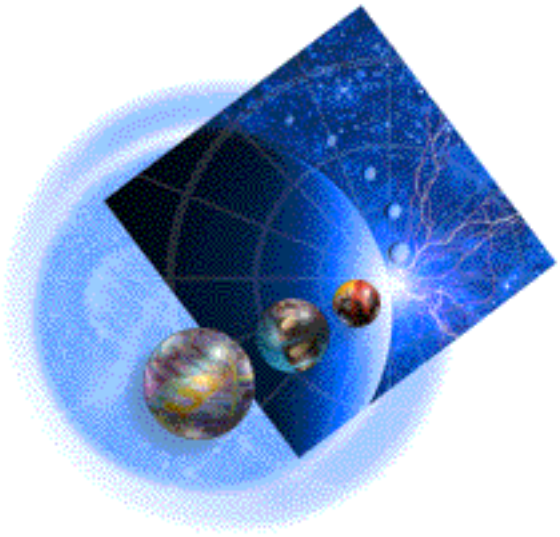
IBM Everyplace Location Based Services version 2.1

(c) Copyright 2001 International Business Machines Corp. All rights reserved.



Everyplace Location Based Services

- **Installing and Configuring**
  - Prerequisites
  - Before installing
  - Installing
  - Configuring Location Based Services
- **Policy Director**
  - Verifying the Policy Director Client
  - Adding an application
  - Deleting an application
  - Querying/viewing Policy Director
  - Enabling an application
  - Disabling an application
  - Enabling a user
  - Disabling a user
- **SignalSoft**
  - Creating the WHEREAMI Service
    - Load required data
    - Load required MAPS extension
    - Save the Cell Sector Table
    - Import the cell_centroids.dbf
    - Add the cell_centroids.dbf
    - Populate the event Theme
    - Load the whereami.shp shapefile
    - Populate the li_content sde Layer
    - Create the WHEREAMI Service
- **Samples**
  - Installing
    - Sample requirements
    - Sample installation
    - Sample location
    - Sample file description

- Reviewing the JavaDoc
- Running samples
- Viewing source
  - With WebSphere Studio
  - Without WebSphere Studio

What is Location Based Services?

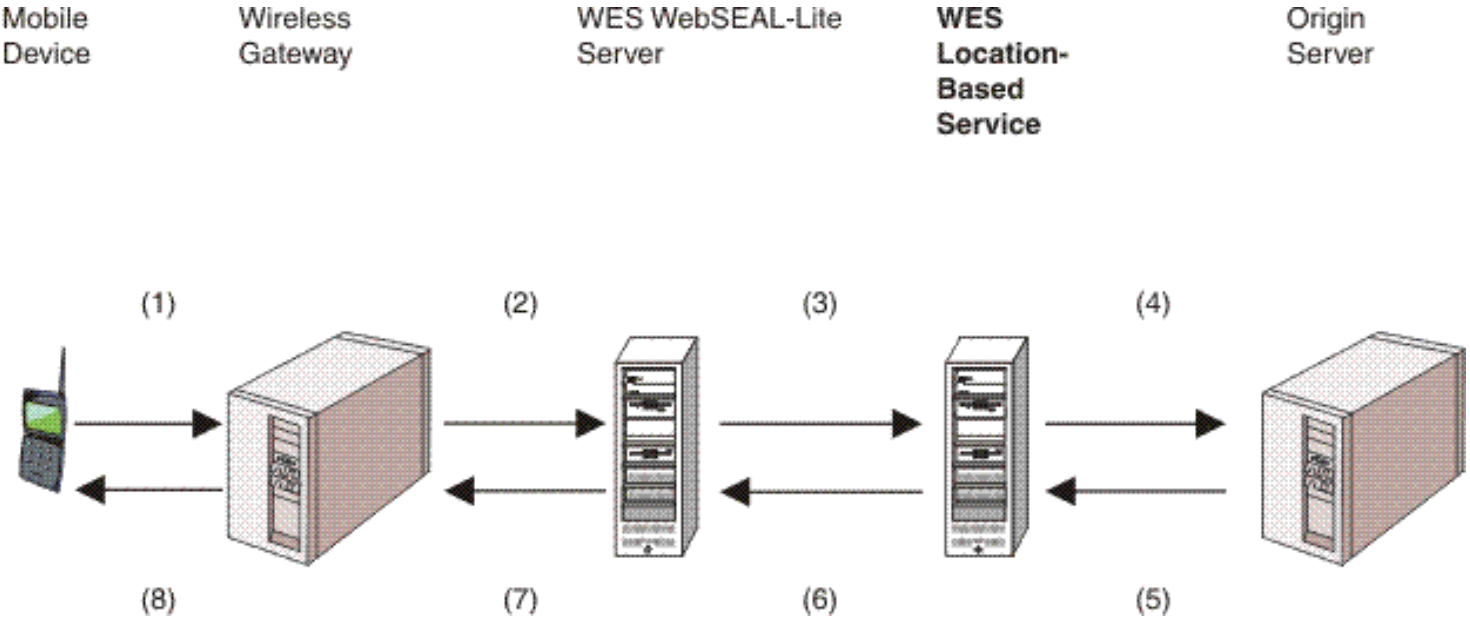
WebSphere Everyplace Server Version 2.1 Location Based Services provides user location information to applications. The applications then deliver content based on the user's location information. For example, an application can provide a user with a list of hotels in the area where he/she is currently traveling. Before location information can be used by an application, the administrator must enable the application as a location based application and the user must allow the application to use their location information. The administrator can also enable a user for an application to use their location information.

Location Based Services is shipped with WebSphere Everyplace Server and is a subcomponent of the WebSphere Edge Server Caching Proxy. Location Based Services uses Signal Soft Local.info Server to provide user location information and Tivoli SecureWay Policy Director to manage privacy. Both subcomponents must be installed separately and configured for Location Based Services to work correctly.

Location Based Services obtains the following information from SignalSoft:

- Latitude
- Longitude
- Uncertainty of the position estimate
- County
- City
- State/province
- ZIP/postal code
- Country
- Nearest Intersection

The following diagram illustrates how Location Based Services works:



1. The user of a mobile device initiates a request.
2. The Wireless Gateway translates the WAP request into an HTTP request. It also authenticates the user and adds the user ID and MIN/MSISDN to the HTTP extension headers on the inbound HTTP request. It then forwards the request to WebSEAL-Lite. Note that the Wireless Gateway must be configured to include MIN/MSISDN number. Refer to the Wireless Gateway documentation for details.
3. WebSEAL-Lite forwards the request to the Location Based Services after it verifies that the client has already been authenticated.
4. Using Policy Director, Location Based Services determines if this is a location based application and the user has authorized the application to have location information. If the application is authorized, the Location Based

Service makes a request to the Location Server (for example SignalSoft Service Invocation Interface (SII)) to obtain the location of the user's mobile device.

5. A location based application receives the HTTP request. It obtains the location information needed via the Location Based Application Programming Interface. The Location Based Application Programming Interface obtains the requested location information from the HTTP headers and returns the location information to the location based application. The location based application builds the HTTP response and returns it to the Location Based Services Proxy.
6. The Location Based Service returns the HTTP response to WebSEAL-Lite.
7. WebSEAL-Lite returns the HTTP response to the Wireless Gateway.
8. The Wireless Gateway translates the HTTP response to a WAP response and returns to the mobile device.

Related information

- Installing Location Based Services
- Working with Policy Director
- Working with Signal Soft
- Working with Location Based Services Sample

Installing and configuring Location Based Services

Location Based Services can be installed during the WebSphere Everyplace Server installation. There are several considerations specific to installing Location Based Services:

- Prerequisites
- Before installing
- Installing Location Based Services
- Configuring Location Based Services
- Related information

Prerequisites

In addition to the prerequisites required by the WebSphere Everyplace Server, Location Based Services, you must install the following prerequisites before installing Location Based Services:

- The Signal Soft Local.info Server Version 3.2 Solaris including the customized "WhereAmI" service.
- WebSphere Everyplace Suite WebSEAL-Lite
- WebSphere Everyplace Suite Wireless Gateway
- Policy Director Server 3.7.1
- Policy Director Client 3.7.1

Before installing

Before installing Location Based Services, do the following:

- Verify that you have enough hard drive and memory to install Location Based Services and the subcomponents. Refer to Component software requirements and prerequisites for more information.
- Determine the host for the Policy Director Server, Policy Director LDAP Server, Location Server, Tivoli Internet Services Manager Server, and Application Server
- Install Policy Director Server. Refer to the Tivoli SecureWay Policy Director documentation for instructions.
- Install Policy Director Client 3.7.1 on the system used for the Location Based Server.
- Install Location Server, such as SignalSoft. Refer to the documentation for SignalSoft for instructions.

Installing Location Based Services

The WebSphere Everyplace Server Setup Manager installs Location Based Services. For AIX, Location Based Server is installed in /usr/IBMEPS/LBS.

During installation, the WebSphere Everyplace Server accepts Location Based Services configuration input from the user, populates the Location Based Services configuration file, creates the Location Based Services configuration file and then creates configuration entries in LDAP.

During the WebSphere Everyplace Setup Installation, you need to make the following selections:

1. On the WebSphere Everyplace Server Configuration dialog box, select WebSphere Edge Server - Caching Proxy. The subcomponents of WebSphere Edge Server are displayed in the Subcomponent list on the dialog box.
2. Select Everyplace Location Based Services and click the Next button. Setup Manager verifies that Policy Director Client is installed. If the Policy Director Client is not installed, a message box is displayed and you cannot continue installation until it is installed. If the Policy Director Client is installed, the Common Administrator User ID Info dialog box is displayed.
3. If you want each component to have a specific ID, select the Different User ID for each component option. If you want each component to use the same ID, select the Same User ID for all components option. Enter the User ID, Group, Password and confirm the password. Click Next. The Everyplace Location Based Services Configuration dialog box is displayed.
4. In the Location Server Host Name field, enter the host name of your location server. This must be a valid host name that is resolvable to an IP address.
5. In the Location Server Port field, enter the port for your location server. This value cannot be null.
6. In the Policy Director Administrator User ID field, enter the user ID. This value is usually sec_master.
7. In the Policy Director Administrator Password field, enter the password. Click Next. The Tivoli SecureWay Policy Director LDAP Configuration dialog box is displayed.
8. In the LDAP Server Name field, enter the hostname of the SecureWay Directory Server used by the Policy Director Server. Note that this is probably a different server than used for other WebSphere Everyplace Server components.
9. In the Administrator ID field, enter the LDAP administrator ID. For example, cn=root.
10. In the LDAP Administrator Suffix field, enter the unique administrator suffix that matches the LDAP settings.
11. In the LDAP Port field, enter the services port for LDAP. This value is usually 389. Click Next. The Tivoli SecureWay Policy Director Population Information dialog box is displayed.
12. If you do not have a Universal Resource Identifier (URI) to populate Policy Director, select the "A URI file does not exist" option. If you have a URI file to populate, select the "A URI file to be populated exist"s option. If you select this option, enter the file to populate in the Universal Resource Identifier (URI). Click Next. Setup Manager verifies that the file does not contain errors. If the file contains errors a dialog box allowing you to correct the errors is displayed. Otherwise, the Setup Manager continues with the WebSphere Everyplace Server installation.
13. After you have installed Location Based Services, you can install Location Based Services API. Refer to Installing the Location Based Services Samples for instructions.

To uninstall Location Based Services, refer to Uninstalling the Everyplace Server components.

Configuring Location Based Services

After installation, you need to perform the following tasks for Location Based Services to work correctly:

- Setting up user preferences in Tivoli Internet Services Manager
- Configuring location based applications in Policy Director
- Preparing Location Based Services Application Registration File
- Configuring Location Based Services in Suite Manager (optional)

Setting up user preferences in Tivoli Internet Services Manager

For location information to be used by location based applications, the user must enable the application by setting up user preferences. Refer to User Preferences for instructions. If Tivoli Internet Service Manager user preferences are not set up, an Administrator can also enable an application to see user preferences through the Policy Director Admin Console.

Configuring location based applications in Policy Director

For users location information to be used by location based applications, the application must be added to Policy Director and the application enabled as a location based application. Refer to Working with Tivoli SecureWay Policy Director for instructions on configuring Policy Director.

Preparing Location Based Services Application Registration File

Optionally, you can prepare a Location Based Services Application Registration File. Location based applications can be registered during Location Based Services WebSphere Edge Server-Caching Proxy initialization and administered using the Policy Director Administration Console during runtime. The Location Based Services WebSphere Edge Server-Caching Proxy initialization populates Policy Director with location based applications in the location based application registration file supplied by the user. The format of the file is one application (URL) listed per line. Entering the characters "http://" before the URL is optional. The file only accepts the special characters "/", ":", "~", and ".". If you use other special characters in the URL name, an error will be returned. At the prompt, enter the following and press Enter. The following is a sample registration file:

```
http://www.ibm.com/a/b/c

http://www.abc.com/d/e

http://www.zwy.com/f
```

Configuring Location Based Services in Suite Manager (optional)

During installation, you entered Location Based Services configuration parameters. After installation, you can use Suite Manager to view and update Location Based Services configuration parameters. In Suite Manager, Location Based Services is displayed as a subcomponent of WebSphere Edge Server-Caching Proxy. Refer to the help in Suite Manager for more information on viewing and updating Location Based Services configuration parameters. From the Help menu in Suite Manager, select Help Topics. The Suite Manager documentation is displayed. In the Configuration Tasks section, select Everyplace Location Based Services.

Related information

- What is Location Based Services?
- Working with Policy Director
- Working with Signal Soft
- Working with Location Based Services Sample

Working with Tivoli SecureWay Policy Director

- Overview
- Verifying the Policy Director Client
- Adding a URL or application to Policy Director using script pd_populate.ksh
- Deleting a URL or application to Policy Director using script pd_populate.ksh
- Query/view Policy Director for the current set of applications in the Policy Director Object Space
- Enabling an application in Policy Director Console
- Disabling an application in Policy Director Console
- Enabling a user in Policy Director Console
- Disabling a user in Policy Director Console
- How does Location Base Server (LBS) interact with Location Base Applications (LBA)

Overview

You can use Tivoli SecureWay Policy Director to register Location Based Services applications and to ensure user privacy. However, we recommend installing the User Preferences Samples to enable applications to use specific user location data. For information on User Preferences, refer to Configuring User Preferences in the WebSphere Everyplace Server section of the InfoCenter.

A location based application is an application available for users to specify that the application can use the his/her location information. If you are using Policy Director to manage location based applications and users, it is assumed that prior to the WebSphere Everyplace Server installation that the Policy Director Client has been installed on the same machine. You also need to configure the Policy Director Client to communicate with a Policy Director Server. During installation, some sample applications are predefined to Policy Director. You can delete the sample applications or add new applications to Policy Director.

For an application to work with Location Based Services, it must be added to Policy Director and enabled as a location based application. If an administrator deletes an application from Policy Director, the application is no longer available for the administrator to enable the application as location based and users can no longer be enabled to allow their location information to be used by the application. If an administrator disables an application, the application still exists in Policy Director. Users can no longer enable their location information to be used by the disabled application. If a user is disabled from an application, the application is still available for other users to allow their location information to be used by the application, but the location information for the specific user disabled can no longer be used.

You can manage applications through Policy Director by using the script pd_populate.ksh and through the Policy Director Console. You can use the script pd_populate to add an application to Policy Director. When you use the script to add an application, the application is automatically enabled as a location based application. If you want to disable the application, you need to use the Policy Director Console to disable the application.

Use Policy Director to perform the following functions:

- Verifying the Policy Director Client
- Adding a URL or application to Policy Director using script pd_populate.ksh
- Deleting a URL or application to Policy Director using script pd_populate.ksh
- Query/view Policy Director for the current set of applications in the Policy Director Object Space
- Enabling an application in Policy Director Console
- Disabling an application in Policy Director Console
- Enabling a user in Policy Director Console
- Disabling a user in Policy Director Console

Verifying the Policy Director Client

The Policy Director client must be configured using AIX to work with the Policy Director Server. You need to perform the following to verify the Policy Director Client is communicating with the Policy Director Server:

1. Open a Terminal Window.
2. At the prompt, enter the following and press Enter.

   `/usr/IBMEPS/LBS/bin/pd_populate.ksh pdTest <password>`

   (Where password is the password for the Policy Director admin id sec_master)
3. If the connection is successful, the system returns a value "return with rc=0". If the connection is not successful, the system returns a non-zero code. To fix the connection, contact your Policy Director System Administrator.

Adding an application to Policy Director using script pd_populate.ksh

For an application to be available for administrators to enable the application as a location based application, the application must be added to Policy Director using the script pd_populate.ksh. When you add an application to Policy Director, the application is automatically enabled as a location based application. If you do not want the application to be a location based application, you must disable the application. You can use script pd_populate to add and enable applications, but you must use the Policy Director Console to view registered applications. The user must use User Preferences in Tivoli Internet Services Manager to enable the application to gain access to their information or the administrator must enable the user through the Policy Director Console.

1. Verify the Policy Director Client. Refer to Verifying the Policy Director Client.
2. Open a Terminal Window.
3. Enter the URL for the application you want to add. Entering the characters "http://" before the URL is optional. Script pd_populate.ksh only accepts the special characters "/", ":", "~", and ".". If you use other special characters in the URL name, Policy Director returns errors. At the prompt, enter the following and press Enter.

   ```
   /usr/IBMEPS/LBS/bin/pd_populate.ksh initAppl <password> <ldap suffixdn> <application URL>
   ```

   (Where <password> is the password for the Policy Director administrator id sec_master)

   (Where <ldapsuffixdn> is the LDAP distinguished name suffix. For example, o=ibm,c=us)

   (Where <application URL> is the URL for the application you are adding to Policy Director. For example, `www.yourco.com/index.html`. The URL is the actual location base address in Policy Director without the preceding `LBS_`. For example, if the URL in Policy Director is `LBS_www.ibm.com`, the URL to add would be `www.ibm.com`)
4. To add another application, repeat step 3.

Deleting an application from Policy Director using script pd_populate.ksh

When an application is deleted from Policy Director, it is no longer available for administrators to enable as a location based application. Applications must be deleted from Policy Director by using the script pd_populate.ksh. You can use this script to delete applications, but you must use the Policy Director Console to view registered applications.

When an application is deleted from Policy Director, it is automatically disabled as a location based application for all users that have enabled this application to see their location information. If you want to disable an application from being location based, you can disable the application instead of deleting the application from Policy Director. If a user wants to simply disable a specific application from receiving their location information, they should use Tivoli Personalized Services Manager to change their user preferences or have the administrator disable them in Policy Director.

1. Verify the Policy Director Client. Refer to Verifying the Policy Director Client.
2. Open a Terminal Window.
3. Enter the URL for the application you want to delete. At the prompt, enter the following and press Enter.

   ```
   /usr/IBMEPS/LBS/bin/pd_populate.ksh delAppl <password> <application URL>
   ```

   (Where password is the password for the Policy Director admin id sec_master)

   (Where <application URL> is the URL for the application you are deleting from Policy Director. For example, `www.yourco.com/index.html`. The URL is the actual location base address in Policy Director without the preceding `LBS_`. For example, if the URL in Policy Director is `LBS_www.ibm.com`, the URL to delete would be `www.ibm.com`)
4. To delete another application, repeat step 3.

Querying/viewing Policy Director for the current set of applications in the Policy Director Object Space

You can review the current set of WebSphere Everyplace Server applications protected by Policy Director by reviewing the WebSphere Everyplace Server Location Based Services Object space tree structure in the Policy Director Console.

WARNING: User WES_LBS, groups LBS_PERMIT_ALL and LBS_DENY_ALL, and applications LBS_ALL and LBS_NONE are reserved for use by IBM. Do not update or delete these users, groups or applications.

1. From the Windows Start Menu, select Policy Director and then Management Console. The Policy Director Management Console is displayed.
2. Click on the Object Space tab. The Login to a Secure Domain dialog box is displayed.
3. Enter the Login_Name and Password. You must enter a login_name with enough authority to view the applications, such as sec_master. Click OK. The Policy Director Object Space is displayed.
4. To expand the root of the tree, click on the + sign for the root of the tree. The list of objects underneath are expanded.
5. To expand WESLBS, click on the + sign for WESLBS. A list of applications registered for Location Based Services is displayed. The

applications LBS_ALL and LBS_NONE are installed when WebSphere Everyplace Server is installed and are reserved for use by IBM. If you entered applications with a slash in the URL, the program creates each piece of text separated by a slash in a separate container.

Enabling an application in Policy Director Console

For an application to be available for users to allow their location based information to be used by an application, the application must be enabled as a location based application. When you add an application to Policy Director by running the script pd_populate.ksh, the application is automatically enabled. You only need to enable an application as location based if you have previously disabled the application as a location based application.

WARNING: User WES_LBS, groups LBS_PERMIT_ALL and LBS_DENY_ALL, and applications LBS_ALL and LBS_NONE are reserved for use by IBM. Do not update or delete these users, groups or applications.

1. From the Windows Start Menu, select Policy Director and then Management Console. The Policy Director Management Console is displayed.
2. Click on the Account Manager tab. The Login to a Secure Domain dialog box is displayed.
3. Enter the Login_Name and Password. You must enter a login_name with enough authority to view the applications, such as sec_master. Click OK. The Policy Director Object Space is displayed.
4. To expand the Groups directory, click on the + sign for Groups. The Load Users dialog box is displayed.
5. Click Load. The groups are loaded. Click Close. All available applications are displayed. All applications are displayed with the prefix LBS_.
6. Highlight the application you want to enable.
7. Click the right mouse button. From the context menu, select Properties. The Group Properties dialog box is displayed.
8. In the Name field, click on the ... button. The Browse Users dialog box is displayed.
9. In the User Name Pattern field, enter a search to limit the users. For example, LBS*.
10. In the Limit to Field, enter the maximum number of users you want displayed.
11. Click Load. The users matching the search entered in the User Name Pattern field are displayed in the Search Results field.
12. In the Search Results field, select the user WES_LBS.
13. Click OK. The Group Properties dialog is displayed. WES_LBS is displayed in the Members List. Click OK.

Disabling an application in Policy Director Console

If you want an application to not be available for users to allow their location based information to be used by application, you must disable the application as a location based application. When an application is disabled as location based, all users enabled for the application are automatically disabled and their location information is no longer transmitted to the application.

WARNING: User WES_LBS, groups LBS_PERMIT_ALL and LBS_DENY_ALL, and applications LBS_ALL and LBS_NONE are reserved for use by IBM. Do not update or delete these users, groups or applications.

1. From the Windows Start Menu, select Policy Director and then Management Console. The Policy Director Management Console is displayed.
2. Click on the Account Manager tab. The Login to a Secure Domain page is displayed.
3. Enter the Login_Name and Password. You must enter a login_name with enough authority to view the applications, such as sec_master. Click OK. The Policy Director Object Space is displayed.
4. To expand the Groups tree, click on the + sign for Groups.
5. Highlight the application you want to disable. All applications are displayed with the prefix LBS_.
6. Click the right mouse button. From the context menu, select Properties. The User Properties dialog is displayed.
7. In the Members List, highlight the user WES_LBS. If WES_LBS is not displayed in the Members List, the application is not enabled for Location Based Services.
8. Click Remove. WES_LBS is removed from the Members List.
9. Click OK . The application is disabled from Policy Director.

Enabling a user in Policy Director Console

If a user wants their location information to be used by an application, you need to enable the user for the application. Note that for a user to be enabled for an application, the application must already have been enabled as a location based application.

WARNING: User WES_LBS, groups LBS_PERMIT_ALL and LBS_DENY_ALL, and applications LBS_ALL and LBS_NONE are reserved for use by IBM. Do not update or delete these users, groups or applications.

1. From the Windows Start Menu, select Policy Director and then Management Console. The Policy Director Management Console is displayed.
2. Click on the Account Manager tab. The Login to a Secure Domain dialog box is displayed.
3. Enter the Login_Name and Password. You must enter a login_name with enough authority to view the applications, such as

sec_master. Click OK. The Policy Director Object Space is displayed.

4. To expand the Groups directory, click on the + sign for Groups. The Load Users dialog box is displayed.
5. Click Load. The groups are loaded. Click Close. All available applications are displayed. All applications are displayed with the prefix LBS_.
6. Highlight the application for which you want to enable a user.
7. Click the right mouse button. From the context menu, select Properties. The Group Properties dialog box is displayed.
8. In the Name field, click on the ... button. The Browse Users dialog box is displayed.
9. In the User Name Pattern field, enter a search to limit the users. For example, LBS*.
10. In the Limit to Field, enter the maximum number of users you want displayed.
11. Click Load. The users matching the search entered in the User Name Pattern field are displayed in the Search Results field.
12. In the Search Results field, select the user you want to enable.
13. Click OK. The Group Properties dialog is displayed. The user you enabled is displayed in the Members List. Click OK

Disabling a user in Policy Director Console

If a user no longer wants their location information to be used by an application, you need to disable the user for the application.

WARNING: User WES_LBS, groups LBS_PERMIT_ALL and LBS_DENY_ALL, and applications LBS_ALL and LBS_NONE are reserved for use by IBM. Do not update or delete these users, groups or applications.

1. From the Windows Start Menu, select Policy Director and then Management Console. The Policy Director Management Console is displayed.
2. Click on the Account Manager tab. The Login to a Secure Domain page is displayed.
3. Enter the Login_Name and Password. You must enter a login_name with enough authority to view the applications, such as sec_master. Click OK. The Policy Director Object Space is displayed.
4. To expand the Groups tree, click on the + sign for Groups.
5. Highlight the application for which you want to disable a user. All applications are displayed with the prefix LBS_.
6. Click the right mouse button. From the context menu, select Properties. The User Properties dialog is displayed.
7. In the Members List, highlight the user you want to disable. If the user is not displayed in the Members List, the application is not enabled for Location Based Services. Click Cancel.
8. Click Remove. The user is removed from the Members List.
9. Click OK. The application is disabled from Policy Director.

How does Location Base Server (LBS) interact with Location Base Applications (LBA)

Three ways that Location Base Server interacts with Location Base Applications are described below.

1. **Wild-card scheme:**
   If you define an application to be an LBA "www.ibm.com/services" and then "user1" allows this LBA access to their user location information, all URL requests to this defined LBA and also anything underneath this URL tree (www.ibm.com/services/*) are permitted to get "user1" user location information.
2. **Specific scheme:**
   Another option is to specifically define an LBA, for example"www.ibm.com/services/index.html". In this case, if "user2" allows access to this LBA, only the particular URL request is allowed user location information. If "user2" requests "www.ibm.com/services/index1.html", the URL is not allowed user location information as it is not defined as an LBA in Policy Director. In this scenario, "www.ibm.com/services/index1.html" only gets "user2" location information if it is an LBA and the user has enabled this application to see their information.
3. **Mixing Wild-card and Specific scheme:**
   The two schemes above can be combined, but it can be difficult. With the LBAs defined above, a user must allow access to the LBA that is at the lowest level of the hierarchy tree to allow this LBA access to their user location information. For example, if you have "www.ibm.com/services/index.html" and "www.ibm.com/services" defined as LBAs, a user must give access to the "www.ibm.com/services/index.html" for that LBA to be permitted to see his user location information. However, with the two LBS defined above a user can access, for example "www.ibm.com/services/index1.html" and it is permitted by the wild-carding scheme.

Related information

- What is Location Based Services?
- Installing Location Based Services
- Working with SignalSoft
- Working with Location Based Services Sample

Working with SignalSoft

SignalSoft is a third party component that provides specific location information. You need to install and configure Signal SignalSoft to work with Location Based Services.

Creating the WHEREAMI Service

You need to create a WHEREAMI Service for the areas where the you want to track users location data. These instructions assume you have read the *local.info User Guide* and are familiar with using the MAPS product. You should be familiar with the following MAPS (Mobile Application Provisioning System) procedures to create the WHEREAMI SERVICE.

- Arcview components: the Project Windows, the View, Tables
- Adding shapefiles to a View
- Adding a SDE layer to the View
- Adding a table to the project
- Saving a shapefile to the hard drive
- Selecting a theme in the View window
- Opening the table associated with a theme
- Calculating fields in a table
- Using the SDE Editing feature
- Using the Database Management Tool
- Creating a Local.Info service
- Creating a local service zone

To create the WHEREAMI Service, you need to perform the following tasks.

- Load required data
- Load required MAPS extensions
- Save the cell sector table as a dbase File
- Import the cell_centroids.dbf into MAPS
- Adding the cell centroids.dbf Table to View as an event theme
- Populate the event theme with the appropriate basemap data
- Load the whereami.shp shapefile into SDE
- Populate the li_content sde layer with the appropriate data
- Create the WHEREAMI Service

Load required data

Before creating the WHEREAMI Service, you need to first load the required data into SignalSoft.

1. Load the Cell Sector data into the Spatial Data Engine (SDE) following the instructions on page 54 of the *local.info User Guide*.

2. Load the local service zone consisting of the zip code following the instructions on page 73 of the *local.info User Guide*.
3. Load Zip Code Polygons as an Arcview shapefile.
4. Load County Polygons as an Arcview shapefile.
5. Load City Polygons as an Arcview shapefile.
6. Load State Polygons as an Arcview shapefile.
7. Load Country Polygons as an Arcview shapefile.

Load required MAPS extensions

The following map extensions are required:

- SignalSoft
- Utilities
- SDE Editing
- Service Zones Assignment
- Location Manager
- Local.Info
- Geoprocessing

Save the Cell Sector Table as a dbase file

1. Open a View in MAPS and add the required data as stated in the above Required Data section.
2. Open the attribute table for the Cell Sector SDE layer.
3. Export the Cell Sector table to a dbf file by selecting File\Export from the menu.
4. From the Export Table dialog box, select Dbase and click OK.
5. Save the table as *cell_centroids.dbf*. Click OK.

Import the cell_centroids.dbf into MAPS

1. From the Project window, select tables.
2. Click Add. The Add Table dialog box is displayed.
3. Select the cell_centroids.dbf table. Click OK.

Add the cell_centroids.dbf Table to view as an event theme

1. From the View, select View/Add Event Theme. The Add Event Theme dialog is displayed.
2. Select the *cell_centroids.dbf* table for the table.
3. For the X field, select Censored_X.
4. For the Y field, select Centroid_Y. Click OK. The *cell_centroids.dbf* table is displayed as a point theme.
5. Activate and select the new theme.

Populate the event theme with the appropriate basemap data

1. From the View menu, select View Geoprocessing Wizard. The Geoprocessing wizard is displayed.
2. Select Assign Data by Location (spatial join) and click the Next button. The Select a Theme to Assign Data To dialog box is displayed.
3. Select the *cell_centroids.dbf* theme.
4. Select Zip Codes Theme and click Finish.
5. Repeat steps 1-4 and modify step 4 for the County, City, State, and Country themes.
6. Convert the theme to a shapefile called whereami.shp.

Load the whereami.shp shapefile into SDE

1. From the Utilities menu, select Load Data.
2. From the Database Management Tool, select the Load Layer option.
3. From the Layer Name box, select Li_content.
4. From the shapefile box, select whereami.shp.
5. Click Column Mapping.
6. From the Column Mapping dialog box, map the columns based on the following table:

City	URL
County	Rating
State	Hours
County	Credit Card
Zip Code	Postcode
Zip Code	Zone

7. Click Apply.
8. Click Finish.

Populate the li_content SDE layer with the appropriate data

For more information, refer to the *ESRI/ArchView User Guide*, page 262.

1. Check out the li_content theme.
2. Open the attribute table for the checked out theme.
3. Calculate the field service_type="WHEREAMI".
4. Calculate the field other_location=[URL]+", "+[Rating]+", "+[Hours]+", "+[Credit Card].
5. Close the table for the checked out theme.
6. Check in the feature.

Create the WHEREAMI Service

To create a new local service called WHEREAMI, follow the instructions on page 100 of the *local.info User Guide*.

Related information

- What is Location Based Services?
- Installing Location Based Services
- Working with Policy Director
- Working with Location Based Services sample

Working with the Location Based Services Sample

This sample demonstrates Location Based Services finding and displaying location information. If the supporting Everyplace software, such as the Everyplace Wireless Gateway, the Location Based Services box, Tivoli SecureWay Policy Director or Signalsoft, is not set up properly or the URL of the location based application is not configured as a location based application in Policy Director, the sample only displays hard-coded, default geographic information for Cary, NC. If you use a phone through the WebSphere Everyplace Server and the required software is set up properly, the sample displays real geographic information for the user's location. To install this sample, follow the instructions in this section.

The latest version of the sample can be downloaded with the IBM WebSphere Everyplace Suite System Development Kit. The SDK can be accessed at http://www-3.ibm.com/pvc/products/wes/dev_resources.shtml. Any additional location based samples can also be found on this site.

This section describes the following:

- Installing the Location Based Services Samples
- Running the Location Based Services Samples
- Viewing Location Based Services Samples Source Code

Installing the Location Based Services Samples

- Sample Requirements
- Sample Installation
- Samples Location
- Sample File Description
- Reviewing the JavaDoc

Sample Requirements

The Location Based Services samples must be installed on a computer that has WebSphere Application Server 3.5.4 or greater installed. Before installing the samples, ensure the WebSphere Application Server is running.

The Location Based Services samples do not have to be installed on the same system as the Location Based Services. If you want to run the samples on a system other than the one on which the Everyplace Suite Location Proxy is installed, copy the entire contents of the samples directory to the other system and follow the installation instructions.

Sample Installation

Run the install script located in the lbs/samples/ directory. The install script places all sample files in the correct locations on the Application Server.

- *install.bat* for Windows
- *install.sh* for Unix

Samples Location

The samples are located in the lbs\samples directory.

Sample File Description

The latest version of the samples can be obtained from http://www-3.ibm.com/PVC/products/wes/dev-resources.shtml

File	Description
GetRegValue.exe	A utility used during sample installation
install.bat	Installation script for Windows systems
install.sh	Installation Script for UNIX systems
javadoc.zip	Location Services Beans API documentation
LocationBasedServices.wsr	WebSphere Studio 3.5.2 Archive containing sample source code
RenameStudioArchiveFiles.bat	Windows script for viewing sample source code
RenameStudioArchiveFiles.class	Java code used by script
RenameStudioArchiveFiles.sh	UNIX script for viewing sample source code
uninstall.bat	Uninstall script for Windows
uninstall.sh	Uninstall script for UNIX systems
weslbssamples.war	Web Archive containing samples for use with Application Server

Reviewing the Javadoc

The samples use Java Bean technology in the JSP pages. These beans provide easy access to the location information in the request. Using these beans in your applications helps protect the application from future changes in the format of the underlying location data. You can review the Javadoc for the API implemented by these beans at the following location. You can also use your favorite zip utility to unzip the javadoc.zip file to a location on your hard drive. You can then browse the Javadoc by opening your Web browser and entering http://<*hostname*>/lbssamples/LocationBasedServices/javadoc/index.html, where <*hostname*> is the

location of the host on which you installed the samples.

Running the Location Based Services Samples

To check your sample installation, open your Web browser and enter http://<*hostname*>/lbssamples/LocationBasedServices/html/DumpLocationInfoHTMLResults.jsp, where <*hostname*> is the location of the host on which you installed the sample. A page is displayed with hard-coded location information for Cary, NC.

To access a similar page using a WAP browser or WAP-enabled telephone, enter http://<*hostname*>/lbssamples/LocationBasedServices/wml/DumpLocationInfoWMLResults.jsw, where <*hostname*> is the location of the host on which you installed the sample.

Viewing Location Based Services Samples Source Code

When you install the Location Based Services samples, a directory named WebSphere Everyplace Serverlbssamples is created as a child of lbs\samples. You can review the source code for the sample by reviewing the contents of the lbs\samples\WebSphere Everyplace Serverlbssamples\servlets and lbs\samples\WebSphere Everyplace Serverlbssamples\web directories.

The sample source is located in *LocationBasedServices.wsr*. This file is an IBM WebSphere Studio 3.5.3 archive file. If you already have IBM WebSphere Studio 3.5.3 installed, you may use it to view the Location Based Services sample source code. If you do not already have WebSphere Studio installed, you can download the application. Otherwise, you can use a common unzip utility program. If you plan to edit the sample files, you should use one of the following unzipping methods:

- Viewing With IBM WebSphere Studio 3.5.3
- Viewing Without IBM WebSphere Studio 3.5.3

Viewing With IBM WebSphere Studio 3.5.3

If you do not already have WebSphere Studio, you can download a complimentary Entry Edition from http://www.ibm.com/software/webservers/studio/

To open the Location Based Services source code using WebSphere Studio:

1. Start WebSphere Studio.
2. From the File menu, select Open Archive.
3. Select the Browse button.
4. Browse to find and select the *LocationBasedServices.wsr* file.

Viewing Without IBM WebSphere Studio

To view the sample source without installing WebSphere Studio:

1. Use an unzip utility to unzip *LocationBasedServices.wsr* into a temporary directory. It is recommended that you create the temporary directory in the same directory as *LocationBasedServices.war*.
2. Open a Command Prompt or shell and change to the temporary directory.
3. Set the JAVA_HOME environment variable to where you have installed a JDK version 1.2 or

greater.

4. Run *..\RenameStudioArchiveFiles.bat* on Windows or *../RenameStudioArchiveFiles.sh* on UNIX

Note: WebSphere Studio archives sometimes store HTML links in a special format. The RenameStudioArchiveFiles utility does not convert this special format into the standard format. Therefore, you may need to unzip the Web archive *weslbssamples.war* to view files with links such as JSP, HTML, WML files.

Related information

- What is Location Based Services?
- Installing Location Based Services
- Working with Policy Director
- Working with Signal Soft