3. Restart the server.

This would allow the machine adminHost to access the configuration, but would allow any client to access the configuration service WSDL.

Example 4

This example will show how to secure a specific resource. The examples 1, 2, and 3 above can also be applied to securing a resource. The only thing that has to change is the Location parameter. For example, using Example 1 as a basis; to only allow “adabas_Employees” to be accessed from the local machine, do the following:

1. Edit the SOA Gateway Apache configuration file
2. Enter the following directives.

```
<IfModule mod_xmiddle.c>
    <Location /adabas_Employees>
        Allow from 127.0.0.1
        Deny from all
    </Location>
</IfModule>
```

3. Restart the server

All remote access to the “adabas_Employees” resource would be denied. Note: This example will restrict access to the “adabas_Employees” service, not the XRD import or export. XRD import/export operations are provided by the configuration Web Service, to secure these operations see examples 1, 2 and 3.

Example 5

This example will show how to secure the resource administration service for SOA Gateway. Again, example 1-4 may be used once the Location parameter has been changed. For example, using Example 1 as a basis; to only allow the resource administration service to be accessed from the local machine, do the following:

1. Edit the SOA Gateway Apache configuration file
2. Enter the following directives.

```
<IfModule mod_xmiddle.c>
    <Location /resourceService>
         Allow from 127.0.0.1
         Deny from all
    </Location>
</IfModule>
```

3. Restart the server

All remote access to the “resourceService” resource would be denied.