Web Application Container Server (WACS): Supported and Unsupported Features for BusinessObjects Enterprise XI 3.1

2008-10-28

Web Application Container Server (WACS)

This documentation describes WACS features that are unsupported in BusinessObjects Enterprise XI 3.1, but are provided as a technical preview. In this release, Business Objects does not support Web Services SDK and QaaWS (DSWS) or Business Process BI Web Services (BPBIWS) , and does not support any features or applications using web services, such as Live Office. However, you are able to preview hosting web services on WACS. It is not recommended that you deploy web services to a WACS in a production deployment, because these features are not supported.

Web Application Container Servers (WACS) provide a platform for hosting BusinessObjects Enterprise web applications. For example, a Central Management Console (CMC) can be hosted on a WACS.

WACS simplifies system administration by removing several manual workflows that were previously required for configuring application servers and deploying web applications, and by providing a simplified, consistent administrative interface.

Web applications such as the CMC are automatically deployed to WACS. WACS does not support deploying Business Objects or external web applications, whether manually or by using wdeploy.

Related Topics

- *Common Tasks* on page 6

What is supported on WACS?

The following table describes the services that are fully supported on WACS, and the services that are provided as a technical preview.

Service	Fully supported	Provided as an unsupported technical pre-view
CMC service (includes viewing Crystal Reports, Web Intelligence documents and Desktop Intelligence documents)	Yes	N/A
Web Services SDK and QaaWS	No	Yes
Business Process BI Web Services	No	Yes
Live Office	No	Yes
InfoView	No	No
Voyager	No	No
Federation	No	No

Do I need WACS?

If you plan to use .NET InfoView, and you do not want to use a Java application server to host your CMC, then you can use WACS to host the Central Management Console (CMC).

If you plan to use a supported Java application server to deploy BusinessObjects Enterprise web applications, or if you are installing BusinessObjects Enterprise on a UNIX system, you do not need to install and use WACS.

What are the advantages of using WACS?

Using WACS to host the CMC provides you with a number of advantages:

- WACS requires a minimum effort to install, maintain, and configure.
- All hosted applications are predeployed on WACS, so that no additional manual steps are required.

- WACS is supported by Business Objects.
- WACS removes the need for Java application server administration and maintenance skills.
- WACS provides an administrative interface that is consistent with other Business Objects servers.

Common Tasks

Task	Description	Topic
How can I improve the performance of the Central Management Console (CMC)?	You can improve the performance of the CMC by installing WACS on multiple machines.	• *Adding or removing additional WACS to your deployment* on page 9 • *Cloning a Web Application Container Server* on page 13
How can I improve the availability of my web-tier?	Create additional WACS in your deployment, so that in the event of a hardware or software failure on one server, another server can continue servicing requests.	*Adding or removing additional WACS to your deployment* on page 9
How can I create an environment where I can easily recover from a misconfigured CMC?	Create a second, stopped, WACS, and use this WACS to define a configuration template. In the event that the primary WACS becomes misconfigured, either use the second WACS until you configure the first server, or apply the configuration template to the first server.	*Adding or removing additional WACS to your deployment* on page 9
How can I improve the security of communication between clients and WACS?	Configure HTTPS on WACS.	• *Configuring HTTPS/SSL* on page 17 • *Using WACS with firewalls* on page 55

Task	Description	Topic
How can I improve the security of communication between WACS and other Business Objects servers in my deployment?	Configure SSL communication between WACS and other BusinessObjects Enterprise servers in your deployment.	• *Configuring HTTPS/SSL* on page 17 • *Using WACS with firewalls* on page 55
Can I use WACS with HTTPS and a reverse proxy?	You can use WACS with HTTPS and a reverse proxy if you create two WACS and configure both servers with HTTPS. Use the first WACS for communication inside your internal network, and the other WACS for communication with an external network through a reverse proxy.	*To configure WACS to support HTTPS with a reverse proxy* on page 55
How does WACS fit in my IT environment?	WACS can be deployed in an IT environment with existing web servers, hardware load balancers, reverse proxies, and firewalls.	• *Using WACS with other web servers* on page 53 • *Using WACS with a load balancer* on page 54 • *Using WACS with a reverse proxy* on page 54 • *Using WACS with firewalls* on page 55
Can I use WACS in a deployment with a load balancer?	You can use WACS in a deployment that uses a hardware load balancer. WACS itself cannot be used as a load balancer.	*Using WACS with a load balancer* on page 54

Task	Description	Topic
Can I use WACS in a deployment with a reverse proxy?	You can use WACS in a deployment that uses a reverse proxy. WACS itself cannot be used as a reverse proxy.	*Using WACS with a reverse proxy* on page 54

Task	Description	Topic
How can I troubleshoot my WACS servers?	If you need to determine the reasons for/causes of the poor performance of your WACS, you can view the log files and view the system metrics.	• *To view server errors* on page 56 • *To view system metrics* on page 58
I don't get any pages served to me on a particular port. What is wrong?	There are a number of reasons why you might not be able to connect to WACS. Check to see if: • The HTTP, HTTP through proxy, and HTTPS ports that you specified for the WACS have been taken by other applications. • The WACS has enough memory allocated to it. • The WACS allows enough concurrent requests. • If necessary, restore the system defaults for the WACS.	• *To resolve HTTP port conflicts* on page 59 • *To change memory settings* on page 61 • *To change the number of concurrent requests* on page 62 • *To restore system defaults* on page 62
Where can I find a list of WACS properties?	The “WACS properties” seection of this quide contains a list of WACS properties.	*WACS properties* on page 65

Adding or removing additional WACS to your deployment

Adding additional WACS to your deployment can give you a number of

advantages:

- Faster recovery from a misconfigured server.
- Improved server availability.
- Better load balancing.
- Better overall performance.

There are three ways to add additional WACS to your deployment:

- Installing WACS on a machine.
- Creating a new WACS.
- Cloning a WACS.

Note:
You can deploy more than one WACS on the same machine so that if the primary WACS in your deployment is misconfigured, you can use a secondary WACS to recover your system. However, it is not recommended that you run more than one WACS on a single machine at the same time, due to high resource utilization.

Installing WACS

Installing WACS on separate machines can provide your deployment with better performance, better load balancing, and higher server availability. If your deployment contains two or more WACS on separate machines, CMC availability won't be affected by hardware or software failures on a specific machine, because the other WACS will continue to provide a CMC service.

You can install a Web Application Container Server by using the BusinessObjects Enterprise installation program. There are two ways that you can install WACS:

- In a New installation, if you choose to not install a new or configure a pre-existing Java application server, a WACS is automatically installed.

  If you select a Java application server in a New installation, WACS is not installed.

- In a Custom or Expand installation, you can choose to install WACS on the "Select Features" screen by expanding **Server Components** and selecting **Web Application Container Server**.

If you install WACS, the installation program automatically creates a server called *<NODE>*.WebApplicationContainerServer, where *<NODE>* is the name of your node. A CMC is then deployed to that server. No manual steps are required to deploy or configure the CMC. The system is ready to use.

When you install WACS, the installation program prompts you to provide an HTTP port number for WACS. Ensure that you specify a port number that is not used. The default port number is 6405. If you plan to allow users to connect to the WACS from outside a firewall, you must ensure that the server's HTTP port is open on the firewall.

WACS is supported only on Windows operating systems.

For more information on installing WACS, see the *BusinessObjects Enterprise XI 3.1 Installation Guide for Windows*.

For information on installing WACS when you're upgrading from BusinessObjects Enterprise XI or XI Release 2, see the *BusinessObjects Enterprise XI Upgrade Guide*.

Note:

The web applications that WACS hosts are automatically deployed when you install WACS or when you apply updates or hot-fixes to WACS or to WACS-hosted web applications. It takes several minutes for the web applications to deploy. The WACS will be in the “Initializing” state until the web application deployment is complete. Users will not be able to access web applications hosted on WACS until the web applications are fully deployed. You can view the server state of the WACS through the Central Configuration Manager (CCM).

This delay only occurs when starting WACS the first time after installing WACS or applying updates to it. This delay does not occur for subsequent WACS restarts.

Web applications cannot be manually deployed to a WACS server. You cannot use wdeploy to deploy web applications to WACS.

Adding a new Web Application Container Server

Note:
You can deploy more than one WACS on the same machine so that if the primary WACS in your deployment is misconfigured, you can use a secondary

WACS to recover your system. However, it is not recommended that you run more than one WACS on a single machine at the same time, due to high resource utilization.

1. Go to the "Servers" management area of the CMC.
2. Select **Manage** > **New** > **New Server**.

   The "Create New Server" screen appears.
3. From the **Service Category** list, select **Core Services**.
4. From the **Select Service** list, select **Central Management Console Service**, and click **Next**.
5. On the next "Create New Server" screen, click **Next**.

   Note:

   In this release, Business Objects does not support Web Services SDK and QaaWS (DSWS) or Business Process BI Web Services (BPBIWS), and does not support any features or applications using web services, such as Live Office. However, you are able to preview hosting web services on WACS. It is not recommended that you deploy web services to a WACS in a production deployment, because these features are not supported.
6. On the next "Create Server Screen", select a node to add the server to, type a server name, server port, and description for the server, and click **Create**.

   Note:
   Only those nodes that have WACS installed will appear in the **Node** list.
7. On the "Servers" screen, double-click the newly created WACS.

   The "Properties" screen appears.
8. In the "Common Settings" pane, ensure that the **Automatically start this server when the Server Intelligence Agent starts** checkbox is unchecked, and click **Save & Close**.

A new WACS is created. The default settings and properties are applied to the server.

Cloning a Web Application Container Server

As an alternative to adding a new WACS to your deployment, you can also clone a WACS, either to the same machine or to another machine. While adding a new WACS creates a server with the default settings, cloning a WACS applies the settings of the source WACS to the new WACS.

Servers can only be cloned to machines that already have WACS installed.

Note:
You can deploy more than one WACS on the same machine so that if the primary WACS in your deployment is misconfigured, you can use a secondary WACS to recover your system. However, it is not recommended that you run more than one WACS on a single machine at the same time, due to high resource utilization.

1. Go to the "Servers" management area of the CMC.
2. Select the WACS that you want to clone, right-click and select **Clone Server**.

   The "Clone Server" screen displays a list of nodes in your deployment that you can clone the WACS to. Only those nodes that have WACS installed appear in the **Clone to Node** list.
3. On the "Clone Server" screen, type a new server name, select the node that you want to clone the server to, and click **OK**.

A new WACS is created. The new server contains the same services as the server that it is cloned from. The destination server and services that it hosts have the same settings as the server it was cloned from, with the exception of the server name.

Note:
If you cloned a WACS to the same machine, you may have port conflicts with the WACS that was used for cloning. If this occurs, you must change the port numbers on the newly cloned WACS instance.

Related Topics

- *To resolve HTTP port conflicts* on page 59

Deleting WACS servers from your deployment

You can only delete a WACS if the server isn't currently serving the CMC to you. If you want to delete a WACS from your deployment, you must log on to a CMC from another WACS or a Java application server. You cannot delete a WACS that is currently serving the CMC to you.

1. Go to the "Servers" management area of the CMC.
2. Stop the server that you want to delete by right-clicking the server and clicking **Stop Server**.
3. Right-click the server and select **Delete**.
4. When prompted for confirmation, click **OK**.

Adding or removing services to WACS

To add a CMC service to a WACS

After you install WACS, a Central Management Console (CMC) service is automatically added to your deployment. There is no need to add a CMC to a WACS unless you create a new WACS without a CMC service, or if you remove a CMC service from a WACS.

To add a CMC service to a WACS, WACS must be installed on the machine. A CMC service can only be added to a WACS that isn't already hosting a CMC.

Adding a CMC service to a WACS requires that you stop the WACS. Therefore, you must have at least one additional CMC hosted on a WACS in your deployment that provides a CMC service while you are stopping and adding a web service to the other WACS.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to add the CMC service to, and view the properties of the server to ensure that a CMC service is not already present.
3. Click **Cancel** to return to the "Servers" screen.
4. To stop the WACS that you want to add a CMC service to, right-click the server and click **Stop Server**.

If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running CMC service on another WACS in your deployment. If you do, click **OK**, log on to another WACS, and start this procedure from the beginning.

5. Right-click the WACS and click **Select Services.**

   The "Select Services" screen appears.

6. On the "Available services" list, select **Central Management Console Service**, click **>** to add it to the server, and click **OK**.
7. To start the WACS, right-click the server and click **Start Server**.

The CMC service is added to the Web Application Container Server. The default settings and properties for the CMC are applied.

To remove a CMC service from a WACS

When you remove a CMC service from a WACS, you must ensure that you don't remove the last CMC from your deployment. You need to have at least one additional CMC service running on a WACS in your deployment before you attempt to remove a CMC service.

You cannot delete the last service from a WACS. Therefore, if you are removing a CMC service from a WACS, you must ensure that the server is hosting another service.

If you want to remove the last service from a WACS, delete the WACS itself.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to remove the CMC from, and view the properties of the server to ensure that a CMC service is present.
3. Click **Cancel** to return to the "Servers" screen.
4. To stop the WACS, right-click the server and click **Stop Server**.

   If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running CMC service on another WACS in your deployment. If you do, click **OK**, log on to another WACS, and start this procedure from the beginning.

5. Right-click the server and click **Select Services**.
6. On the "Services" list, select **Central Management Console Service**, click **<** to remove it from the server, and click **OK**.

7. To start the WACS, right-click the server and click **Start Server**.

To add a web service to a WACS

Note:
In this release, Business Objects does not support Web Services SDK and QaaWS (DSWS) or Business Process BI Service (BPBIWS), and does not support any features or applications using web services, such as Live Office. However, you are able to preview hosting web services on WACS. It is not recommended that you deploy web services to a WACS in a production deployment, because these features are not supported.

Adding a Web Services SDK and QaaWS (DSWS) or Business Process BI Service (BPBIWS) to a WACS requires that you stop the WACS. Therefore, you must have at least one additional CMC hosted on a WACS in your deployment that provides a CMC service while you are stopping and adding a web service to the other WACS.

When you add a web service to WACS, the web services are automatically deployed to WACS when the server is restarted.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to add the web services to, and view the properties of the server to ensure that a Web Services SDK and QaaWS or Business Process BI Service is not already present.
3. Click **Cancel** to return to the "Servers" screen.
4. Stop the server by right-clicking the server and clicking **Stop Server**.

   If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running CMC service on another WACS in your deployment. If you do, click **OK**, log on to another WACS, and start this procedure from the beginning.
5. Right-click the server and select **Select Services**.

   The "Select Services" screen appears.
6. Select **Web Services SDK and QaaWS** or **Business Process BI Service**, add the service to the server by clicking **>**, and click **OK**.
7. Start the WACS by right-clicking the server and clicking **Start Server**.

The services are added to the WACS. The default settings and properties for the web services are applied.

To remove a web service from a WACS

In order to remove a web service from a WACS, you must log on to a CMC on another WACS or on a Java application server. You cannot stop the WACS that is currently serving the CMC to you.

You cannot delete the last service from a WACS. Therefore, if you are removing a web service from a WACS, you must ensure that the server is hosting a CMC service or another web service.

If you want to remove the last service from a WACS, delete the WACS itself.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to remove the web service from, and view the properties of the server to ensure that the web service that you want to remove is present.
3. Click **Cancel** to return to the "Servers" screen.
4. Stop the WACS by right-clicking the server and clicking **Stop Server**.

   If you are trying to stop the WACS that is currently serving the CMC to you, a warning message appears. Don't proceed unless you have at least one additional running CMC service on another WACS in your deployment. If you do, click **OK**, log on to another WACS, and start this procedure from the beginning.
5. Right-click the WACS and select **Select Services.**

   The "Select Services" screen appears.
6. Select the web service that you to remove, click **<**, and then click **OK**.
7. Start the WACS by right-clicking the server and clicking **Start Server**.

The web service is removed from the WACS.

Configuring HTTPS/SSL

You can use the Secure Sockets Layer (SSL) protocol and HTTP for network communication between clients and WACS in your BusinessObjects Enterprise deployment. SSL/HTTPS encrypts network traffic and provides improved security.

There are two types of SSL:

- SSL used between Business Objects servers, including WACS and other BusinessObjects Enterprise servers in your deployment. This is known as CorbaSSL. For more information on using SSL between the Business Objects servers in your deployment, see the “Understanding communication between BusinessObjects Enterprise components” section of the “Working with Firewalls” chapter of the *BusinessObjects Enterprise Administrator's Guide*.
- HTTP over SSL, which occurs between WACS and clients (for example, browsers) that communicate with WACS.

Note:
If you are deploying WACS in a deployment with a proxy or reverse proxy, and want to use SSL to secure the network communication in your deployment, you must create two WACS. For more information, see *Using WACS with a reverse proxy*.

To configure HTTPS/SSL on a WACS, you must:

- Generate or obtain a PKCS12 certificate store or JKS keystore which contains your certificates and private keys. You can use Microsoft's Internet Information Service (IIS) and Microsoft Management Console (MMC) to generate a PCKS12 file, or use openssl or the Java keytool command line tool to generate a keystore file.
- If you want only certain clients to connect to a WACS, then you must generate a certificate trust list file.
- When you have a certificate store and, if necessary, a certificate trust list file, copy the files to the WACS machine.
- Configure HTTPS on the WACS.

Related Topics
- *Using WACS with a reverse proxy* on page 54

To generate a PKCS12 certificate file store

There are many ways of generating a PKCS12 certificate file stores or Java keystores, and tools that you can use. The method that you use depends on the tools that you have access to and are familiar with.

This example demonstrates how to generate a PKCS12 file using Microsoft's Internet Information Services (IIS) and the Microsoft Management Console (MMC).

1. Log on to the machine that hosts WACS as an administrator.
2. In IIS, request a certificate from Certificate Authority. For information on doing this, see the IIS help documentation.
3. Start the MMC by clicking **Start** > **Run**, typing mmc.exe, and clicking **OK**.
4. Add Certificates Snap-in to the MMC:
   a. From **File** menu, click **Add/Remove Snap-in**.
   b. Click **Add**.
   c. On the "Add Standalone Snap-in" dialog, select **Certificates**, and click **Add**.
   d. Select **Computer account**, and click **Next**.
   e. Select **Local Computer**, and click **Finish**.
   f. Click **Close**, and click **OK**.

   The Certificates Snap-In is added to the MMC.
5. In the MMC, expand **Certificates**, and select the certificate that you want to use.
6. On the **Action** menu, select **All Tasks** > **Export**.

   The "Certificate Export Wizard" starts.
7. Click **Next**.
8. Select **Yes, export the private key**, and click **Next**.
9. Select **Personal Information Exchange - PKCS #12 (.PFX)**, and click **Next**.
10. Enter the password you used when you created the certificate and click **Next**. You must specify this password in the **Private Key Access Password** field when you configure HTTPS for the WACS.

A PKCS12 certificate file store is created.

To generate a Certificate Trust List

1. Log on to the machine that hosts WACS as an administrator.
2. Start the Microsoft Management Console (MMC).
3. Add the Internet Information Services Snap-in:
   a. From the **File** menu, select **Add/Remove Snap-in**, and click **Add**.

b. In the "Add Standalone Snap-in" dialog, select **Internet Information Services (IIS) Manager**, and click **Add**.
c. Click **Close**, and click **OK**.

   The IIS snap-in is added to the MMC.

4. In the left pane of the MMC, find the web site for which you want to create the Certificate Trust List.
5. Right-click the web site, and select **Properties**.
6. Click the **Directory Security** tab, and under "Secure Communications", click **Edit**.
7. Click **Enable certificate trust list**, and click **New**.

   The "Certificate Trust List Wizard" starts.
8. Click **Next**.
9. Click **Add from Store** or **Add from File**, select the certificate that you want to add to the Certificate Trust List, click **OK**, and click **Next**.
10. Type a name and description for the Certificate Trust List, and click **Next**.
11. Click **Finish**, and then click **OK**.

    The Certificate Trust List is displayed in the **Current CTL** field.
12. Select the Certificate Trust List and click Edit.

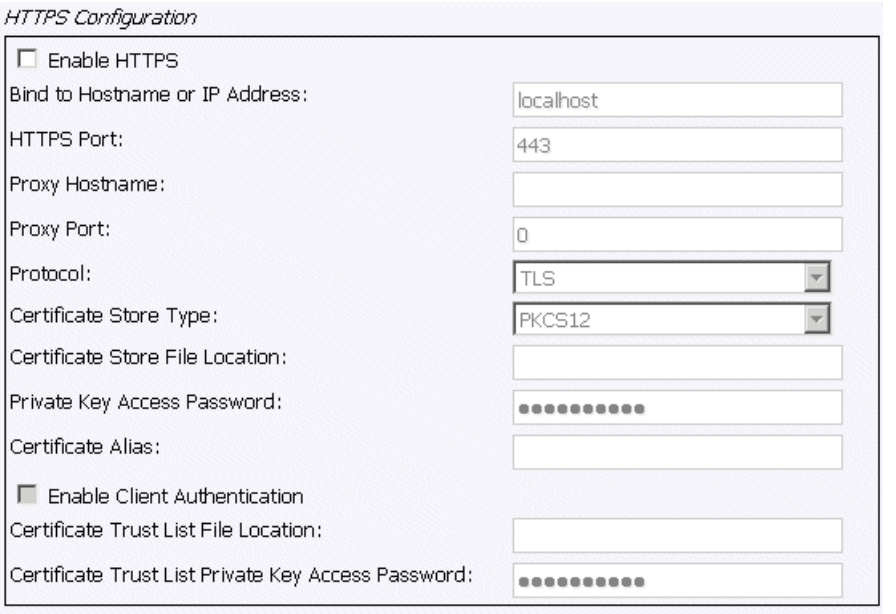
    The "Certificate Trust List Wizard" starts.
13. Click **Next**.
14. On the **Current CTL certificates** list, select the Trust List, and click **View Certificates**.
15. Click the **Details** tab, and click **Copy to File**.

    The "Certificate Export Wizard" starts.
16. Click **Next**.
17. Select **Yes, export the private key**, and click **Next**.
18. Select **Personal Information Exchange - PKCS #12 (.PFX)**, and click **Next**.
19. Enter the password you used when you created the certificate and click **Next**. You must specify this password in the **Certificate Trust List Private Key Access Password** field when you configure HTTPS for the WACS.

To configure HTTPS/SSL

Before you configure HTTPS/SSL on your WACS, ensure that you've already created a PCKS12 file or JKS keystore, and that you've copied or moved the file to the machine that is hosting the WACS.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS the server for which you want to enable HTTPS.
   The "Properties" screen appears.
3. In the "HTTPS Configuration" section, check the **Enable HTTPS** checkbox.



4. In the **Bind to Hostname or IP Address** field, specify the IP address for which the certificates were issued and to which WACS will bind.
   HTTPS services will be provided through IP address that you specify.
5. In the **HTTPS Port** field, specify a port number for WACS to provide HTTPS service. You must ensure that this port is free. If you plan to allow users to connect to the WACS from outside a firewall, you must also ensure that this port is open on the firewall.

6. If you are configuring SSL with a reverse proxy, specify the proxy server's hostname and port in the **Proxy Hostname** and **Proxy Port** fields.
7. On the **Protocol** list, select a protocol. The available options are:
   - **SSL**

     SSL is the Secure Sockets Layer protocol, which is a protocol for encrypting network traffic.
   - **TLS**

     TLS is the Transport Layer Security protocol, and is a newer, enhanced protocol. The differences between SSL and TLS are minor, but include stronger encryption algorithms in TLS.
8. Under the **Certificate Store Type** field, specify the file type for the certificate. The available options are:
   - **PKCS12**

     Select PKCS12 if you are more comfortable working with Microsoft tools.
   - **JKS**

     Select JKS if you are more comfortable working with Java tools.
9. In the **Certificate Store File Location** field, specify the path where you copied or moved the certificate file store or Java keystore file.
10. In the **Private Key Access Password** field, specify the password.

    PKCS12 certificate stores and JKS keystores have private keys that are password protected, to prevent unauthorized access. You must specify the password for accessing the private keys, so that WACS can access the private keys.
11. It is recommended that you either use a certificate file store or keystore that either contains a single certificate, or where the certificate that you want to use is listed first. However, if you are using a certificate file store or keystore that contains more than one certificate, and that certificate is not the first one in the filestore, in the **Certificate Alias** field, you must specify the alias for the certificate.
12. If you want the WACS to only accept HTTPS requests from certain clients, enable client authentication.

    Client authentication doesn't authenticate users. It ensures that WACS only serves HTTPS requests to certain clients.

a. Check **Enable Client Authentication**.
b. In the **Certificate Trust List File Location**, specify the location of the PCKS12 file or JKS keystore that contains the trust list file.

Note:
The Certificate Trust List type must be the same as the Certificate Store type.

c. In the **Certificate Trust List Private Key Access Password** field, type the password that protects the access to the private keys in the Certificate Trust List file.

Note:
If you enable client authentication, and a browser or web service consumer is not authenticated, the HTTPS connection is rejected.

13. Click **Save & Close**.
14. Go to the "Metrics" screen, and ensure that HTTPS connector appears under List of Running WACS Connectors. If HTTPS does not appear, then ensure that the HTTPS connector is configured correctly.

Supported authentication methods

WACS supports the following authentication methods:

- Enterprise
- LDAP
- AD Kerberos

WACS does not support the following authentication methods:

- NT
- AD NTLM
- LDAP with Single sign-on

Using AD Kerberos Single sign-on for Web Services SDK and QaaWS is provided as a technical preview. Adding Web Services SDK and QaaWS to a WACS in a production environment is not supported, and is provided as a preview.

Configuring AD Kerberos for WACS

To configure AD Kerberos authentication for WACS, you must first configure your machine to support AD. You must perform the following steps.

- Enabling the Windows AD security plug-in.
- Mapping users and groups.
- Setting up a service account.
- Setting up constrained delegation.
- Enabling Kerberos authentication in the Windows AD plug-in for WACS.
- Creating configuration files.

After you've setup the machine that is hosting WACS to use AD Kerberos authentication, you must perform additional configuration steps through the Central Management Console (CMC).

If you are configuring single sign on through AD Kerberos for Web Services SDK and QaaWS, you must also configure both WACS and the machine that is hosting WACS.

Related Topics

- *Using AD users and groups* on page 25
- *Windows AD security plug-in* on page 24
- *Mapping AD accounts* on page 26
- *Setting up a service account* on page 32
- *Setting up constrained delegation* on page 35
- *Configuring the servers* on page 37
- *Enabling Kerberos authentication in the Windows AD plug-in for WACS* on page 39
- *Creating configuration files* on page 41
- *Configuring WACS for AD Kerberos* on page 44
- *Configuring WACS for AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 51

Windows AD security plug-in

Windows AD security plug-in enables you to map user accounts and groups from your Microsoft Active Directory (AD) 2000, 2003, and 2008 user

database to BusinessObjects Enterprise. It also enables BusinessObjects Enterprise to verify all logon requests that specify Windows AD Authentication. Users are authenticated against the Windows AD user database, and have their membership in a mapped AD group verified before the Central Management Server grants them an active BusinessObjects Enterprise session.

The AD security plug-in is compatible with both Microsoft Active Directory 2000, 2003, and 2008 domains running in either native mode or mixed mode.

Once you have mapped your AD users and groups, all of the BusinessObjects Enterprise client tools support AD authentication. You can also create your own applications that support AD authentication. For more information, see the developer documentation available on the `collaterals` disk of your product distribution.

- AD authentication only works if the CMS is run on Windows. For single sign on to database to work, the reporting servers must also run on Windows. Otherwise all other servers and services can run on all supported platforms.
- The Windows AD plug-in for BusinessObjects Enterprise supports domains within multiple forests.

Using AD users and groups

BusinessObjects Enterprise supports Active Directory (AD) authentication with the Windows security plug-in, which is included by default when the product is installed on Windows. Support for AD authentication means that users and groups created in Microsoft Active Directory 2000, 2003, and 2008 can be used to authenticate with BusinessObjects Enterprise. This allows you, the administrator, to map previously created user accounts and groups, instead of setting up each user and group within BusinessObjects Enterprise.

Note:
AD authentication only works if the CMS is run on Windows. For single sign on to database to work, the reporting servers must also run on Windows.

Mapping AD accounts

To simplify administration, BusinessObjects Enterprise supports Windows AD authentication for user and group accounts. However, before users can use their AD user name and password to log on to BusinessObjects Enterprise, their Windows AD user account needs to be mapped to BusinessObjects Enterprise. When you map an Windows AD account, you can choose to create a new BusinessObjects Enterprise account or link to an existing BusinessObjects Enterprise account.

To map AD users and groups and configure the Windows AD security plug-in

Regardless of which protocol is used, you must complete the following steps to allow AD users to authenticate.

1. Go to the "Authentication" management area of the CMC.
2. Double-click **Windows AD**.
3. Ensure that **Enable Windows Active Directory (AD)** box is selected.
4. In the **Windows AD Configuration Summary** area, click the link beside **AD Administration Name**.

   Note:
   Before the Windows AD plug-in is configured, this link will appear as two double quotes. After the configuration has been saved, the link with be populated with the AD Administration names.

5. Enter the name and password of an enabled domain user account. BusinessObjects Enterprise will use this account to query information from AD.

   Administration credentials can use one of the following formats:

   - NT name (`DomainName\UserName`)
   - UPN (`user@DNS_domain_name`)

   BusinessObjects Enterprise never modifies, adds or deletes content from AD. It only reads information, therefore only the appropriate rights are required.

Note:
AD authentication will not continue if the AD account used to read the AD directory becomes invalid (for example, if the account's password is changed or expires or the account is disabled).

6. Complete the **Default AD Domain** field.

   Note:
   - Groups from the default domain can be mapped without specifying the domain name prefix.
   - If you enter the Default AD Domain name, users from the default domain do not have to specify the AD domain name when they log on to BusinessObjects Enterprise via AD authentication.

7. In the "Mapped AD Member Groups" area, enter the AD domain\group in the **Add AD Group (Domain\Group)** field.

   Groups can be mapped using one of the following formats:

   - Security Account Manager account name (SAM), also referred to as NT name (`DomainName\GroupName`)
   - DN (`cn=GroupName, ....., dc=DomainName, dc=com`)

   Note:
   If you want to map a local group, you can use only the NT name format (\\ServerName\GroupName). Windows AD does not support local users. This means that local users who belong to a mapped local group will not be mapped to BusinessObjects Enterprise. Therefore, they will not be able to access BusinessObjects Enterprise.

8. Click **Add**.

   The group is added to the list.

9. In the "AD Alias Options" area specify how new aliases are added and updated to BusinessObjects Enterprise.
   a. In "New Alias Options", select how new aliases are mapped to Enterprise accounts. Select one of the following choices:
      - **Assign each new AD alias to an existing User Account with the same name**

        Use this option when you know users have an existing Enterprise account with the same name; that is, AD aliases will be assigned to existing users (auto alias creation is turned on). Users who do

not have an existing Enterprise account, or who do not have the same name in their Enterprise and AD account, are added as new users.

- **Create a new user account for each new AD alias**

  Use this option when you want to create a new account for each user.

b. In "Alias Update Options", select how to manage alias updates for the Enterprise accounts. Select one of the following choices:
   - **Create new aliases when the Alias Update occurs**

     Use this option to automatically create a new alias for every AD user mapped to BusinessObjects Enterprise. New AD accounts are added for users without BusinessObjects Enterprise accounts, or for all users if you selected the "Create a new account for each new AD alias" option and clicked **Update**
   - **Create new aliases only when the user logs on**

     Use this option when the AD directory you are mapping contains many users, but only a few of them will use BusinessObjects Enterprise. BusinessObjects Enterprise does not automatically create aliases and Enterprise accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to BusinessObjects Enterprise.

c. In "New User Options" specify how new users are created by selecting one of the following choices:
   - **New users are created as named users.**

     New user accounts are configured to use named user licenses. Named user licenses are associated with specific users and allow people to access the system based on their user name and password. This provides named users with access to the system regardless of how many other people are connected. You must have a named user license available for each user account created using this option
   - **New users are created as concurrent users.**

     New user accounts are configured to use concurrent user licenses. Concurrent licenses specify the number of people who can connect to BusinessObjects Enterprise at the same time. This type of

licensing is very flexible because a small concurrent license can support a large user base. For example, depending on how often and how long users access BusinessObjects Enterprise, a 100 user concurrent license could support 250, 500, or 700 users.

10. To configure how to schedule AD alias updates, click **Schedule AD Alias Updates**.
    a. In the "Schedule" dialog box, select a recurrence from the **Run object** drop-down list.
    b. Set any of the other schedule options and parameters as required.
    c. Click **Schedule**.

    When the alias update occurs, the group graph is also updated.

11. In the "Attribute Binding Options" area you can select the following optional settings:
    - **Import Full Name and Email Address**

      If selected, the AD user account full names and descriptions are imported and stored with the user object in BusinessObjects Enterprise.
    - **Give AD attribute binding priority over LDAP attribute binding**

      If selected, AD attributes take priority in scenarios where both Windows AD and LDAP are enabled.

12. You can configure AD group graph updates in the "AD Group Graph Options" area.
    a. Click **Schedule AD Group Graph Updates**.

    The "Schedule" dialog box appears.
    b. Select a recurrence from the **Run object** drop-down list.
    c. Set any of the other schedule options and parameters as required.
    d. Click **Schedule**.

    The system will schedule the update and run it according to the schedule information you specified. You can view the next scheduled update for the AD group accounts under the " AD Group Graph Options".

13. Use the settings in the "On-demand AD Update" area to specify what should be updated. You can select from one of the following options:
    - **Update AD Group Graph now**

Select this option if you want to update the group graph. The update will occur only after you click **Update**.

Note:
This option affects any scheduled group graph updates. The next scheduled group graph update is listed under " AD Group Graph Options".

- **Update AD Group Graph and Aliases now**

  Select this option if you want to update the group graph and user aliases. The updates will occur only after you click **Update**.

  Note:
  This option affects any scheduled group graph or updates. The next scheduled updates are listed under "AD Group Graph Options" and "AD Alias Options".

- **Do not update AD Group Graph and Aliases now**

  If you click **Update**, neither the group graph nor the user aliases will be updated.

  Note:
  This option affects any scheduled group graph or updates. The next scheduled updates are listed under "AD Group Graph Options" and "AD Alias Options".

14. Click **Update**.
15. Click **OK**.

Scheduling AD updates

BusinessObjects Enterprise enables administrators to schedule updates for AD group graphs or user aliases. This feature is available for AD authentication with either Kerberos or NTLM. The CMC also enables you to view the time and date when the last update was performed.

When scheduling an update, you can choose from the recurrence patterns summarized in the following table:

Recurrence pattern	Description
Hourly	The update will be run every hour. You specify at what time it will start, as well as a start and end date.
Daily	The update will be run every day or run every number of specified days. You can specify at what time it will run, as well as a start and end date.
Weekly	The update will be run every week. It can be run once a week or several times a week. You can specify on which days and at what time it will run, as well as and a start and end date.
Monthly	The update will be run every month or every several months. You can what time it will run, as well as a start and end date.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, what time it will run, as well as a start and end date.
1st Monday of Month	The update will run on the first Monday of each month. You can specify what time it will run, as well as and a start and end date.
Last Day of Month	The update will run on the last day of each month. You can specify what time it will run, as well as and a start and end date.
X Day of Nth Week of the Month	The update will run on a specified day of a specified week of the month. You can specify what time it will run, as well as and a start and end date.
Calendar	The update will be run on the dates specified in a calendar that has previously been created.

Scheduling group graph updates

BusinessObjects Enterprise relies on Active Directory (AD) for user and group information. To minimize the volume of queries sent to AD, the AD

plug-in caches information about groups and how they relate to each other and their user membership. The group graph is recreated every fifteen minutes when no specific schedule is defined.

You can use the CMC to configure the recurrence of the group graph refresh. This should be scheduled to reflect how frequently you will be changing groups and group membership information.

Scheduling AD user alias updates

User objects can be aliased to a Windows Active Directory (AD) account, allowing users to use their AD credentials to log on to BusinessObjects Enterprise. Updates to AD accounts are propagated to BusinessObjects Enterprise by the AD plug-in. Accounts created, deleted, or disabled in AD will be correspondingly created, deleted, or disabled in BusinessObjects Enterprise.

If you do not schedule AD alias updates, updates will only occur when:

- A user logs on: the AD alias will be updated.
- An administrator selects the **Update AD Group Graph and Aliases now** option from the "On-demand AD Update" area of the CMC.

Note:
No AD passwords are stored in the user alias.

Configuring your machine for AD Kerberos

Setting up a service account

To configure BusinessObjects Enterprise for Kerberos and Windows AD authentication, you require a service account. You can either create a new domain account or use an existing domain account. The service account will be used to run the BusinessObjects Enterprise servers.

After you set up the service account, you will need to grant the account appropriate rights, see *Granting the service account rights* on page 37.

How you create this account varies slightly depending on what version of Active Directory Domain you are using:

- If you are using a Windows 2000 Domain, see *Setting up a service account on a Windows 2000 Domain* on page 33.
- If you are using a Windows 2003 or 2008 Domain, see *Setting up a service account on a Windows 2003 or 2008 Domain* on page 34.
- If you are using a Windows 2003 or 2008 Domain, you also have the option of setting up constrained delegation. See *Setting up constrained delegation* on page 35 for more information.

Note:
If you are setting up SSO2DB, the service account must be a domain account that has been trusted for delegation.

Note:
In a forest with multiple domains you can create this service account in any domain. All domains that trust the domain you have created the service account in will be able to authenticate.

Setting up a service account on a Windows 2000 Domain

To set up the service account on a Windows 2000 Domain

1. Create an account on the domain controller or use an existing account.

   For detailed instructions, refer to http://msdn.microsoft.com/

2. Right-click the user account, then select **Properties**.
3. Click the **Account** tab.
4. Select the **Use DES encryption types for this account** option.

   Note:
   If you need to set up SSO2DB, you must also select the **Account is trusted for delegation** option.

To run the SPN utility on Windows 2000

1. Download the utility from this location to your Domain controller:

   ```
   http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/setspn-o.asp
   ```

   Note:
   The SETSPN utility is a program that allows you to manage the Service Principal Name (SPN) for service accounts in Active Directory.

2. Open a command prompt and enter this command:

```
SETSPN.exe -A <ServiceClass>/<DomainName> <Serviceaccount>
```

Replace *<ServiceClass>* with any desired name. For example, BOBJ CentralMS. (For clustered CMSs, use a generic name; do not use the host name of a CMS machine.) Replace *<DomainName>* with the domain name of the service account. For example, domain.com. Replace *<ServiceAccount>* with the domain user account that you've configured.

Note:

- The name of your service account is case-sensitive.
- The SPN must be unique in the forest in which it is registered. One way to check is to use Windows support tool `Ldp.exe` to search for the SPN.

3. Verify that you receive a message similar to this one:

```
Registering ServicePrincipalNames for CN=Ser
viceCMS,CN=Users,DC=DOMAIN,DC=COM BOBJCentralMS/domain.com
Updated object
```

Setting up a service account on a Windows 2003 or 2008 Domain

To set up the service account on a Windows 2003 or 2008 Domain

Note:
With a Windows 2003 or 2008 Domain, RC4 is the default encryption type and should be used. You will need BusinessObjects Enterprise to be running with JDK 1.5 or higher. (It ships with BusinessObjects Enterprise and is installed by default.) If you want to use a lower JDK, you must check "Use DES encryption".

1. Create a new account on the domain controller or use an existing account.

   For detailed instructions, refer to http://msdn.microsoft.com/

2. Open a command prompt and enter this command:

```
SETSPN.exe -A <ServiceClass>/<DomainName> <Serviceaccount>
```

Replace *<ServiceClass>* with any desired name. For example, BOBJ CentralMS. (For clustered CMSs, use a generic name; do not use the host name of a CMS machine.) Replace *<DomainName>* with the domain

name of the service account. For example, domain.com. Replace `<ServiceAccount>` with the domain user account that you've configured.

Note:

- The name of your service account is case-sensitive.
- The SPN must be unique in the forest in which it is registered. One way to check is to use Windows support tool `Ldp.exe` to search for the SPN.

3. Verify that you receive a message similar to this one:

   Registering ServicePrincipalNames for CN=ServiceCMS,CN=Users,DC=DOMAIN,DC=COM
   BOBJCentralMS/domain.com Updated object

4. If you are using SSO2DB, open the account properties, click the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**.

   Note:
   You will not see the Delegation tab until after you have entered the SETSPN command.

5. Click **OK**.

Setting up constrained delegation

If your company has a policy against trusting a specific service account for delegation to any service, and you are using Active Directory on Windows 2003 or 2008, you may set up constrained delegation. Setting up constrained delegation is done after you create the service account. Constrained delegation allows you to limit what services an account or computer can delegate to, rather than allowing an authorized user to delegate to all services. You can set up constrained delegation for WACS by using a service account.

This method allows you to limit the amount of delegation permitted. Constrained delegation for a service account allows you to do further limit delegation to a specific service for a specific user on a specific computer. Because constrained delegation for a service account is more restrictive, it is considered a more secure option.

Note:

- Constrained delegation is supported only on Active Directory 2003 and 2008.
- The account needs to be trusted for delegation only if you plan to use SSO2DB.

To set up constrained delegation for a service account

1. Create an SPN for the CMS server.

   Type the following command:

   ```
   SETSPN.exe -A <ServiceClass>/<DomainName> <Serviceaccount>
   ```

   - Replace *<ServiceClass>* with any desired name. For example, BOBJCentralMS. For clustered CMSs do not use the hostname of a CMS machine; use a generic name.
   - Replace *<DomainName>* with the domain name of the service account. For example, domain.com.
   - Replace *<ServiceAccount>* with the name of the service account you just created.

2. Open **Active Directory Users and Computers**.
3. Select the **Users** folder.
4. Select the service account user.
5. Right-click, then select **Properties**.
6. Click on the **Delegation** tab.
7. Select **Trust this user for delegation to specified services only**.
8. Ensure **Use Kerberos only** is selected.
9. Click **Add**.
10. Click **Users and Computers**.
11. Enter the *serviceaccount* you specified in step 2, then click **OK**.
12. Select `BOBJCentralMS` from the list of services, then click **OK**.
13. Click **OK**.

Configuring the servers

Configuring the BusinessObjects Enterprise servers includes these steps:

- *Granting the service account rights* on page 37
- *Adding the Service Account to the servers' Local Administrators group* on page 38
- *Configuring the servers to use the service account* on page 38

Granting the service account rights

In order to support AD and Kerberos, you must grant the service account the right to act as part of the operating system.

Note:
If you're using SSO2DB, you require a service account that has been trusted for delegation. See *Setting up a service account* on page 32.

To grant the service account rights

1. Click **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Expand **Local Policies**, then click **User Rights Assignment**.
3. Double-click **Act as part of the operating system**.
4. Click **Add**.
5. Enter the name of the service account you created, then click **OK**.
6. Ensure that the **Local Policy Setting** check box is selected, and click **OK**.
7. Repeat the above steps on each machine running a BusinessObjects Enterprise server.

   Note:
   It is important that the Effective Right ends up being checked after **Act as part of the operating system** is selected. Typically, you will need to restart the server for this to occur. If, after restarting the server, this option is still not on, your Local Policy settings are being overridden by your Domain Policy settings.

Adding the Service Account to the servers' Local Administrators group

In order to support Kerberos, the service account must be part of the local Administrators group.

Note:
If you're using SSO2DB, you require a service account that has been trusted for delegation. See *Setting up a service account* on page 32 . You must also have administrative rights on the server.

To add an account to the Administrator's group

1. On the desired machine, right-click **My Computer** and click **Manage**.
2. Go to **System Tools > Local Users and Groups > Groups**.
3. Right-click **Administrators**, then click **Add to Group**.
4. Click **Add** and type the logon name of the service account.
5. Click **Check Names** to ensure that the account resolves.
6. Click **OK**, then click **OK** again.
7. Repeat these steps for each Business Objects server that has to be configured.

Configuring the servers to use the service account

To support Kerberos single sign-on, you must configure the SIA that contains the WACS to log on as the service account:

Note:
If you're using SSO2DB, you require a service account that has been trusted for delegation. See *Setting up a service account* on page 32 .

To configure a server

Note:
You need to perform the following steps for any Server Intelligence Agent that is running services used in the previous steps for configuring the service account.

1. In the Central Configuration Manager (CCM), stop the Server Intelligences Agent (SIA).

Note:
When you stop the SIA, all services managed by the SIA are stopped.

2. Double-click the SIA to view its properties.
3. On the Properties tab, in the Log On As area, deselect the **System Account** check box.
4. Provide the user name and password for the service account you created earlier, click **Apply**, then click **OK**.

   Note:
   For information about creating the service account, see *Setting up a service account* on page 32 .

5. Restart the SIA.
6. If necessary, repeat steps 1 through 5 for each SIA that is running a service that has to be configured.

Enabling Kerberos authentication in the Windows AD plug-in for WACS

In order to support Kerberos, you have to configure the Windows AD security plug-in in the CMC to use Kerberos authentication. This includes:

- Ensuring Windows AD authentication is enabled.
- Entering the AD Administrator account.

  Note:
  This account requires read access to Active Directory only; it does not require any other rights.

- Enabling Kerberos authentication and single sign-on, if single sign-on is desired.
- Entering the service principal name (SPN) for the service account.

Prerequisites

Before you configure the Windows AD security plug-in for Kerberos, you must have completed the following tasks:

- *Setting up a service account* on page 32

- *Granting the service account rights* on page 37
- *Configuring the servers to use the service account* on page 38
- *Mapping AD accounts* on page 26

To configure the Windows AD security plug-in for Kerberos

1. Go to the **Authentication** management area of the CMC.
2. Double-click **Windows AD**.
3. Ensure that the **Windows Active Directory Authentication is enabled** check box is selected.
4. Under **Authentication Options**, select **Use Kerberos authentication**.
5. If you want to configure single sign-on to a database, select the **Cache Security context** (required for SSO to database) check box.
6. In the **Service principal name** field, enter the account and domain of the service account or the SPN mapping to the service account.

   Use the following format, where *svcacct* is the name of the service account or SPN you created earlier, and *DNS.COM* is your fully qualified domain in uppercase. For example, the Service Account would be svcacct@DNS.COM and the SPN would be BOBJCentralMS/some_name@DOMAIN.COM.

   Note:
   - If you plan to allow users from other domains than the default domain to log on, you must provide the SPN you mapped earlier.
   - The service account is case sensitive. The case of the account you enter here must match with what is set up in your Active Directory Domain.
   - This must be the same account that you use to run the BusinessObjects Enterprise servers or the SPN that maps to this account.

7. If you want to configure single sign-on, select **Enable Single Sign On for selected authentication mode**.

   Note:
   If you selected to enable single sign-on, you will need to configure the WACS.

Related Topics

- *Configuring AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 47

Creating configuration files

The general process of configuring Kerberos on your application server involves these steps:

- Creating the Kerberos configuration file.
- Creating the JAAS login configuration file.

Note:

- The default Active Directory domain must be in uppercase DNS format.
- You don't need to download and install MIT Kerberos for Windows. You also no longer require a keytab for your service account.

To create the Kerberos configuration file

Follow these steps to create the Kerberos configuration file.

1. Create the file `krb5.ini`, if it does not exist, and store it under C:\WINNT for Windows.

   Note:
   You can store this file in a different location. However if you do, you need to specify its location in the **Krb5.ini File Location** field on the "Properties" page for the WACS server, in the CMC.

2. Add the following required information in the Kerberos configuration file:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
```

```
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

Note:

- `DNS.COM` is the DNS name of your domain which must be entered in uppercase in FQDN format.
- `kdc` is the Host name of the Domain Controller.
- You can add multiple domain entries to the [realms] section if your users log in from multiple domains. To see a sample of this file with multiple domain entries, see *Sample Krb5.ini files* on page 43.
- In a multiple domain configuration, under `[libdefaults]` the `default_realm` value may be any of the desired domains. The best practice is to use the domain with the greatest number of users that will be authenticating with their AD accounts.

To create the JAAS login configuration file

1. Create a file called `bscLogin.conf` if it does not exist, and store it in the default location: C:\WINNT.

   Note:
   You can store this file in a different location. However if you do, you will need to specify its location in the **bscLogin.conf File Location** field on the "Properties" page for the WACS server, in the CMC.

2. Add the following code to your JAAS `bscLogin.conf` configuration file:

   ```
   com.businessobjects.security.jgss.initiate {
   com.sun.security.auth.module.Krb5LoginModule required;
   };
   ```

3. Save and close the file.

Sample Krb5.ini files

Sample multiple domain Krb5.ini file

The following is a sample file with multiple domains:

```
[domain_realm]
  .domain03.com = DOMAIN03.COM
  domain03.com = DOMAIN03.com
  .child1.domain03.com = CHILD1.DOMAIN03.COM
  child1.domain03.com = CHILD1.DOMAIN03.com
  .child2.domain03.com = CHILD2.DOMAIN03.COM
  child2.domain03.com = CHILD2.DOMAIN03.com
  .domain04.com = DOMAIN04.COM
  domain04.com = DOMAIN04.com
[libdefaults]
  default_realm = DOMAIN03.COM
  dns_lookup_kdc = true
  dns_lookup_realm = true
[realms]
  DOMAIN03.COM = {
   admin_server = testvmw2k07
   kdc = testvmw2k07
   default_domain = domain03.com
  }
  CHILD1.DOMAIN03.COM = {
   admin_server = testvmw2k08
   kdc = testvmw2k08
   default_domain = child1.domain03.com
  }
  CHILD2.DOMAIN03.COM = {
   admin_server = testvmw2k09
   kdc = testvmw2k09
   default_domain = child2.domain03.com
  }
  DOMAIN04.COM = {
   admin_server = testvmw2k011
   kdc = testvmw2k011
   default_domain = domain04.com
  }
```

Sample single domain Krb5.ini file

Following is a sample krb5.ini file with a single domain.

```
[libdefaults]
  default_realm = ABCD.MFROOT.ORG
  dns_lookup_kdc = true
```

```
  dns_lookup_realm = true
[realms]
  ABCD.MFROOT.ORG = {
   kdc = ABCDIR20.ABCD.MFROOT.ORG
   kdc = ABCDIR21.ABCD.MFROOT.ORG
   kdc = ABCDIR22.ABCD.MFROOT.ORG
   kdc = ABCDIR23.ABCD.MFROOT.ORG
   default_domain = ABCD.MFROOT.ORG
  }
```

Configuring WACS for AD Kerberos

After you've configured the machine that is hosting WACS for AD Kerberos authentication, you must configure the WACS itself, through the Central Management Console (CMC).

To configure WACS for AD Kerberos

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to configure AD for.

   The "Properties" screen appears.
3. In the **Krb5.ini File Location** field, specify the path to the `krb5.ini` configuration file.
4. In the **bscLogin.conf File Location** field, specify the path to the `bscLogin.conf` configuration file.
5. Click **Save & Close**.
6. Restart the WACS.

Troubleshooting Kerberos

These steps may help you if you encounter problems when configuring Kerberos:

- Enabling logging
- Testing your Kerberos configuration

To enable Kerberos logging

1. Start the Central Configuration Manager (CCM), and click the **Manage Servers** icon  .
2. Specify the logon credentials.
3. On the "Manage Servers" screen, stop the WACS.
4. Click the **Web Tier Configuration** icon  .

   Note:
   The **Web Tier Configuration** icon is only enabled when you select a WACS that is stopped.

   The "Web Tier Configuration" screen appears.
5. Under **Command Line Parameters**, copy the following text to the end of the parameters:

   ```
   "-Dcrystal.enterprise.trace.configuration=verbose
    -Djcsi.kerberos.debug=true"
   ```
6. Click **OK**.
7. On the "Manage Servers" screen, start the WACS.

To test your Kerberos configuration

- Run the following command to test your Kerberos configuration, where `servact` is the service account and domain under which the CMS is running, and `password` is the password associated with the service account.

  ```
  <Install Directory>\Business Objects\javasdk\bin\kinit.exe
  servact@TESTM03.COM Password
  ```

  For example:

  ```
   C:\Program Files\Business Objects\javasdk\bin\kinit.exe
  servact@TESTM03.COM Password
  ```

  If you still have a problem, ensure that the case you entered for your domain and service principal name match exactly with what is set in Active Directory.

Mapped AD user unable to log on to BusinessObjects Enterprise on WACS

The following two issues may occur, despite the fact that the users have been mapped to BusinessObjects Enterprise:

- *Logon failure due to different AD UPN and SAM names* on page 46
- *Pre-authentication error* on page 46

Logon failure due to different AD UPN and SAM names

A user's Active Directory ID has successfully been mapped to BusinessObjects Enterprise. Despite this fact, they are unable to successfully log on to CMC with AD authentication and Kerberos in the following format: `DOMAIN\ABC123`

This problem can happen when the user is set up in Active Directory with a UPN and SAM name that are not the same, either in case or otherwise. Following are two examples which may cause a problem:

- The UPN is abc123@company.com but the SAM name is DOMAIN\ABC123.
- The UPN is jsmith@company but the SAM name is DOMAIN\johnsmith.

There are two ways to address this problem:

- Have users log in using the UPN name rather than the SAM name.
- Ensure the SAM account name and the UPN name are the same.

Pre-authentication error

A user who has previously been able to log on, can no longer log on successfully. The user will receive this error: Account Information Not Recognized. The WACS logs reveal the following error: `"Pre-authentication information was invalid (24)"`

This can occur because the Kerberos user database didn't get a change made to UPN in AD. This may mean that the Kerberos user database and the AD information are out of sync.

To resolve this problem, reset the user's password in AD. This will ensure the changes are propagated correctly.

Configuring AD Kerberos single sign-on for Web Services SDK and QaaWS

Note:
In this release, Business Objects does not support Web Services SDK and QaaWS (DSWS) or Business Process BI Service (BPBIWS), and does not support any features or applications using web services, such as Live Office. However, you are able to preview hosting web services on WACS. It is not recommended that you deploy web services to a WACS in a production deployment, because these features are not supported.

If you are configuring AD Kerberos single sign-on for Web Services SDK and QaaWS, you must ensure that you have configured both the WACS and the machine that is hosting WACS for AD Kerberos authentication. For more information, see *Configuring AD Kerberos for WACS* on page 24.

To configure WACS for AD Kerberos single sign-on, you must first configure the machine that is hosting WACS, and then configure the WACS itself.

- *Configuring your machine for AD Kerberos single sign-on to Web Services SDK and QaaWS* on page 48
- *Configuring WACS for AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 51

Note:
If you plan to use single sign-on to Web Services SDK and QaaWS in a reverse proxy environment, read the “Modifying Default Security Behavior” chapter of the *BusinessObjects Enterprise Administrator's Guide* before proceeding.

Single sign-on with Windows AD

The Windows AD security plug-in supports single sign-on, thereby allowing authenticated AD users to log on to BusinessObjects Enterprise without explicitly entering their credentials. The single sign-on requirements depend upon the way in which users access BusinessObjects Enterprise: either via a thick client, or over the Web. In both scenarios, the security plug-in obtains the security context for the user from the authentication provider, and grants

the user an active BusinessObjects Enterprise session if the user is a member of a mapped AD group.

To obtain AD single sign-on functionality from a thick-client application (such as the Publishing Wizard), the user must be running a Windows operating system, and the application must use the BusinessObjects Enterprise SDK. In this scenario, the Windows AD security plug-in queries the operating system for the current user's credentials when the client is launched.

Configuring your machine for AD Kerberos single sign-on to Web Services SDK and QaaWS

To configure AD Kerberos single sign-on for Web Services SDK and QaaWS, you must first configure the machine that is hosting WACS :

The following sections describe how to complete each of these steps.

To create a service account with delegation to be used for Vintela single sign-on

To set up user authentication for a service, you must register the service as a user in AD on the Domain Controller.

1. To register the service, on the Domain Controller, open the Active Directory Users and Computers snap in.
2. Click the Users folder to display a list of users and on the Action menu, click **New** and then click **User**.
3. Enter a name and logon name for the new service, and then click **Next**.
4. On the next screen, enter a password for the service.

   Ensure that the **User must change password at next logon** option is not selected.

5. Click **Next** and then click **Finish**.
6. Right-click the user you have entered in the User folder list, and then click **Properties**.
7. Click the Account tab and then select **Account is trusted for delegation** and **Password never expires**.

   This prevents the service account from expiring, which would cause Kerberos errors.

   Note:

   - If AD is deployed in a Windows 2003 or 2008 Domain, the Account is trusted for delegation option is not available until a Service Principal Name has been created and mapped to this account. If you do not see this option, complete the steps in the next section, then open the user account in the AD Users and Computers snap in and select the Delegation tab.
   - This service account cannot currently be set up with Microsoft's constrained delegation.
8. If your Domain Controller is running in a lower Domain Functional Level (lower than Windows 2003 Domain), view the Account properties for the user you created in step 2, and select **Use DES encryption types for this account**.

   Note:
   In Windows 2003 and 2008, Domain Functional Level RC4 is used by default.
9. Click **OK**.

To create an SPN

Note:
Make sure that the SPN you are creating does not already exist and is mapped to another account. If so, you must remove this SPN with the setspn utility or delete the account that the SPN is mapping to.

1. Launch a command prompt and navigate to your Support Tools folder.
2. Execute the following command:

```
ktpass -princ HTTP/<myurl>@<REALM> -mapuser <user>
```

where

- `<myurl>` is the name of the machine that is hosting WACS. For example, examplemachine.exampledomain.com.
- `<REALM>` is the Active Directory realm in which the server is located. (For example, EXAMPLE.COM).
- `<user>` is the logon name of the user account you created above.

To reset the service account password

To prevent Kerberos integrity-check failures, you should reset the password of the user account you created earlier.

1. On the Domain Controller with Active Directory installed, on the **Start** menu click **Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the user account you created previously and click **Reset Password**.
3. Enter and confirm the same password that you entered previously.
4. Ensure that **User must change password at next logon** is not selected and click **OK**.

To create and place a keytab file

You can configure the KerberosFilter to use either a password or a keytab file. A keytab file is the recommended method because it is more secure. A keytab file allows the KerberosFilter to be configured without exposing the password of the user account on the machine hosting WACS.

1. Run `ktpass` with the following arguments at command prompt:

```
ktpass -out keytab_filename -princ HTTP/host@REALM -pass
user_password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto
encryption_type
```

where

- `keytab_filename` is the name of the keytab file we want to generate. (host.keytab, for example).
- `HTTP/host@REALM` is the SPN created in *To create an SPN* on page 49 (for example, HTTP/myurl.mydomain.com@MYDOMAIN.COM).
- `user_password` is the password of the user used in the Map a Service Principle Name (SPN) section.

- `encryption_type` is the type of encryption associated with the service account you created in *To create a service account with delegation to be used for Vintela single sign-on* on page 48. If you are using DES encryption, use `DES-CBC-MD5`. If you are using RC4 encryption, use `RC4-HMAC-NT`.

2. Copy the generated keytab file onto the java application machine and place in your chosen location.

   Note:
   - The keytab is usually found in the same folder as your ktpass support tool unless you specified a different location.
   - Typically the keytab is stored in C:/WINNT or C:/Windows.

Setting up multiple SPNs

Using multiple SPNs is not supported.

To increase the header size limit of your WACS

Active Directory creates a Kerberos token which is used in the authentication process. This token is stored in the HTTP header. Your WACS will have a default HTTP header size. This header size cannot be configured.

Configuring WACS for AD Kerberos single sign-on for Web Services SDK and QaaWS

You can configure Web Application Container Server that hosts a Web Services SDK and QaaWS web service to use AD Kerberos single sign-on. AD Kerberos single sign-on is supported. AD NTLM is not supported.

Before you configure WACS, you must configure AD Kerberos single sign-on for the machine that is hosting the WACS.

Note:
In this release, Business Objects does not support Web Services SDK and QaaWS (DSWS) or Business Process BI Service (BPBIWS), and does not support any features or applications using web services, such as Live Office. However, you are able to preview hosting web services on WACS. It is not

recommended that you deploy web services to a WACS in a production deployment, because these features are not supported.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to configure.

   The "Properties" screen appears.
3. Check **Enable Kerberos Active Directory Single Sign On**.
4. Specify values for Default AD Domain, Service Principal Name, and Keytab File properties, and click **Save & Close** .
5. Restart the WACS.

Active Directory single sign-on is ready for use.

Configuring Kerberos and single sign-on to the database

Single sign-on to the database is supported for deployments that meet all these requirements:

- The deployment of BusinessObjects Enterprise is on WACS.
- WACS has been configured with AD with Kerberos.
- The database to which single sign-on is required is a supported version of SQL Server or Oracle.
- The groups or users that need access to the database must have been granted permissions within SQL Server or Oracle.
- The Cache Security context check box (which is required for single sign-on to the database) in the AD Authentication page of the CMC is checked.

The final step is to modify the `krb5.ini` file to support single sign-on to the database.

Note:
These instructions explain how to configure single sign-on to the database. If you want to configure end-to-end single sign-on to the database, you must also perform the configuration steps required for Vintela single sign-on. For details, see *Configuring AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 47.

To enable single sign-on to the database

1. Open the `krb5.ini` file that is being used for your deployment of BusinessObjects Enterprise.

   The default location for this file is the WINNT directory on your web application server.
2. Go to the `[libdefaults]` section of the file.
3. Enter this string prior to the start of the `[realms]` section of the file:

   ```
   forwardable = true
   ```
4. Save and close the file.
5. Restart your WACS.

WACS and your IT environment

This section describes how to configure WACS in a complex environment.

Using WACS with other web servers

When a Web Application Container Server (WACS) is installed, it works as an application server and a web server without requiring any extra configuration. You can configure supported web servers like Internet Information Services (IIS) and Apache to perform URL forwarding to the WACS server.

Note:
Request forwarding from IIS by using an ISAPI filter to WACS is not supported.

WACS does not support a deployment scenario where a web server hosts static content and WACS hosts dynamic content. Static and dynamic content must always reside on WACS.

Using WACS with a load balancer

To use WACS in a deployment with a hardware load balancer, you must configure the load balancer so that it uses either IP routing or active cookies. This way, once a user's session is established on one WACS, all subsequent requests by the same user are sent to the same WACS.

WACS is not supported with hardware load balancers using passive cookies.

If your hardware load balancer forwards SSL-encrypted HTTPS requests to your WACS, then you must configure HTTPS on the WACS, and install SSL certificates on every WACS.

If your hardware load balancer decrypts HTTPS traffic and forwards decrypted HTTP requests to your WACS, then no additional WACS configuration is required.

Related Topics

- *Configuring HTTPS/SSL* on page 17

Using WACS with a reverse proxy

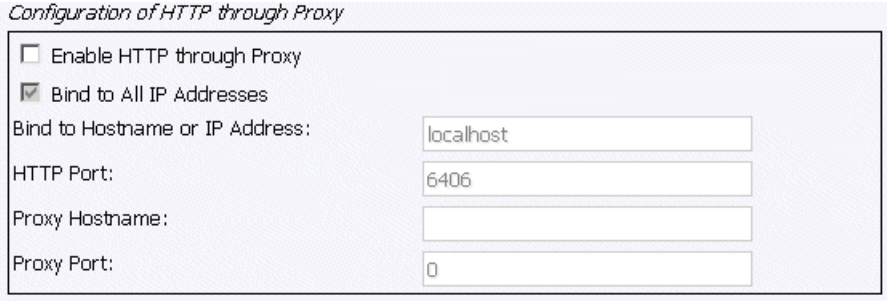
You can use WACS in a deployment with a forward or reverse proxy server. You cannot use WACS itself as a proxy server.

To configure WACS to support HTTP with a reverse proxy

To use WACS in a deployment with a reverse proxy, configure your WACS so that the HTTP Port is used for communication inside a firewall (for example on a secure network), and the HTTP through Proxy port is used for communication from outside the firewall (for example, the internet).

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to configure.
   The "Properties" screen appears.
3. In the "Configuration of HTTP through Proxy" section:
   a. Check **Enable HTTP through Proxy**.

b. Specify the HTTP port of the WACS to be used for communication through the proxy.
c. Specify the Proxy Hostname and Proxy Port of the proxy server.



4. Click **Save & Close**.

To configure WACS to support HTTPS with a reverse proxy

Some load balancers and reverse proxy servers can be configured to decrypt HTTPS traffic and then forward the decrypted traffic to your application servers. In this case, you can configure WACS to use HTTP or HTTP through proxy.

If your load balancer or reverse proxy forwards HTTPS traffic, and you want to configure HTTPS with a reverse proxy, create two WACS. Configure one WACS for HTTPS for external traffic through the reverse proxy, and the other WACS to communicate with clients on your internal network through HTTPS.

Using WACS with firewalls

Deploying WACS in an IT environment with firewalls is supported.

By default, WACS bind to all IP addresses on the machine that it is installed on. If you plan to use a firewall between clients and your WACS, you must force WACS to bind to a specific IP address for HTTP or HTTP through proxy. To do this, uncheck **Bind to All IP Addresses**, and then specify a Hostname or IP address to bind to.

If you plan to use a firewall between a WACS server and the other Business Objects servers in your deployment, see the “Working with Firewalls” chapter of the *BusinessObjects Enterprise Administrator's Guide*.

Configuring WACS on a multihomed machine

A multihomed machine is one that has multiple network addresses. By default, a Web Application Container Server instances binds its HTTP port to all IP addresses. If you want to bind WACS to a specific Network Interface Card (NIC), for example, when you want to bind the HTTP port of the WACS to one NIC and bind the request port to another NIC:

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to configure.

   The "Properties" screen appears.
3. In the "Configuration of HTTP through Proxy" section of the "Web Application Container Service" pane, uncheck **Bind to all IP addresses**, and type an IP address for the WACS to bind to.
4. In the "HTTPS Configuration" section, uncheck **Bind to all IP addresses**, and type an IP address or hostname for the WACS to bind to.
5. Under "Common Settings", deselect **Auto assign**, and then specify the Hostname or IP Address of the NIC that's used for communication between WACS and the other Business Objects servers in your deployment.
6. Click **Save & Close**.
7. Restart the WACS.

Troubleshooting

To view server errors

The log file is located in the *<InstallDir>*/Logging directory, where *<InstallDir>* is the directory where BusinessObjects Enterprise is installed.

The name of the log file is in the format *<servername>_<datestarted>_<timestarted>_<processId>*.log, where *<servername>* is the name of the WACS, *<datestarted>* is the date that the WACS was started, *<timestarted>* is the time it was started, and *<processId>* is the server's process ID.

Note:
All errors are written to the log file. No error messages are written to the Windows Event Viewer.

To change the logging level

You can change the logging severity through the CMC. The levels of severity are:

Logging Level	Description
DEBUG	Logs all WACS activity. This option logs the most amount of information. It is not recommended to select **DEBUG** in a production environment.
INFO	Logs general information. Selecting **INFO** also logs **WARN**, **ERROR**, and **FATAL** messages to the log file.
WARN	Logs a message when the application encounters a problem. Selecting **WARN** also logs **ERROR** and **FATAL** messages to the log file.
ERROR	Logs a message when a service encounters an error or is not available. Selecting **ERROR** also logs **FATAL** messages to the log file.
FATAL	Logs a message when an event occurs that results in the failure of the server or service that it provides.
AUTO	Retrieves the logging level that is specified in the WACS command line. By default, this value is **ERROR**.

To change the logging level of a WACS:

1. Go to the "Servers" management area of the CMC.
2. Double-click the server.
   Stopping the server is not required.
   The "Properties" screen appears.
3. On the **Log Level** list, select a logging severity level, and click **OK**.

4. On the "Servers" screen, restart the WACS.

To view system metrics

You can view the system metrics of a WACS from the Central Management Console (CMC).

1. Go to the "Servers" management area of the CMC.
2. Right-click the WACS, and click **Metrics**.

A list of system metrics appears. For a descriptions of the metrics that are on the list, see *WACS metrics*.

Related Topics

- *WACS metrics* on page 58

WACS metrics

The following table describes the metrics that appear on the "Metrics" screen.

Metric	Description
"Total Memory (MB)"	The total memory used by WACS, in mega bytes.
"List Running WACS Connectors"	A list of all running connectors.
WACS Connector(s) Failed at Start-up	Whether there are any failed connectors. If true, at least one connector failed. If false, all connectors are running.

To view the state of a WACS

To view the state of a WACS, go to the "Servers" area of the CMC. The **Servers List** includes a **State** column that provides the state for each server in the list.

WACS has a new server state called “Started with Errors”. A WACS that is in this state is running, but has at least one misconfigured HTTP, HTTP through Proxy, or HTTPS connector.

If a WACS status is “Started with Errors”, go to the "Metrics" page and view the "Running WACS Connector" metric. If an enabled connector does not appear in the list, the connector has not been configured properly.

Resolving port conflicts

If you cannot get any pages when you try to access the CMC through a particular port, ensure that another application has not taken over the HTTP, HTTP through proxy, or HTTPS ports that you have specified for WACS.

There are two ways to determine if there are port conflicts with your WACS. If you have more than one WACS in your deployment, log on to the CMC and check the Running WACS Connectors and WACS Startup Errors metrics. If the HTTP, HTTP through Proxy, or HTTP connectors do not appear in the Running WACS Connectors list, these connectors are not able to start due to a port conflict.

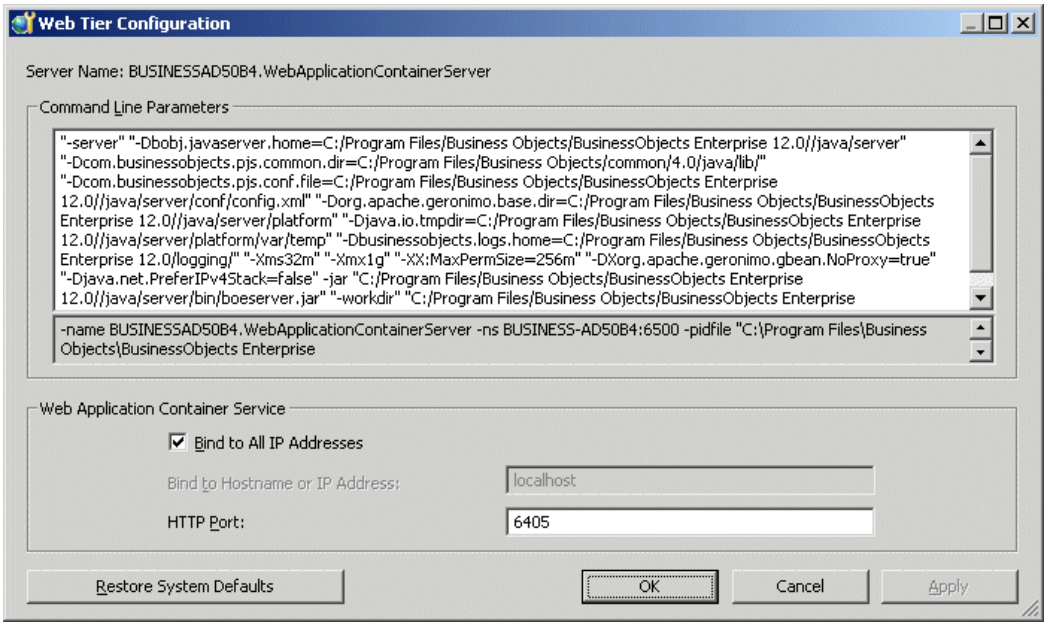
If your deployment has only one WACS, or If you are not able to access the CMC through any WACS, use a utility such as netstat to determine if another application has taken a WACS port.

To resolve HTTP port conflicts

1. Start the Central Configuration Manager (CCM), and click the **Manage Servers** icon  .
2. Specify the logon credentials.
3. On the "Manage Servers" screen, stop the WACS.
4. Click the **Web Tier Configuration** icon  .

   Note:
   The **Web Tier Configuration** icon is only enabled when you select a WACS that is stopped.

   The "Web Tier Configuration" screen appears.



5. In the **HTTP Port** field, specify a free HTTP port to be used by the Web Application Container Server, and click **OK**.
6. On the "Manage Servers" screen, start the WACS.

To resolve HTTP through proxy or HTTPS port conflicts

If you cannot access a WACS through the HTTP through proxy or HTTPS ports, but you can still connect to the Central Management Console (CMC) through the HTTP port, change the port numbers through the CMC.

1. Go to the "Servers" management area of the CMC.
2. To stop the WACS that you want to configure, right-click the server and click **Stop Server**.
3. Double-click the WACS that you want to configure.

   The "Properties" screen appears.
4. In the "Configuration of HTTP through Proxy" section, specify a new HTTP port.
5. To change the HTTPS port, in the "HTTPS Configuration" section, type a new value in the **HTTPS Port** field.

6. Click **Save & Close**.
7. To start the WACS, right-click the server and click **Start Server**.

To change memory settings

To improve the server performance of a WACS, you can change the amount of memory that is allocated to the server through the Central Configuration Manager (CCM).

1. Start the CCM, and click the **Manage Servers** icon  .
2. Specify the logon credentials for the CMC.
3. On the "Manage Servers" screen, stop the WACS.
4. Click the **Web Tier Configuration** icon  .

   Note:
   The **Web Tier Configuration** icon is only enabled when you select a WACS that is stopped.

   The "Web Tier Configuration" screen appears.
5. Under "Command Line Parameters", specify a new memory value by editing the command line:
   a. Find the -Xmx option. This option normally has a value specified.

      For example “-Xmx1g”. This setting allocates one giga byte of memory to the server.
   b. Specify a new value for the parameter.
      - To specify a value in mega bytes, use “m”. For example, “-Xmx640m” allocates 640 mega bytes of memory to the WACS.
      - To specify a value in giga bytes, use “g”. For example, “-Xmx2g” allocates two giga bytes of memory to the WACS.

   c. Click **OK**.
6. On the "Manage Servers" screen, start the WACS.

To change the number of concurrent requests

The default number of concurrent HTTP requests that WACS is configured to handle is 150. This should be acceptable for most deployment scenarios. To improve the performance of WACS, you can increase the maximum number of concurrent HTTP requests. Although increasing the number of concurrent requests can improve performance, setting this value too high can hurt performance. The ideal setting depends on your hardware, software, and IT requirements.

1. Go to the "Servers" management area of the CMC.
2. To stop the WACS that you want to configure, right-click the server and click **Stop Server**.
3. Double-click the WACS that you want to configure.

   The "Properties" screen appears.
4. In the **Maximum Concurrent Requests** field, type the desired number of concurrent requests, and click **Save & Close**.
5. To start the WACS, right-click the server and click **Start Server**.

To restore system defaults

If you've misconfigured a WACS, you can restore the system defaults through the Central Configuration Manager (CCM).

1. Start the CCM, and click the **Manage Servers** icon  .
2. Specify the logon credentials.
3. On the "Manage Servers" screen, stop the WACS.
4. Click the **Web Tier Configuration** icon  .

   Note:
   The **Web Tier Configuration** icon is only enabled when you select a WACS that is stopped.

   The "Web Tier Configuration" screen appears.
5. Click **Restore System Defaults**.
6. If necessary, specify a free HTTP port, and click **OK**.

7. On the "Manage Servers" screen, start the WACS.

To prevent users from connecting to WACS through HTTP

In certain cases, you may want to only allow users from the local machine to connect to a WACS through HTTP or HTTPS. For example, although you cannot close the HTTP port, you may want to configure your WACS so that it only accepts HTTP requests from the clients located on the same machine as the WACS. In this way, you can perform maintenance or configuration tasks on the WACS through a browser from the same machine as the WACS, while preventing other users from accessing the server.

1. Go to the "Servers" management area of the CMC.
2. Double-click the WACS that you want to modify.

   The "Properties" screen appears.
3. Uncheck **Bind to all IP Addresses**.
4. In the **Bind to Hostname or IP address** field, type 127.0.0.1, and click **OK**.
5. To start the WACS, right-click the server and click **Start Server**.

   The WACS that is configured this way only accepts connections from the local machine.

WACS glossary

AD

Active Directory.

BPBIWS

BusinessObjects Business Process Business Intelligence Web Service.

BPBIWS service

A BPBIWS hosted on a WACS server.

Central Management Console (CMC)

The Central Management Console (CMC) is a web-based tool to perform day-to-day administrative tasks, including user management, content management, and server management. It also allows you

to publish, organize, and set security levels for all of your BusinessObjects Enterprise content.

CMC service

A CMC hosted on a WACS.

Configuration template

A configuration template stores a list of settings for BusinessObjects Enterprise services. Configuration templates allow you to easily configure multiple instances of servers. There is one configuration template for each service type.

Connector

WACS provides services through HTTP, HTTP through Proxy, and HTTPS. Each of these is treated as a connector in WACS. There are three connectors.

DSWS

Web Services SDK and QaaWS Web Service

DSWS service

A DSWS hosted on a WACS server.

HTTPS

HTTPS stands for “Hypertext Transfer Protocol over Secure Socket Layer”. It refers to HTTP communication over an encrypted Secure Sockets Layer (SSL). Communication over HTTPS is more secure than communication over HTTP.

Network Interface Card (NIC)

A Network Interface Card is computer hardware that allows computers to communicate over a network. A computer can have more then one NIC.

Server

In BusinessObjects Enterprise, a server is a running process that can host one or more service.

Service

A service is an item that provides business functionality from within a server.

Single sign-on (SSO)

Single sign-on is a method of access control that enables a user to access multiple software systems only having to provide log on credentials once.

SSL

SSL stands for “Secure Sockets Layer”, a protocol that provides secure, encrypted data transfer.

System defaults

The original settings of a service when it was initially installed.

WACS service

A service that provides web application hosting services.

WACS properties

The following tables describe the general, HTTP, HTTP through Proxy, and HTTPS configuration properties for WACS. Each of these properties can be specified in the "Servers" area of the Central Management Console (CMC).

WACS service properties

Table 11-1: General Properties

Property	Description	Range of Values
Log level	Specifies the minimum severity of warning that you want to be logged. The **DEBUG** level logs the most amount of activity, and the **FATAL** logs the least amount; only critical messages are logged. It is not recommended to set the log level to **DEBUG** or **INFO** in a production environment, because this may affect server performance. Changing the log level does not require that you restart the WACS.	The levels that are available, in increasing level of severity are: • **AUTO** • **DEBUG** • **INFO** • **WARN** • **ERROR** • **FATAL** By default, the **AUTO** level is set to **ERROR**.

Property	Description	Range of Values
Service Startup Timeout (seconds)	How long the WACS will wait for its hosted services to start before it times out. If the timeout passes, the WACS will not provide CMC services. On a slower machine, you can consider specifying a longer value. If you specify a value that is too small, and the WACS doesn't start before timing out, restore the default settings of the WACS through the Central Configuration Manager (CCM).	The default value is 300 seconds.

Table 11-2: Concurrency Settings (Per Connector)

Property	Description	Range of Values
Maximum Concurrent Requests	The number of concurrent HTTP or HTTPS requests that each connector (HTTP, HTTP through Proxy, or HTTPS) can process simultaneously.	Numeric values from 1 to 1000. The default value is 150.

Table 11-3: Active Directory Configuration Settings

Property	Description	Range of Values
Krb5.ini File Location	The full name of a `krb5.ini` file that stores Kerberos configuration properties.	The full name of the `krb5.ini` file.
bscLogin.conf File Location	The full name of a `bscLogin.conf` file.	The full name of the `bscLogin.conf` file.

Table 11-4: HTTP Configuration Properties

Property	Description	Range of Values
Bind to All IP Addresses	Whether to bind to all network interfaces or not. If your server has more than one NIC, and you want to bind to a specific network interface, uncheck this property.	True or False. The default value is True.
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTP service is provided. You can only specify a value if you uncheck **Bind to All IP Addresses**.	The IPv4 address, IPv6 address, host name, or fully-qualified domain name.
HTTP Port	The port on which HTTP service is provided.	Numeric values from 1 to 65535. The default value is 6405.

Table 11-5: Configuration of HTTP through Proxy

Property	Description	Range of Values
Enable HTTP through Proxy	Whether to enable the HTTP through Proxy connector on the WACS. This is typically checked in deployments with a reverse proxy.	True or False. The default value is False.
Bind to All IP Addresses	Whether to bind the HTTP through proxy port to all network interfaces or not.	True or False. The default value is True.
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTP through Proxy service is provided. You can only specify a value if you uncheck **Bind to All IP Addresses**.	The IPv4 address, IPv6 address, host name, or fully-qualified domain name.
HTTP Port	The port on which HTTP service in a reverse proxy deployment is provided. You can only specify a value if you check **Enable HTTP through Proxy**.	Numeric values from 1 to 65535. The default value is 6406.
Proxy Hostname	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can only specify a value if you check **Enable HTTP through Proxy**.	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of the proxy server.

Property	Description	Range of Values
Proxy Port	The port of your forward or reverse proxy server. You can only specify a value if you check **Enable HTTP through Proxy**.	Numeric values from 1 to 65535. By default, this value is empty.

Table 11-6: HTTPS Configuration

Property	Description	Range of Values
Enable HTTPS	Whether to enable HTTPS/SSL communication.	True or False. The default value is False.
Bind to Hostname or IP Address	Specifies the network interface (IP address or host name) on which HTTPS service is provided. You can only specify a value if you check **Enable HTTPS**.	The IPv4 address, IPv6, host name, network interface name, or fully-qualified domain name of the network interface.
HTTPS Port	The port on which HTTPS service is provided. You can only specify a value if you check **Enable HTTPS**.	Numeric values from 1 to 65535. The default value is 443.
Proxy Hostname	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of your proxy server. You can only specify a value if you check **Enable HTTPS**.	The IPv4 address, IPv6 address, hostname, or fully-qualified domain name of the proxy server.

Property	Description	Range of Values
Proxy Port	The port of your forward or reverse proxy server. You can only specify a value if you check **Enable HTTPS**.	Numeric values from 1 to 65535. By default, this value is empty.
Protocol	The encryption protocol to use. You can only specify a value if you check **Enable HTTPS**.	TLS or SSL. The default value is TLS.
Certificate Store Type	The type of certificate store that contains your certificates and private keys. In most cases, this will be **PCKS12**. You can only specify a value if you check **Enable HTTPS**.	PKCS12 or JKS. The default value is PKCS12.
Certificate Store File Location	The full name to the certificate file. You can only specify a value if you check **Enable HTTPS**.	The full name of the certificate file. For example, the full name of your PKCS12 file that contains your certificates.
Private Key Access Password	PKCS12 certificate stores and JKS keystores have private keys that are password protected, to prevent unauthorized access or theft. Enter the password that you specified when you generated the certificate store here, so that WACS can access private keys from the certificate store. You can only specify a value if you check **Enable HTTPS**.	The password for the private keys in your certificate stores.

Property	Description	Range of Values
Certificate Alias	The alias of the certificate inside the certificate store. If this is not specified, and a certificate store that contains more than one certificate is used, the first certificate in the store is used. In most cases, you do not need to specify a value. You can only specify a value if you check **Enable HTTPS**.	The alias for the certificate that you want to use.
Enable Client Authentication	If client authentication is enabled, only clients that have keys stored in the Certificate Trust List file are can get WACS services. Other clients are rejected. You can only enable client authentication if you check **Enable HTTPS**.	True or False. The default value is False.
Certificate Trust List File Location	The full name of the certificate trust list file. You can only specify a value if you check **Enable HTTPS** and **Enable Client Authentication**.	The full name of the certificate trust list file.
Certificate Trust List Private Key Access Password	The password that protects access to the private keys in the Certificate Trust List file. You can only specify a value if you check **Enable HTTPS** and **Enable Client Authentication**.	The Certificate Trust List File password.

Web Services SDK and QaaWS web services properties

The following table describes the properties for Web Services SDK and QaaWS (DSWS) web services. Each of these properties can be specified in the "Servers" area of the Central Management Console (CMC).

Table 11-7: Web Services SDK and QaaWS Properties

Property	Description	Range of Values
Enable Kerberos Active Directory Single Sign On	Whether to enable Kerberos AD Single Sign-on for Web Services SDK and QaaWS.	True or False. The default value is False.
Default AD Domain	The default Active Directory domain is used so that users do not have to supply a domain when they log in. For example, if the default domain is set to “mydomain” and a user logs on with the username “user”, the Active Directory logon authority tries to authenticate “user@mydomain.com”.	The default AD domain that you want to use.
Service Principal Name	A service principal name (SPN) is used by clients to uniquely identify an instance of a service. The Kerberos authentication service uses an SPN to authenticate a service.	The principal service name.

Property	Description	Range of Values
Keytab File	A keytab file allows Kerberos Filters to be configured without exposing the password of the user account on the web application machine.	The full name of the Keytab file.

Business Process BI web service properties

There are no configurable properties for Business Process BI Web Services.

Get More Help

Online documentation library

Business Objects offers a full documentation set covering all products and their deployment. The online documentation library has the most up-to-date version of the Business Objects product documentation. You can browse the library contents, do full-text searches, read guides on line, and download PDF versions. The library is updated regularly with new content as it becomes available.

To access the online documentation library, visit *http://help.sap.com/* and click **Business Objects** at the top of the page.

Additional developer resources

https://boc.sdn.sap.com/developer/library/

Online customer support

The Business Objects Customer Support web site contains information about Customer Support programs and services. It also has links to a wide range of technical information including knowledgebase articles, downloads, and support forums.

http://www.businessobjects.com/support/

Looking for the best deployment solution for your company?

Business Objects consultants can accompany you from the initial analysis stage to the delivery of your deployment project. Expertise is available in relational and multidimensional databases, in connectivities, database design tools, customized embedding technology, and more.

For more information, contact your local sales office, or contact us at:

http://www.businessobjects.com/services/consulting/

Looking for training options?

From traditional classroom learning to targeted e-learning seminars, we can offer a training package to suit your learning needs and preferred learning style. Find more information on the Business Objects Education web site:

http://www.businessobjects.com/services/training

Send us your feedback

Do you have a suggestion on how we can improve our documentation? Is there something you particularly like or have found useful? Drop us a line, and we will do our best to ensure that your suggestion is included in the next release of our documentation:

documentation@businessobjects.com

Note:
If your issue concerns a Business Objects product and not the documentation, please contact our Customer Support experts. For information about Customer Support visit: *http://www.businessobjects.com/support/*.

Business Objects product information

For information about the full range of Business Objects products, visit: *http://www.businessobjects.com*.