Sun Java™ System Portal Server Release Notes for Microsoft Windows

Version 6 2005Q4

Part Number 819-4270-10

These Release Notes contain important information available at the time of release of Sun Java System Portal Server 6 2005Q4 for Windows. Known issues and limitations, and other information are addressed here. Read this document before you begin using Portal Server 6.

The most up-to-date version of these release notes can be found at the Sun Java System documentation web site: `http://docs.sun.com/app/docs/prod/entsys.05q4#hic`. Check the web site prior to installing and setting up your software and then periodically thereafter to view the most up-to-date release notes and product documentation.

These release notes contain the following sections:

Third-party URLs may be referenced in this document and provide additional, related information.

NOTE Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Release Notes Revision History

Table 1 Revision History

Date	Description of Changes
February 2006	Revenue release.
November 2005	Beta release.

About Portal Server 6 2005Q4

The Sun Java System Portal Server 6 2005Q4 product gives end users a Portal Desktop, which provides access to resources and applications. The Portal Server software also provides a search engine infrastructure that enables intranet content to be organized and accessed from the Portal Desktop. Additionally, in this release, the communication channels are now installed with the Portal Server software. The communication channels consist of mail, calendar, address book, and instant messaging channels.

Portal Server also offers Secure Remote Access support, which enables remote users to securely access their organization's network and the services offered over the Internet. Additionally, it gives your organization a secure Internet portal, providing access to content, applications, and data to any targeted audience: employees, business partners, or the general public.

What's New in Portal Server 6 2005Q4

The following Secure Remote Access features are new and have not been documented in the *Sun Java System Portal Server Secure Remote Access 6 2005Q4 Administration Guide*.

- HTTPS Support in Proxylet. This implementation has the following results:
  - Decryption is done at the client server.
  - You can access destination servers running in SSL mode.
  - Can directly present client certificate to the destination server.
  - Basic authentication single sign on is no longer available at the gateway. (The Gateway can not insert SSO information in http headers.)
  - URL-based access control is no longer supported, only host-based access control,

- External accelerators and external reverse proxies in front of the GW are not currently supported.
- This support is not for Proxylet with Portal Server on HTTPS.

- The Proxylet Java applet now has rules that determine the content of the PAC file. All HTTP requests go to Proxylet. The Proxylet rules allow the administrator to specify mappings based on protocol, host, or port to domains.

  For example an administrator can make a rule so that all FTP traffic is routed through Netlet and all HTTP traffic is routed through Proxylet.

- Using the Access Manager administration console, the Portal Server administrator can choose whether to launch Netlet with Java Web Start or the Netlet applet. If the administrator chooses Java Web Start, when the user clicks Netlet icon on the desktop, the browser is launched and Netlet runs. When using Java Web Start, once it is deployed, Netlet does not need to be downloaded again.

Hardware and Software Requirements

The following hardware and software are required for this release of Portal Server.

Table 2 Hardware and Software Requirements

Component	Platform Requirement
Supported Platforms	Windows 2000, Windows 2003, Windows XP
Operating System	Windows 2000 Advanced Server SP4 Windows 2003 Enterprise Server Windows XP SP1 and SP2
RAM	1 Gbytes
Disk space	1 Gbytes

For software requirements, see the *Sun Java Enterprise System Release Notes* at http://docs.sun.com.

Default Paths and File Names

The following table describes the default paths and file names used in this book.

Table 3 Default Paths and File Names Used in This Book

Term	Description
PortalServer-base	Represents the base installation directory for Portal Server. The Portal Server 2005Q1 default base installation and product directory depends on your specific platform: `C:\Sun` For example, if the install root is `C:\Sun` (the default) the Portal Server is installed in `C:\Sun\PortalServer`
AccessManager-base	Represents the base installation directory for Access Manager. The Access Manager 2005Q2 default base installation and product directory depends on your specific platform: `C:\Sun\AccessManager`
DirectoryServer-base	Represents the base installation directory for Sun Java System Directory Server. Refer to the product documentation for the specific path name.
ApplicationServer-base	Represents the base installation directory for Sun Java System Application Server. Refer to the product documentation for the specific path name.
WebServer-base	Represents the base installation directory for Sun Java System Web Server. Refer to the product documentation for the specific path name.

Post Installation Configuration

This section is organized as follows:

The psconfig batch file

If you have installed Portal Server with the Sun Java Enterprise System installer with the "Configure Later" option, use psconfig to configure the Portal Server component product. The following checklists in this section describe the parameters used to configure the Portal Server component product.

To run psconfig:

1. In the command prompt, go to the directory that contains the psconfig batch:

   `cd` *PortalServer-base*`/config`

2. Configuration can be performed in either the interactive mode or using a silent mode.
   - To configure in the interactive mode, execute the psconfig batch file by typing `psconfig` and then enter appropriate answers for the configuration questions.

     See "Configuring Portal Server in Interactive Mode."
   - To configure using the sample silent file, execute the psconfig batch file by typing

     ```
     psconfig -s
     ```

     See "Configuring Portal Server in Silent Mode."

If you have performed a minimal installation, you will need to use the psconfig script to configure your Portal Server installation. The following checklists describe the values that you will need for a post-install configuration. Depending on the type of installation you perform, the values that you use might vary.

The Checklists are organized in the following way:

- Components
- Base Directory
- Configuration Mode
- Deployment Information
- Web Container Information
  - Sun Java Web server
  - Sun Java Application Server 8.1
- Portal Server Information
- Identity Server Information
- Secure Remote Access Information

- Gateway
- Netlet Proxy
- Rewriter Proxy

Portal Server And Secure Remote Access Configuration Checklist

Table 4 is a three column table that lists all the values that you might need for a post-install configuration. Depending on the type of installation you perform, the values that you use might vary.

NOTE The Portal Server 2005Q1 default base installation and product directory depends on your specific platform:

C:\Sun\PortalServer

For example, if the install directory is C:\Sun (the default) the Portal Server is installed in C:\Sun\PortalServer.

NOTE If a parameter is not applicable to a container, it is not included in the table.

Table 4 Portal Server Configuration Checklist

Parameter	Default Value	Description
BASEDIR		
BASEDIR The directory where Sun Java System Portal Server configurator components are installed		This is the base directory in which the Portal Server software is installed using Java Enterprise System Installer. The base directory depends on the platform you are using. For example, if the install directory is C:/Sun (the default) the Portal Server is installed in: C:\Sun\PortalServer

Table 4 Portal Server Configuration Checklist *(Continued)*

Parameter	Default Value	Description
PS_CONFIGURATION_MODE The Configuration mode in which you want the Sun Java System configurator needs to be executed	configure	Possible values are: configure–Configure the Portal Server Components. scrubds–Remove the Portal Server Components entries from the Directory Server. unconfigurewithoutscrubds–Unconfigure the Portal Server Components without removing the entries from the Directory Server. unconfigurewithscrubds–Unconfigure the Portal Server and also remove the entries from the Directory Server.
Deployment Information		
PS_DEPLOY_TYPE The web container on which Portal Server is being deployed. The Portal Server can be deployed on Sun Java System Web Server Sun Java System Application Server 8.1	SUNONE8	Possible values are: IWS = Sun Java System Web Server SUNONE8 = Sun Java System Application Server 8.1
Web Container Information Sun Java System Web Server		
PS_DEPLOY_DIR	`C:\Sun\WebServer`	Directory in which the Sun Java System Web Server is installed.
PS_DEPLOY_INSTANCE	myportalbox.mydomain.com	The web server instance you want the Portal Server to use. Note: The instance name should not contain spaces.
PS_DEPLOY_DOCROOT	`C:\Sun\WebServer\docs`	The Web Server Directory where static pages are kept.
PS_DEPLOY_ADMIN	admin	The administrator user ID.
PS_DEPLOY_ADMIN_PROTOCOL	http	The administration server Protocol.
PS_DEPLOY_ADMIN_HOST	myportalbox.mydomain.com	The administration server hostname.
PS_DEPLOY_ADMIN_PORT	8888	The port number of the administration server.

Table 4 Portal Server Configuration Checklist *(Continued)*

Parameter	Default Value	Description
PS_DEPLOY_JDK_DIR		The JDK Dir that is being used by the web container.
Web Container Information Sun Java System Application Server 8.1		
PS_DEPLOY_DIR	`C:\Sun\ApplicationServer`	Directory in which the Sun Java System Application Server 8.1 is installed
PS_DEPLOY_DOMAIN	domain1	The Sun Java System Application Server domain contains a set of instances. The domain specified will contain the instance used by the Portal Server. This domain must already be configured.
PS_DEPLOY_INSTANCE_DIR	`C:\Sun\ApplicationServer\domains\domain1`	The full path of the domain specified that will be configured for the Portal Server.
PS_DEPLOY_INSTANCE	server	The name of the Sun Java System Application Server instance to which the Portal Server will be deployed. This instance must already be configured. The instance name should not contain spaces.
PS_DEPLOY_DOCROOT	`C:\Sun\ApplicationServer\domains\domain1\docroot`	The Application Server Directory where static pages are kept.
PS_DEPLOY_ADMIN	admin	The administrator user ID.
PS_DEPLOY_ADMIN_PROTOCOL	https	The administration server Protocol.
PS_DEPLOY_ADMIN_HOST	myportalbox.mydomain.com	The administration server hostname.
PS_DEPLOY_ADMIN_PORT	4849	The port number of the administration server.
PS_DEPLOY_JDK_DIR		The JDK Directory that is being used by the web container.
Portal Server Information		

Table 4 Portal Server Configuration Checklist *(Continued)*

Parameter	Default Value	Description
PS_DEPLOY_URI	/portal	The URI is the space on the web server or application server that the Portal Server uses. The value for the deployment URI must have a leading slash and must contain only one slash. However, the deployment URI can not be a "/" by itself.
PS_LOAD_BALANCER_URL Load balancer controlling Portal Server Instances	`http://myportalbox.mydomain.com:80/portal`	If you are not using any Load Balancer URL then use the Portal Server URL. `http://`*fully-qualified-domain*`:`*port*`/`*portal-deploy_uri* For example `http://myportalbox.mydomain.com:80/portal`
PS_PROTOCOL	http	The Protocol to be used while accessing the Portal Server. Possible values are http and https.
PS_HOST		Fully Qualified Name of the Portal Server
PS_PORT		Port number to be used for accessing the Portal Server.
Identity Server Information		
PS_IDSAME_ADMIN_PASSWORD Administrator (amadmin) Password		The top level administrator (amadmin) password chosen during the Sun Java System Identity Server software installation.
PS_IDSAME_LDAPUSER_PASSWORD Internal LDAP Authentication User Password		The Internal LDAP Authentication User Password chosen during the Sun Java System Identity Server installation.
PS_DS_DIRMGR_DN Directory Manager DN	cn=Directory Manager	The directory manager DN chosen during the installation of the Sun Java System Directory Server.
PS_DS_DIRMGR_PASSWORD Directory Manager Password		The directory manager Password chosen during the installation of the Sun Java System Directory Server.
PS_DEPLOY_ADMIN_PASSWORD Deploy Administrator Password		This is the web-container's Administrator Password.

Table 4 Portal Server Configuration Checklist *(Continued)*

Parameter	Default Value	Description
Secure Remote Access Information (for configuring Secure Remote Access Support)		
SRA_GW_PROTOCOL Gateway Protocol	https	The Protocol used by the gateway. The gateway will communicate using Secure Sockets Layer (SSL).
SRA_GW_PORT Gateway Port	443	The port on which the gateway listens.
SRA_GATEWAY_PROFILE Gateway Profile Name	default	A gateway profile contains all the information related to gateway configuration, such as the port on which gateway listens, SSL options, and proxy options. You can create multiple profiles in the gateway administration console and associate different instances of gateway with different profiles. See “Creating a Gateway Profile” in the Sun Java System Portal Server, Secure Remote Access 6 2005Q1 Administrator’s Guide.
SRA_SERVER_DOMAIN	*portal-server-domain-name*	The domain name for the machine on which the Portal Server is installed.
SRA_GW_DOMAIN Gateway Domain	*gateway-domain-name*	The domain name of the gateway machine.
SRA_IDSAME_ADMIN_PASSWORD Administrator (amadmin) Password		The top level administrator (amadmin) password chosen during the Sun Java System Identity Server software installation.
SRA_IDSAME_LDAPUSER_PASSWORD Internal LDAP Authentication User Password		The Internal LDAP Authentication User Password chosen during the Sun Java System Identity Server installation.
SRA_DS_DIRMGR_DN Directory Manager DN	cn=Directory Manager	The directory manager DN chosen during the installation of the Sun Java System Directory Server.
SRA_DS_DIRMGR_PASSWORD Directory Manager Password		The directory manager Password chosen during the installation of the Sun Java System Directory Server.
SRA_DEPLOY_ADMIN_PASSWORD Deploy Administrator Password		This is the web-container’s Administrator Password.

Table 4 Portal Server Configuration Checklist *(Continued)*

Parameter	Default Value	Description
SRA_LOG_USER_PASSWORD Gateway Logging User Password		This allows administrators with non-root access to look at gateway log files.

Gateway Configuration Checklist

Table 5 is a three column table for the Gateway Installation Checklist.

Table 5 Gateway Configuration Checklist

Parameter	Default Value	Description
GW_PROTOCOL	https	The protocol used by the gateway. The gateway will usually communicate using Secure Sockets Layer (SSL).
GW_HOST	mygwbox.mydomain.com	The host name of the machine on which the gateway is installed.
GW_PORT	443	The port on which the gateway machine listens.
GW_IP	gw-host-ip-address	The IP Address should be that of the machine where Gateway is installed and not that of the Sun Java System Identity Server.
GW_GATEWAY_PROFILE Gateway Profile Name	default	A gateway profile contains all the information related to gateway configuration, such as the port on which gateway listens, SSL options, and proxy options. You can create multiple profiles in the gateway administration console and associate different instances of gateway with different profiles. See "Creating a Gateway Profile" in the *Sun Java System Portal Server, Secure Remote Access 6 2005Q1 Administrator's Guide*.
GW_LOAD_BALANCER_URL Load balancer controlling Portal Server Instances.		If you are not using any Load Balancer URL then use the Portal Server URL. `http://`*fully-qualified-domain*`:`*port*`/`*portal-deploy_uri* for example: `http://myportalbox.mydomain.com:80/portal`

Table 5 Gateway Configuration Checklist

Parameter	Default Value	Description
GW_CERT_INFO		The Certificate Information should be provided in the following format: "CN=$GW_HOST, L=*The name of your city or locality*, ST=*The name of your state*, C=*The two letter country code for your country*, O=*The name of your organization*, OU=*The name of your division*" For example, "CN=$GW_HOST,L=SantaClara,ST=California,C=us,O=Portal,OU=Sun"
GW_SRA_LOG_USER_PASSWORD Gateway Logging User Password		This allows administrators with non-root access to look at gateway log files.
GW_CERT_DB_PASSWORD Certificate Database Password		This can be any password you choose.
Certificate Information		
Organization (O)	MyOrganization	The name of your organization.
Division (OU)	MyDivision	The name of your division.
City or Locality (L)	MyCity	The name of your city or locality
State or Province (ST)	MyState	The name of your state
Two-Letter Country Code (C)	us	The two letter country code for your country.
Certificate Database Password		This can be any password you choose.
Retype Password		Retype the password to verify.

Netlet Proxy Configuration Checklist

Table 6 is a three column table for the Netlet Proxy Installation Checklist. The first column lists the parameters. The second column lists the default value. The third column lists a description for the parameter.

Table 6 Netlet Proxy Configuration Checklist

Parameter	Default Value	Description
NLP_PROTOCOL	https	The protocol used by the Netlet Proxy. The Netlet Proxy will usually communicate using Secure Sockets Layer (SSL).
NLP_HOST	myportalbox.mydomain.com	The host name of the machine on which Netlet Proxy is installed.
NLP_PORT	10555	The port on which the Netlet Proxy listens.
NLP_IP	host-ip-address	The IP address should be that of the machine where Netlet Proxy is installed and not that of Sun Java System Identity Server.
NLP_GATEWAY_PROFILE Gateway Profile Name	default	Specify the same profile name specified when you installed Portal Server or Secure Remote Access support. See “Creating a Gateway Profile” in the Sun java System Portal Server, Secure Remote Access 6 2005Q1 Administrator’s Guide for more information.
NLP_LOAD_BALANCER_URL Load balancer controlling Portal Server Instances.		If you are not using any Load Balancer URL then use the Portal Server URL. http://*fully-qualified-domain*:*port*/*portal-deploy-uri* For example `http://myportalbox.mydomain.com:80/portal`
NLP_CERT_INFO		The Certificate Information should be mentioned in the following format “CN=$GW_HOST, L=<The name of your city or locality>,ST=<The name of your state>,C=<The two letter country code for your country>,O=<The name of your organization>,OU=<The name of your division>” For example, “CN=$GW_HOST,L=SantaClara,ST=California, C=us,O=Portal,OU=Sun”
NLP_SRA_LOG_USER_PASSWORD Gateway Logging User Password		This allows administrators with non-root access to look at gateway log files.

Rewriter Proxy Configuration Checklist

Table 7 is a three column table for the Rewriter Proxy Installation Checklist. The first column lists the parameters. The second column lists the default value. The third column lists a description for the parameter.

Table 7 Rewriter Proxy Checklist

Parameter	Default Value	Description
RWP_PROTOCOL	https	The protocol used by the Rewriter Proxy. The Rewriter Proxy will usually communicate using Secure Sockets Layer (SSL).
RWP_HOST	myportalbox.mydomain.com	The host name of the machine on which Rewriter Proxy is installed.
RWP_PORT	10443	The port on which the Rewriter Proxy listens.
RWP_IP	host-ip-address	The IP address should be that of the machine where Rewriter Proxy is installed and not that of Sun Java System Identity Server.
RWP_GATEWAY_PROFILE Gateway Profile Name	default	Specify the same profile name specified when you installed Portal Server or Secure Remote Access support. See “Creating a Gateway Profile” in the Sun java System Portal Server, Secure Remote Access 6 2005Q1 Administrator’s Guide for more information.
RWP_LOAD_BALANCER_URL Load balancer controlling Portal Server Instances.		If you are not using any Load Balancer URL then use the Portal Server URL. `http://`*fully-qualified-domain*`:`*port*`/`*portal-deploy-uri* for example `http://myportalbox.mydomain.com:80/portal`
RWP_CERT_INFO		The Certificate Information should be provided in the following format “CN=$GW_HOST,L=<The name of your city or locality>,ST=<The name of your state>,C=<The two letter country code for your country>,O=<The name of your organization>,OU=<The name of your division>” For example “CN=$GW_HOST,L=SantaClara,ST=California,C=us,O=Portal,OU=Sun”
RWP_SRA_LOG_USER_PASSWORD Gateway Logging User Password		This allows administrators with non-root access to look at gateway log files.

Configuring Portal Server in Interactive Mode

1. As root in a terminal window, go to the directory that contains the psconfig batch file:

   `cd` *PortalServer-base*`/config`

2. To configure Portal Server in interactive mode, execute the psconfig batch file by typing `psconfig-c <component name>` and then enter appropriate answers for the configuration questions.

Portal Server

Table 8 is a three column table that lists all the values that you might need for a post-minimal install configuration. Depending on the type of installation you perform, the values that you use might vary.

Table 8 Portal Server Configuration Checklist

Question	Default Value	Description
Portal Server Configuration Information		
What is the Portal Server Web Containers host	myportalbox.mydomain.com	Fully Qualified Name of the Portal Server
Is the Portal Server Web Containers port secure	No	The Protocol to be used while accessing the Portal Server. Possible values are No: If the Protocol is http. Or Yes: If the Protocol is https
What is the Portal Server Web Containers port	80	Port number to be used for accessing the Portal Server.
What is the Portal Server deployment URI	`/portal`	The URI is the space on the web server or application server that the Portal Server uses. The value for the deployment URI must have a leading slash and must contain only one slash. However, the deployment URI can not be a “/" by itself.
Choose the container to which the portal server needs to be configured: 1. Sun Java System Web Server 2. Sun Java System Application Server 8.1	1	The web container on which Portal Server is being deployed. Possible values are 1 = Sun Java System Web Server 2 = Sun Java System Application Server 8.1
Web Container Information Sun Java System Web Server		
Where is the Web Container installed	`C:\Sun\Appplication Server`	Directory in which the Sun Java System Web Server is installed.

Table 8 Portal Server Configuration Checklist

Question	Default Value	Description
What is the Web Container instance	myportalbox.mydomain.com	The web server instance you want the Portal Server to use. Note: The instance name should not contain spaces.
Web Container Information Sun Java System Application Server 8.1		
Where is the Web Container installed	`C:\Sun\Appplication Server`	Directory in which the Sun Java System Application Server 8.1 is installed
What is the Web Container domain	domain1	The Sun Java System Application Server domain contains a set of instances. The domain specified will contain the instance used by the Portal Server. This domain must already be configured.
What is the Web Container Deploy Instance Dir	`C:\Sun\Appplication Server\domains\domain1`	The full path of the domain specified that will be configured for the Portal Server.
What is the Web Container Deploy Instance	server	The name of the Sun Java System Application Server instance to which the Portal Server will be deployed. This instance must already be configured. The instance name should not contain spaces.
What is the Web Container Document Directory	`C:\Sun\Appplication Server\domains\domain1\docroot`	The Application Server Directory where static pages are kept.
Who is the Web Container administrator	admin	The administrator user ID.
What is the HostName of the Machine where Web Container is Installed	myportalbox.mydomain.com	The administration server hostname.
Is the Web Container administration port secure	Yes	The Protocol to be used while accessing the Portal Server. Possible values are No If the Protocol is http Or Yes If the Protocol is https.
What is the Web Container administration port	4849	The port number of the administration server. Note: The default Administrator Port for Sun Java System Application Sever 8.1 is “4849.”
What is the Web Container administrator password		This is the web-container’s Administrator Password.
Identity Server Information		

Table 8 Portal Server Configuration Checklist

Question	Default Value	Description
What is the Access Manager Administrator (amadmin) Password Administrator (amadmin) Password		The top level administrator (amadmin) password chosen during the Sun Java System Identity Server software installation.
Again		Re-enter the top level administrator (amadmin) password.
What is the Access Manager Internal LDAP Authentication User Password Internal LDAP Authentication User Password		The Internal LDAP Authentication User Password chosen during the Sun Java System Identity Server installation.
Again		Re-enter the Internal LDAP Authentication User Password.
What is the Directory Manager DN Directory Manager DN	cn=Directory Manager	The directory manager DN chosen during the installation of the Sun Java System Directory Server.
What is the Directory Manager Password Directory Manager Password		The Directory Manager Password chosen during the installation of the Sun Java System Directory Server.
Again		Re-enter the Directory Manager Password.
PS_DEPLOY_ADMIN_PASSWORD Deploy AdministratorPassword		This is the web-container's Administrator Password.
Secure Remote Access Core Configuration Information (for configuring Secure Remote Access Support)		
What is the Gateway protocol Gateway Protocol	https	The Protocol used by the gateway. The gateway will communicate using Secure Sockets Layer (SSL).
What is the Portal Server domain Portal Server Domain	portal-server-domain-name	The domain name for the machine on which the Portal Server is installed.
What is the Gateway domain Gateway Domain	gateway-domain-name	The domain name of the gateway machine.
What is the Gateway port Gateway Port	443	The port on which the gateway listens.

Table 8 Portal Server Configuration Checklist

Question	Default Value	Description
What is the Gateway profile Gateway Profile Name	default	A gateway profile contains all the information related to gateway configuration, such as the port on which gateway listens, SSL options, and proxy options. You can create multiple profiles in the gateway administration console and associate different instances of gateway with different profiles. See “Creating a Gateway Profile” in the Sun Java System Portal Server, Secure Remote Access 6 2005Q1 Administrator’s Guide.
What is the Gateway logging user password Gateway Logging User Password		This allows administrators with non-root access to look at gateway log files.
Again		Re-enter the Gateway Logging User Password.

Gateway

Table 9 is a three column table that contains the checklist for gateway configuration. Column one lists the parameter. Column two contains the default value for the parameter. Column three lists the description.

Table 9 Gateway Configuration Checklist

Parameter	Default Value	Description
What is the Gateway protocol	https	The protocol used by the gateway. The gateway will usually communicate using Secure Sockets Layer (SSL).
What is the Gateway host	mygwbox.mydomain.com	The host name of the machine on which the gateway is installed.
What is the Gateway port	443	The port on which the gateway machine listens.
What is the Gateway IP Address	*gw-host-ip-address*	The IP Address should be that of the machine where Gateway is installed and not that of the Sun Java System Identity Server.

Table 9 Gateway Configuration Checklist

Parameter	Default Value	Description
What is the Gateway profile Gateway Profile Name	default	A gateway profile contains all the information related to gateway configuration, such as the port on which gateway listens, SSL options, and proxy options. You can create multiple profiles in the gateway administration console and associate different instances of gateway with different profiles. See "Creating a Gateway Profile" in the *Sun Java System Portal Server, Secure Remote Access 6 2005Q1 Administrator's Guide*.
What is the Gateway logging user password		This allows administrators with non-root access to look at gateway log files.
Gateway Logging User Password		
Again		Re-enter the Gateway Logging User Password.
What is the Portal Server Load Balancer URL Load balancer controlling Portal Server Instances.		If you are not using any Load Balancer URL then use the Portal Server URL. http://*fully-qualified-domain*:*port*/*portal-deploy-uri* For example, `http://myportalbox.mydomain.com:80/portal`
Certificate Information		
What is the name of your organization	MyOrganization	The name of your organization.
What is the name of your division	MyDivision	The name of your division.
What is the name of your city or locality	MyCity	The name of your city or locality
What is the name of your state or province	MyState	The name of your state
What is the two-letter country code	us	The two letter country code for your country.
What is the password for the Certificate Database		This can be any password you choose.
Again		Retype the Certificate Database password to verify.

Netlet Proxy

Table 10 is a three column table for the Netlet Proxy configuration checklist. Column one lists the parameter. Column two lists the default value. Column three contains the description.

Table 10 Netlet Proxy Configuration Checklist

Parameter	Default Value	Description
What is the Netlet Proxy protocol	https	The protocol used by the Netlet Proxy. The Netlet Proxy will usually communicate using Secure Sockets Layer (SSL).
What is the Netlet Proxy host	myportalbox.mydomain.com	The host name of the machine on which Netlet Proxy is installed.
What is the Netlet Proxy port	10555	The port on which the Netlet Proxy listens.
What is the Netlet Proxy IP Address	*host-ip-address*	The IP address should be that of the machine where Netlet Proxy is installed and not that of Sun Java System Identity Server.
What is the Gateway profile Gateway Profile Name	default	Specify the same profile name specified when you installed Portal Server or Secure Remote Access support. See “Creating a Gateway Profile” in the *Sun Java System Portal Server, Secure Remote Access 6 2005Q1 Administrator’s Guide* for more information.
What is the Gateway logging user password Gateway Logging User Password		This allows administrators with non-root access to look at gateway log files.
Again		Re-enter the Gateway Logging User Password.
What is the Portal Server Load Balancer URL Load balancer controlling Portal Server Instances.		If you are not using any Load Balancer URL then use the Portal Server URL. http://*fully_qualified_domain*:*port*/*portal_deploy_uri* For example `http://myportalbox.mydomain.com:80/portal`
Certificate Information		
What is the name of your organization	MyOrganization	The name of your organization.
What is the name of your division	MyDivision	The name of your division.
What is the name of your city or locality	MyCity	The name of your city or locality

Table 10 Netlet Proxy Configuration Checklist

Parameter	Default Value	Description
What is the name of your state or province	MyState	The name of your state
What is the two-letter country code	us	The two letter country code for your country.
What is the password for the Certificate Database		This can be any password you choose.
Again		Retype the Certificate Database password to verify.

Rewriter Proxy

Table 11 is a three column table that contains the Rewriter Proxy configuration checklist. Column one lists the parameter. Column two lists the default value. Column three contains the description.

Table 11 Rewriter Proxy Configuration Checklist

Parameter	Default Value	Description
What is the Rewriter Proxy protocol	https	The protocol used by the Rewriter Proxy. The Rewriter Proxy will usually communicate using Secure Sockets Layer (SSL).
What is the Rewriter Proxy host	myportalbox.mydomain.com	The host name of the machine on which Rewriter Proxy is installed.
What is the Rewriter Proxy port	10443	The port on which the Rewriter Proxy listens.
What is the Rewriter Proxy IP Address	*host-ip-address*	The IP address should be that of the machine where Rewriter Proxy is installed and not that of Sun Java System Identity Server.
What is the Gateway profile Gateway Profile Name	default	Specify the same profile name specified when you installed Portal Server or Secure Remote Access support. See “Creating a Gateway Profile” in the *Sun java System Portal Server, Secure Remote Access 6 2005Q1 Administrator’s Guide* for more information.
What is the Gateway logging user password Gateway Logging User Password		This allows administrators with non-root access to look at gateway log files.
Again		Re-enter the Gateway Logging User Password.

Table 11 Rewriter Proxy Configuration Checklist

Parameter	Default Value	Description
What is the Portal Server Load Balancer URL Load balancer controlling Portal Server Instances.		If you are not using any Load Balancer URL then use the Portal Server URL. http://*fully-qualified-domain*:*port*/*portal-deploy-uri* For Example, `http://myportalbox.mydomain.com:80/portal`
Certificate Information		
What is the name of your organization	MyOrganization	The name of your organization.
What is the name of your division	MyDivision	The name of your division.
What is the name of your city or locality	MyCity	The name of your city or locality
What is the name of your state or province	MyState	The name of your state
What is the two-letter country code	us	The two letter country code for your country.
What is the password for the Certificate Database		This can be any password you choose.
Again		Retype the Certificate Database password to verify.

For information on post-installation tasks see "Portal Server Post-Installation Tasks" on page 23.

Configuring Portal Server in Silent Mode

To configure the Portal Server using the samplesilent file, modify the pssamplesilent file located at *PortalServer-base*/`config` and execute the psconfig batch file.

1. As root in a terminal window, go to the directory that contains the psconfig batch file:

   `cd` *PortalServer-base*`/config`

2. Type:

   `psconfig -s -c` <component name>

For information on post-installation tasks see "Portal Server Post-Installation Tasks" on page 23

Portal Server Post-Installation Tasks

Post-installation tasks need to be performed for each of the following components:

- Portal Server
- Secure Remote Access
- Gateway
- Netlet and Rewriter Proxy

Portal Server

To access the Portal Server or the Identity Server administration console the directory server and the web container must first be started.

The following post-installation tasks depend on the type of web container on which you deployed the Portal Server.

- Sun Java System Web Server
- Sun Java System Application Server

Sun Java System Web Server

To start the Sun Java System Web Server:

1. Start the web instance in Windows Services:

or

1. Access the Sun Java System Web Server administration console.
2. Click Apply Changes to restart the web container.

Sun Java System Application Server 8.1

To configure the Application Server Instance, do the following:

1. Stop the domain instance. In a terminal window, type:

   AppServer-base`\bin\asadmin.bat stop-domain` *domainname*

   For example

   ```
   C:\Sun\ApplicationServer\bin\asadmin.bat stop-domain domain1
   ```

2. Start the domain instance. In a terminal window, type:

   ```
   AppServer-base\bin\asadmin.bat start-domain --user
   ```

   administrator-user-name --password administartor-user-password domainname

   For example,

   ```
   C:\Sun\ApplicationServer\bin\asadmin.bat start-domain --user admin --password
    password domain1
   ```

Secure Remote Access

When using the Portal Server with the gateway, the gateway Certificate Authority (CA) certificate must be added to the Portal Server trusted CA list, regardless of whether the Portal Server is running in HTTP or HTTPs mode.

When a user session time out or user session logout action happens, the Sun Java System Identity Server sends a session notification to the gateway. Even when the Sun Java System Identity Server is running in HTTP mode, it will act as an SSL client using HttpsURLConnection to send the notification. Since it is connecting to an SSL server (the gateway), it should have the gateway CA certificate as part of the Trusted CA list or it should have an option to allow self signed certificate.

NOTE The method for adding the CA to the trusted CA list depends on the protocol handler defined.

To create HttpsURLConnection, the Java Virtual Machine (JVM™) property `-Djava.protocol.handler.pkgs` needs to be set.

If Portal Server is running on the Sun Java System Web Server, Sun Java System Application Server, or BEA WebLogic Server, this property is correctly set to com.iplanet.services.com by default. The Sun Java System Identity Server package has the implementation of HttpsURLConnection and it provides an option to accept self-signed certificates from any SSL server by adding the flag com.iplanet.am.jssproxy.trustAllServerCerts=true in the `AMConfig.properties` file.

The -Djava.protocol.handler.pkgs is not set by default for the IBM WebSphere Application Server. The HttpsURLConnection implementation for supported application servers must use their own default handler (this could be JSSE or custom SSL implementation).

Configuring Multiple Gateways on Multiple Portals

When installing a second gateway on a second portal, you must manually update the Forward Cookie URLs value to point to the second Portal.

1. Log in to the Access Manager Administration Console.

2. Select the Service Configuration tab.
3. Click Gateway.
4. Add the second Portal to the Forward Cookie URLs list.

Starting and Stopping the Gateway

1. Start the gateway using the following command:

   ```
   Net Start SRA.Gateway.new-profile-name
   ```

   default is the default name of the gateway profile that is created during installation. You can create your own profiles later, and restart the gateway with the new profile. See "Creating a Gateway Profile" in Chapter 2 of the *Sun Java System Portal Server, Secure Remote Access 6 2005Q1 Administration* Guide.

NOTE This step is not required if you chose y for the Start Gateway after installation option during the gateway installation.

Netlet and Rewriter Proxy

Before starting the Netlet Proxy and the Rewriter Proxy, ensure that the gateway profile is updated with the Netlet Proxy and the Rewriter Proxy options.

- If you did not choose the option to start the Netlet Proxy during installation, you can start the Netlet Proxy manually:

  ```
  net start SRA.Netlet.default
  ```

- If you did not choose the option to start the Rewriter Proxy manually during installation, you can start it manually:

  ```
  net start SRA.rewriter.default
  ```

NOTE Ensure that you enable the Access List service for all users, to allow access through the gateway.

The Sun Java System Portal Server software NetFile needs jCIFS libraries (bundled as SUNWjcifs) for Windows access. This needs to be installed in Portal Server node only.

Verifying the Portal Server Installation

Access the Portal Server Administration Console and Desktop

To Access the Sun Java System Identity Server Administration Console

1. Open a browser.
2. Type `protocol://hostname.domain:port/amconsole`

   For example,

   `http://example.com:80/amconsole`
3. Enter the administrator's name and password to view the administration console.

   This is the name and password you specified at the time of installing the Sun Java System Identity Server software.

To Access the Portal Server Desktop

Verify the Portal Server installation by accessing the Desktop. Use the following URL to access the Desktop: `protocol://fully-qualified-hostname:port/portal-URI`

For example,

`http://example.com:80/portal`

When you access the Desktop, the Authless Desktop is displayed. This allows users accessing the Desktop URL to be authenticated automatically and granted access to the Desktop.

If the sample Portal Desktop displays without any exception, then your Portal Server installation is good.

Verifying the Gateway Installation

1. Run the following command to check if the gateway is running on the specified port (the default port is 443):

   ```
   net start
   ```

   If the gateway is not running, start the gateway in the debug mode, and view messages that are printed on the console. Use the following command to start the gateway in debug mode:

   ```
   net start debug
   ```

Also view the log files after setting the gateway.debug attribute in the platform.conf.profilename file to message. See the section Understanding the `platform.conf` File in Chapter 2, "Administering Gateway" in the *Sun Java System Portal Server, Secure Remote Access 6 2005Q1 Administration Guide*, for details.

2. Run the Portal Server in secure mode by typing the gateway URL in your browser:

   `https://`*gateway-machine-name*`:`*portnumber*

   If you have chosen the default port (443) during installation, you need not specify the port number.

3. Login to the Identity Server administration console as administrator using the user name amadmin, and using the password specified during installation.

You can now create new organizations, roles, and users and assign required services and attributes in the administration console.

Bugs Fixed in This Release

The following table describes the bugs fixed in Portal Server 6 2005Q4.

Table 12 Fixed Bugs in Portal Server 6 2005Q4

Bug ID	Description
6302434	JES3 SF b12c:Lack of two links in "My Application" channel on CCJK locales.
6294644	Unable to display "JSPTableContainer" page it shows The page cannot be displayed.
6316742	pdeploy does not take WAR argument as documented.
6316749	dpadmin does not work on windows.
6317223	pdeploy does not undeploy from web container.

Important Information

This section contains the latest information that is not contained in the core product documentation. This section covers the following topics:

- Installation Notes
- Deprecated Features
- Compatibility Issues

Installation Notes

Portal Server

For Java Enterprise System 6 2005Q4, Portal Server can be installed and configured to run with either:

- Access Manager installed and configured in the same installation session on the same physical machine
- Access Manager previously installed and configured on a separate machine

To Run the Liberty Samples

The liberty samples are designed for a Portal Server and Access Manager installation on same system.

To run the Liberty samples on a Portal Server/Access Manager separated install, do the following:

1. Make sure the SP_HOST_DOMAIN value in `configSP.sh` points to the Access Manager full install host.
2. In the administration console of Access Manager that is acting as Service Provider, set the Provider Home Page to `URL=http://`*portal-server-host*`:`*port*`/portal/dt`

   To set this value:

   a. Select the federation management tab.

   b. Select the service provider in navigation frame.

   c. Select provider in the drop-down in data frame.

   d. Scroll down to Access Manager Configuration section.

   e. Set the Provider Home Page to `URL=http://`*portal-server-host*`:`*port*`/portal/dt.`

   For Liberty Sample 3 only, perform Step 3 and Step 4.
3. Change “Single Sign-On Failure Redirect URL” and set it to `http://`*portal-server-host*`:`*port*`/portal/dt?libertySSOFailed=true`

   To set this value:

   a. Select the federation management tab.

b. Select the service provider in navigation frame.

c. Select provider in the drop-down in data frame.

d. Scroll down to Access Manager Configuration section.

e. Set the Single Sign-On Failure Redirect URL to
`http://`*portal-server-host*`:`*port*`/portal/dt?libertySSOFailed=true`

4. Set the PreLogin URL to
`http://`*portal-server-host*`:`*identity-server-port*`/amserver/preLogin?metaAlias=is-host&goto=http://`*portal-server-host*`:`*portal-server-port*`/portal/dt`

To set this value:

a. Go to Identity Management, Select Users from the drop down Menu.

b. Click on authlessanonymous user and then select Portal Desktop from the View drop down list in the Navigation Frame.

c. Click on the Edit link.

d. Click on Manage Channels and Containers.

e. Click on Edit properties of the Login Channel

f. Set the PreLogin URL to
`http://`*portal-server-host*`:`*identity-server-port*`/amserver/preLogin?metaAlias=is-host&goto=http://`*portal-server-host*`:`*portal-server-port*`/portal/dt`.

5. Set the following in the `AMConfig.properties` file on the Portal Server host:

- `com.iplanet.am.notification.url=http://`*portal-server-host*`:`*port*`/servlet/com.iplanet.services.comm.client.PLLNotificationServlet`
- `com.iplanet.am.session.client.polling.enable=false`

Web Containers

For detailed instructions on installing the Sun Java Server component products, refer to the *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* at
http://docs.sun.com/app/docs/doc/819-4280.

Patch Requirement Information

The following table gives the numbers and minimum versions for the alignment patches. All patches referred to in this section are the minimum version number required for upgrade. It is possible that a new version of the patch has been issued since this document was published. A newer version is indicated by a different version number at the end of the patch. For example: 123456-04 is a newer version of 123456-02 but they are the same patch ID. Refer to the README file for each patch listed for special instructions.

To access the patches, go to http://sunsolve.sun.com.

Table 13 Portal Server 6 2005Q4 Alignment Patches Required For Windows

Patch Number	Patch Description
121523-01	Windows (MSI): Shared Components Patch
121532-01	Windows (MSI): Sun Java™ System Portal Server 6 2005Q4

For detailed information about Upgrade procedure of the Portal Server from JES3 to JES4 refer *Sun Java Enterprise System 2005Q4 Upgrade Guide for Microsoft Windows* located at http://docs.sun.com/app/docs/doc/819-4461.

Compatibility Issues

Deprecation Notifications and Announcements

Portal Server CLIs

Existing Portal Server command line utilities are deprecated, and their functions will be replaced with a single Portal Server command line utility in a future release. The following Portal Server command line utilities are deprecated, and their functions will be replaced with a single Portal Server command line utility in a future release:

- deploy
- dpadmin
- gwmultiinstance
- multiserverinstance
- par
- pdeploy

- rwadmin
- rwpmultiinstance
- undeploy

Administration Console

The existing Portal Server administration console is deprecated, and its functions will be replaced with a new Portal Server management console in a future release.

Portal Server Desktop Template Container Provider

The Portal Desktop Template Container Provider interface is being deprecated and will be removed in a future release. Interface components being deprecated include:

- Global display profile Desktop template container provider definitions
- Desktop template container provider presentation files
- Desktop template container provider resource bundles
- Desktop template container provider presentation images

Installation Issues

When you run the Java Enterprise System Installer, Access Manager 7 2005Q4 has two installation types (or modes):

- Compatible (6.x) type supports Access Manager 6 features, including the Access Manager 6 Console and directory information tree (DIT).
- Enhanced (7.x) type supports Access Manager 7 features, including the new Access Manager 7 Console.

Portal Server, Messaging Server, Calendar Server, Instant Messaging, and Delegated Administrator are not compatible with Access Manager 7 2005Q4 Enhanced (7.x) type.

If you are installing Access Manager with Portal Server, Messaging Server, Calendar Server, Instant Messaging, or Delegated Administrator, you must select the Access Manager Compatible (6.x) installation type (which is the default value).

Deprecated Features

The NetMail application is being deprecated in this release of the Sun Java System Portal Server product.

Documentation Updates for Portal Server 6 2005Q4

The following sections provide updates and additional documentation for the Portal Server 6 2005Q1 documentation set.

Portal Server Administration Guide

The settings on the Instant Messaging Channel edit page have changed. The Desktop user now has to configure only two settings (if the administrator has not configured the channel for a single Instant Messaging Server).

The two Instant Messaging Server settings are now:

- Instant Messaging Host
- Instant Messaging Port

Secure Remote Access Administration Guide

The following items are not documented in the online help or *Sun Java System Portal Server 6 2005Q1 Secure Remote Access Administration Guide*, but are part of the Access Manager administration console.

- Gateway -> Core -> Gateway Minimum Authentication Level is not documented in the online help or the administration guide.
- The Proxylet rules (as shown on the Access Manager console) are not documented in the online help or the administration guide. For information on configuring Proxylet rules, see "Proxylet Rules."

Enabling Basic HTTP Authentication

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
4. The Gateway page is displayed.
5. Select the gateway profile for which you want to set the attribute.
6. The Edit Gateway Profile page is displayed.
7. Click the Core tab.
8. Select the Enable HTTP Basic Authentication checkbox to enable HTTP basic authentication.
9. Click Save to record the change.

10. Restart the Gateway from a terminal window:

    ```
    net start SRA.Gateway.gateway-profile-name
    ```

Proxylet Rules

A Proxylet rules field has been added to the Access Manager administration console.

The Proxylet rules specify the domain and proxy settings in the Proxy Auto Configuration (PAC) file.

To modify the Proxylet rules, do the following:

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Proxylet under SRA Configuration.
7. Click Edit.
8. Enter the proxy-host and proxy-port, using the following syntax:

   ```
   [Protocol:]Domain1[,Domain2,...]:IP or Host:Port
   ```

   where,

   Protocol – can contain http/ftp/https. (This field is optional).

   Domain – is any domain such as sun.com. Multiple domains are separated by a comma.

   IP – is the IP address of the domain.

   proxy-host – proxy server used for this domain(s)

   proxy-port – proxy server port
9. Click Save.

The following special constructs allow dynamic insertions into the rule.

If a rule contains the string `proxylet-host:proxylet-port` as the proxy server, then the generated PAC file replaces the string with the host and port of Proxylet.

Online Help

The Search channel Help page states in the Advanced Search section:

- URL – The Uniform Resource Locator (web address) of the document. Keep in mind the following points when specifying URLs:
  - The `http://` portion of the address must be entered if you are using the *Is* or *Begins with* operators.

The *Is* and *Begins with* operators are no longer used.

Accessibility Features for People With Disabilities

To obtain accessibility features that have been released since the publishing of this media, consult Section 508 product assessments available from Sun upon request to determine which versions are best suited for deploying accessible solutions. Updated versions of applications can be found at: `http://sun.com/software/javaenterprisesystem/get.html`.

For information on Sun's commitment to accessibility, visit `http://sun.com/access`.

Known Issues and Limitations

This section describes the known issues and limitations of Portal Server 6 2005Q1 for Windows. This section consists the following:

dpadmin

dpadmin utility is not displaying the contents with 'list' & ‘merge’ options (6341854)

The `dpadmin` command line utility is not returning the command line output for ‘list’ & ‘merge’ options.

Workaround

After invoking the `dpadmin` command with ‘list’ & ‘merge’ options, list/merge.txt file will be generated in the same location; this file will contain the output of the command.

For example:

```
C:/Sun/PortalServer/bin>dpadmin list -u amadmin -w admin123 -b –g
```

This will create list.txt in `C:/Sun/PortalServer/bin` directory. For merge option, it will create `merge.txt` file.

Installation

Gateway redirection not happening in any multi-session installation. (4971011)

Regardless of the installation mode, gateway redirection does not occur during a multi-session installation.

Workaround

1. Launch a Portal Server browser and access the amconsole.
2. Under “Service Configuration” tab, select “gateway.”
3. In the lower right corner of the window, click the “default” and the “security” tab.

4. Then, add a URL like `http://IS-Host:port/amserver/UI/Login` into "Non-authenticated URLs:" field.

   An example URL is `http://boa.prc.sun.com:80/amserver/UI/Login`.

5. Finally, restart the Portal gateway by doing the following as superuser:

   ```
   net start SRA.Gateway.default
   ```

Configurator

The Portal Server configurator does not work if Identity Server is running its Directory Server in LDAPS. (5044585)

Workaround

Disable the SSL for DS and update the AMConfig.properties with non SSL port to successfully install portal server.

Proxylet

iNotes and Microsoft Exchange 2000 SP3 are not supported with Proxylet. (no issue ID)

Page can not be displayed in iNotes when performing some functionalities. (6190570)

An error occurs with a message "Page cannot be displayed" in iNotes for the following modules:

- Mail
- Appointments
- To Do
- Contacts
- Notebook

This message occurs when using the Save and Delete buttons.

Workaround

None.

NetFile help does not come up after Proxylet is downloaded. (6180420)

If Proxylet and NetFile are downloaded, the NetFile Help is not displayed and an exception is thrown in the Java console.

Workaround

None.

Unable to access the Portal Desktop in SSL mode after Proxylet is downloaded. (4990035)

The Portal Desktop can not be downloaded after Proxylet is downloaded if Portal Server is in SSL mode.

Workaround

None.

No help provided for the Proxylet rules. (5107957)

See "Documentation Updates for Portal Server 6 2005Q4" for instructions on configuring Proxylet rules.

Accessing amconsole for a user from Proxylet gives "Action cancelled" page. (6190566)

If you log in to the Portal Desktop through the gateway, then load Proxylet, and then try to access the Administration console, the view list box will return an "Action Cancelled" page.

Workaround

None.

Portlet

The portlet session is not stored across managed servers in a cluster. (6190600)

HTTP session failover for portlets doesn't work.

Workaround

None.

Online Help

The Online Help button for the Address Book channel is missing. (6193284)

The “Help” icon for AddressBook channel displays a “page not found” exception in the Browser.

Workaround

None.

Communication Channels

The Mail Channel does not display the login page. (4873659)

The Mail Channel will not successfully launch the Messenger Express client when the ipsecurity setting of the Sun Java System Messaging Server is set to “yes.” In order for the Mail Channel to successfully launch the Messenger Express client, the ipsecurity setting of the Messaging Server must be set to “no.”

Workaround

Set the ipsecurity setting of the Messaging Server to “no.”

The MailProvider will not work with SSL secured IMAP. (4919693)

The current MailProvider implementation will not work with SSL secured IMAP.

Workaround

After configuring the IMAPS channel, if the channel shows error on Portal Server with Web Server as container, change the mail.jar as the first entry in the CLASSPATH.

To add the mail.jar file as the first file in the classpath:

1. Open the file `ws-install-dir/https-ws-instance-name/config/server.xml`
2. Change the mail.jar file to be the first entry in the classpath.
3. Restart the Web Server.

A newly created Address Book channel does not appear on the Desktop.(4922220)

The Address Book service must first be configured. Because the AddressBookProvider is not pre-configured, any channel the user creates based on the AddressBookProvider will not appear on the user's Desktop or on the Content link unless the AddressBookProvider has been configured. See "Configuring the Address Book Channel" section in Chapter 17, and "SSO Adapter Templates and Configurations" in Appendix A of the Sun Java System Portal Server Administration Guide for more information.

Creating channels based on the other communications channels in the pre- populated, user-defined channels set may result in the created channel displaying the message: "Please specify a valid configuration." Although the other Communication Channels are defined to a sufficient extent to appear on the user's Desktop, they require additional administrative tasks in order to ascertain which back-end service to use.

Additionally, the communication channels require the desktop user to specify back-end credentials (such as user name and password) after the administrative tasks are completed. The desktop user can specify these values in the channel by using the channel's Edit button.

NOTE The userDefinedChannels set might need to be administered on a per install basis because this set includes references to back-end services which might not apply to your particular setup. For example, all Lotus Providers in this set refer to interaction with Lotus back-end services for the communication channels which do not apply if none in the Portal user base will be using Lotus back-end services.

The Calendar channel will not launch if the domain name is not set. (4946959)

If the Server name in the Calendar channel does not include the fully qualified domain name, the Calendar channel does not launch.

Workaround

Verify that the fully qualified host name is used for the Server name setting.

The SSO Adapter Configuration Does Not Support Distributed and Redundant Personal Address Books. (5020452)

Prior version of the SSO Personal Address Book (PAB) Adapter expects the container o=pab to co-exist within the User and Group directory. Portal Server6 2005Q1 introduced support in the "SUN-ONE-ADDRESS-BOOK" adapter template to specify the PAB directory server. The following properties are now supported:

ugHost: LDAP host name for PAB lookup

ugPort: LDAP port for PAB lookup

Workaround

These properties need to be manually added to the "SUN-ONE-ADDRESS-BOOK" SSO adapter template by the admin in the Identity Server Administration Console.

1. Log in to the Access Manager administration console.
2. Select Service Configuration > SSO Adapter.
3. Select "SUN-ONE-ADDRSS-BOOK" as the SSO Adapter template.
4. Select Edit Properties > New Default.
   a. Specify "ugHost" for Name.
   b. Specify the LDAP host name.
   c. Select Create.
5. Select Edit Properties > New Default.
   a. Specify "ugPort" for Name.
   b. Specify the LDAP port.
   c. Select Create.

The links in the Mail channel lead to the Portal Desktop instead of the Mail Client. (5053733)

When a user selects the Logout link from the Mail Channel, the logout page for the client logout page is not displayed (instead the Portal Desktop page is displayed).

Workaround

If this problem occurs, perform the following steps:

1. Refresh the Portal Desktop.
2. Click the Launch Mail link in the previous portal page, and the Mail client can launch again.

If you want a webmail login page after a logout (instead of the Portal desktop) do the following.

1. Change the following code on the messaging server.

The file `<messaginserve-installdir>/config/html/main.js` has a method restart(), which is called from exit(), which in turn is called from logout().

```
function restart() {
    var ref = window.document.referrer != '' ? window.document.referrer : '/'
    if (ref.indexOf('mail.html') > 0)
    ref = '/'
    var ind = ref.indexOf('?')
```

```
    self.location.replace(ind > 0 ? ref.substring(0, ind) : ref)
}
```

Change the first line and provide the url of the mail server login page as follows:

```
var ref = window.document.referrer != '' ? "http://pavoni:2080" : '/'
```

2. Restart the mail server.
3. Clear the browser cache.

To test:

1. Click Launch Mail.
2. Log out from webmail.
3. Click Launch Mail, which will take you to the webmail login page as the old session is not valid.

On clicking on the Launch Mail Link of Universal Web Client (UWC) Mail Channel does not open MailBox. (6179802)

On clicking on the link of launch mail it takes to Web Server index page instead of the user's inbox.

In Java Server Enterprise 3 the Portal Mail channel can launch the UWC from the Portal Desktop.

A new channel has been added called "UWCMail" and is based on the MailProvider. The UWCMail channel is available in the default organization or root suffix but is not associated with a Container out of the box. The UWCMail channel must be added to a container.

The UWCMail channel defines the following properties:

- title
- description
- ssoAdapter
- applicationHelperEdit
- applicationHelperURL

The SSO adapter configuration is sunUWCMail and the SSO adapter template is `SUN-UWC-MAIL`.

Workaround

To use the new UWCMail channel, add the UWCMail channel to a container for the channel to be visible on the desktop.

1. From the Access Manager Administration console, add the UWCMail channel to the My Front Page Tab.

2. Edit the UWCMail channel and specify the server settings. For example, login to the Portal Desktop as a new user and edit the UWCMail channel by specifying the following values:

- server name: `messaging-server-name`
- imap server port: `messaging-server-imap-port`
- user name: `uid`
- user password: `password`
- smtp server name: `messaging-server-smtp-server-name`
- smtp server port: `messaging-server-smtp-port`
- client port: `messenger-express-client-port`
- mail domain: `hosted-domain`

The calendar does not come up on the UWC Calendar Channel. (6179806)

In Java Server Enterprise 3 the Portal Calendar channel can launch the UWC from the Portal Desktop.

A new channel has been added called UWCCalendar and is based on the CalendarProvider. The UWCCalendar channel is available in the default organization or root suffix but is not associated with a Container out of the box. The UWCCalendar channel must be added to a container.

The UWCCalendar channel defines the following properties:

- title
- description
- ssoAdapter
- ssoEditAttributes (exposes clientHost and clientPort)
- applicationHelperEdit
- applicationHelperURL

The SSO adapter configuration is "sunUWCCalendar" and the SSO adapter template is "`SUN-UWC-CALENDAR`."

Workaround

To use this new channel:

Add the UWCCalendar channel to a container for the channel to be visible on the desktop.

1. From the Access Manager Administration console, add the UWCCalendar channel to the My Front Page Tab.

2. Edit the UWCCalendar channel and specify the server settings. For example, login to the Portal Desktop as a new user and edit the UWCCalendar channel by specifying the following values:

- server name: `calendar-server-name`
- server port: `calendar-server-port`
- user name: `uid`
- user password: `password`
- client server name: `uwc-client-server-name`
- client port: `uwc-client-port`

UWC Address Book is not being displayed on the UWC AddressBook channel. (6179807)

The SSO adapter implementation, WabpSSOAdapter, is using port instead of clientPort for the back end connection to the Address Book Server. This causes the Portal UWC Address Book to fail when the UWC client is not installed on port 80.

Workaround

You can workaround this problem by doing one of the following:

- Install the UWC client on port 80
- Set the SSO adapter template or configuration property port and the value to be the same as clientPort.

To set the SSO adapter template or configuration property port and the value to be the same as clientPort is to add the "port" as a "Merge" property specified at the Organization level. The Channel does not expose the "port" on the Channel's edit page.

To add the port as a "Merge" property:

1. Log in to the Access Manager Administration console.
2. Select Service Configuration.
3. Select SSO adapter.
4. Select Edit Properties... for SUN-UWC-ADDRESS-BOOK.
5. Select New Merge and specify:

   Name: port
6. Select Create.
7. Select Finished.

8. Select Identity Management.
9. Select the organization.
10. Select Services.
11. Select SSO adapter.
12. Select Edit Properties... for sunUWCAddressBook and specify the properties.
13. Select New Default and specify the port value and select Save.

NOTE If there are existing users with SSO adapter attributes written at the User level, this solution might not work since the existing users do not inherit the Organization level changes to the SSO adapter configuration. Instead, the SSO adapter template can be updated with the "host" and port defined as Default properties.

Microsoft Calendar and Microsoft AddressBook throw "Content not available" error. (6213120)

An error message stating that content is not available may be displayed when configuring the Microsoft Calendar and Address Book channels on a WebLogic server. This problem can occur when other files take precedence over the `jintegra.jar file`.

Workaround

Add the `jintegra.jar` file as the first file to the classpath.

Lotus Address Book and Calendar does not work with old NCSO.jar. (6216069)

Lotus Address Book and Calendar need the latest version of NCSO.jar to work.

Workaround

Use the latest version of Domino, for example NCSO.jar from Domino 6.5.1.

Secure Remote Access

Calendar links not accessible via Portal Secure Remote Access. (#4929710)

If the desktop user selects to display non-secure items, the Calendar desktop shows. However, none of the links appear. If the desktop user selects not to display non-secure items, the Calendar desktop does not show. The effect is that the Calendar desktop items can not work through the gateway.

Workaround

Edit `ics.conf` on the Calendar Server. Change the line, render.xslonclient.enable = “yes”

The Proxylet rules edit page gets displayed very late through the gateway. (6181714)

When invoking the Proxylet rules edit page through the gateway, the response is very slow, and Proxylet rules page takes a while to be displayed.

Workaround

None.

Gateway

Can not login to Portal Server through the gateway when Portal Server components are in separate sessions. (6214635)

The problem occurs when Portal Server components are installed in separate sessions.

Workaround

When you add Portal Server services in separate sessions, ensure that:

- All Portal Servers are listed under Gateway > Core in the administration console.
- All Portal Server URLs are listed in the Non-authenticated URLs under Gateway >Security.

After stopping and starting the Application Server, users can not log in through the Gateway. (6191449)

If the Portal Server is using the Sun Java System Application server as its web container, stopping and restarting the web container in some cases causes an error that prevents the user from being able to log in to the Portal Server through the gateway.

Workaround

Stop and restart the gateway. In a terminal window, type:

```
net stop SRA.Gateway.instancename

net start SRA.Gateway.instancename
```

NetFile

A local file can not be opened in NetFile. (5033644)

A local file can not be opened in NetFile because the file's base directory is removed. When a user expands a file directory tree and tries to find a local file such as `/tmp/1.txt` and the user clicks Open, the alert dialog pops up with the following error message: The file `/1.txt` can not be found. Please check the location and try again.

Workaround

None.

Netlet

Netlet fails to load after relogin. (2102626)

If Netlet is loaded, and you log out of the Desktop and then try to log back in, you will not be able to restart Netlet.

Workaround

Close the browser and open a new browser to load it again.

Microsoft Internet Explorer crashes while Loading Netlet with Default Microsoft JVM. (2120110)

When Netlet is loading, a security message is displayed. Clicking "yes" to continue causes Microsoft Internet Explorer to crash.

Workaround

None.

Netlet does not work if a Pac file is specified in the browser option with Java 1.4.2. (6204073)

This problem can happen if the plug-in is not able to understand the format in which the pac file location is specified.

Workaround

The format for the location of pac file needs to be specified for various versions of Java.

Rewriter

When using Microsoft Exchange 2003, gif files are missing in some of the pages. (6186547)

Many interface image files are missing.

Workaround

None.

In iNotes, under the Contacts tab, the Help page is redirected to the Administration console. (6186541)

Clicking the Help button from the Contacts tab in iNotes displays the Administration console page instead of the Help page.

Workaround

None.

iNotes does not logout correctly. (6186544)

Clicking on logout in iNotes displays two options. Neither of these options will log out of iNotes.

Workaround

None.

Microsoft Exchange 2000 SP3 gives warning messages and action cancelled messages. (6186535)

The following actions in Exchange 2000 SP3 it causes security warning messages and Action cancelled messages:

- Clicking New tab under Mail.
- Selecting any item in the drop box list.
- Clicking New tab under Calendar.
- Clicking on Empty Deleted Items folder.
- Creating a new task.

Workaround

None

Microsoft Exchange 2003 returns a login page when clicking on the Calendar reminder page on the "open item" button. (6186528)

Workaround

None

When using Microsoft Exchange 2000 SP3, Moving or Copying messages to specific folders doesn't work. (6186534)

If you login to the Portal Server through the gateway, and you edit the bookmark channel with the Microsoft Exchange machine details, the Move/Copy buttons on the Microsoft Exchange interface produce the error "Operation could not be performed."

Workaround

None.

When using Microsoft Exchange 2000 SP3, selecting any item in the drop box list gives Action Cancelled message. (6186533)

If you log in to the Portal Server through the gateway, and you edit the bookmark channel with the Microsoft Exchange machine details, the mail and calendar drop box list on the Microsoft Exchange interface do not work. An "Action cancelled" message is displayed.

Workaround

None.

When using Microsoft Exchange 2000 SP3, Clicking on empty deleted items folder displays Action Cancelled. (6186540)

If you log in to the Portal Server through the gateway, and you edit the bookmark channel with the Microsoft Exchange machine details, deleted items can not be emptied in the Microsoft Exchange interface.

Workaround

None.

Documentation

Chapter 9 of the Sun Java System Portal Server 6 2005Q1 Secure Remote Access Administration Guide contains an inaccurate title for subsection. (no issue ID)

The subsection "Enable Rewriting of All URLs" should read "Enable Rewriting of All URIs."

The rewriter documentation should state that only http and https are supported. (5082368)

The section “Supported URLs” in chapter 12 “Administering the Rewriter Service” of the Sun Java System Portal Server 6 2005Q1 Administration Guide states that “Rewriter supports rewriting of all standard URLs as specified by RFC-1738.” This information is incorrect. Rewriter supports only HTTP and HTTPs URLs.

Workaround

None.

Mobile Access

The native JSP desktop does not handle the case when the frontPageSize exceeds the maximum deck size (Wm1DeckSize). Please refer to http://docs.sun.com/source/817-5323/index.html. (4950078)

Workaround

None.

Mail is sometimes displayed as HTML document. (4938743)

Email messages sent with HTML in the body are displayed with the HTML source.

Workaround

No workaround is available. However, to preserve the original formatting of messages, change the settings for mail application to plain text.

To do this in Netscape, use the mail client to complete the following tasks:

1. From the Edit option on the menu > Preferences > Mail & Newsgroups
2. From the Mail & Newsgroups menu, click Send Format and it will display the Send Format Preferences.
3. Select Convert the Message to Plain Text option and click OK.

For the Outlook Express client:

1. Select tools -> Options -> Send.
2. In the "Mail Sending Format" section, pick "Plain text" instead of "HTML".
3. Select Save.

The default value shown in the Document Root Directory of the Portal Server Configuration Panel during JES installer is incorrect. (6203728)

This issue arises when Portal Server is installed independently after other dependent products have been installed and configured and while installing Portal Server on a separate instance other than that of Access Manager.

Workaround

If the Web container on which the Portal Server is deployed is Sun Java Enterprise System Web Server, make sure that the correct path for Document Root Directory is entered in the Portal Server Configuration Panel that appears while running the JES installer.

For example, if you have installed the Sun Java Enterprise System Web Server in `*C:\Sun\WebServer*`, then the Document Root Directory would be `*C:\Sun\WebServer\docs*`.

The Contents link in the Mobile Application Services page displays "bad request" message. (5043783)

A bad request error occurs only when you click the Contents link in the Help page for the Services option. This happens while accessing Help from the Administration Console for Access Manager > Identity Management tab.

Workaround

None.

The Views: Rule for Date Contains does not work. (6212818)

Date search using a string format as dd/mm/yyyy in the search filter will not work.

Workaround

IMAP stores dates in this format: Wed, 04 Jun 2003 13:06:55 -700. Search filters using this format should work.

When a View name contains a space, the View link does not display. (6212854)

The View link does not display on a device if the View name begins or ends with a space. Clicking Edit View results in a null pointer exception.

Workaround

Do not use leading or trailing spaces in view and rule names.

URL forwarding to minimize URL length for mobile and desktop users. (5020380)

URL forwarding will be required to minimize URL length for desktop and phone users.

Workaround

You can use redirection to seamlessly send users requesting a document on one server to a document on another server. For example, if the user types `http://home.suncom.net`, it is without a destination URI. This prefix is not interpreted and translated in the web server administration console as the following:

```
Prefix: /index.html
```

To fixed URL:

```
http://home.suncom.net/amserver/UI/Login?module=MSISDN
```

The web server will forward all Portal URLs with an URI /index.html to the fixed URL. Check the web server instance obj.conf file for this entry:

```
NameTrans fn="redirect" from="/index.html"

url-prefix="http://portal.mobile.suncom.net/amserver/UI/Login?module=MSISDN"
```

Mobile Mail & AddressBook Preferences are not documented. (5011510)

Workaround

None.

Using Application Server 7.1 UR1 in the cookieless mode. (5107310)

Workaround

When using Application Server 7.1 Update Release 1 (UR1), if users need to use the cookieless mode, add the following JVM option to the Application Server configuration:

-DJ2EEDecodeURI

Invalid Rule/View URL Syntax error when rule is applied properly on a browser using Japanese language. (6190033)

When users add a rule on a browser using Japanese language, “Invalid Rule/View URL Syntax” error message is displayed. This error does not occur on browsers using English language.

Workaround

None.

Web server always sets content type to text/html when servlet filter is set. (6174754)

When a user deploys the Portal Gateway with an Access Manager instance, which is deployed on Sun Java System Web server, the Web Server always sets the content type to text/html. The following workaround provided will help users to work through the Web Server bug 6173293, which causes gateway bug 5093084.

Workaround

Make the following change to the obj.conf file in web-server-instance/config directory.

1. Change the ObjectType from:

   ```
   ObjectType fn=force-type type=text/html
   ```

   to:

   ```
   # ObjectType fn=force-type type=text/html
   ```

2. Restart the web server after you have made this change.

Changing client type in palmOne Treo 180 device to cHTML. (6190070)

When a palmOne Treo 180 mobile device accesses Mobile Access, the contents are rendered using the WML markup language. The Treo 180 is a cHTML capable mobile device. Though the Treo180 devices are capable of displaying WML, cHTML is preferable because cHTML is a richer markup language.

Workaround

The following steps will enable you to change the client type to cHTML using amconsole:

1. Navigate your browser to `http://hostname:port/amconsole`.
2. Login as an administrator.
3. Click on Service Configuration tab -> Client Detection -> Client Types: Edit (on the right panel).

   The Client Manager is displayed.
4. Select the WML category to get the list of WML capable devices.
5. Edit UPG1_UP_4.0_(compatible__Blazer_1.0) and change the "Immediate parent type for this device" to cHTML.
6. Save the device settings, and then save global Client Detection settings.

For more information about changing Client types, see Using the Client Manager in Chapter 2, Managing Mobile Devices of the Sun™ Java System Portal Server, Mobile Access 6.2 Administrator's Guide.

Anonymous Portal login from a mobile throws a serious desktop error. (6184377)

When users access Portal Server using anonymous login from a mobile using XHTML or WML Browser or WML / XHTML Simulators the following error message is displayed.

"A serious error has occurred in the Desktop. This may have been caused by a mis-configuration on the server. Please report this problem to your administrator."

Workaround

None.

Views menu option from mail is not displayed on Mobile desktop. (6185041)

When using a CC/PP enabled phone, the correct device name may not be displayed in the "Mobile Devices" section of the Portal Desktop. Users will be unable to associate views with the device. It may not be possible for users to customize content or layout for the device. Using amconsole, the following workaround will enable the Views menu option on your mobile device.

Workaround

Users must add the device name manually to the user's profile. The correct device name for a CC/PP compliant device is the URL of the CC/PP profile with special characters replaced with "_" and with a "_" character at the beginning and the end. For example, if the URL is `http://developer.openwave.com/uaprof/OPWVSDK62.xml`, then the device name is `_http___developer.openwave.com_uaprof_OPWVSDK62.xml_`. The following steps describes how you can add the device name to the user's profile.

1. Navigate your browser to `http://hostname:port/amconsole`.
2. Login as an administrator.
3. Click on Users -> click a user -> Services -> Portal Desktop -> Edit -> Edit XML directly.
4. Locate the `<Collection name="selectedClients">` tag.

   This tag lists all the selected client devices.
5. Add the following tag:

   ```
   <String name="_http___developer.openwave.com_uaprof_OPWVSDK62.xml_" value=""/>
   ```
6. Save your changes.
7. Login to the Portal Desktop as an User.
8. New mobile device called

   `_http___developer.openwave.com_uaprof_OPWVSDK62.xml_` displays.
9. Attach a new mail view to this device.
10. Login using the Openwave 6.2 (xhtml) simulator.
11. The Views menu displays.

NOTE NOTE The string added to the selectedClients collection is the URL of the CC/PP profile, with special characters replaced with "_". You need to repeat the above steps for each CC/PP device you plan to support. The URL can be found either in the HTTP headers, or in the CCCPPClientDetector log file (in `C:\Sun\AccessManager\debug`).

No Online Help available for Mobile Mail Preferences. (6185112)

When users access Mobile Mail Preferences link by clicking Edit Mail from the Portal Desktop, no help is displayed for Mobile Mail Preferences.

Workaround

None.

Devices rendering HDML content display garbage for Japanese characters for detail pages for Calendar, Mail, and Address Book. (6191363)

When users view their Calendar, Mail, and Address Book the content gets corrupted for Japanese locale when viewing HDML content. For example, when users:

1. Login to mobile desktop. The contents are displayed and Japanese characters are also displayed.
2. Navigate to the Calendar. The Calendar page contents are displayed and Japanese characters are also displayed
3. View Calendar. The Japanese characters in the Calendar events get corrupted.

   Same problem happens for Mail and Address Book. Mobile desktop (top page) and the primary page of the Calendar, Mail, and Address Book are OK but when users are browsing the contents, the pages become garbage. For other types of content this issue does not appear.

Workaround

None.

Mail and calendar events sent in Japanese from browser, and then viewed on handset are corrupted and vice versa. (6191389)

While adding a Japanese calendar event from a mobile device, the event is displayed on a device but when displayed on a browser the Japanese characters gets corrupted. Also, when users add a Japanese event from a browser the event displays on a browser but gets corrupted when displayed

on a mobile device. Similarly, when users use a browser to send a mail in Japanese, and view the mail on a mobile device the characters are corrupted. When users send a mail from the mobile device the email is displayed on a device but gets corrupted when displayed on a browser.

Workaround

None.

Mobile Desktop does not appear properly (6368308)

While accessing the portal and amserver/UI/Login pages from the mobile, it will not appear properly.

Workaround

Workaround is possible in both Configure Automatically During Installation and Configure Manually After Installation mode of installations. However Configure Manually After Installation is recommended.

Saving `ma.pl` perl script

Copy the following perl script and save it as `ma.pl`

```
sub copyfiles()
{
$dname=$_[0];
opendir(DIRHANDLE, $dname) or warn "couldn't open $dname : $!";
while ( defined ($filename = readdir(DIRHANDLE)) )
            {
if($filename =~ /$\.jsp/)
                {
$srcfile=$filename;
$filename =~ s/$\.jsp//g;
$filename .= "_UTF-8.jsp";
$cpcmd="copy \"$dname\\$srcfile\" \"$dname\\$filename\" \n";
print "$cpcmd";
$etst=`$cpcmd`;
                }
            }
}
```

```
&copyfiles("config\\auth\\default\\aml");
&copyfiles("config\\auth\\default\\wml");
&copyfiles("config\\auth\\default\\vxml");
&copyfiles("config\\auth\\default\\vxml\\Nuance");
&copyfiles("config\\auth\\default_de\\aml");
&copyfiles("config\\auth\\default_de\\wml");
&copyfiles("config\\auth\\default_fr\\aml");
&copyfiles("config\\auth\\default_fr\\wml");
&copyfiles("config\\auth\\default_ja\\aml");
&copyfiles("config\\auth\\default_ja\\wml");
&copyfiles("config\\auth\\default_es\\aml");
&copyfiles("config\\auth\\default_es\\wml");
&copyfiles("config\\auth\\default_ko\\aml");
&copyfiles("config\\auth\\default_ko\\wml");
&copyfiles("config\\auth\\default_zh\\aml");
&copyfiles("config\\auth\\default_zh\\wml");
&copyfiles("config\\auth\\default_zh_CN\\aml");
&copyfiles("config\\auth\\default_zh_CN\\wml");
&copyfiles("config\\auth\\default_zh_TW\\aml");
&copyfiles("config\\auth\\default_zh_TW\\wml");
```

Saving the `ma-filepath.pl` perl script

Copy the following perl script and save it as `ma-filepath.pl`

```
sub ReplaceFilePath
{
open (CONF_FD, "<config\\ldif\\sunAMClient_data.ldif") or
&fopen_error("config\\ldif\\sunAMClient_data.ldif", "ReadParameterFromConfigFile",
__FILE__, __LINE__);
my(@lines) = <CONF_FD>;
close (CONF_FD);
open (TMP_FD, ">config\\ldif\\sunAMClient_data.ldif.new") or
```

```
&fopen_error("config\\ldif\\sunAMClient_data.ldif.new", "ReadParameterFromConfigFile",
__FILE__, __LINE__);
foreach (@lines)
{
chomp;
$line = $_;
if ($line =~ /vxml\/Nuance/)
{
$line =~ s/vxml\/Nuance/vxml\\Nuance/g;
}
elsif ($line =~ /aml\/chtml/)
{
$line =~ s/aml\/chtml/aml\\chtml/g;
}
elsif ($line =~ /aml\/hdml/)
{
$line =~ s/aml\/hdml/aml\\hdml/g;
}
elsif ($line =~ /aml\/ihtml/)
{
$line =~ s/aml\/ihtml/aml\\ihtml/g;
}
elsif ($line =~ /aml\/jhtml/)
{
$line =~ s/aml\/jhtml/aml\\jhtml/g;
}
elsif ($line =~ /wml\/Nokia/)
{
$line =~ s/wml\/Nokia/wml\\Nokia/g;
}
elsif ($line =~ /aml\/wml/)
```

```
{
$line =~ s/aml\/wml/aml\\wml/g;
}
elsif ($line =~ /aml\/xhtml/)
{
$line =~ s/aml\/xhtml/aml\\xhtml/g;
}
print TMP_FD "$line\n";
}
close (TMP_FD);
`del config\\ldif\\sunAMClient_data.ldif`;
`ren config\\ldif\\sunAMClient_data.ldif.new sunAMClient_data.ldif`;
}
&ReplaceFilePath();
```

Configure Automatically During Installation

1. Edit the web.xml of access manager's service web module. Filter tag will be commented. Remove the comment.

   If Web Server is the container,

   ```
   <webserver-installdir>\<instancedir>\is-web-apps\services\WEB-INF\web.xml
   ```

   If Application Server is the container,

   ```
   <appserver-installdir>\domains\<domain-name>\applications\j2ee-modules\amserve
   r\WEB-INF\web.xml
   ```

   E.g.

   Replace

   ```
   <! --      <filter>
   <filter-name>amlcontroler</filter-name>
   <filter-class>com.sun.mobile.filter.AMLController</filter-class>
   </filter>
   <filter-mapping>
   <filter-name>amlcontroler</filter-name>
   ```

```
<url-pattern>/*</url-pattern>
</filter-mapping>-->
```

To

```
<filter>
<filter-name>amlFilter</filter-name>
<filter-class>com.sun.mobile.filter.AMLController</filter-class>
</filter>
<filter-mapping>
<filter-name>amlFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

2. Run the `ma.pl` in the following directory.

   If Web Server is the container,

   `<webserver-installdir>\<instancedir>\is-web-apps\services\`

   If Application Server is the container,

   `<appserver-installdir>\domains\<domain-name>\applications\j2ee-modules\amserver\`

3. Restart the web container.
4. Change the client's file path in amconsole.
   a. Go to amconsole->service configuration ->client detection.
   b. Select edit link.
   c. Select the client and edit.
   d. Replace / to \ in the 'The file path to pick up templates from: '
   e. Save it.

Configure Manually After Installation

1. Before configuring the Access Manager, run the `ma-filepath.pl` in `<am-installdir>` directory.

   e.g, C:\Sun\AccessManager

2. Configure the Access Manager.

3. Configure the Portal Server.
4. Edit the `web.xml` of access manager's service web module. Filter tag will be commented. Remove the comment.

   If Web Server is the container,

   ```
   <webserver-installdir>\<instancedir>\is-web-apps\services\WEB-INF\web.xml
   ```

   If Application Server is the container,

   ```
   <appserver-installdir>\domains\<domain-name>\applications\j2ee-modules\amserve
   r\WEB-INF\web.xml
   ```

   E.g.

   Replace

   ```
   <! --      <filter>
   <filter-name>amlcontroler</filter-name>
   <filter-class>com.sun.mobile.filter.AMLController</filter-class>
   </filter>
   <filter-mapping>
   <filter-name>amlcontroler</filter-name>
   <url-pattern>/*</url-pattern>
   </filter-mapping>-->
   ```

   To

   ```
   <filter>
   <filter-name>amlFilter</filter-name>
   <filter-class>com.sun.mobile.filter.AMLController</filter-class>
   </filter>
   <filter-mapping>
   <filter-name>amlFilter</filter-name>
   <url-pattern>/*</url-pattern>
   </filter-mapping>
   ```

5. Run the `ma.pl` in the following directory.

   If Web Server is the container,

   ```
   <webserver-installdir>\<instancedir>\is-web-apps\services\
   ```

   If Application Server is the container,

   ```
   <appserver-installdir>\domains\<domain-name>\applications\j2ee-modules\amserver\
   ```

6. Restart the container.

Cookie less mode does not work in mobile access

When trying to access the login page in cookie less mode, it does not work.

Workaround

None.

Localization

The date and time are not displayed according to the locale in the Calendar. (4971337)

On the Portal Desktop, the date and time are not displayed in the correct locale format. For example, if the Korean locale package is installed, the date and time format in the Calendar are not displayed in Korean. This issue will occur for any localized installation of Mobile Access Pack.

Workaround

None.

Reminder time for Calendar task does not accept modification. (5031431)

Add a task to the Calender and set the reminder time as 15 minutes. When modified, that task's reminder time is shown as 1 minute though it shows as 15 minutes in Calendar Express.

Workaround

None.

The Date in NetFile depends on locale of the server. (5026281)

The date format should depend on the user's locale not the server's locale.

Workaround

None.

Chinese text file attachment can not be saved correctly in Netmail. (5031446)

When using Netmail to attach a text file that contains Chinese characters, users who receive that file by Netmail, can not save the file correctly. The file characters are corrupted.

Workaround

None.

Unzipping a multibyte file in which the filename is a multibyte filename causes the filename to get corrupted. (5033641)

If a multibyte file that has a multibyte filename is unzipped the filename gets corrupted.

Workaround

None.

The naming order of address book entries is strange for Japanese users. (6197714)

The address book channel and map address book displays first name then last name. It should display last name, then first name.

Workaround

None.

When using Netmail Lite to send mail in Japanese, the end of the message displays either question marks or garbage charaters.(6197737)

Workaround

None.

When using the de_DE locale, the advanced search page is incorrect. (6208359)

After clicking the search tab, the advanced search page comes up but part of the page is missing.

Workaround

None.

The Proxylet (under Secure Remote Access) configuration page in the Administration Console is not localized. (6208800)

Workaround

None.

The edit page of the Instant Messaging Channel displays an error page. (6210507)

Clicking the edit button of the Instant Messaging channel causes an error page to be displayed.

Workaround

Change to user locale to English and then edit the Instant Messaging channel.

Multibyte filenames in NetFile can not be displayed under an NFS server's shared folder. (6193843)

Non-English users can not access NetFile files through the Portal Server desktop under NFS server's shared folder if the file has a multibyte character file name.

Workaround

None.

Clicking on the "Edit" button of a channel with a multibyte name causes an empty page to be displayed. (6193860)

Workaround

None.

Can not post a note in the Notes channel. (6193889)

Portal desktop users are unable to post a note in Notes Channel because the channel can not be edited.

Workaround

Change the display profile fragment for NoteProvider in dp-providers.xml file as shown (in bold) below:

<Provider name="NotesProvider" class="com.sun.portal.providers.notes.NotesProvider">

<Boolean name="isEditable" value="true" advanced="true"/>

The time format in the Calendar channel is incorrect for Japanese users. (6196579)

For Japanese users, the time format on calendar channel should be PM: HH:MM - AM: HH:MM.

Workaround

None.

Users can not cancel the Netlet warning dialog box. (2112878)

When Portal Server desktop users try to access an FTP or telnet service through Netlet in a localized Portal Server configuration, Netlet displays a warning dialog box with the options "OK" and "Cancel." If the user clicks Cancel, the dialog box hangs.

Workaround

None.

Instant Messenger can not be invoked as Java Web start style in with some JDK versions. (6199908)

This problem occurs when the user tries to access the Portal Server desktop on a Windows machine with J2SE 1.5.0 installed.

Workaround

None.

Unable to send mail using NetFile Java1. (4910252)

Files can not be sent using the mail button from NetFile Java1, when file path or file name contains multi-byte characters.

Files can be mailed using NetFile Java2.

Workaround

None.

The date format specified in the Netmail Online Help is wrong. (4920181)

The Netmail Online Help states that the date format to search for mail is mm-dd-yy. This format is incorrect in many locales.

Workaround

The date format for searching mail depends on the user's locale. For example, in the Japanese locale, users should use the following date format:

yyyy/mm/dd

The date format used in the Calendar channel for some European (EMEA) locales is wrong. (5033728)

The date format used is Month Day, Year. The format should be Day Month Year.

Workaround

None.

Events in the Calendar channel use the wrong time format for European locales. (5033735)

Events displayed in the Calendar channel use the wrong time format (12-hours). They should use the 24-hour format as it is set in Calendar Server.

Workaround

None.

The Korean version of Netmail's Find application does not locate all messages properly. (5036419)

The before/on option does not highlight messages that match the on value. The after/on option highlights messages that match the on value.

Workaround

None.

For simplified Chinese users, the default language in the User Information channel's editing page is English. (5036625)

The locale XML files are set for en, not zh.

Workaround

None.

The Anonymous desktop (/portal/dt) is not displayed according to the preferred language set in the browser. (5059646)

The first time the anonymous desktop is accessed it is displayed according to the preferred language specified in the browser. If the preferred language is changed in the browser and the page is refreshed, only part of the desktop contents are displayed in browser locale.

Workaround

None.

When languages are selected, configuration of localization is slow. (5074720)

Portal Server software configuration requires several minutes for each language. Each language uses many XML files, and dpadmin is called for each.

Workaround

None.

Localized authentication JSPs for Portal Server Mobile Access are not deployed into the Access Manager. (6191601)

These JSPs are delivered in the `AccessManager/mobile_auth_jsps.jar` and must be unjarred into `AccessManager/web-src/services`. The `AccessManager/amserver.war` also must be recreated and redeployed into the web container.

Workaround

None.

Portal Server May Not Deploy for Spanish Locale. (6214289)

Portal Server may not start when deployed with Sun Java System Web Server if Portal Server was installed using the text-based interface.

Workaround

None.

NetFile Does Not Correctly Display Windows 2000 Shared Folder Names for Japanese Locale. (6215099)

The folder name is displayed as garbage only for the Japanese locale.

Workaround

None.

Can not register new user for Chinese locale (6358271)

Workaround

Use mozilla browser for registering.

Known Issues and Limitations for the Sun Java Enterprise System Release 4

Deploying Portal Server Using a remote Access Manager does not work. (6284663)

Deploying Portal Server using a Remote Access Manager does not work in this Beta release. A fix is under development and it is Sun's intention to support this configuration in the final version of the release. Please check the release notes in the final product for more information on this subject.

For the Linux Beta version you cannot deploy Portal Server in a configuration where Portal Server is installed on one host where Access Manager and Directory Server are installed on another host.

A workaround is available. However, it is not recommended because it is complex and difficult to correctly implement. If this configuration is absolutely required for your Beta evaluation, Sun has published the workaround, for your information only. The work around is as follows:

Workaround

1. Install Access Manager and Directory Server on a host using the Java Enterprise System installer in Configure Now mode.

2. Install the Access Manager SDK on a separate host using the Java Enterprise System installer in Configure Later mode.
3. Configure Access Manager using the amconfig script with DEPLOY_LEVEL=4 set after populating the amsamplesilent file with appropriate data for the specific configuration you are evaluating for Beta.
4. Configure Portal Server using the psconfig script after populating the pssamplesilent file with appropriate data for the specific configuration you are evaluating for Beta.

See "Portal Server Using a Remote Access Manager Example" in the Sun Java Enterprise System 2005Q4 Installation Guide for more information.

Access Manager Authentication pages are not available on mobile devices. (6264551)

Mobile device users are not able to log in to the mobile Desktop using the "amserver/UI/Login" URL

Workaround

None.

Access Manager registered Portal Server services are not added to users when users are created through the SDK. (6280171)

A user created using the Delegated Administrator utility, commadmin, (which uses the Access Manager SDK), does not have the default services required to login into Portal Server.

Workaround

For each user that is created using the commadmin utility, you must register the missing services for the user using the Access Manager administrator Console.

You can also use the amadmin utility or ldapmodify utility to add the registered services. If you have a number of users, consider writing a script to add the users.

The password field for the communication channels, contains the value before the channel is configured. (6280707)

Workaround

None.

The UWC Calendar does not come up through the gateway. (6218353)

Clicking the Launch Calendar link displays an error message.

Workaround

To perform the following steps in the gateway for UWC to work with the gateway.

1. Login to Admin Console and click on the gateway profile under Service Management.
2. Enable cookie management under the core tab.
3. Add Calender, Messaging and UWC urls with port numbers in the list box for "URls to which session forwarded."
4. Under the Rewriter tab, enable Rewrite all URLs.
5. Restart the gateway

The Launch Address Book link does not appear if proxy authentication is enabled. (2126154)

By default, when UWC is enabled, the cookie "webmailsid" is used by Messenger Express. The Launch Address Book does not appear for the Portal AddressBook channel. The appropriate options must be set in order to workaround this bug.

Workaround

Use one of the following workarounds:

- If UWC is installed, the option `local.webmail.sso.uwcenabled` is set to "1" for Messaging Server. This value signals Messenger Express to use a cookie. Set the option `local.webmail.sso.uwcenabled` to "0" with the configutil tool.
- Verify that the option local.service.http.cookiename is left blank or is not set.

When invoking the Proxylet rules window, an error is message is displayed. (6285755)

When invoking the Proxylet rules window in the Access Manager console an error message is displayed. This error occurs only with the BEA WebLogic web container.

Workaround

None.

The Login and Logout pages are displayed incorrectly through the gateway. (6285748)

When accessing the Access Manager console Login page and Logout page through the gateway, the font size, page layout and frame width gets changed.

Workaround

None.

Redistributable Files

Sun Java System Portal Server 6 2005Q4 does not contain any files which you can redistribute.

How to Report Problems and Provide Feedback

If you have problems with Sun Java System Portal Server, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at
  http://www.sun.com/service/sunone/software

  This site has links to the Knowledge Base, Online Support Center, and Product Tracker, as well as to maintenance programs and support contact numbers.
- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

If your problems seem to be associated with a client, please have the following information available:

- What client types are new
- What default client type settings have changed and how
- What errors or exceptions are reported in the `/var/opt/SUNWam/debug/render.debug` file or the `/var/opt/SUNWam/debug/MAPFilterConfig` file for Solaris platform. For HP-UX platform `/var/opt/Sun/identity/debug/MAPFilterConfig`. For Windows platform `[INSTALLDIR]\AccessManager\debug`.
- What exceptions are reported in the taglibs log file `\var\opt\SUNWam\debug\mapJsp`

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Use the web-based form to provide feedback to Sun:

http://www.sun.com/hwdocs/feedback

Please provide the full document title and part number in the appropriate fields. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the part number of these Release Notes document is 819-4270-10.

Additional Sun Resources

Useful Sun Java System information can be found at the following Internet locations:

- Sun Java System Documentation
  http://docs.sun.com/app/docs/prod/entsys.05q4#hic
- Sun Java System Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun Java System Software Products and Service
  http://www.sun.com/software
- Sun Java System Software Support Services
  http://www.sun.com/service/sunone/software
- Sun Java System Support and Knowledge Base
  http://www.sun.com/service/support/software
- Sun Support and Training Services
  http://training.sun.com
- Sun Java System Consulting and Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun Developer Information
  http://developers.sun.com
- Sun Developer Support Services
  http://www.sun.com/developers/support
- Sun Software Data Sheets
  http://wwws.sun.com/software