Sametime
Version 8.5.2 IFR 1

# *Sametime 8.5.2 Interim Feature Release (IFR) 1 Software Development Kit*

## *Login Extensibility Guide*

# Edition Notice

**Note:** Before using this information and the product it supports, read the information in "Notices."

This edition applies to version 8.5.2 Interim Feature Release (IFR) 1 of IBM Lotus Sametime (program number 5724–J23) and to all subsequent releases and modifications until otherwise indicated in new editions.

**© Copyright IBM Corporation 2008, 2011.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

# Login Extensibility in Sametime

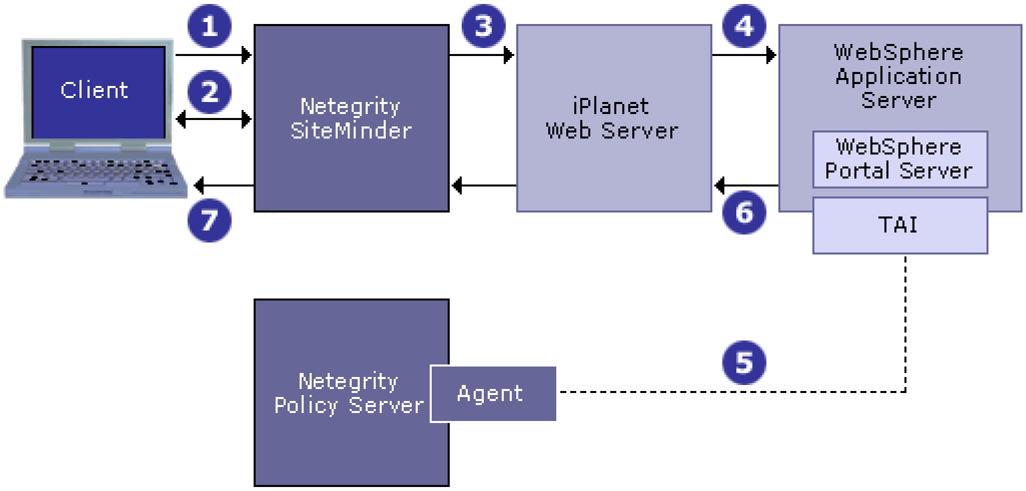
## *Introduction*

IBM® Lotus® Sametime® 8.0.1 introduced JAAS-based login extensibility that allows for insertion of third party token-based authentication routines into the Sametime login sequence. The login modules may include a callback UI to allow end users to enter credentials, and can execute whatever logic is necessary in order to retrieve an LTPA token. The login framework will then use the LTPA token to log into Sametime. For example, a login module can present the user with a form dialog to capture credentials, and then use the Apache HttpClient framework to authenticate with a protected URL in order to retrieve an LTPA token. A fully functioning example demonstrating how to implement a custom login module is included in the Sametime SDK.

### Example Scenario

The following example, adapted from Using Netegrity SiteMinder Authentication for WebSphere Portal, demonstrates how a login module might obtain an LTPA token in a SiteMinder environment.

Figure 1. **Using SiteMinder for authentication with WebSphere**



1. The login module requests a protected resource without credentials. SiteMinder responds to the request with an HTTP response 401 (Authorization required).

2. The login module challenges the user to provide a user name and password using a CallbackHandler UI dialog.

3. The login module uses the Apache HttpClient framework to post an HTTP request to the secured resource using these credentials. SiteMinder forwards the request to the Web server.

4. The Web server, in turn, forwards the request to the WebSphere Application Server.

   If you configure WebSphere Application Server to enable trust associations, it will accept requests with credentials from trusted servers and not require the request to be authenticated again. You must install the SiteMinder Trust Association Interceptor (TAI) to handle requests from the trusted server.

5. If you have configured WebSphere Application Server to not directly accept credentials provided by SiteMinder, it will check the credentials with the Policy Server before creating the LTPA token.

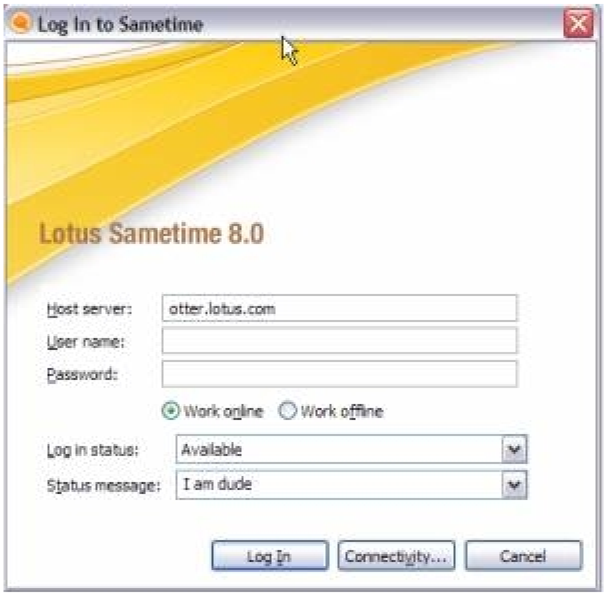
6. After the TAI has successfully checked the credentials, WebSphere Application Server generates the LTPA token for the current session.

7. Finally, the LTPA token is stored as a cookie on the login module's HttpClient, which the login module can then extract and set on the Subject.

## UI Overview

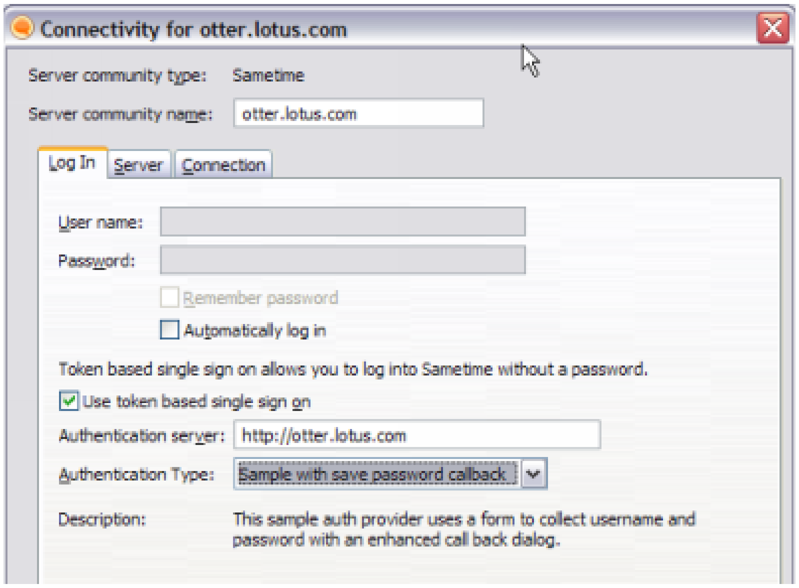
The following steps show how an end user would configure token based login during the initial launch of Sametime. However, a more likely scenario is that the default community settings are preset ahead of time in the install packaging so that the user does not need to fill them out. Preconfiguration details found in the "Login Extensibility Options" section below.

When the login dialog appears for the first time, if not preset, user fills in the host  and selects "Connectivity".



Host server: otter.lotus.com
User name:
Password:
● Work online ○ Work offline
Log in status: Available
Status message: I am dude

If not preset, user selects “Use token based single sign on” and fills out authentication URL and type and selects “OK”.



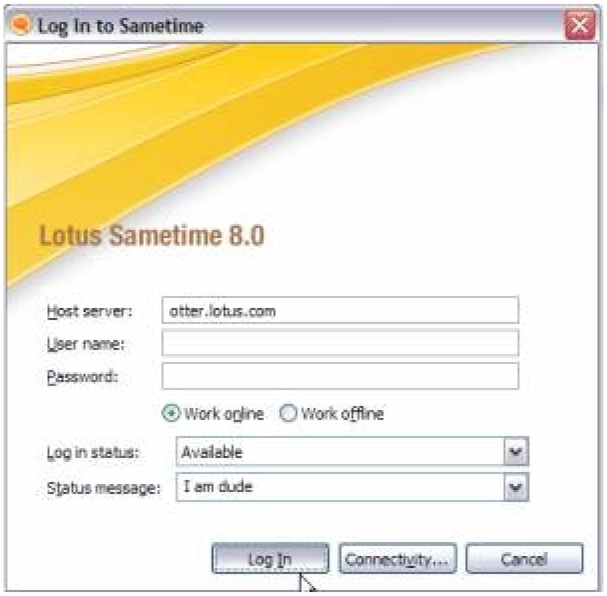
Server community type: Sametime
Server community name: otter.lotus.com

User name:
Password:
□ Remember password
□ Automatically log in

Token based single sign on allows you to log into Sametime without a password.

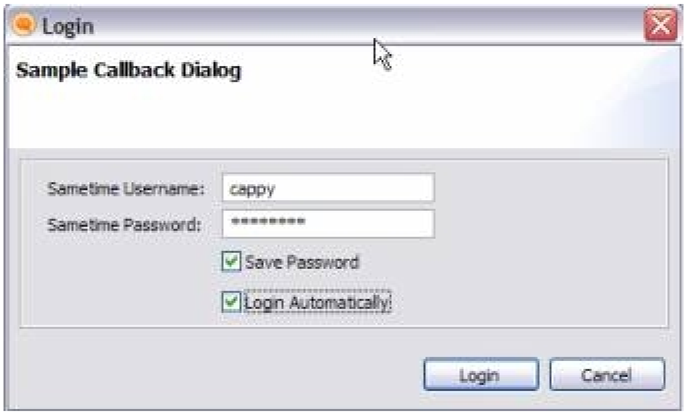
☑ Use token based single sign on
Authentication server: http://otter.lotus.com
Authentication Type: Sample with save password callback
Description: This sample auth provider uses a form to collect username and password with an enhanced call back dialog.

Back in the main login dialog, user selects Login.



Host server: otter.lotus.com
User name:
Password:
● Work online ○ Work offline
Log in status: Available
Status message: I am dude

The custom login module corresponding to the selected authentication type is invoked. In this example, a call back UI is surfaced to the end user.



Sametime Username: cappy
Sametime Password: *********
☑ Save Password
☑ Login Automatically

## *Login Extensibility Options*

You can preconfigure different preferences before rolling out the Sametime installer to create a customized login experience. The preferences below should be added to the plugin_customization.ini file found in the install packaging.

Option 1 – Preset your authentication type as the default.

Sametime ships with a default authentication type set to “SPNEGO”. A different authentication type can be specified as the default by defining the following preference:

```
com.ibm.collaboration.realtime.community/defaultAuthType=ACME_SSO
```

Option 2 – Filter out other authentication types, such as SPNEGO

You can filter out other authentication types using a comma delimited list. For example, to filter out the SPNEGO option, define the following preference:

```
com.ibm.collaboration.realtime.community/filteredAuthTypes=TAM_SPNEGO
```

Option 3 – Presetting the default community for token login

If you would like to preset the default community to use a custom authentication type, you can define the following preferences:

```
com.ibm.collaboration.realtime.community/host=acme.com
com.ibm.collaboration.realtime.community/useAuthServer=true
com.ibm.collaboration.realtime.community/authServerUrl=http://acme.com/auth
com.ibm.collaboration.realtime.community/defaultAuthType=ACME_SSO
com.ibm.collaboration.realtime.community/loginByToken=true
#set loginAtStartup to true to skip the Sametime login dialog and go
straight to the login module
com.ibm.collaboration.realtime.community/loginAtStartup=true
```

Optional – Force clients to login by token

If you wish to prevent users from executing password based login, you can define the following preference:

```
com.ibm.collaboration.realtime.community/tokenLoginOnly=true
```

#### Implementing Login Extensibility

The implementation of a custom authentication routine involves the following JAAS classes:

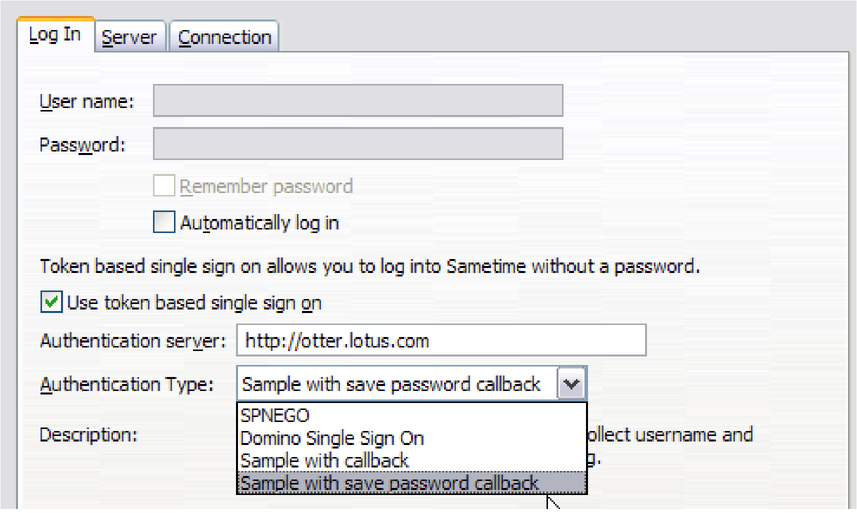
- `javax.security.auth.login.Configuration`
- `javax.security.auth.login.AppConfigurationEntry`
- `javax.security.auth.spi.LoginModule`
- `javax.security.auth.callback.CallbackHandler`

More information on these interfaces and their relationship to one another can be found in the JAAS LoginModule Developer's Guide.

When the user submits the main login dialog, the login framework checks the community's authentication type settings. If configured to use token based login, prior to logging into the Sametime server, the Community's underlying account login method is invoked. This in turn invokes the `javax.security.auth.login.Configuration` implementation providing the opportunity to return an array of `javax.security.auth.login.AppConfigurationEntry` objects, each of which contains a LoginModule. Each LoginModule is given the opportunity to authenticate the Subject, and may utilize a CallbackHandler to do so. Finally, after authenticating the Subject, the LoginModule must add an object of `com.ibm.rcp.security.auth.SingleSignonToken` type, which contains the LTPA token, to the list of private credentials in the Subject.

The `com.ibm.collaboration.realtime.sample.login.extensiblity` plug-in in the Sametime SDK contains a functioning sample custom authentication type that demonstrates these steps. The sample login modules' methodology for obtaining the LTPA token – posting the user's unencrypted credentials to a protected domino URL – is impractical, and intended only for demonstration purposes.

There are two sample authentication types included:



User name:

Password:

□ Remember password

□ Automatically log in

Token based single sign on allows you to log into Sametime without a password.

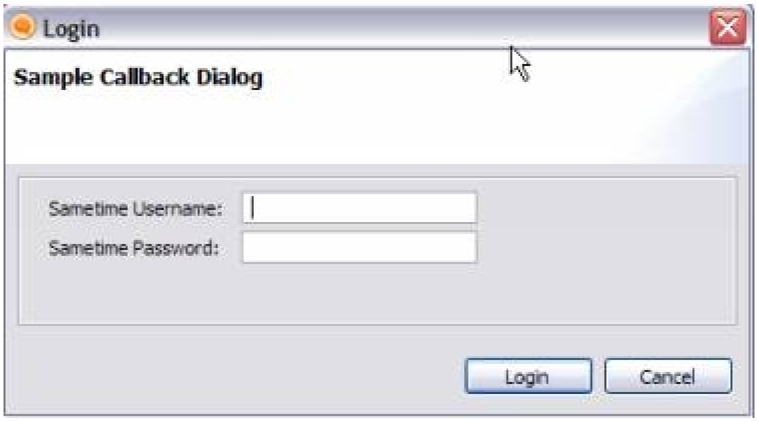
☑ Use token based single sign on

Authentication server: http://otter.lotus.com

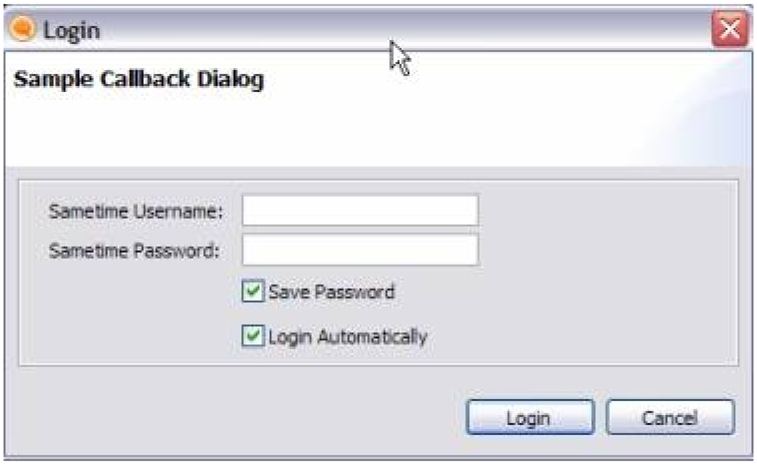
Authentication Type: Sample with save password callback

Description: ollect username and g.

If the “Sample with callback” authentication type is selected, the login module presents a callback UI for each login.



If the “Sample with save password callback” is selected, the login module will present a call back UI which includes options to save the password and login automatically. This updates the save password and login automatically options in the underlying account which are also reflected in the community preference UI. If the default community is not set to login automatically, when Sametime is started, the main login window will appear, and will be followed by the call back handler UI if needed.



☑ Save Password

☑ Login Automatically

## *Implementation Steps*

The following instructions document the basic steps necessary to implement a custom token authentication routine within the Sametime login extensibility framework. These instructions are based on the corresponding sample login extensibility plug-in.

1) Extend the "`com.ibm.collaboration.realtime.community.authTypes`" extension point.

This extension point allows a custom authentication type to be set for a given community.  For example:

```
<extension
      point="com.ibm.collaboration.realtime.community.authTypes">
   <authType
         id="ACME-SAMPLE"
         name="Sample Callback"
         provider="com.acme.SampleAuthProvider"/>
</extension>
```

These extension appear in the client UI allowing end users to associate a given authentication type with a given community. Note that it is possible to preset your authentication type as the default, and to filter out other authentication types, such as the SPNEGO default (detailed in the Login Extensibility Options section).

The authTypes extension point requires a "provider" that is an implementation of the `com.ibm.collaboration.realtime.im.community.AuthTypeProvider` interface. This interface provides various hooks to control authentication behavior including visibility hooks, authentication hooks, and validation hooks.

2) Create a Configuration implementation and extend the `com.ibm.rcp.security.auth.loginConfigurationProvider` extension point.

See `com.ibm.collaboration.realtime.sample.login.extensiblity.SampleConfigurationProvider.java` for implementation details.

See Contributing a login configuration for extension point details.

```
<extension
      id="sampleConfigurationProvider"
```

```
            name="Sample Configuration Provider"

            point="com.ibm.rcp.security.auth.loginConfigurationProvider">

        <loginConfigurationProvider
class="com.ibm.collaboration.realtime.sample.login.extensiblity.SampleConfiguration
Provider"/>

    </extension>
```

3) Create a LoginModule implementation and extend the `com.ibm.rcp.security.auth.loginModule` extension point.

Reference your Login Module implementation in the <loginModule> class attribute.

See `com.ibm.collaboration.realtime.sample.login.extensiblity.SampleLoginModule2.java` for implementation details.

See Contributing a login configuration for extension point details.

```
    <extension

            id="sampleLoginModule"

            name="Sample Login Module"

            point="com.ibm.rcp.security.auth.loginModule">

        <loginModule

class="com.ibm.collaboration.realtime.sample.login.extensiblity.SampleLoginModule"

                description="Sample Login Module"/>

    </extension>
```

4a) Create a CallbackHandler implementation and extend the `com.ibm.rcp.security.auth.callbackHandler` extension point.

If your LoginModule does not require a callback handler, this step is not needed.

See `com.ibm.collaboration.realtime.sample.login.extensiblity.SampleCallbackHandler2.java` for implementation details.

See Contributing a login configuration for extension point details.

```
    <extension id="sampleCallbackHandler"
```

```
              name="Sample CallbackHandler"
              point="com.ibm.rcp.security.auth.callbackHandler">
        <callbackHandler
class="com.ibm.collaboration.realtime.sample.login.extensiblity.SampleCallbackHandler"/>
   </extension>
```

4b) Extend the `com.ibm.rcp.security.auth.callbackHandlerMapping` extension point.

If your LoginModule does not require a callback handler, this step is not needed.

```
   <extension
          name="Sample CallbackHandler Mapping"
          point="com.ibm.rcp.security.auth.callbackHandlerMapping">
      <callbackHandlerMapping
callbackHandlerId="com.ibm.collaboration.realtime.sample.login.extensiblity.sampleCallbackHandler"
             configName="SAMPLE"/>
   </extension>
```

5) Implement `com.ibm.rcp.security.auth.SingleSignonToken`

See `com.ibm.collaboration.realtime.sample.login.extensiblity.SampleLtpaToken.java` for implementation details

In the LoginModule’s commit method, an object of type `com.ibm.rcp.security.auth.SingleSignonToken` must be created, and must contain the LTPA token. This SingleSignonToken implementation must then be added to the list of private credentials in the Subject.

**References**

Contributing a login configuration

JAAS LoginModule Developer's Guide

Using Netegrity SiteMinder Authentication for WebSphere Portal

# Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
5 Technology Park Drive
Westford Technology Park
Westford, MA 01886

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp.
Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

## *Trademarks*

These terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM

AIX

DB2

DB2 Universal Database Domino

Domino

Domino Designer

Domino Directory

i5/OS

iSeries

Lotus

Notes

OS/400

Sametime

System i

WebSphere

AOL is a registered trademark of AOL LLC in the United States, other countries, or both.

AOL Instant Messenger is a trademark of AOL LLC in the United States, other countries, or both.

Google Talk is a trademark of Google, Inc, in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.