Deploying DMZ Secure Proxy Server

October 2012
Note: Before using this information and the product it supports, read the information in "Notices."

This edition applies to version 8.5.2 IFR1 of IBM Sametime (program number 5724–J23) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2011, 2012.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

Introduction .................................................................................................................. 3  
The dual DMZ approach ................................................................................................. 3  
DMZ Secure Proxy Server ............................................................................................. 4  
Required software .......................................................................................................... 5  
Setting up Sametime Gateway ......................................................................................... 6  
  Installing and configuring Sametime Gateway .............................................................. 6  
  Updating Sametime Gateway with interim fixes ........................................................... 6  
    Downloading files ....................................................................................................... 6  
    Installing WebSphere Update Installer ..................................................................... 7  
    Installing interim fixes on a Sametime Gateway Server ............................................. 9  
Setting up DMZ Secure Proxy Server ............................................................................ 12  
  Installing DMZ Secure Proxy Server ........................................................................ 12  
    Downloading files ..................................................................................................... 12  
    Installing the DMZ Secure Proxy Server ................................................................. 12  
  Updating DMZ Secure Proxy Server ........................................................................... 17  
    Downloading files ..................................................................................................... 17  
    Installing WebSphere Update Installer ................................................................... 17  
    Installing the version 7.0.0.15 fix pack on the DMZ Secure Proxy Server ............ 19  
    Installing interim fixes on the DMZ Secure Proxy server ....................................... 22  
Creating the DMZ Secure Proxy Server profile ............................................................ 25  
Installing WebSphere 7.0.0.15 Network Deployment ................................................... 31  
    Downloading files ..................................................................................................... 31  
    Installing Network Deployment 7.0.0.15 ................................................................. 31  
Installing interim fixes for WebSphere Network Deployment ....................................... 36  
    Downloading files ..................................................................................................... 36  
    Installing interim fixes on a Network Deployment server .................................... 36  
Creating an administrative agent and a secure proxy (configuration-only) profile ........ 39  
Registering the secure proxy (configuration-only) profile with the administrative agent 48  
Setting up a tunnel connection between Sametime Gateway and the DMZ Secure Proxy Server ........................................................................................................ 51  
  Creating tunnel access points on the Sametime Gateway cell .................................. 51  
    Creating the tunnel peer access points ................................................................... 51  
    Creating a tunnel template ....................................................................................... 53  
    Creating a tunnel access point group ..................................................................... 54  
    Creating a bridge interface for the Sametime Gateway cell ................................... 57  
Exporting the Sametime Gateway cell's tunnel template .............................................. 58  
Creating custom properties for the Sametime Gateway cell ......................................... 61
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importing the Sametime Gateway cell's tunnel template to a DMZ Secure Proxy Server</td>
<td>63</td>
</tr>
<tr>
<td>Configuring a DMZ Secure Proxy Server</td>
<td>65</td>
</tr>
<tr>
<td>Configuring SIP proxy settings</td>
<td>65</td>
</tr>
<tr>
<td>Configuring custom properties for the DMZ Secure Proxy Server</td>
<td>66</td>
</tr>
<tr>
<td>Configuring ports on the DMZ Secure Proxy Server</td>
<td>71</td>
</tr>
<tr>
<td>Configuring transport settings on the DMZ Secure Proxy Server</td>
<td>74</td>
</tr>
<tr>
<td>Configuring JVM settings for the DMZ Secure Proxy Server</td>
<td>80</td>
</tr>
<tr>
<td>Establishing trust between the DMZ Secure Proxy Server and the Network Deployment cell</td>
<td>84</td>
</tr>
<tr>
<td>Exporting the secure proxy (config-only) profile</td>
<td>84</td>
</tr>
<tr>
<td>Importing the secure proxy (configuration-only) profile</td>
<td>84</td>
</tr>
<tr>
<td>Configuring the trust association</td>
<td>85</td>
</tr>
<tr>
<td>Updating the trust file later</td>
<td>86</td>
</tr>
<tr>
<td>Setting up IBM Load Balancer 7.0</td>
<td>87</td>
</tr>
<tr>
<td>Preparing static IP addresses</td>
<td>87</td>
</tr>
<tr>
<td>Preparing the Load Balancer's cluster host name</td>
<td>87</td>
</tr>
<tr>
<td>Installing IBM Load Balancer</td>
<td>88</td>
</tr>
<tr>
<td>Downloading files</td>
<td>88</td>
</tr>
<tr>
<td>Installing Load Balancer</td>
<td>88</td>
</tr>
<tr>
<td>Configuring Load Balancer</td>
<td>95</td>
</tr>
<tr>
<td>Configuring the cluster IP address on the network adapter</td>
<td>102</td>
</tr>
<tr>
<td>Configuring loopback adapters on the DMZ Secure Proxy Servers</td>
<td>103</td>
</tr>
<tr>
<td>Creating a custom property for Office Collaboration Server</td>
<td>105</td>
</tr>
<tr>
<td>Setting up SSL/TLS security</td>
<td>107</td>
</tr>
<tr>
<td>Setting up SSL/TLS on one or more DMZ Secure Proxy Servers</td>
<td>107</td>
</tr>
<tr>
<td>Requesting a certificate signed by a Certificate Authority</td>
<td>107</td>
</tr>
<tr>
<td>Importing a signed certificate issued into the keystore</td>
<td>109</td>
</tr>
<tr>
<td>Configuring trust for certificate authorities used by external communities</td>
<td>110</td>
</tr>
<tr>
<td>Defining the SSL configuration for a DMZ Secure Proxy Server</td>
<td>111</td>
</tr>
<tr>
<td>Enabling SSL/TLS on a DMZ Secure Proxy Server</td>
<td>113</td>
</tr>
<tr>
<td>Configuring firewalls</td>
<td>117</td>
</tr>
<tr>
<td>Setting inner firewall rules</td>
<td>117</td>
</tr>
<tr>
<td>Setting middle firewall rules</td>
<td>118</td>
</tr>
<tr>
<td>Middle firewall rules</td>
<td>118</td>
</tr>
<tr>
<td>Setting outer firewall rules</td>
<td>119</td>
</tr>
<tr>
<td>Outer firewall rules</td>
<td>119</td>
</tr>
</tbody>
</table>
Introduction

This guide explains how to enhance security by deploying a DMZ Secure Proxy Server for IBM® WebSphere® Application Server in a DMZ between an IBM Sametime® Gateway servers and the Internet.

The dual DMZ approach

The Sametime Gateway connects an organization's Sametime Community Server to the outside world through the Internet. This outside connectivity poses risks and requires firewall protection. Normally, an organization would meet this requirement by deploying the Sametime Gateway in a DMZ (demilitarized zone) situated between the company's own intranet and the Internet. Clients attempting to access Sametime Gateway from the Internet tunnel through an outer firewall to a SIP proxy server, which then routes client requests through an inner firewall to the corporate intranet where Sametime servers are deployed.

When you deploy Sametime Gateway using a single DMZ, the deployment looks like this, where each of the colored blocks represents a different zone with different firewall settings:

For some organizations, a single DMZ does not provide a sufficient level of security, and an additional DMZ is required to further isolate Internet-facing servers. This "dual DMZ" approach increases security by inserting an additional "middle" firewall between the Internet and the corporate intranet, creating another network zone called an Application DMZ:

In this type of deployment, the Sametime Gateway servers are moved outside the inner firewall but are separated from the original (Web) DMZ by a new middle firewall, creating an Application DMZ. The SIP proxy server in the Web DMZ is replaced a more secure version of the server, called the DMZ Secure Proxy Server.
DMZ Secure Proxy Server

Unlike a traditional proxy server, the DMZ Secure Proxy is designed for use outside the corporate firewall and incorporates a higher level of security to protect your deployment. For example, the DMZ Secure Proxy Server does not include an application server or a web container; limiting the software on the server helps protect it from unauthorized access. This added security comes at a cost, in that the DMZ Secure Proxy Server requires some additional configuration during deployment.

To deploy the DMZ Secure Proxy Server, you will set up a dual DMZ deployment where the Sametime Gateway servers reside in the Application DMZ and the DMZ Secure Proxy Server resides in the Web DMZ. External users can access only the DMZ Secure Proxy Server, which in turn passes on requests for data to the Sametime Gateway servers, which in turn connect to the Sametime Community Servers on the corporate intranet before routing data back to the users.

In the illustration below, the base Sametime deployment is contained within the company's inner firewall. The Sametime Gateway cell (one or more servers) resides in the Application DMZ, and the DMZ Secure Proxy Server resides in the Web DMZ.
Required software

To deploy the WebSphere DMZ Secure Proxy Server and configure a core bridge across the firewall between the DMZ Secure Proxy Server and Sametime Gateway, you will need the following software, available in the Sametime 8.5.2 kit. Details on locating each package are included in the installation instructions that follow.

**Note:** Sametime 8.5.2 IFR1 is an update to version 8.5.2 and requires that you install version 8.5.2 before applying the update, so you will use the base 8.5.2 kit to obtain these packages.

✔ WebSphere Update Installer V7.0.0.15
   *Apply updates and interim fixes to base installation.*

✔ WebSphere Network Deployment V7.0.0.15
   *Provide an Administrative Agent to manage the DMZ Secure Proxy Server.*

✔ DMZ Secure Proxy Server for WebSphere Application Server V7.0
   *Deploy one or more proxy servers outside the firewall protecting the Sametime Gateway servers.*
   Included with WebSphere Network Deployment

✔ WebSphere DMZ Secure Proxy Server fix packs
   *Apply to the DMZ Secure Proxy Server to update security.*
   Download the fix packs listed from the following directory within the kit:
   - 7.0.0-WS-NDDMZ-your_operating_system-FP0000015.pak
   - 7.0.0-WS-WASSDK-your_operating_system-FP0000015.pak

✔ WebSphere Application Server interim fixes:
   *Apply to the WebSphere Application Server hosting each type of server below.*

   **Sametime Gateway server (hosted on WebSphere Application Server)**
   - 7.0.0.15-WS-WAS-IFPM20204.pak
   - 7.0.0.15-WS-WAS-IFPM37276.pak
   - 7.0.0.15-WS-WAS-IFPM35730.pak
   - 7.0.0.15-WS-WAS-IFPM49926.pak

   **WebSphere DMZ Secure Proxy Server**
   - 7.0.0.7-WS-NDDMZ-IFPM34361.pak
   - 7.0.0.15-WS-NDDMZ-IFPM20204.pak
   - 7.0.0.15-WS-NDDMZ-IFPM30141.pak
   - 7.0.0.15-WS-NDDMZ-MultiOS-IFPM35730.pak

   **WebSphere Network Deployment for DMZ Secure Proxy Server**
   - 7.0.0.1-WS-WASND-IFPM27226.pak

✔ WebSphere Edge Components V7.0 Load Balancer for IBM WebSphere Network Deployment
   *Deploy in front of two or more DMZ Secure Proxy Servers to manage connections from external users.*
Setting up Sametime Gateway

Start by installing and configuring one or more IBM Sametime Gateway servers as explained in this section.

Installing and configuring Sametime Gateway

Install and configure either a stand-alone Sametime Gateway server, or a cluster of Sametime Gateway servers, as described in the Sametime wiki.

Deployment notes:

- Do not deploy any SIP servers, WebSphere proxy servers, or a load balancer in front of the cluster as instructed in the product documentation, because SIP communications from external clients will be routed through the DMZ Secure Proxy Server instead.
- Do not deploy an XMPP server for Sametime Gateway -- this dual DMZ configuration does not support the use of an XMPP server.
- Configure the inner firewall (between the Sametime Community Servers in the Intranet zone and the Sametime Gateway servers in the Application DMZ) as explained in the Sametime wiki topic, Opening ports in the firewall.
- You will create one Sametime Gateway cell, containing either a single, stand-alone server, or a cluster of servers.

Updating Sametime Gateway with interim fixes

Update all Sametime Gateway servers with WebSphere Application Server interim fixes that became available after Sametime 8.5.2 was released.

Updating Sametime Gateway requires that you download the WebSphere Update Installer and some WebSphere fix packs, install the Update Installer, and then run it to apply the fix packs.

Note: Complete this ask on every Sametime Gateway server in the cluster.

Downloading files

You can download files from CD/DVD or Passport Advantage.

Note: Complete this task on every Sametime Gateway server in the cluster.

1. Log in to the computer as the system administrator (Microsoft® Windows®) or as root (IBM AIX®, Linux, Solaris).
2. Navigate to a temporary location where you want to store downloaded files.
3. Download the following package:
   IBM WebSphere V7.0.0.15 iFixes for Sametime V8.5.2 Windows, AIX, Linux x86, Solaris, IBM i Multilingual
4. Extract the package into the temporary location.
Installing WebSphere Update Installer

Applying fixes to WebSphere servers requires that you first install the WebSphere Update Installer. 

Note: The package from Sametime 8.5.2 includes V7.0.0.15 of the WebSphere Update Installer. Because the update installer is backward-compatible, you can also use later versions of it to install 7.0.0.15 fixes to WebSphere servers.

1. Prepare the WebSphere Update Installer:
   a. Within the download location, navigate to the following directory:
      `SametimeWASSecureProxyiFixes/WebSphereUPDI`
   b. Extract the Update Installer (`7.0.0.15-WS-UPDI-operating_system.zip`) into this location.

2. Install the Update Installer:
   a. Navigate to the new `UpdateInstaller` subdirectory.
   b. Start the installation with the following command:
      - AIX, Linux, Solaris
        `./install`
      - Windows
        `install.exe`
   c. On the "Installation Wizard for Update Installer" welcome screen, click Next.
   d. On the "Software License Agreement" screen, click I accept both the IBM and non-IBM terms, and then click Next.
e. On the "System Prerequisites Check" screen, verify that your computer satisfies the prerequisites and then click **Next**.

If your computer does not meet the prerequisites, you must exit the wizard, modify the computer until prerequisites are met, and then begin again from substep d.

f. On the "Installation Directory" screen, accept or change the **Directory path**, and then click **Next**.

If the summary is not correct, click **Previous** as needed to back up and correct any settings as needed before clicking **Next** to return to the summary and begin the installation.
h. On the "Installation Complete" screen, click **Launch IBM Update Installer for WebSphere Software on exit**, and then click **Finish**.

![Image of Installation Wizard](image)

The Update Installer launches automatically at this point; leave it open for the next task.

**Installing interim fixes on a Sametime Gateway Server**

Use the WebSphere Update Installer to apply these interim fixes that became available after Sametime 8.5.2 was released:

- 7.0.0.15-WS-WAS-IFPM20204.pak
- 7.0.0.15-WS-WAS-IFPM37276.pak
- 7.0.0.15-WS-WAS-IFPM35730.pak
- 7.0.0.15-WS-WAS-IFPM49926.pak

**Note:** This fix is recent and may have been delivered separately. If so, copy it to the same location as the other fixes (listed below.)

Within the download location from the previous task, the fixes are stored in the following location:

`SametimeWASSecureProxyiFixes/WebSphereiFixes/SametimeGateway`

**Note:** Complete this task on every Sametime Gateway server.

1. Use the Update Installer to apply the interim fixes to the Sametime Gateway server:
   a. On the "IBM Update Installer for WebSphere Software" welcome screen, click **Next**.

![Image of IBM Update Installer](image)
b. On the "Product Selection" screen, set the **Directory path** to the Sametime Gateway server's installation directory, and then click **Next**.

![IBM Update Installer for WebSphere Software 7.0.0.15](image)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Default installation directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>/opt/IBM/WebSphere/STgateway</td>
</tr>
<tr>
<td>IBM i</td>
<td>/QIBM/UserData/STgateway/[profile name]</td>
</tr>
<tr>
<td>Linux</td>
<td>/opt/IBM/WebSphere/STgateway</td>
</tr>
<tr>
<td>Solaris</td>
<td>/opt/IBM/WebSphere/STgateway</td>
</tr>
<tr>
<td>Windows</td>
<td>[drive]:\Program Files\IBM\WebSphere\STgateway</td>
</tr>
</tbody>
</table>

c. On the "Maintenance Operation Selection" screen, click **Install maintenance package**, and then click **Next**.

![IBM Update Installer for WebSphere Software 7.0.0.15](image)

d. On the "Maintenance Package Directory Selection" screen, browse to the location where the interim fixes are stored, and then click **Next**.

```
temporary_location/SametimeWASSecureProxyiFixes/WebSphereiFixes/SametimeGateway
```

![IBM Update Installer for WebSphere Software 7.0.0.15](image)
e. On the "Available Maintenance Package to Install" screen, select the interim fixes, and then click **Next**.

![Image of IBM Update Installer for WebSphere Software 7.0.0.15](image)

f. On the "Installation Summary" screen, review the summary and if it is correct, click **Next** to begin the installation.

   If the summary is not correct, click **Previous** as needed to back up and correct any settings as needed before clicking **Next** to return to the summary and begin the installation.

g. On the "Installation Complete" screen, click **Finish** to exit the Update Installer.
Setting up DMZ Secure Proxy Server

Install and configure a DMZ Secure Proxy Server by installing the DMZ Secure Proxy Server application, configuring its server profile, and then installing WebSphere Network Deployment, which provides an Administrative Agent that can manage the DMZ Secure Proxy Server.

Important:

- If you install multiple DMZ Secure Proxy Servers, be sure to complete all of this tasks in this section for every server.
- If you install the DMZ Secure Proxy Server manually, make sure that its WebSphere cell name is different from the Sametime Gateway server's WebSphere cell name. If you use the same cell name for both installations, the deployment will not function properly.
- Each DMZ Secure Proxy Server will operate as a separate cell and will require its own Administrative Agent.

Installing DMZ Secure Proxy Server

Download and install the WebSphere 7 DMZ Secure Proxy Server, and then update it to the latest version by applying the necessary fix pack and interim fixes.

Downloading files

You can download files from CD/DVD or Passport Advantage.

1. Log in to the computer as the system administrator (Microsoft® Windows®) or as root (IBM AIX®, Linux, Solaris).
2. Navigate to a temporary location where you want to store downloaded files.
3. Download the following package:
   IBM DMZ Secure Proxy Server V7.0 for operating_system, Multilingual
4. Extract the package into the temporary location.

Installing the DMZ Secure Proxy Server

Use the launchpad to start the installation wizard.

1. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Log in to the computer as root.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting and change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Navigate to the temporary location where you extracted the DMZ Secure Proxy Server V7 package.
3. Start the installation launchpad:
   a. Verify that the computer has a Web browser available or else install one now.
      The launchpad requires a Web browser on the local machine (you cannot use the launchpad remotely).
      Supported browsers include Mozilla Firefox and Windows Internet Explorer.
b. Start the launchpad by running the following command:
   - AIX, Linux, Solaris
     ./launchpad.sh
   - Windows
     launchpad.exe

c. When the launchpad opens, click **WebSphere DMZ Secure Proxy Server Installation** on the navigator.

d. On the WebSphere DMZ Secure Proxy Server page, click the **Launch the installation wizard for the DMZ Secure Proxy Server** link.

4. Use the wizard to install the DMZ Secure Proxy Server:
   a. On the "Welcome to the WebSphere DMZ Secure Proxy Server installation wizard" screen, click **Next**.
b. On the "Software License Agreement" screen, review the agreement and when ready to proceed, click I accept both the IBM and the non-IBM terms, and then click Next.

c. On the "System Prerequisites Check" screen, verify that your computer satisfies the prerequisites (look for the "Passed" notice), and then click Next.

If your computer does not meet the prerequisites, you must exit the wizard, modify the computer until prerequisites are met, and then begin again from step 4.

d. On the "Installation Directory" screen, accept or change the Product Installation location, note down the location so you can use it later, and then click Next.

Specify a different directory or click Browse to select a different install location.

Product installation location:
C:\Program Files\IBM\WebSphere\AppServer

You will install fix packs to the same location, so it's helpful to make a note of that location now.
e. On the "WebSphere Application Server Environments" screen, select \textbf{None} and then click \textbf{Next}.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{webSphere.png}
\caption{WebSphere Application Server Environments screen.}
\end{figure}

f. When the warning prompts you to choose whether to proceed without creating a profile, click \textbf{Yes} to continue.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{warning.png}
\caption{Warning dialog box.}
\end{figure}

Do not create the profile now; you will create a special type of secure profile for this server in a later task.

g. On the "Installation Summary" screen, review the summary and if it is correct, click \textbf{Next} to begin the installation.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{installationSummary.png}
\caption{Installation Summary screen.}
\end{figure}

If the summary is not correct, click \textbf{Previous} as needed to back up and correct any settings as needed before clicking \textbf{Next} to return to the summary and begin the installation.
h. On the "Installation Results" screen, de-select **Create a new WebSphere Application Server profile using the Profile Management tool** and then click **Finish**.

![Image of Installation Results screen with selected option to create a new profile]  
You will create the profile later, so there is no need to launch the Profile Management Tool at this point.

5. Close the launchpad:
   a. Back on the launchpad, click **Exit** in the navigator.

   ![Image of launchpad with 'Exit' highlighted]  

   b. When prompted to confirm, click **OK**.
Updating DMZ Secure Proxy Server

The base installation of DMZ Secure Proxy Server uses WebSphere version 7.0, but Sametime 8.5.2 requires servers in the deployment to use at least version 7.0.0.15 of WebSphere.

Updating DMZ Secure Proxy Server requires that you download the WebSphere Update Installer and some WebSphere fix packs, install the Update Installer, and then run it to apply the fix packs.

**Downloading files**

You can download files from CD/DVD or Passport Advantage.

1. Log in to the computer as the system administrator (Microsoft® Windows®) or as root (IBM AIX®, Linux, Solaris).
2. Navigate to a temporary location where you want to store downloaded files.
3. Download the following package:
   IBM WAS DMZ V7.0.0.15 iFixes for Sametime V8.5.2 Multiplatform Multilingual
4. Extract the package into the temporary location.

**Installing WebSphere Update Installer**

Applying fixes to WebSphere servers requires you to first install the WebSphere Update Installer.

**Note:** The package from Sametime 8.5.2 includes V7.0.0.15 of the WebSphere Update Installer. Because the update installer is backward-compatible, you can also use later versions of it to install 7.0.0.15 fixes to WebSphere servers.

1. Prepare the WebSphere Update Installer:
   a. Within the download location, navigate to the following directory:
      SametimeWASSecureProxyiFixes/WebSphereUPDI
   b. Extract the Update Installer (7.0.0.15-WS-UPDI-operating_system.zip) into this location.
2. Install the Update Installer:
   a. Navigate to the new UpdateInstaller subdirectory.
   b. Start the installation with the following command:
      AIX, Linux, Solaris
         ./install
      Windows
         install.exe
   c. On the "Installation Wizard for Update Installer" welcome screen, click Next.
d. On the "Software License Agreement" screen, click **I accept both the IBM and non-IBM terms**, and then click **Next**.

![Software License Agreement screen]

**Image:** Software License Agreement screen with options to accept both IBM and non-IBM terms or the IBM terms only.

---

e. On the "System Prerequisites Check" screen, verify that your computer satisfies the prerequisites and then click **Next**.

![System Prerequisites Check screen]

**Image:** System Prerequisites Check screen indicating "Passed: Your operating system completed the prerequisites check successfully."

---

f. On the "Installation Directory" screen, accept or change the **Directory path**, and then click **Next**.

![Installation Directory screen]

**Image:** Installation Directory screen with the directory path set to `C:\Program Files\IBM\WebSphere\UpdateInstaller` and options to create a start menu icon.
g. On the "Installation Summary" screen, review the summary and if it is correct, click Next to begin the installation.

If the summary is not correct, click Previous as needed to back up and correct any settings as needed before clicking Next to return to the summary and begin the installation.

h. On the "Installation Complete" screen, click Launch IBM Update Installer for WebSphere Software on exit, and then click Finish.

The Update Installer launches automatically at this point; leave it open for the next task.

**Installing the version 7.0.0.15 fix pack on the DMZ Secure Proxy Server**

Use the WebSphere Update Installer to apply these fix packs, which will update the DMZ Secure Proxy Server to version 7.0.0.15:

- 7.0.0-WS-NDDMZ-your_operating_system-FP0000015.pak
- 7.0.0-WS-WASSDK-your_operating_system-FP0000015.pak

Within the download location from the previous task, the fixes are stored in the following location:

SametimeWASSecureProxyiFixes/WebSphereSecureProxyFixPack
1. Use the WebSphere Update Installer to apply the fix packs to the DMZ Secure Proxy Server:
   a. On the "IBM Update Installer for WebSphere Software" welcome screen, click **Next**.

   ![IBM Update Installer for WebSphere Software](image1)

   b. On the "Product Selection" screen, set the **Directory path** to the DMZ Secure Proxy Server's installation directory, and then click **Next**.

   ![Product Selection](image2)

   This is the **Product Installation location** path that you noted in step 4.d. while installing the DMZ Secure Proxy Server.

   c. On the "Maintenance Operation Selection" screen, click **Install maintenance package**, and then click **Next**.

   ![Maintenance Operation Selection](image3)
d. On the "Maintenance Package Directory Selection" screen, browse to the location where you downloaded the fix packs in step 1, and then click **Next**.

![Image of Maintenance Package Directory Selection](image1.png)

```
On the "Maintenance Package Directory Selection" screen, browse to the location where you downloaded the fix packs in step 1, and then click Next.
```

e. On the "Available Maintenance Package to Install" screen, select both the DMZ Secure Proxy Server and the JAVA SDK fix packs, and then click **Next**.

![Image of Available Maintenance Package to Install](image2.png)

```
e. On the "Available Maintenance Package to Install" screen, select both the DMZ Secure Proxy Server and the JAVA SDK fix packs, and then click Next.
e```

f. On the "Installation Summary" screen, review the summary and if it is correct, click **Next** to begin the installation.

![Image of Installation Summary](image3.png)

```
f. On the "Installation Summary" screen, review the summary and if it is correct, click Next to begin the installation.
f```

If the summary is not correct, click **Previous** as needed to back up and correct any settings as needed before clicking **Next** to return to the summary and begin the installation.
g. On the "Installation Complete" screen, click **Relaunch** to restart the Update Installer for the next task.

![Relaunch](image)

**Installing interim fixes on the DMZ Secure Proxy server**

After you have brought the DMZ Secure Proxy Server up to version 7.0.0.15, you must use the Update Installer again to apply some additional interim fixes that became available after the 7.0.0.15 fix pack was released:

- 7.0.0.7-WS-NDDMZ-IFPM34361.pak
- 7.0.0.15-WS-NDDMZ-IFPM20204.pak
- 7.0.0.15-WS-NDDMZ-IFPM30141.pak
- 7.0.0.15-WS-NDDMZ-MultiOS-IFPM35730.pak

Within the download location from the previous task, the fixes are stored in the following location:

```bash
/home/your/location/SametimeWASSecureProxyiFixes/WebSphereiFixes/WebSphereSecureProxy
```

1. Use the Update Installer to apply the interim fixes to the DMZ Secure Proxy Server:
   a. On the "IBM Update Installer for WebSphere Software" welcome screen, click **Next**.

![Welcome screen](image)
b. On the "Product Selection" screen, set the **Directory path** to the DMZ Secure Proxy Server's installation directory, and then click **Next**.

This is the **Product Installation location** path that you specified in step 4.d. when you installed the DMZ Secure Proxy Server.

c. On the "Maintenance Operation Selection" screen, click **Install maintenance package**, and then click **Next**.

d. On the "Maintenance Package Directory Selection" screen, browse to the location where you downloaded the interim fixes in step 1 of this task, and then click **Next**.
e. On the "Available Maintenance Package to Install" screen, select all of the interim fixes that you downloaded, and then click **Next**.

![Available Maintenance Package to Install](image1)

f. On the "Installation Summary" screen, review the summary and if it is correct, click **Next** to begin the installation.

![Installation Summary](image2)

If the summary is not correct, click **Previous** as needed to back up and correct any settings as needed before clicking **Next** to return to the summary and begin the installation.

g. On the "Installation Complete" screen, click **Finish** to exit the Update Installer.
Creating the DMZ Secure Proxy Server profile

Use the Profile Management Tool to create an application server profile for the new DMZ Secure Proxy Server. When you installed the DMZ Secure Proxy Server, you skipped this task in the installer because it was necessary to install server updates before creating the profile. Now you are ready to create the application server profile.

**Note:** If you installed multiple DMZ Secure Proxy Servers, complete this task on each server.

1. On the DMZ Secure Proxy Server, navigate to the following directory:
   
   **DMZ_Secure_Proxy_install_directory/bin/ProfileManagement**

   This is the "Product Installation Location" from step 5.e when you installed the DMZ Secure Proxy Server.

2. Start the Profile Management Tool by running the following command:
   
   **AIX, Linux, Solaris**
   
   `pmt.sh`
   
   **Windows**
   
   `pmt.bat`

3. Use the Profile Management Tool to create the server's profile:
   
   a. On the "Welcome to the Profile Management Tool" screen, click the **Launch Profile Management Tool** button.

   ![Launch Profile Management Tool](image1.png)

   b. On the "Profiles" screen, click the **Create** button.

   ![Create](image2.png)
c. On the "Environment Selection" screen, click **Secure proxy**, and then click **Next**.

d. On the "Profile Create Options" screen, click **Advanced profile creation**, and then click **Next**.

e. On the "Profile Name and Location" screen, accept the defaults and click **Next**.

f. On the "Node and Host Names" screen, accept the defaults and click **Next**.
g. On the "Security Level Selection" screen, click Low, and then click Next.

h. On the "Administrative Security" screen, choose whether to enable security:
   • If you want to enable security, do the following:
     i. Click Enable administrative security.
     ii. Type a User name for the new administrator account that will be created.
     iii. Type a Password for the administrator account.
     iv. Type the password again in the Confirm password field.
     v. Click Next and proceed to the next substep.
   • If you do not want to enable security, leave the fields on this screen blank, and just click Next.
i. On the "Security Certificate (Part 1)" screen, accept the defaults and click **Next**.

![Security Certificate (Part 1) Screen](image1)

j. On the "Security Certificate (Part 2)" screen, accept the defaults and click **Next**.

![Security Certificate (Part 2) Screen](image2)
k. On the "Port Values Assignment" screen, accept the defaults and click Next.

l. On the "Service Definition" screen, accept the defaults and click Next.
m. On the "Profile Creation Summary" screen, note down the values in the following fields (you will need these names later when you configure the Network Deployment), and then click Create:

- Profile name
- Node name
- Server name

n. On the "Profile Creation Complete" screen, de-select Launch the First steps console, and then click Finish.

o. On the "Profile Management Tool" screen, click File > Exit.
**Installing WebSphere 7.0.0.15 Network Deployment**

Install WebSphere Network Deployment on the computer hosting the DMZ Secure Proxy Server. Network Deployment provides the Administrative Agent that will be used to manage the DMZ Secure Proxy Server. After running the wizard to install the Network Deployment server, you will update it to the latest version by using the WebSphere Update Installer to apply the necessary interim fixes.

*Note:* If you install multiple DMZ Secure Proxy Servers, complete this task on each server so that every DMZ Secure Proxy Server resides on a computer with Network Deployment.

**Downloading files**

You can download files from CD/DVD or Passport Advantage.

*Note:* Complete this task on every Sametime Gateway server.

1. Log in to the computer as the system administrator (Microsoft® Windows®) or as root (IBM AIX®, Linux, Solaris).
2. Navigate to a temporary location where you want to store downloaded files.
3. Download the following package:
   
   WASND V7.0.0.15 Customized Installation Package *operating_system* for Sametime V8.5.2 Multilingual

4. Extract the package into the temporary location.

**Installing Network Deployment 7.0.0.15**

1. Navigate to the *ifpackage/WAS* directory below the temporary location where you extracted the Network Deployment V7.0.0.15 package.
2. Start the installation wizard by running the following command: `install`
   
   This command is available on all operating systems.
3. Use the wizard to install the Network Deployment:
   
   a. On the "Welcome to the IBM WebSphere Application Server Network Deployment installation wizard" screen, click *Next*.
b. On the "Software License Agreement" screen, click **I accept both the IBM and the non-IBM terms** and then click **Next**.

c. On the "System Prerequisites Check" screen, verify that your computer satisfies the prerequisites and then click **Next**.

If your computer does not meet the prerequisites, you must exit the wizard, modify the computer until prerequisites are met, and then begin again from step 4.

d. On the "Optional Features Installation" screen, don't select any optional features -- just click **Next**.
e. On the "Installation Directory" screen, accept or change the **Product Installation location** and then click **Next**.

![Installation Directory Screen](image)

f. On the "WebSphere Application Server Environments" screen, select **None** and then click **Next**.

![WebSphere Environments Screen](image)

g. Click **Yes** when the warning message prompts you to choose whether to continue without creating a profile:

![Warning Screen](image)

You will create a profile in a later task, after you have installed interim fixes on the server.
h. On the "Repository for Centralized Installation Managers" screen, do not select the option to create the repository -- just click **Next**.

![Repository for Centralized Installation Managers](image1)

i. On the "Installation Summary" screen, review the summary and if it is correct, click **Next** to begin the installation.

![Installation Summary](image2)

If the summary is not correct, click **Previous** as needed to back up and correct any settings as needed before clicking **Next** to return to the summary and begin the installation.

j. On the "Installation Results" screen, do the following:
i. Verify that the server was successfully installed.

ii. De-select Create a new WebSphere Application Server profile using the Profile Management tool.

   It is important to make sure this option is not selected because you already created an application server profile on this computer.

iii. Click Finish.
Installing interim fixes for WebSphere Network Deployment

After you have installed Network Deployment V7.0.0.15, you must use the WebSphere Update Installer apply an additional interim fix that became available after the base product was released.

Note: Complete this task on every DMZ Secure Proxy Server (every Network Deployment server).

Downloading files

You can download files from CD/DVD or Passport Advantage.

1. Log in to the computer as the system administrator (Microsoft® Windows®) or as root (IBM AIX®, Linux, Solaris).
2. Navigate to a temporary location where you want to store downloaded files.
3. Download the following package:
   IBM WebSphere V7.0.0.15 iFixes for Sametime V8.5.2 operating_system Multilingual
4. Extract the package into the temporary location.

Installing interim fixes on a Network Deployment server

Use the WebSphere Update Installer to apply this interim fix:

- 7.0.0.1-WS-WASND-IFPM27226.pak

Within the download location from the previous task, the fix is stored in the following location:

    SametimeWASiFixes/WebSphereiFixes

1. Navigate to the UpdateInstaller directory.
   This is the directory where you already installed the Update Installer on this computer while updating the DMZ Secure Proxy Server. You can use the same instance of the Update Installer now.
2. Run the update command to start the Update Installer:
   AIX, Linux, Solaris
   ./update.sh
   Windows
   update.bat
3. Use the Update Installer to apply the interim fix to the Network Deployment:
   a. On the "IBM Update Installer for WebSphere Software" welcome screen, click Next.
b. On the "Product Selection" screen, set the **Directory path** to the Network Deployment's installation directory, and then click **Next**.

![Product Selection Screen]

This is the **Product Installation location** path that you specified in step 3.e. when you installed the Network Deployment server.

c. On the "Maintenance Operation Selection" screen, click **Install maintenance package**, and then click **Next**.

![Maintenance Operation Selection Screen]

d. On the "Maintenance Package Directory Selection" screen, browse to the location where you downloaded the interim fix, and then click **Next**.

![Maintenance Package Directory Selection Screen]

e. On the "Available Maintenance Package to Install" screen, select the interim fix that you downloaded, and then click **Next**.

![Available Maintenance Package to Install Screen]
f. On the "Installation Summary" screen, review the summary and if it is correct, click **Next** to begin the installation.

![Installation Summary Screen](image1.png)

If the summary is not correct, click **Previous** as needed to back up and correct any settings as needed before clicking **Next** to return to the summary and begin the installation.

g. On the "Installation Complete" screen, click **Finish** to exit the Update Installer.

![Installation Complete Screen](image2.png)
Creating an administrative agent and a secure proxy (configuration-only) profile

Use the WebSphere Profile Management Tool (installed with WebSphere Network Deployment) to configure an administrative agent and a secure proxy (configuration-only) profile for a DMZ Secure Proxy Server. The DMZ Secure Proxy Server does not contain a web container and therefore does not provide an Integrated Solutions Console for administration. To administer the server, you will use the Network Deployment application server residing on the same computer to create a secure "configuration-only" profile for the DMZ Secure Proxy Server, and then import that configuration into the DMZ Secure Proxy Server. Any time you want to modify the DMZ Secure Proxy Server's configuration, you must follow the same process to update the secure (configuration-only) profile and then re-import it into the DMZ Secure Proxy Server.

Note: If you installed multiple DMZ Secure Proxy Servers, complete this task on each server.

1. On the server where you installed DMZ Secure Proxy Server and WebSphere Network Deployment, navigate to the following directory:
   
   NetworkDeployment_install_directory/bin/ProfileManagement

2. Start the Profile Management Tool by running the following command:
   
   AIX, Linux, Solaris
   pmt.sh

   Windows
   pmt.bat

3. Use the Profile Management Tool to create the administrative agent:
   
   a. On the "Welcome to the Profile Management Tool" screen, click the Launch Profile Management Tool button.

   ![Profile Management Tool](image1.png)

   b. On the "Profiles" screen, click the Create button.

   ![Profiles screen](image2.png)
c. On the "Environment Selection" screen, click **Management**, and then click **Next**.

d. On the "Server Type Selection" screen, click **Administrative agent**, and then click **Next**.

e. On the "Profile Creation Options" screen, select **Typical profile creation**, and then click **Next**.
f. On the "Administrative Security" screen, choose whether to enable security:

   **Note:** If you enable security for the administrative agent now, then you must also enable it for the secure proxy profile in step 4.

   - If you want to enable security, do the following:
     
     ![Administrative Security Screen]

     i. Click **Enable administrative security**.
     
     ii. Type a **User name** for the new administrator account that will be created.
     
     iii. Type a **Password** for the administrator account.
     
     iv. Type the password again in the **Confirm** password field.
     
     v. Click **Next** and proceed to the next substep.

   - If you do not want to enable security, leave the fields on this screen blank, and just click **Next**.

g. On the "Profile Creation Summary" screen, note down the **Profile Location** (you will use it in the next task) and then click **Create**.

   ![Profile Creation Summary Screen]

   - **Profile Location:** C:\Program Files\IBM\WebSphere\AppServer\profiles\AdminAgent01
   
   - **Disk space required:** 30 MB
   
   - **Profile name:** AdminAgent01
   
   - **Cell name:** dclvm669AACC01
   
   - **Node name:** dclvm669AANode01
   
   - **Host name:** dclvm669.mdr.1l4.ibm.com
   
   - **Deploy the administrative console (recommended):** True
   
   - **Enable administrative security (recommended):** True
h. On the "Profile Creation Complete" screen, de-select **Launch the First steps console**, and then click **Finish**.

Leave the Profile Management Tool open for the next step.

4. Now use the Profile Management Tool to create the secure proxy (configuration-only) profile:
   a. On the "Profiles" screen, click the **Create** button.

   b. On the "Environment Selection" screen, click **Secure proxy (configuration-only)**, and then click **Next**.

Although this profile is only used for configuring the DMZ Secure Proxy Server, you will register it with the Network Deployment administration agent on the same server; the agent will run and manage the profile.
c. On the "Profile Create Options" screen, click **Advanced profile creation**, and then click **Next**.

d. On the "Profile Name and Location" screen, type the **Profile Name** of the DMZ Secure Proxy Server, and then click **Next**.

You noted this name down in step 3.m. of the "Configuring the DMZ Secure Proxy Server profile" task.

e. On the "Node and Host Names" screen, type the **Node Name** and **Host Name** of the DMZ Secure Proxy Server, and then click **Next**.

You also noted these names in step 3.m. of the "Configuring the DMZ Secure Proxy Server profile" task.
f. On the "Security Level Selection" screen, look under "Proxy security level" and click **Low**.

![Security Level Selection](image)

- **High**: Represents the highest level of proxy server security based on certain proxy server settings. By default, static routing is enabled, the process will run as an unprivileged user id, and local error page handling is enabled.
- **Medium**: Represents the mid-level of proxy server security based on certain proxy server settings. By default, dynamic routing is enabled, the process will run as an unprivileged user id, and local error page handling is enabled.
- **Low**: Represents the lowest level of proxy server security based on certain proxy server settings. By default, dynamic routing is enabled, the process will run as an unprivileged user id, and remote error page handling is enabled.

g. On the same screen, look under "Supported protocols" and do the following:
   
   i. De-select **Web**.
   
   ii. Select **SIP**.
   
   iii. Click **Next**.
h. On the "Administrative Security" screen, choose whether to enable security:

**Note:** If you enabled security for the administrative agent in step 3, then you must enable it for the secure proxy profile as well.

- If you want to enable security, do the following:
  
  i. Click **Enable administrative security**.
  
  ii. Type a **User name** for the new administrator account that will be created.
  
  iii. Type a **Password** for the administrator account.
  
  iv. Type the password again in the **Confirm** password field.
  
  v. Click **Next** and proceed to the next substep.

- If you do not want to enable security, leave the fields on this screen blank, and just click **Next**.

  i. On the "Security Certificate (Part 1)" screen, accept the defaults and click **Next**.
j. On the "Security Certificate (Part 2)" screen, accept the defaults and click **Next**.

![Security Certificate (Part 2) Screen]

k. On the "Port Values Assignment" screen, click the **Default Port Values** button to set the same ports as used by the DMZ Secure Proxy Server, and then click **Next**.

![Port Values Assignment Screen]
l. On the "Profile Creation Summary" screen, verify that the following values match those used for the DMZ Secure Proxy Server, and then click **Create**:
   - **Profile name**
   - **Node name**
   - **Server name**

m. On the "Profile Creation Complete" screen, de-select **Launch the First steps console**, and then click **Finish**.

n. On the "Profile Management Tool" screen, click **File > Exit**.
Registering the secure proxy (configuration-only) profile with the administrative agent

Register the new secure proxy (configuration-only) profile with the administrative agent so that the profile can be managed as part of the Network Deployment application server that resides on the same computer.

Note: If you installed multiple DMZ Secure Proxy Servers, complete this task on each server.

1. Navigate to the following directory: AdminAgent_profile_directory/bin
   
   where AdminAgent_profile_directory is the Profile Location that was assigned to the administrative agent when you created it in the previous task (you noted down the name in step 3.g of the "Creating the administrative agent and the secure proxy profile").

   For example, on Windows 2003 this is:
   
   C:\Program Files\IBM\WebSphere\AppServer1\profiles\AdminAgent01\bin

2. Start the administrative agent with the following command:
   
   AIX, Linux, Solaris
   ./startServer.sh adminagent
   
   Windows
   
   startServer.bat adminagent

3. After the administrative agent has started, register the secure proxy (configuration-only) profile with the agent by running the following command with the parameters shown:

   Note: Line breaks appear for readability -- you must type the entire command on a single line.
   
   AIX, Linux, Solaris
   ./registerNode.sh
   -conntype SOAP
   -port SOAP_port
   -profilePath Secure_proxy_config_profile_directory
   -username AdminAgent_user
   -password AdminAgent_password
   -nodeusrename Secure_proxy_config_profile_user
   -nodepassword Secure_proxy_config_profile_password
Windows

registerNode.bat
-conntype SOAP
-port SOAP_port
-profilePath Secure_proxy_config_profile_directory
-username AdminAgent_user
-password AdminAgent_password
-nodeusername Secure_proxy_config_profile_user
-nodepassword Secure_proxy_config_profile_password

where:

• **SOAP_port** is the SOAP port value listed in the AboutThisProfile.txt file located at AdminAgent_profile_directory/logs (the default SOAP port is 8877).

• **Secure_proxy_config_profile_directory** is the directory where the secure proxy (configuration-only) profile is stored (the Profile Location value in step 3.g of "Creating the administrative agent and the secure proxy profile").

• **AdminAgent_user** is the user name that you provided when you chose to enable administrative security for the administrative agent in step 3.f of "Creating the administrative agent and the secure proxy profile"). If you did not enable security, you can skip this parameter.

• **AdminAgent_password** is the password that you provided when you chose to enable administrative security for the administrative agent in step 3.f of "Creating the administrative agent and the secure proxy profile"). If you did not enable security, you can skip this parameter.

• **Secure_proxy_config_profile_user** is the user name that you provided when you chose to enable administrative security for the secure proxy (configuration-only) profile in step 4.h of "Creating the administrative agent and the secure proxy profile"). If you did not enable security, you can skip this parameter.

• **Secure_proxy_config_profile_password** is the password that you provided when you chose to enable administrative security for the secure proxy (configuration-only) profile in step 4.h of "Creating the administrative agent and the secure proxy profile"). If you did not enable security, you can skip this parameter.

**Example**

registerNode.bat -conntype SOAP -port 8877 -profilePath "C:\Program Files\IBM\WebSphere\AppServer1\profiles\SecureProxySrv01" -username stgwadmin
-password stgwadmin -nodeusername stgwadmin -nodepassword stgwadmin
After the secure proxy (configuration-only) profile has been registered, you can update it using the Integrated Solutions Console at:

```
http://AdminAgent_host_name:Administrative_port/ibm/console
```

Note: The Administrative_port defaults to 9060; you can look up your port setting in the AboutThisProfile.txt file located at ND_AdminAgent_profile_directory/logs.
Setting up a tunnel connection between Sametime Gateway and the DMZ Secure Proxy Server

To enable the Sametime Gateway servers and the DMZ Secure Proxy Servers to communicate across the firewall, you must configure a tunnel connection consisting of a core group bridge with peer access points on each end. To do this, you will configure tunnel peer access points on the Sametime Gateway cell to accept connections from processes in the DMZ Secure Proxy Server cell, plus a core group bridge that allows the cell processes to connect via the tunnel peer access points. Once the tunnel connection is defined, you will save the settings in a template and export it for use in the DMZ Secure Proxy Server cells. Then you will create some custom properties that enable the Sametime Gateway cell to support the new tunnel connection.

If you deploy multiple DMZ Secure Proxy Servers, each will operate as a separate cell so you will need to create the tunnel connection between every DMZ Secure Proxy Server and the Sametime Gateway cell.

Creating tunnel access points on the Sametime Gateway cell

Set up the tunnel access points and the core group bridge on the Sametime Gateway cell so you can export the settings to the DMZ Secure Proxy Server cell later.

Creating the tunnel peer access points

Working on the Sametime Gateway cell's Deployment Manager, create one tunnel peer access point for each of the DMZ Secure Proxy Server cells that will connect to the Sametime Gateway server or cluster.

1. Log in to the Integrated Solutions Console on the Sametime Gateway cell's Deployment Manager.
2. In the navigation tree, click **Servers > Core Groups > Core group bridge settings**.
3. On the Configuration page, look under "Additional Properties", and click **Tunnel peer access points**.
4. Create a tunnel peer access point for each DMZ Secure Proxy Server:
   a. In the tunnel peer access points table, click **New**.

```
Core group bridge settings > Tunnel peer access points
Use this page to view the tunnel peer access points that are defined on your system. Each tunnel peer access point can be used to establish communication with a core group in another cell. Each tunnel peer access point corresponds to a core group access point in that other cell. You can also use this page to create a new tunnel peer access point, or delete an existing tunnel peer access point.

Preferences

<table>
<thead>
<tr>
<th>New</th>
<th>Delete</th>
</tr>
</thead>
</table>

Select: Name

None

Total 0
```
b. On the Configuration page, look under "General Properties" and in the Name field, type a unique, descriptive name for the access point.

c. In the Cell field, type the case-sensitive name of the DMZ Secure Proxy Server cell.

   Note: Each DMZ Secure Proxy Server deploys as a cell. If you don't know the name of the cell, you can locate its subdirectory on the computer hosting the DMZ Secure Proxy Server cell's Deployment Manager; look for it within the following directory:

   \WAS_HOME\profiles\DMZ_Secure_Proxy_Profile_name\config\cells

   For example, in Windows, the cell's directory is located in this path:

   c:\Program Files\IBM\WebSphere\AppServer\profiles\SecureProxySvr01\config\cells

d. Accept the default values for the remaining settings for this new tunnel access point, and click OK.

e. Click the Save link in the "Messages" box at the top of the page to save the changes to the master configuration.

4. Repeat step 4 until you have created and saved a tunnel peer access point for every DMZ Secure Proxy Server.
Creating a tunnel template

Create a tunnel template that will contain information about how the DMZ Secure Proxy Server can access the Sametime Gateway cell through tunnel peer access points.

1. In the navigation tree, click **Servers > Core Groups > Core group bridge settings**.
2. On the Configuration page, look under "Additional Properties", and click **Tunnel templates**.
3. In the tunnel templates table, click **New**.

4. Create a tunnel template for use by the DMZ Secure Proxy Servers:
   a. On the Configuration page, look under "General Properties" and in the **Name** field, type a unique, descriptive name for the template.

b. Click **OK**.
   The new tunnel template now appears in the table.
5. Click the **Save** link in the "Messages" box at the top of the page.

---

**Creating a tunnel access point group**

Modify the tunnel template to associate peer access points between Sametime Gateway cell and the DMZ Secure Proxy Server. To do this, you will create a tunnel access point group to collect the individual tunnel peer access points that you created for the DMZ Secure Proxy Servers, and associate that group with the Sametime Gateway cell's default core group (of access points).

1. In the navigation tree, click **Servers > Core Groups > Core group bridge settings**.
2. On the Configuration page, look under "Additional Properties", and click **Tunnel templates**.
3. In the tunnel templates table, click the name of the tunnel template that you created in the previous task.
4. On the template's Configuration page, click the **Create New Tunnel Access Point Group** button.

![Configuration page](image)

5. Define the tunnel access point group by completing the dialog boxes that follow:
   a. Step 1: Type a name for the new tunnel access point group, and then click **Next**.

   ![Step 1 dialog](image)

   b. Step 2: Add the Sametime Gateway cell's default core group to the new tunnel access point group by selecting `CGAP_1\DefaultCoreGroup`, clicking the ![add button](image) to add it to the group; then click **Next**.

   ![Step 2 dialog](image)
c. Step 3: Add the tunnel peer access points to the group by selecting each tunnel peer access point and clicking the button to add it to the group; then click Next.

In this example, the tunnel peer access point for the myDualDMZ1 server have been added to the group, and now the tunnel peer access point for the myDualDMZ2 server will be added.

d. Step 4: Review the summary and click the Finish button.

6. Click the Save link in the "Messages" box at the top of the page.
Creating a bridge interface for the Sametime Gateway cell

The bridge interface manages connections between the local cell processes and the remote processes that connect to the cell through the core bridge. For the Sametime Gateway cell, configure the Deployment Manager to provide the bridge interface so that the DMZ Secure Proxy Server cells can connect through the core bridge.

1. In the navigation tree, click **Servers > Core Groups > Core group bridge settings**.
2. On the Configuration page, look under "Additional Properties" and click **Access point groups**.
3. In the access point groups table, click the **DefaultAccessPointGroup** link.

4. On the Configuration page, look under "Access points" and click **Core group access points**.
5. Select **CGAP_1\DefaultCoreGroup** (make sure it is highlighted), and then click **Show Detail**.

6. On the Configuration page, look under "Additional Properties" and click **Bridge interfaces**.
7. In the bridge interfaces table, click **New** and define the bridge interface:
a. On the Configuration page, select the Sametime Gateway cell's Deployment Manager from the list of Bridge interfaces.

b. Click OK.

8. Click the Save link in the "Messages" box at the top of the page.

Exporting the Sametime Gateway cell's tunnel template

Now that the complete tunnel connection has been configured for the Sametime Gateway cell, you can export those settings and later import them to the DMZ Secure Proxy Server cells.

The properties file for the exported tunnel template is saved in the \$\{USER_INSTALL_ROOT\} directory that applies to the management profile for the DMZ Secure Proxy Server (hosted on the Sametime Gateway cell's Deployment Manager to support the core bridge functionality).

1. Associate the tunnel access point group with the tunnel template:
   a. In the navigation tree, click Servers > Core Groups > Core group bridge settings > Tunnel templates.
b. In the tunnel templates table, click the name of the tunnel template.

![Image of tunnel templates table]

- **Core group bridge settings** > **Tunnel templates**
  - Use this page to define and export tunnel templates. A tunnel template represents the Core Group Bridge tunnel settings that can be exported for use in a foreign cell.

<table>
<thead>
<tr>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>New...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Use SSL</th>
<th>Tunnel Access Point Group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MyTunnel</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>

- **Total 1**

c. In the **Tunnel Access Point Group** list, click the appropriate group and make sure the selected name displays in the field (the selected group will be associated with the current template).

![Image of Tunnel Access Point Group]

- **Core group bridge settings** > **Tunnel templates** > **MyTunnel**
  - Use this page to define and export tunnel templates. A tunnel template represents the Core Group Bridge tunnel settings that can be exported for use in a foreign cell.

![Configuration section]

- **General Properties**
  - **Name**: MyTunnel
  - **Use SSL**: 
  - **Tunnel Access Point Group**: MyTunnelAP

![Create New Tunnel Access Point Group button]

- **Apply | OK | Reset | Cancel**

d. Click **OK**.

e. Click the **Save** link in the "Messages" box at the top of the page.

![Messages]

- **Messages**
  - **Changes have been made to your local configuration. You can:**
    - **Save** directly to the master configuration.
    - **Review** changes before saving or discarding.
  - An option to synchronize the configuration across multiple nodes can be disabled in **Preferences**.
  - **The server may need to be restarted for these changes to take effect.**
2. Export the tunnel template:
   a. Back on the tunnel templates table, verify that the tunnel access point group now displays in the tunnel template's row in the table (if not, repeat step 1 to associate the group with the template).

   ![Tunnel templates table with MyTunnel template and MyTunnelAP group]

   b. In the table, click the box next to the tunnel template's name.

   ![Tunnel templates table with the MyTunnel template selected]

   c. Click **Export**.

   When the export is complete, a notice appears in the "Messages" box at the top of the page:

   ![Messages box with export notice]

   d. Verify that the tunnel template properties file is now stored in the following directory:

   \[\text{WAS\_Home/Dmgr\_Profile/tunnel\_template\_name.props}\]

3. Copy the exported properties file to a temporary location on the DMZ Secure Proxy Server so you can import it later.

   **Attention:** If you installed multiple DMZ Secure Proxy Servers, copy the file to every server.
Creating custom properties for the Sametime Gateway cell

Enable the Sametime Gateway cell to support the tunnel connection by creating two custom properties for the SIP container on every Sametime Gateway server in the cell:

- **ignore.ucf.messages.from.proxy** - Required. This property instructs the SIP container to ignore UCF routing messages. This property must be set to true for the tunnel connection to work.
- **disable.failover.suicide** - Optional. This property determines whether the SIP container will shut itself down ("suicide") when the it detects that all connections with the DMZ Secure Proxy Servers are unavailable. The default setting is false, meaning the SIP container will shut itself down when it detects no available connections. Setting this value to true prevents the SIP container from shutting itself down when connections are unavailable.

1. In the navigation tree, click **Servers > Server types > WebSphere application servers**.
2. In the application servers table, click the name of the server hosting the Sametime Gateway cell's Deployment Manager.
3. On the Configuration page, look under "Container Settings" and click **SIP Container Settings > SIP container**.
4. Look under "Additional Properties" and click **Custom properties**.

![Application servers > RTCGWServer > SIP container > Custom properties](image)

Use this page to specify an arbitrary name and value pair. The value that is specified for the name and value pair is a string that can set internal system configuration properties.

5. Add the first custom property:
   a. In the custom properties table, click **New**.
   b. Type **ignore.ucf.messages.from.proxy** in the **Name** field.
   c. Type **true** in the **Value** field.
   d. Click **OK**.
6. Add the second custom property:
   a. In the custom properties table, click **New**.
   b. Type **disable.failover.suicide** in the **Name** field.
   c. Type **true** in the **Value** field.
   d. Click **OK**.
7. Click the **Save** link in the "Messages" box at the top of the page.

8. Synchronize and restart nodes in the Sametime Gateway cluster as follows:
   a. In the navigation tree, click **System Administration > Nodes**.
   b. Select all nodes in the cluster, and then click the **Full Resynchronize** button at the top of the table.
   c. Back in the navigation tree, click **System Administration > Node Agents**.
   d. Select all nodes in the cluster, and then click the **Restart** button at the top of the table.
Importing the Sametime Gateway cell's tunnel template to a DMZ Secure Proxy Server

Now that the tunnel access points have been configured on the Sametime Gateway cluster, you will configure a corresponding set of access points on each DMZ Secure Proxy Server. You do this by importing the tunnel template file that you exported from the Sametime Gateway cell earlier.

When you created the tunnel template for the Sametime Gateway cell, you exported a copy of the template. Now you will import the tunnel template for use with the DMZ Secure Proxy Server and the Network Deployment secure proxy (configuration-only) profile to enable the DMZ Secure Proxy Server cell to communicate with the Sametime Gateway cell.

**Note:** If you install multiple DMZ Secure Proxy Server/WebSphere Network Deployment servers, complete this task on each server.

1. On the computer hosting the DMZ Secure Proxy Server, navigate to the following directory:

   Secure_proxy_config_profile_directory/bin

   Where `Secure_proxy_config_profile_directory` is the directory where the secure proxy (configuration-only) profile is stored (the **Profile Location** value in step 3.g of "Creating the administrative agent and the secure proxy profile").

2. Run the following command to open the wsadmin scripting tool:

   **AIX, Linux, Solaris**

   ```bash
   wsadmin.sh -conntype NONE -username Secure_proxy_config_profile_user -password Secure_proxy_config_profile_password -lang jython
   ```

   **Windows**

   ```batch
   wsadmin.bat -conntype NONE -username Secure_proxy_config_profile_user -password Secure_proxy_config_profile_password -lang jython
   ```

   **Example**

   ```batch
   wsadmin.bat -connType NONE -username stgwadmin -password stgwadmin -lang jython
   ```

3. Import the tunnel template by running the following command:

   **Note:** Line breaks were inserted for readability; you must enter this command on a single line.

   ```batch
   AdminTask.importTunnelTemplate(["-inputFileName', 'Path_and_Name_of_tunnel.props',
   '-bridgeInterfaceNodeName', 'Secure_proxy_config_profile_node_name',
   '-bridgeInterfaceServerName', 'Secure_proxy_config_profile_server_name'])
   ```

   where:

   - **Path_and_Name_of_tunnel.props** is the complete path and file name of the Network Deployment's secure proxy (configuration-only) profile's tunnel properties file. You exported this file from Sametime Gateway and then copied to the DMZ Secure Proxy Server in the "Exporting the Sametime Gateway cell's tunnel template" task.

IBM Sametime Gateway 8.5.2 IFR1  Deploying DMZ Secure Proxy Server  63
• Secure_proxy_config_profile_node_name is the value of the Node Name field for the Network Deployment's secure proxy (configuration-only) profile (see step 4.1 in "Creating the administrative agent and the secure proxy profile").

• Secure_proxy_config_profile_server_name is the value of the Server Name field for the Network Deployment's secure proxy (configuration-only) profile (see step 4.1 in "Creating the administrative agent and the secure proxy profile").

**Example**

```bash
code
wsadmin> AdminTask.importTunnelTemplate([  
'-inputFileName', 'c:/MyTunnel.props',  
'-bridgeInterfaceNodeName', 'esx5dualdmz1Node01',  
'-bridgeInterfaceServerName', 'proxy1']
```

4. Run the following command to save the imported tunnel template to the master configuration:

```bash
code
wsadmin> AdminConfig.save()
```

5. Run the following command to exit the wsadmin scripting tool:

```bash
code
wsadmin> quit
```
Configuring a DMZ Secure Proxy Server

Use the Integrated Solutions Console to configure settings for the DMZ Secure Proxy Server. You will configure settings in several different areas as explained in this section:

- Custom properties
- Ports
- Transport settings
- JVM settings

Note: If you install multiple DMZ Secure Proxy Servers, complete this task on each server, making sure to configure any additional settings that are required when multiple servers are in use (indicated in the steps).

Configuring SIP proxy settings

Configure the DMZ Secure Proxy Server to route traffic to the Sametime Gateway cluster.

1. Log in to the server you will configure:
   a. Open the Integrated Solutions Console for the DMZ Secure Proxy Server cell:
      http://AdminAgent_host_name:Administrative_port/ibm/console
      Note: The Administrative_port defaults to 9060; you can look up your port setting in the AboutThisProfile.txt file located at ND_AdminAgent_profile_directory/logs
   b. Select the server you want to configure, and then click the Continue button.
   c. Log in as the WebSphere administrator.

2. In the navigator, click Servers > Server Types > WebSphere proxy servers.

3. In the proxy servers table, click the name of the server that you want to configure.

4. On the Configuration page, look under "Proxy Settings", click SIP Proxy Server Settings, and then click SIP proxy settings.

5. On the Configuration page, locate the Default cluster field under "General properties" and type the name of the Sametime Gateway cluster where you want the DMZ Secure Proxy Server to route traffic.
Note: You can look up the Sametime Gateway cluster's name as follows:

i. On the Sametime Gateway cluster's Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.

ii. In the navigation tree, click Servers > Clusters > WebSphere application server clusters.

iii. Look for the cluster's name in the clusters table.

6. Click OK.

7. Save this change to the master configuration by clicking the Save link in the "Messages" box at the top of the page.

Configuring custom properties for the DMZ Secure Proxy Server

Create a set of custom properties for the DMZ Secure Proxy Server.

If you installed multiple DMZ Secure Proxy Servers, you will need to create an additional set of custom properties (explained in step 7, below) on each server to enable them to work with a load balancer. Create the complete set of properties on each DMZ Secure Proxy Server.

1. Log in to the server you will configure:
   a. Open the Integrated Solutions Console for the DMZ Secure Proxy Server cell:
      
      http://AdminAgent_host_name:Administrative_port.ibm/console

      Note: The Administrative_port defaults to 9060; you can look up your port setting in the
      AboutThisProfile.txt file located at AdminAgent_profile_directory/logs

   b. Select the server you want to configure, and then click the Continue button.

   c. Log in as the WebSphere administrator.

2. In the navigator, click Servers > Server Types > WebSphere proxy servers.

3. In the proxy servers table, click the name of the server that you want to configure.

4. On the Configuration page, look under "Proxy Settings", click SIP Proxy Server Settings, and then click SIP proxy settings.

   This displays the same SIP proxy settings page as in the previous task.
5. Look under "Additional Properties" and click **Custom Properties**.

**WebSphere proxy servers** > **proxy1** > **Custom properties**

Use this page to specify an arbitrary name and value pair. The value that is specified for the name and value pair is a string that can set internal system configuration properties.

<table>
<thead>
<tr>
<th>Preferences</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>

You can administer the following resources:

None

- Total 0
6. Create the custom properties as follows:
   a. In the custom properties table, click **New**.
   b. Type a **Name** and a **Value** for the new custom property.
   c. Click **OK**.
   d. Repeat for each additional custom property.

   **Tip:** Print this page so you can mark each custom property as you create it.

   **Custom properties to create:**

<table>
<thead>
<tr>
<th>✓</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sipClusterCellName</td>
<td>Cell_Name_of_Sametime_Gateway_cluster</td>
</tr>
<tr>
<td></td>
<td>UDPMultiThreadingEnabled</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td>burstResetFactor</td>
<td>120</td>
</tr>
<tr>
<td></td>
<td>clusterRouteConfigUpdateDelay</td>
<td>60000</td>
</tr>
<tr>
<td></td>
<td>isSipComplianceEnabled</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>keepAliveFailures</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>keepAliveInterval</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>localOutboundTCPAddress</td>
<td>Host_name_of_current_DMZ_Secure_Proxy_Server</td>
</tr>
<tr>
<td></td>
<td>localOutboundTCPPort</td>
<td>1080</td>
</tr>
<tr>
<td></td>
<td>maxDeflatorRatio</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>maxThroughputFactor</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>minDeflatorRatio</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>perSecondBurstFactor</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>proxyTransitionPeriod</td>
<td>360</td>
</tr>
<tr>
<td></td>
<td>receiveBufferSizeSocket</td>
<td>3000000</td>
</tr>
<tr>
<td></td>
<td>sendBufferSizeSocket</td>
<td>3000000</td>
</tr>
</tbody>
</table>

If you installed only one DMZ Secure Proxy Server, skip to step 8 after you have created the custom properties.
7. **Multiple DMZ Secure Proxy Servers only:** If you installed multiple DMZ Secure Proxy Servers, you must deploy a load balancer to distribute connections among the different servers and create an additional set of custom properties for use with the load balancer, as follows:
   a. In the custom properties table, click **New**.
   b. Type a **Name** and a **Value** for the new custom property.
   c. Click **OK**.
   d. Repeat for each additional custom property.

   **Tip:** Print this page and the next page, so you can mark each custom property as you create it.

### Custom properties for use with a load balancer:

<table>
<thead>
<tr>
<th>✔</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LBIPAddr</td>
<td>IP_address_of_load_balancer</td>
</tr>
<tr>
<td></td>
<td>SIPAdvisorMethodName</td>
<td>OPTIONS</td>
</tr>
<tr>
<td></td>
<td>defaultTCPChainName</td>
<td>SIP_TCP_LB_CHAIN</td>
</tr>
<tr>
<td></td>
<td>defaultUDPChainName</td>
<td>SIP_LB_CHAIN</td>
</tr>
<tr>
<td></td>
<td>defaultTLSChainName</td>
<td>SIPS_LB_CHAIN</td>
</tr>
</tbody>
</table>

### Custom properties for use with an IP sprayer and a load balancer

The following properties are required for getting the correct content in the contact header for outgoing SIP messages in an environment using multiple DMZ Secure Proxy Servers with a load balancer:

<table>
<thead>
<tr>
<th>✔</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tls.IPSprayer.host</td>
<td>Load_balancer_cluster_host_name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The virtual host name of the load balancer that you will deploy in front of the DMZ Secure Proxy Servers. The load balancer uses this name as the &quot;cluster name&quot; to define a publicly available host name for external clients to access and this property must use that same value. <strong>Important:</strong> You must provide the same virtual host name when you configure the load balancer later; write the name down now so you will remember to use it.</td>
</tr>
<tr>
<td></td>
<td>tls.IPSprayer.port</td>
<td>TLS_port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The port used by the TLS encrypted connections; for example: 5061</td>
</tr>
<tr>
<td></td>
<td>tcp.IPSprayer.host</td>
<td>Load_balancer_cluster_host_name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The virtual host name of the load balancer that you will deploy in front of the DMZ Secure Proxy Servers. <strong>Note:</strong> This is the same virtual host name that you provided for the TCP IP Sprayer property, above.</td>
</tr>
<tr>
<td></td>
<td>tcp.IPSprayer.port</td>
<td>TCP_port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The port used by the TCP non-secure connections; for example: 5060</td>
</tr>
</tbody>
</table>
(Optional) UDP IP sprayer properties

Use these settings if you want to define an IP sprayer for UDP connections as well.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp.IPSprayer.host</td>
<td>Load_balancer_cluster_host_name</td>
</tr>
<tr>
<td></td>
<td>The virtual host name of the load balancer that you will deploy in</td>
</tr>
<tr>
<td></td>
<td>front of the DMZ Secure Proxy Servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is the same virtual host name that you provided for</td>
</tr>
<tr>
<td></td>
<td>the TCP and TLS IP Sprayer properties, above.</td>
</tr>
<tr>
<td>udp.IPSprayer.port</td>
<td>UDP_port</td>
</tr>
<tr>
<td></td>
<td>The port used by the UDP non-secure connections; for example: 5060</td>
</tr>
</tbody>
</table>

8. Click the **Save** link in the "Messages" box at the top of the page to save all of the new custom properties to the master configuration.
Configuring ports on the DMZ Secure Proxy Server

Configure the SIP ports on the DMZ Secure Proxy Server.

If you installed multiple DMZ Secure Proxy Servers, you will need to configure additional ports (explained in step 7 below) for use with a load balancer so it can distribute connections among the individual servers. Configure the complete set of ports for every DMZ Secure Proxy Server.

1. Log in to the server you will configure:
   a. Open the Integrated Solutions Console for the DMZ Secure Proxy Server cell:
      
      http://AdminAgent_host_name:Administrative_port/ibm/console

      Note: The Administrative_port defaults to 9060; you can look up your port setting in the AboutThisProfile.txt file located at AdminAgent_profile_directory/logs
   b. Select the server you want to configure, and then click the Continue button.
   c. Log in as the WebSphere administrator.

2. In the navigator, click Servers > Server Types > WebSphere proxy servers.

3. In the proxy servers table, click the name of the server that you want to configure.

4. On the Configuration page, look under "Communications" and click Ports.

   WebSphere proxy servers > proxy1 > Ports

   Specifies the TCP/IP ports this server uses for connections.

   Preferences

   ![Ports Table]

   You can administer the following resources:

<table>
<thead>
<tr>
<th>Select</th>
<th>Port Name</th>
<th>Host</th>
<th>Port</th>
<th>Transport Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPC.CONNECTOR_ADDRESS</td>
<td>localhost</td>
<td>9633</td>
<td>No associated transports</td>
</tr>
<tr>
<td></td>
<td>PROXY_SIPS_ADDRESS</td>
<td>*</td>
<td>5061</td>
<td>View associated transports</td>
</tr>
<tr>
<td></td>
<td>PROXY_SIP_ADDRESS</td>
<td>*</td>
<td>5060</td>
<td>View associated transports</td>
</tr>
</tbody>
</table>

   Total 3

5. In the Ports table, change the PROXY_SIPS_ADDRESS port as follows:
   a. Click on PROXY_SIPS_ADDRESS.
   b. Change the * value to the host name of the current DMZ Secure Proxy Server.
   c. Click OK.
6. Now change the **PROXY_SIP_ADDRESS** port:
   a. Click on **PROXY_SIP_ADDRESS**.
   b. Change the * value to the host name of the current DMZ Secure Proxy Server.
   c. Click **OK**.

7. **Multiple DMZ Secure Proxy Servers only**: If you installed multiple DMZ Secure Proxy Servers, you must define two additional ports for use with a load balancer as follows:
   a. In the ports table, click **New**.
   b. Select **User-defined Port**, and then type a **Port name**, a **Host** address, and a **Port** value.
   c. Click **OK**.
   d. Repeat for each additional port.

    | Port settings |
    |---------------|
    | **Port name** | **Host**                  | **Port** |
    | User-defined  | SIP_LB_ADDRESS            | Load_balancer_cluster_IP The physical IP address of the computer hosting the load balancer. | 5060 |
    | User-defined  | SIPS_LB_ADDRESS           | Load_balancer_cluster_IP The physical IP address of the computer hosting the load balancer. | 5061 |

If you installed only one DMZ Secure Proxy Server, skip to step 8.
8. Click the **Save** link in the "Messages" box at the top of the page to save all of the port settings to the master configuration.
Configuring transport settings on the DMZ Secure Proxy Server

Modify the transport chain and remove the UDP transport option to prevent it from being used on the DMZ Secure Proxy Server.

If you installed multiple DMZ Secure Proxy Servers, you will need to configure additional transport chains (explained in step 6, below) for use with a load balancer. Configure the complete set of transport chains on every DMZ Secure Proxy Server.

1. Log in to the server you will configure:
   a. Open the Integrated Solutions Console for the DMZ Secure Proxy Server cell:
      
      \[\text{http://AdminAgent\_host\_name:Administrative\_port/ibm/console}\]
      
      \textbf{Note:} The \textit{Administrative\_port} defaults to 9060; you can look up your port setting in the \textit{AboutThisProfile.txt} file located at \textit{AdminAgent\_profile\_directory/logs}.

   b. Select the server you want to configure, and then click the \textbf{Continue} button.

   c. Log in as the WebSphere administrator.

2. In the navigator, click \textbf{Servers > Server Types > WebSphere proxy servers}.

3. In the proxy servers table, click the name of the server that you want to configure.

4. On the Configuration page, look under "Proxy Settings", expand \textbf{SIP Proxy Server Settings}, and then click \textbf{SIP proxy server transports}.

   \textit{WebSphere proxy servers > proxy1 > Transport Chain}

   Use this page to view and manage a transport chain. Transport chains represent network protocol stacks that are operating within a client or server.

   \textbf{UDP SIP PROXY CHAIN}

   \begin{tabular}{|c|c|c|c|c|}
   \hline
   Select & Name & Enabled & Host & Port & SSL Enabled \\
   \hline
   & SIPS\_PROXY\_CHAIN & Enabled & myDualDM1.example.com & 5061 & Enabled \\
   & SIP\_PROXY\_CHAIN & Enabled & myDualDM1.example.com & 5060 & Disabled \\
   & UDP\_SIP\_PROXY\_CHAIN & Enabled & myDualDM1.example.com & 5060 & Disabled \\
   \hline
   \end{tabular}

   \textbf{Total 3}
5. In the transport chain table, click the box in front of **UDP_SIP_PROXY_CHAIN**, and then click the **Delete** button to remove it.

![Transport Chain Table](image)

If you installed only one DMZ Secure Proxy Server, skip to step 8.

6. **Multiple DMZ Secure Proxy Servers only:** If you installed multiple DMZ Secure Proxy Servers, you must define additional transport chains for use with a load balancer; this requires that you first copy the transport chain template from the administrative agent profile to the secure proxy (configuration-only) profile:

   a. Open a command window on this server (leave the Integrated Solutions Console open so you can return to it).
   
   b. Create a new subdirectory called **chains** below the
      
      `Secure_proxy_config_profile_directory/config/templates/` directory.
   
   c. Copy the files from the `AdminAgent_profile_directory/config/templates/chains/` directory to the new `Secure_proxy_config_profile_directory/config/templates/` directory.
   
   d. Return to the Integrated Solutions Console.
7. **Multiple DMZ Secure Proxy Servers only**: Back in the transport chains table, click **New**, and then fill in the dialog boxes that follow to create three new transport chains, using the following information:

**Additional transport chains for use with a load balancer**:

<table>
<thead>
<tr>
<th>Transport name</th>
<th>Transport chain template</th>
<th>Use existing port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_LB_CHAIN</td>
<td>Proxy-UDP</td>
<td>Select SIP_LB_ADDRESS</td>
</tr>
<tr>
<td>SIP_TCP_LB_CHAIN</td>
<td>Proxy-TCP</td>
<td>Select SIP_LB_ADDRESS</td>
</tr>
<tr>
<td>SIPS_TCP_LB_CHAIN</td>
<td>Proxy-Secure</td>
<td>Select SIPS_LB_ADDRESS</td>
</tr>
</tbody>
</table>

a. Step 1: Type the **Transport name** and select the **Transport chain template**, and then click **Next**.

b. Step 2: Select **Use existing port**, select a **Port** from the list, and then click **Next**.
c. Step 3: Click Finish.

The complete set of transport chains now shows in the table:

<table>
<thead>
<tr>
<th>WebSphere proxy servers &gt; proxy1 &gt; Transport Chain</th>
</tr>
</thead>
</table>

Use this page to view and manage a transport chain. Transport chains represent network protocol stacks that are operating within a client or server.

<table>
<thead>
<tr>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
</tr>
</tbody>
</table>

Select | Name | Enabled | Host | Port | SSL Enabled |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SIPS_PROXY_CHAIN</td>
<td>Enabled</td>
<td>myDualDMZ1.example.com</td>
<td>5061</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>SIP_LB_CHAIN</td>
<td>Enabled</td>
<td>9.148.63.79</td>
<td>5060</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>SIP_PROXY_CHAIN</td>
<td>Enabled</td>
<td>myDualDMZ1.example.com</td>
<td>5060</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>SIP_TCP_LB_CHAIN</td>
<td>Enabled</td>
<td>9.148.63.79</td>
<td>5060</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>SIPS_TCP_LB_CHAIN</td>
<td>Enabled</td>
<td>9.148.63.79</td>
<td>5061</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Total 5
8. Create custom properties for the SIP_LB_CHAIN transport chain as follows:
   a. In the transport chains table, click SIP_LB_CHAIN.

   ![Image of transport chains table]

   b. On the SIP_LB_Chain Configuration page, click UDP inbound channel(UDP_1).

   ![Image of UDP inbound channel configuration]

   c. On the UDP inbound channel(UDP_1) Configuration page, look under "Additional Properties" and click Custom Properties.
d. Create two custom properties as follows, using the information in the table:

**Custom properties for the SIP_LB_CHAIN transport chain:**

<table>
<thead>
<tr>
<th>✓</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>receiveBufferSizeSock</td>
<td>3000000</td>
</tr>
<tr>
<td></td>
<td>sendBufferSizeSock</td>
<td>3000000</td>
</tr>
</tbody>
</table>

i. In the custom properties table, click **New**.

ii. Type the **Name** and **Value** for a new custom property.

iii. Click **OK**.

9. Click the **Save** link in the "Messages" box at the top of the page to save all of the transport chain settings to the master configuration.
Configuring JVM settings for the DMZ Secure Proxy Server

Configure settings to manage the Java Virtual Machine that runs on the DMZ Secure Proxy Server. If you installed multiple DMZ Secure Proxy Servers, configure these settings on every server.

1. Log in to the server you will configure:
   a. Open the Integrated Solutions Console for the DMZ Secure Proxy Server cell:
      http://AdminAgent_host_name:Administrative_port/ibm/console
      Note: The Administrative_port defaults to 9060; you can look up your port setting in the AboutThisProfile.txt file located at AdminAgent_profile_directory/logs
   b. Select the server you want to configure, and then click the Continue button.
   c. Log in as the WebSphere administrator.
2. In the navigator, click Servers > Server Types > WebSphere proxy servers.
3. In the proxy servers table, click the name of the server that you want to configure.
4. Configure the Java Virtual Machine settings as follows:
d. Set the **Initial help size** to 300 MB.

e. Set the **Maximum heap size** to 450 MB.

f. Type the following **Generic JVM arguments**:

   **Note:** the string has been formatted for readability here, but you must type it all on a single line with a space after each argument as shown in the picture above.

   ```
   -Xtrace:none -Xmo120m -Xgcppolicy:gencon -Xtgcc:parallel -Xgc:noAdaptiveTenure,tenureAge=8, stdGlobalCompactToSatisfyAllocate
   -Xdump:heap:events=user,request=exclusive+prepwalk+compact
   -Xloa
   -Xloaminimum0.03
   -Xgc:noAdaptiveTenure,tenureAge=8, stdGlobalCompactToSatisfyAllocate
   -Xdump:heap:events=user,request=exclusive+prepwalk+compact
   -Xloa
   -Xloaminimum0.03
   ```
g. Click **OK**.

h. Click the **Save** link in the "Messages" box at the top of the page to save the JVM settings to the master configuration.

5. Configure the monitoring settings as follows:
   a. Back on the proxy server Configuration page, look under "Server Infrastructure" and click **Java and Process Management > Monitoring policy**.
   b. On the Monitoring Policy Configuration page, set the **Maximum startup attempts** to 2.
   c. Set the **Ping interval** to 30.
   d. Set the **Ping timeout** to 60.
   e. Click **OK**.
   f. Click the **Save** link in the "Messages" box at the top of the page to save the monitoring settings to the master configuration.
6. Create a custom property as follows to prevent a failover operation from timing out when the DMZ Secure Proxy Server is routing client requests to the Sametime Gateway cluster:
   b. In the custom properties table, click New.
   c. Set the Name to IBM_CLUSTER_RUNRULES_TIMER_TIME.
   d. Set the Value to 1000.
   e. Click OK.
   f. Click the Save link in the "Messages" box at the top of the page to save the monitoring settings to the master configuration.
Establishing trust between the DMZ Secure Proxy Server and the Network Deployment cell

Complete the tasks in this section to configure the DMZ Secure Proxy Server to work with the WebSphere Network Deployment cell:

1. Exporting the secure proxy (configuration-only) profile.
2. Importing the secure proxy (configuration-only) profile to the DMZ Secure Proxy Server's profile.
3. Configuring trust association between the DMZ Secure Proxy Server and the Network Deployment Cell.

If you install multiple DMZ Secure Proxy Servers, complete the tasks on each server.

Exporting the secure proxy (config-only) profile

Export the secure proxy (configuration-only) profile as an archive file so you can import it into the DMZ Secure Proxy Server's profile. If you install multiple DMZ Secure Proxy Servers, you will need to export this profile on each server.

Create a jython script and a batch file to run the script; the script will export the profile for you and then you will manually copy the exported profile to another location.

1. Log in to the DMZ Secure Proxy Server as the system administrator (Windows) or as root (AIX, Linux, Solaris).
2. Use an editor to create a file called `export.py` and type the following command into the file:
   ```python
   AdminTask.exportProxyProfile('[-archive c:/Output_File_Name.car]')
   ``
3. Save and close the `export.py` file.
4. Now use the editor to create a file called `export.cmd` and type the following two commands into the file:
   ```cmd
   Windows example of file:
   del /f c:\myCell.car
   “Secure_proxy_config_profile_directory\bin\wsadmin.bat” -connType NONE -username WAS_admin_user -password WAS_admin_password -lang jython -f export.py
   ``
5. Save and close the `export.cmd` file.
6. Run the `export.cmd` file.
7. Copy the exported profile (Output_File_Name.car in the example) to the following directory:
   ```
   DMZ_Secure_Proxy_Server_profile/bin
   ```

Importing the secure proxy (configuration-only) profile

Import the secure proxy (configuration-only) profile's archive file into the DMZ Secure Proxy Server's profile. If you install multiple DMZ Secure Proxy Servers, you will need to import this profile on each server (working with the current server's own archive file).

Create a jython script and a batch file to run the script; the script will import the profile for you.

1. Log in to the DMZ Secure Proxy Server as the system administrator (Windows) or as root (AIX, Linux, Solaris).
2. Use an editor to create a file called `import.py` and type the following two commands into the file:
   ```python
   AdminTask.importProxyProfile ('[-archive c:/Output_File_Name.car]
   AdminConfig.save()
   ```
3. Save and close the `import.py` file.
4. Now use the editor to create a file called `import.cmd` and type the following two commands into the file:
   ```cmd
   Windows example of file:
   call "DMZ_Secure_Proxy_Server_profile\bin\wsadmin.bat" -connType NONE
   -username WAS_admin_user -password WAS_admin_password -lang jython -f import.py
   ```
5. Save and close the `import.cmd` file.
6. Run the `import.cmd` file.
7. Copy the `serverindex.xml` from:
   Secure_proxy_config_profile_directory/config/cells/Cell_name/nodes/Node_name
   to:
   DMZ_Secure_Proxy_Server_profile/config/cells/Cell_name/nodes/Node_name

## Configuring the trust association

Configure a trust association between the DMZ Secure Proxy Server and the WebSphere Network Deployment cell so that the cell's administrative agent can be used to manage the server. If you install multiple DMZ Secure Proxy Servers, you will need to configure the trust association for each server.

Configure the trust association by using the WebSphere `retrieveSigners` command to add the cell's signer to the DMZ Secure Proxy Server's trust store.

1. Log in to the DMZ Secure Proxy Server as the system administrator (Windows) or as root (AIX, Linux, Solaris).
2. Open a command window.
3. Navigate to the following directory: DMZ_Secure_Proxy_Server_profile/bin
4. Run the `retrieveSigners` command as follows:
   ```cmd
   Note: The command is shown here on multiple lines for readability; you must enter the entire command on a single line.
   retrieveSigners -conntype SOAP -port Dmgr_SOAP_port -host Dmgr_host_name
   -username Dmgr_admin_user -password Dmgr_admin_password
   -listRemoteKeyStoreNames -listLocalKeyStoreNames
   ```
   For example:
   ```cmd
   retrieveSigners -conntype SOAP -port 8879 -host esx5dualdmz2.haifa.ibm.com
   -username stgwadmin -password stgwadmin
   -listRemoteKeyStoreNames -listLocalKeyStoreNames
   ```
5. When the `Add signer to the trust store now? (y/n)` prompt appears, click `y`.
6. Copy the new trust.p12 file:
   from: 
   DMZ_Secure_Proxy_Server_profile/etc 
   to: 
   DMZ_Secure_Proxy_Server_profile/config/cells/Cell_name/nodes/Node_name 

7. Stop and restart the DMZ Secure Proxy Server.
   If you have trouble stopping the server, do the following:
   a. Navigate to the following directory: DMZ_Secure_Proxy_Server_profile/bin
   b. Run the following command:
      Note: The command is shown here on multiple lines for readability; you must enter the entire command on a single line.
      retrieveSigners.sh NodeDefaultTrustStore ClientDefaultTrustStore -conntype ipc 
       -host localhost -port proxy_ipc_port
      For example:
      retrieveSigners.bat NodeDefaultTrustStore ClientDefaultTrustStore -conntype ipc 
       -host localhost -port 9633
   c. When the Add signer to the trust store now? (y/n) prompt appears, click y.

**Updating the trust file later**

Each time you modify a DMZ Secure Proxy Server's configuration, you will need to update its trust association as follows:

1. Export the secure proxy (configuration-only) profile as described earlier in this section.
2. Import the secure proxy (configuration-only) profile to the DMZ Secure Proxy Server's profile as described earlier in this section.
3. Copy the updated trust.p12 file
   from: 
   DMZ_Secure_Proxy_Server_profile/etc/
   to:
   DMZ_Secure_Proxy_Server_profile/config/cells/DMZCellName>/nodes/DMZNodeName/

4. Copy the serverindex.xml file
   from:
   secure_proxy_config-only_profile/config/cells/Cell_name/nodes/Node_name/
   to:
   DMZ_Secure_Proxy_Server_profile/config/cells/Cell_name/nodes/Node_name/
   where:
   • DMZ_Secure_Proxy_Server_profile is the directory where you installed the DMZ Secure Proxy Server.
   • Secure_proxy_config_profile_directory is the directory where the secure proxy (configuration-only) profile is stored (the Profile Location value in step 3.g of "Creating the administrative agent and the secure proxy profile").
Setting up IBM Load Balancer 7.0

If you installed two or more DMZ Secure Proxy Servers, you must deploy a load balancer to distribute client connections between them. In this deployment, the load balancer will intercept data requests from Internet-based clients and distribute the requests among the DMZ Secure Proxy Servers. The load balancing is transparent to the clients. For more information, see the "Load balancing multiple content hosts" section of the Availability topic in the WebSphere Application Server Edge Components version 7 information center.

This section explains how to deploy IBM Load Balancer (a WebSphere Edge component) in front of the DMZ Secure Proxy Servers. WebSphere Edge components, including IBM Load Balancer, are included in the Sametime 8.5.2 package.

**Attention:** The Load Balancer server must reside on the same subnet as the DMZ Secure Proxy Servers to ensure it can properly route client connections to those servers.

### Preparing static IP addresses

To work with Load Balancer, each of the DMZ Secure Proxy Servers requires a static physical IP address. In addition, the Load Balancer server requires two static IP addresses:

- **Non-Forwarding Address:** The NFA is the address of the Load Balancer server itself. It is used for logging in and administering the load balancer.

- **Cluster Address:** This is the address by which clients and other servers will access the load-balanced "cluster." It must be DNS-resolvable.

For the purposes of load balancing, a "cluster" is a group of servers that can be identified by a single host name. By defining a cluster address for Load Balancer, you create a single, publicly known address for clients to use when connecting to Sametime Gateway; Load Balancer will intercept the connections and route them to individual DMZ Secure Proxy Servers, which in turn will pass requests to Sametime Gateway.

For example, suppose you deployed two DMZ Secure Proxy Servers, and you want to configure IBM Load Balancer in front of them. Your static IP addresses will look like this:

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Static IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer: loadbal.example.com</td>
<td>Load balancer</td>
<td>Load balancer (NFA): 9.51.251.115</td>
</tr>
<tr>
<td>Cluster: dmz-cluster.acme.com</td>
<td>(Cluster address)</td>
<td>Cluster: 9.51.251.44</td>
</tr>
<tr>
<td>myDualDMZN ode01.example.com</td>
<td>Primary Node</td>
<td>9.51.251.103</td>
</tr>
<tr>
<td></td>
<td>(DMZ Secure Proxy Server)</td>
<td></td>
</tr>
<tr>
<td>myDualDMZN ode02.example.com</td>
<td>Secondary Node</td>
<td>9.51.251.109</td>
</tr>
<tr>
<td></td>
<td>(DMZ Secure Proxy Server)</td>
<td></td>
</tr>
</tbody>
</table>

Configure the static IP addresses before proceeding.

### Preparing the Load Balancer's cluster host name

The cluster host name allows you to map multiple IP addresses to a single computer; this allows a single Load Balancer to front multiple DMZ Secure Proxy Servers. All requests directed to the cluster address will be intercepted by the load balancer, which will then distribute the requests among the DMZ Secure Proxy Servers.

**Attention:** When you created custom properties for the DMZ Secure Proxy Servers, you provided the load balancer's cluster host name in the (IPSprayer properties) so it could be used as the load balancer's cluster name -- you must use that same value now when configuring the virtual host name of the load balancer.
Installing IBM Load Balancer

Download and install IBM Load Balancer in the Web DMZ. Note that the Load Balancer server must reside on the same LAN network as the DMZ Secure Proxy Servers.

**Note:** Additional information on installing and administering IBM Load Balancer is available in the WebSphere Application Server Edge Components version 7 information center.

**Downloading files**

You can download files from CD/DVD or Passport Advantage.

1. Log in to the computer as the system administrator (Microsoft® Windows®) or as root (IBM AIX®, Linux, Solaris).
2. Navigate to a temporary location where you want to store downloaded files.
3. Download the following package, depending on the IP protocol you are using:
   - **IPv4:** IBM Edge Components V7.0 for `operating_system`, Multilingual
   - **IPv6:** IBM Edge Components for IPv6 V7.0 for `operating_system`, Multilingual
4. Extract the package into the temporary location.

**Installing Load Balancer**

Use the launchpad to start the installation wizard.

1. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Log in to the computer as root.
   b. Open the `/etc/selinux/config` file for editing.
   c. Locate the SELINUX setting and change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Navigate to the temporary location where you extracted the Load Balancer V7 package.
3. Start the installation launchpad:
   a. Verify that the computer has a Web browser available or else install one now.
      The launchpad used for installing Load Balancer requires a Web browser on the local machine (you cannot use the launchpad remotely). Supported browsers include **Mozilla Firefox** and **Windows Internet Explorer**.
   b. Start the launchpad by running the following command:
      - **AIX, Linux, Solaris**
        ```
        ./launchpad.sh
        ```
      - **Windows**
        ```
        launchpad.exe
        ```
c. When the launchpad opens, click **IBM Edge Components** in the navigator.

d. On the "Edge Components: Load Balancer and Caching Proxy" page, click one of the following according to the package you downloaded:

IPv4: Launch the installation wizard for Edge Components Load Balancer and Caching Proxy

IPv6: Launch the installation wizard for Edge Components Load Balancer IPv6
4. Use the wizard to install the Load Balancer, following the appropriate set of steps below for your version of Load Balancer:

**Installing Load Balancer for IPv6**

a. On the "Welcome" screen, click **Next**.

![Welcome Screen](image1)

b. On the "Software License Agreement" screen, click **I accept both the IBM and the non-IBM terms** and then click **Next**.

![License Agreement Screen](image2)

c. On the installation location screen, use the **Directory Name** field to indicate where you want to install Load Balancer, and then click **Next**.

![Installation Location Screen](image3)
d. On the localized data screen, select a language, and then click **Next**.

![Image of localized data screen]

e. On the installation type screen, select **Typical**, and then click **Next**.

![Image of installation type screen]

f. On the installation summary screen, verify that the information is correct, and then click **Next**.

![Image of installation summary screen]

If the information is not correct, use the **Back** button to correct it and work through your selections until you are satisfied with the settings.

g. When the installer indicates that installation is complete, click **Next**.

![Image of installation completion message]

---

IBM Sametime Gateway 8.5.2 IFR1  *Deploying DMZ Secure Proxy Server*  91
h. Finally, choose whether to restart the computer now or later, and click **Finish**.

![MessageBoxRestart](image)

i. Back on the launchpad, click **Exit** in the navigator.

![LaunchpadExit](image)

j. When prompted for confirmation, click **OK**.
Installing Load Balancer for IPv4

a. Close other applications to avoid conflicts during installation.

b. On the "Welcome" screen, click Next.

c. On the "Software License Agreement" screen, click Yes.

d. On the "Component Selection" screen, click the Select All button, and then click Next.
e. On the "Installation Selection Summary" screen, verify that the information is correct, and then click Finish.

![Installation Confirmation](image)

If the information is not correct, use the Back button to correct settings as needed, and then work back to this screen.

f. On the "Setup Complete" screen, choose whether to restart the server now and whether to open the ReadMe file, and then click Finish.

**Attention:** You must restart the server before you can configure or use Load Balancer.

![Setup Complete](image)

g. Back on the launchpad, click Exit in the navigator.

![Exit](image)

h. When prompted for confirmation, click OK.
Configuring Load Balancer

Use the Load Balancer's configuration wizard to complete the initial configuration.

1. Start Load Balancer:
   a. (AIX, Linux, Solaris) The installation process does not add the command directories for Load Balancer into the PATH environment variable. If you want to be able to run Load Balancer commands from the system root, add the command directories to the PATH environment variable.
   b. Start Load Balancer by running the following commands:
      - AIX, Linux, Solaris
        dsserver
        lbadmin
      - Windows
        Start > All Programs > IBM WebSphere > Edge Components > Load Balancer > Load Balancer

2. Log in to the Dispatcher component and start the configuration wizard:
   a. In the navigator, right-click on Dispatcher and then click Connect to host.
   b. At the Dispatcher "Login" message, select the local host name (the server where you installed Load Balancer), and then click OK.
   c. Back in the navigator, right-click on the host you selected, and then click Start executor.
d. Right-click on **Dispatcher** and then click **Start Configuration Wizard**.

3. Define the load balancing cluster:
   a. On the configuration wizard's "Welcome" screen, click **Next**.

   ![Dispatcher Configuration Wizard Welcome](image)

   b. On the "What to expect" screen, click **Next**.

   ![Dispatcher Configuration Wizard What to Expect...](image)

   c. On the "What must I do before I begin?" screen, click **Create Configuration**.

   ![Dispatcher Configuration Wizard What Must I Do Before I Begin?](image)
d. On the "Choosing a host to configure" screen, select the Load Balancer server, and then click **Update Configuration & Continue**.

![Choosing a Host to Configure](image)

```
 ds1vm607 mulle.ibm.com on port 10099
```

e. On the "Defining a cluster" screen, type the static IP address that will serve as the cluster address for the Load Balancer, and then click **Update Configuration & Continue**.

![Defining a Cluster](image)

```
10.1.2.80
```

f. On the "Cluster added successfully" screen, click **Next**.
4. Define port 5060 for use by non-secure (TCP) connections:

   a. On the "Adding a Port" screen, select **Enter your own** as the port.
   b. In the port field that appears, type **5060**, and then click **Next**.
   c. On the "Port added successfully" screen, click **Next**.
   d. Now add the host names (or IP addresses) of all DMZ Secure Proxy Servers so that they can be accessed using port 5060:

      i. On the "Adding server" screen, click **Add a server**.
      ii. Type the static IP address of a DMZ Secure Proxy Server, and then click **Next**.
      iii. Repeat until all DMZ Secure Proxy Servers have been added to port 5060.
      iv. Click **Update Configuration & Continue**.
5. Create an Advisor component for Load Balancer:

![Image of the Starting an Advisor screen]

- a. On the "Starting the Advisor" screen, select Yes and type HTTP as the Advisor's name, and then click Update Configuration & Continue.
- b. On the "Advisor started successfully" screen, click Next.

6. On the "Setting Up the Server Machine" screen, select the server's operating system, and then click View Loopback Instructions.

![Image of the Setting Up the Server Machine screen]

- 7. On the "Loopback Instructions" screen, click Next.

You will create a loopback address for each DMZ Secure Proxy Server in the next section.
8. On the "Congratulations" screen, click **Exit** to close the configuration wizard. The Load Balancer cluster, with port 5060 defined, displays in the navigator.

You will create a second port directly in this Load Balancer interface.

9. Add port 5061 to Load Balancer for use by secure (SSL/TLS) connections:
   a. In the navigator, right-click **Cluster: ip_address**, and select **Add Port**.

   ![Diagram of Load Balancer interface showing Cluster and Add Port options]

   b. In the "Add a port" screen, type **5061** in the **Port number** field, and then click **OK**.

   ![Diagram of Add a port screen with Port number set to 5061]
c. Add all of the DMZ Secure Proxy Servers to port 5061:
   i. In the navigator, right-click **Port: 5061** and select **Add Server**.
   ii. In the "Add Server" screen, type the server's static IP address in the **Server name** field, and then click **OK**.
   iii. Repeat substeps i. and ii. until all of the DMZ Secure Proxy Servers have been added to port 5061.

At this point, Load Balancer is configured and you can proceed to configure the cluster IP address on the network adapter.
Configuring the cluster IP address on the network adapter

The cluster's static IP address must be added to the network adapter that browser clients use to gain access to Load Balancer's Dispatcher component. The cluster IP address is configured by the `goidle` batch file, which is executed by the Dispatcher when it starts up in stand-alone mode. This batch file must be present in the following directory on the Load Balancer server:

```
loadbalancer_server_dir/nd/servers/bin
```

A sample file is provided in the `/nd/samples` directory.

1. Copy the `loadbalancer_server_dir/nd/servers/bin/goidle.cmd` sample file to the `loadbalancer_server_dir/nd/servers/bin` directory.

2. Open the file for editing.

3. Edit the script so that it will alias the cluster IP address on the network adapter. For this you will need three pieces of information:
   - Name of the network adapter
     - The name of the first network adapter would normally be `en0` for ethernet.
   - Cluster IP address
   - Net mask

   ```
   set CLUSTER=10.1.1.88
   set INTERFACE=en0
   set NETMASK=255.255.255.0
   ```

4. Save and close the file.
Configuring loopback adapters on the DMZ Secure Proxy Servers

When you deploy Load Balancer in front of two or DMZ Secure Proxy Servers, client requests are directed to the Load Balancer server using its cluster IP address, which it publishes. Each of the DMZ Secure Proxy Servers must have a loopback address using the same IP address, so they can accept unmodified packets from the Load Balancer.

**Note:** For more information, see the topic, Configuring the server machines in the WebSphere Application Server Edge Components version 7 information center's Load Balancer documentation.

For example, use the following instructions for Windows 2003 (the user interface may vary depending on your operating system).

1. Add the Microsoft Loopback Adapter driver:
   a. Click **Start** > **Control Panel** > **Add Hardware**.
   b. On the "Welcome to the Hardware Wizard" screen, click Next.
   c. Click **Yes, I have already connected the hardware**, and then click Next.
   d. In the list of "Installed hardware", select **Add a new hardware device** (at the bottom of the list) and then click Next.
      **Note:** If "Microsoft Loopback Adapter" appears in the list, it is already installed: click Cancel and skip to step 2.
   e. On the "What do you want the wizard to do?" screen, select **Install the hardware that I manually select from a list (Advanced)** and then click Next.
   f. In the "Common hardware types" list, select **Network adapters** and click Next.
   g. On the "Select Network Adapter" screen, do the following:
      i. In the "Manufacturer" list, select Microsoft.
      ii. In the **Network Adapter** list, select **Microsoft Loopback Adapter**.
      iii. Click Next.
   h. On the "The wizard is ready to install your hardware" screen, click Next.
      i. When the installation is complete, click **Finish** to exit the wizard.

2. Configure the loopback adapter:
   a. Click **Start** > **Control Panel** > **Network Connections**.
   b. In the "Network Connections" window, right-click the connection with the Device Name **Microsoft Loopback Adapter** and then click **Properties**.
   c. In the "Properties" dialog box, click **Internet Protocol (TCP/IP)** and then click the **Properties** button.
d. In the "Internet Protocol (TCP/IP) Properties" dialog box:

   ![Internet Protocol (TCP/IP) Properties dialog box]

   i. Click **Use the following IP address** and provide the following values:
      - **IP address**: type the Load Balancer's cluster IP address.
      - **Subnet mask**: type the subnet mask of the Load Balancer server.

   ii. Click **Use the following DNS server addresses** and provide the following value:
      - **Preferred DNS server**: type the localhost IP address.

   iii. Click **OK** to close the "Internet Protocol (TCP/IP) Properties" dialog box.
      Do not enter a default gateway address.

   e. Click **OK** to close the "Properties" dialog box.

3. Configure advanced connection settings:
   a. Back in the "Network Connections" window, click **Advanced > Advanced Settings**.
   b. In the "Advanced Settings" dialog box, verify that the cluster IP address appears first in the list within the Connections field (re-order the list as needed).
   c. Click **OK** to close the Advanced Settings" dialog box.
   d. Close the "Network Connections" window.
   e. Close the Control Panel.

4. Restart the DMZ Secure Proxy Server.
Repeat this task on every DMZ Secure Proxy Server.
Creating a custom property for Office Collaboration Server

If your Sametime Gateway deployment includes a Microsoft Office Collaboration Server, create a custom property for the Gateway cluster to specify the publicly known host name (fully qualified domain name) of the Load Balancer server so the OCS community can respond to client requests routed from that server.

1. On the server hosting the Sametime Gateway cluster's Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
2. In the navigation tree, click System Administration > Cell.
3. On the cell configuration page, look under "Additional Properties" and click Custom properties.
4. Add the custom property:

   a. In the custom properties table, click New.
   b. Type com.ibm.sametime.gateway.fdqn in the Name field.
   c. Type the fully qualified host name of the Load Balancer server in the Value field.
   d. Click OK.
7. Click the **Save** link in the "Messages" box at the top of the page.

![Messages]

- Changes have been made to your local configuration. You can:
  - **Save directly to the master configuration.**
  - **Review** changes before saving or discarding.
  - An option to synchronize the configuration across multiple nodes can be disabled in Preferences.
  - The server may need to be restarted for these changes to take effect.

8. Restart the Sametime Gateway cluster as follows:
   a. In the navigation tree, click **Servers > Clusters > WebSphere application server clusters**.
   b. Click the name of the Sametime Gateway cluster.
   c. Click the **Stop** button at the top of the table; then wait for the status to update.
   d. Click the **Start** button at the top of the table.
Setting up SSL/TLS security

SSL (Secure Socket Layer) and TLS (Transport Layer Security) provide encrypted communications over the Internet. SSL is the precursor to TLS encryption; you may find their names used interchangeably. Set up SSL/TLS encryption to secure communications between the DMZ Secure Proxy Server and the Sametime Gateway cluster.

Setting up SSL/TLS on one or more DMZ Secure Proxy Servers

Setting up SSL/TLS communications for a DMZ Secure Proxy Server requires that you complete the following tasks:

1. Request a certificate signed by a Certificate Authority
2. Import the signed certificate into the server's keystore
3. Import certificate authorities used by external communities into the server's trust store
4. Define the SSL/TLS configuration for two or more DMZ Secure Proxy Servers
5. Enable SSL/TLS on each DMZ Secure Proxy Server

These tasks are described below.

Requesting a certificate signed by a Certificate Authority

SSL and TLS depend on the use of shared certificates that are generated by a trusted third party, called a Certificate Authority. Before you can establish secure communications in your deployment, you must obtain a certificate for the servers to share.

Note: Before requesting a certificate, you should consult with your network administrator to decide on a common name (CN) for the certificate, which you will provide on the request form. The common name serves as the CN portion of the certificate's distinguished name but it does not have to match any of the domains that your company users for email addresses.

1. On a DMZ Secure Proxy Server, log in to the Integrated Solutions Console as the WebSphere administrator.
2. On the navigator, click Security > SSL certificate and key management.
3. Look under "Related items" and click Key stores and certificates.
4. In the keystores and trust stores table, click NodeDefaultKeyStore.
5. On the NodeDefaultKeyStore page, look under "Additional Properties" and click Personal certificate requests.
6. In the personal certificate requests table, click New.
7. Fill in the certificate request as follows and then click OK:
   - File for certificate request: Type the full path (including the file name) where the certificate request will be stored; for example: c:\servercertreq.arm (on Windows).
   - Key label: Type an alias for the certificate; for example: stgwcertificate. You will use the alias to identify the certificate request in the keystore.
   - Common name: This serves as the "CN" portion of the certificate's distinguished name. Type the (externally visible) DNS address to which the external community would open a TCP connection. If you deployed a load balancer for the DMZ Secure Proxy Servers, use the load balancer cluster host name. The common name does not have to match any of the email domains associated with your community.
The following fields are optional; if used, they comprise the corresponding fields in the certificate's distinguished name:

- **Organization**
- **Organizational unit**
- **Locality**
- **State or province**
- **Zip code**
- **Country or region**

8. Click the **Save** link in the "Messages" box at the top of the page.

9. Rename the certificate request file (specified in step 7) to use ".csr" as its file extension.

   For example, if you named the file `servercertreq.arm` you should rename it to `servercertreq.csr`.
10. Submit the request to a certificate authority; for information, see List of supported Certificate Authorities in the Sametime wiki.

For the most recent list of Certificate Authorities accepted by Sametime Gateway, see the IBM Technote List of Certificate Authorities (CAs) accepted by Sametime Gateway.

**Importing a signed certificate issued into the keystore**

When you receive a certificate signed by a Certificate Authority, you must import it into the keystore on every DMZ Secure Proxy server, as well as on every server that will communicate directly with the DMZ Secure Proxy Servers.

Import the signed certificate into the keystore on every DMZ Secure Proxy Server.

1. Copy the certificate file to a temporary location on the server where you want to import it.
2. Log in to the Integrated Solutions Console as the WebSphere administrator.
3. On the navigator, click **Security > SSL certificate and key management**.
4. Look under "Related items" and click **Key stores and certificates**.
5. In the keystores and trust stores table, click **NodeDefaultKeyStore**.
6. On the NodeDefaultKeyStore page, look under "Additional Properties" and click **Personal certificates**.
7. In the personal certificates table, click **Receive from a certificate authority**.
8. In the **Certificate file name** field, type the full path and file name of the certificate.
   Do not change the default **Data type** value (Base64-encoded ASCII Data).

   ![SSL certificate and key management > Key stores and certificate](image)

9. Click **OK** to import the certificate into the keystore.
The certificate appears in the personal certificates table, using the alias and distinguished name that you provided when requesting the certificate.

10. Click the **Save** link in the "Messages" box at the top of the page.

---

### Configuring trust for certificate authorities used by external communities

Clients communicating with the DMZ Secure Proxy Server from the internet will use the SSL/TSL certificates provided by their own communities. To exchange data with those clients, the DMZ Secure Proxy Server must be configured to "trust" those certificates by importing a copy of the community's certificate (signed by the Certificate Authority) into the server's keystore.

Complete this task on every DMZ Secure Proxy server, making sure to establish trust with every external community supported by your deployment. For example, if your company supports AOL and Yahoo! Messenger, you must establish trust for both of those communities on every DMZ Secure Proxy Server.

1. Obtain a copy of the certificate file used by the external community.

   To support AOL communities, import the following standard certificates:
   
   - Navigate to [https://pki-info.aol.com/AOL/](https://pki-info.aol.com/AOL/) and download the following two certificates titled:
     
     "America Online Root CA 1 certificate"
     
     "America Online Root CA 2 certificate"
   
   - Navigate to [https://pki-info.aol.com/AOLMSPKI/index.html](https://pki-info.aol.com/AOLMSPKI/index.html) and download the certificate titled:
     
     "AOL Member CA certificate"

2. Copy the certificate files to a temporary location on the DMZ Secure Proxy Server.

3. Log in to the Integrated Solutions Console as the WebSphere administrator.

4. On the navigator, click **Security > SSL certificate and key management**.

5. Look under "Related items" and click **Key stores and certificates**.

6. In the keystores and trust stores table, click **NodeDefaultTrustStore**.
7. On the NodeDefaultTrustStore page, look under "Additional Properties" and click **Signer certificates**.
8. In the signer certificates table, click **Add**.
9. In the **Alias** field, type a name for the external community's certificate.
10. In the **File name** field, type the full path and file name where you stored the certificate file.
11. Select the certificate file's data type (the default is usually correct).

   ![SSL certificate and key management screen](image)

12. Click **OK** to add the signer certificate to the truststore.

   The certificate appears in the signer certificates table, using the alias that you provided.
13. Click the **Save** link in the "Messages" box at the top of the page.

---

**Defining the SSL configuration for a DMZ Secure Proxy Server**

Define the SSL configuration on every DMZ Secure Proxy Server.

1. On the DMZ Secure Proxy Server, log in to the Network Deployment's Integrated Solutions Console as the WebSphere administrator.
2. On the navigator, click **Security > SSL certificate and key management**.
3. Look under "Related items" and click **SSL configurations**.
4. In the SSL configurations table, click **NodeDefaultSSLSettings**.
5. In the **Trust store name** field, select **NodeDefaultTrustStore**.
The truststore name (your DMZ Secure Proxy Server's name) refers to the truststore for that server, which contains signer certificates that will be used to determine whether to trust connections from clients or other servers. The signed certificates stored here are those that you imported in the previous task.

6. In the **Keystore name** field, select **NodeDefaultKeyStore**.
   This is the keystore where you imported your new certificate that you received from the certificate authority.

7. Click the **Get certificate aliases** button.

8. In the **Default server certificate alias** field, select your certificate.

9. In the **Default client certificate alias** field, select your certificate.

10. Click **OK**.

11. Click the **Save** link in the "Messages" box at the top of the page.

8. Repeat steps 1 through 7 on every DMZ Secure Proxy Server.
Enabling SSL/TLS on a DMZ Secure Proxy Server

Enable the use of SSL/TLS on every DMZ Secure Proxy Server. When you enable SSL/TLS, you select the certificate that the current server should use for communications. In addition, all of the DMZ Secure Proxy Servers in the cell will trust all of the certificates that you imported into the truststore that you selected in the previous task.

1. On the DMZ Secure Proxy Server, log in to the Integrated Solutions Console as the WebSphere administrator.
2. On the navigator, click Security > SSL certificate and key management.
3. Look under "Configuration settings" and click Manage endpoint security configurations.
4. Configure SSL for inbound traffic as follows:
   a. In the Inbound node on the local topology tree, expand the following items:
      
      DMZ_Secure_Proxy_Server_cell_name > nodes > cell_primary_node_name(NodeDefaultSSLSettings) > servers.
   b. In the servers sub-tree, click the name of the DMZ Secure Proxy Server.
   c. On the "Configuration" page, click Override inherited values.
   d. In the SSL configuration field, select NodeDefaultSSLSettings.
   e. Click the Update certificate alias list button.
   f. In the certificate alias in key store field, select your certificate (the one you requested and imported into the keystore).
   g. Click OK.
5. Configure SSL for outbound traffic as follows:
   a. In the **Outbound** node on the local topology tree, expand the following items:
      - DMZ_Secure_PROXY_Server_cell_name > nodes >
      - cell_primary_node_name(NodeDefaultSSLSettings) > servers.
   b. In the servers sub-tree, click the name of the DMZ Secure Proxy Server.
   c. On the "Configuration" page, click **Override inherited values**.
   d. In the **SSL configuration** field, select **NodeDefaultSSLSettings**.
   e. Click the **Update certificate alias list** button.
f. In the certificate alias in key store field, select your certificate (the one you requested and imported into the keystore).

g. Click OK.

6. Change the DMZ Secure Proxy Server's configuration to use SSL/TLS on transports:
   a. In the navigation tree, click Servers > Server types > WebSphere proxy Servers.
   b. In the proxy servers table, click the name of your DMZ Secure Proxy Server.
   c. On the "Configuration" page, look under "Proxy Settings" and click SIP Proxy Server Settings > SIP proxy server transports.
   d. In the transports table, click SIPS_PROXY_CHAIN.
   e. On the SIPS_PROXY_CHAIN configuration page, click SSL inbound channel (SSL_4).
   f. On the Configuration page, look under "SSL Configuration" and click Centrally managed.
g. Click OK.

7. Click the **Save** link in the "Messages" box at the top of the page.

8. Repeat steps 1 through 7 on every DMZ Secure Proxy Server.
Configuring firewalls

The dual DMZ deployment requires that you create an additional demilitarized zone (a Web DMZ) by deploying another firewall between the DMZ Secure Proxy Server cell and the Internet, and then configure the firewall settings between the Web DMZ and the Application DMZ where the Sametime Gateway cluster resides.

Setting inner firewall rules

The inner firewall separates the corporate intranet (where the Sametime Community Servers are hosted) from the Application DMZ (where the Sametime Gateway servers are hosted) and should be configured as explained in the Sametime wiki topic, *Opening ports in the firewall*.
## Setting middle firewall rules

The middle firewall separates the Application DMZ (where Sametime Gateway is hosted) from the Web DMZ (where the DMZ Secure Proxy Servers are hosted) and should be configured according to the following rules:

### Middle firewall rules

<table>
<thead>
<tr>
<th>From IP</th>
<th>From Port</th>
<th>To IP</th>
<th>To Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS containers</td>
<td>5060, 5062, or other defined ports</td>
<td>DMZ Secure proxies</td>
<td>Any</td>
<td>UDP</td>
<td>Inbound</td>
<td>SIP UDP</td>
</tr>
<tr>
<td>WAS containers</td>
<td>Any</td>
<td>DMZ Secure proxies</td>
<td>5060, 5061, or other defined ports</td>
<td>TCP/TLS</td>
<td>Inbound</td>
<td>SIP TCP,TLS</td>
</tr>
<tr>
<td>Core Bridge server (Dmgr)</td>
<td>Core Bridge DCS port</td>
<td>DMZ Secure proxies</td>
<td>Any</td>
<td>TCP</td>
<td>Inbound</td>
<td>Incoming DCS</td>
</tr>
<tr>
<td>Dmgr of WAS nodes</td>
<td>SOAP</td>
<td>DMZ Secure proxies</td>
<td>Ephemeral</td>
<td>TCP</td>
<td>Inbound</td>
<td>Incoming SOAP</td>
</tr>
<tr>
<td>DMZ Secure proxies</td>
<td>Any</td>
<td>WAS containers</td>
<td>5060, 5062, or other defined ports</td>
<td>UDP</td>
<td>Outbound</td>
<td>SIP UDP</td>
</tr>
<tr>
<td>DMZ Secure proxies</td>
<td>Any</td>
<td>WAS containers</td>
<td>5060-5063, or other defined ports</td>
<td>TCP/TLS</td>
<td>Outbound</td>
<td>SIP TCP, TLS</td>
</tr>
<tr>
<td>DMZ Secure proxies</td>
<td>Any</td>
<td>Core Bridge server</td>
<td>Bridge DCS port</td>
<td>TCP</td>
<td>Outbound</td>
<td>Outgoing DCS</td>
</tr>
<tr>
<td>DMZ Secure proxies</td>
<td>Any</td>
<td>DM of WAS nodes</td>
<td>SOAP port 8879 (default)</td>
<td>TCP</td>
<td>Outbound</td>
<td>Dmgr SOAP</td>
</tr>
<tr>
<td>Block all other DMZ ports not used</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**IBM Sametime Gateway 8.5.2 IFR1  Deploying DMZ Secure Proxy Server  118**
Setting outer firewall rules

The outer firewall separates the Web DMZ (where the DMZ Secure Proxy Servers are hosted) from the Internet, and should be configured according to the following rules:

![Diagram of firewall zones]

### Outer firewall rules

<table>
<thead>
<tr>
<th>From IP</th>
<th>From Port</th>
<th>To IP</th>
<th>To Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Virtual IP of Load Balancer</td>
<td>5060, 5061, or other defined ports</td>
<td>UDP, TCP/TLS</td>
<td>Inbound</td>
<td>Incoming Clients</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>Any</td>
<td>DMZ Secure proxies</td>
<td>5060 or other defined ports</td>
<td>TCP</td>
<td>Inbound</td>
<td>LB Advisor traffic</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>DMZ Secure proxies</td>
<td>9060</td>
<td>TCP</td>
<td>Inbound</td>
<td>AdminAgent Console</td>
</tr>
<tr>
<td>DMZ Secure proxies</td>
<td>5060</td>
<td>Clients</td>
<td>Any</td>
<td>UDP</td>
<td>Outbound</td>
<td>Outgoing Clients</td>
</tr>
<tr>
<td>DMZ Secure proxies</td>
<td>Ephemeral port range of OS</td>
<td>Clients</td>
<td>Any</td>
<td>TCP/TLS</td>
<td>Outbound</td>
<td>Outgoing Clients</td>
</tr>
</tbody>
</table>

Block all other DMZ ports not used

---

IBM Sametime Gateway 8.5.2 IFR1  *Deploying DMZ Secure Proxy Server* 119
**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.

**Trademarks**

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

IBM
AIX
DB2
IBM i
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.
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.